



Section I: Submittal Letter

April 10, 2020

Ms. Jessica Chambers
Department of Administration
Purchasing Division
2019 Washington Street, East
Charleston, WV 25305

RECEIVED

2020 APR -9 PM 3:43

WV PURCHASING
DIVISION

Dear Ms. Chambers:

Thank you for the opportunity to present our Technical Proposal to the State of West Virginia (the "State") in response to the Data Center 2.0 CRFP 0231 OOT2000000001 for On-Premise Infrastructure (the "RFP"). Software Information Systems, LLC ("SIS") has reviewed the RFP and has composed a response offering a solution for "enterprise-class hardware, enterprise data backup capability, infrastructure operations monitoring capability, and on-demand professional services."

SIS is confident that we are uniquely positioned to assist the State of West Virginia with meeting its important goals, given our experience in information technology and knowledge of the intricacies of technology and associated services. SIS has recently completed projects providing the State with technology solutions for their Production and DR infrastructure upgrades at West Virginia OASIS, West Virginia State Treasurer's Office, and West Virginia Department of Education. We feel this experience will lend well towards our ability to continue providing the State with the quality service it requires.

In support of this RFP, we certify that:

- The pricing quoted in the Cost Proposal shall remain valid for 180 days following the submission of this proposal.
- SIS will accept financial responsibility for all expenses incurred by SIS in responding to this RFP, including but not limited to preparation, delivery, and travel.

We thank you for your consideration of our solution proposal and we look forward to the oral presentations.

Sincerely,

Charles D. Arnett
Senior Client Executive
Email: carnett@thinksis.com
Phone: 304-768-1645
Cell: 304-549-7698
Software Information Systems, LLC
200 Association Drive, Suite 210
Charleston, WV 25311

Table of Contents

SECTION I: SUBMITTAL LETTER	2
SECTION II: SIS OVERVIEW	3
RANGE OF SERVICES	4
SIS COMPANY OVERVIEW.....	5
MARKET AWARDS... ..	6
SECTION III: SOLUTION OVERVIEW	8
INTRODUCTION.....	9
ON-PREMISE INFRASTRUCTURE.....	10
ENTERPRISE DATA BACKUP	12
INFRASTRUCTURE OPERATIONS MONITORING	13
ON-DEMAND PROFESSIONAL SERVICES.....	14
SUMMARY.....	14
SECTION IV: RFP FROM THE STATE OF WEST VIRGINIA	15
4.1 BACKGROUND AND CURRENT OPERATING ENVIRONMENT.	15
4.2 PROJECT GOALS AND MANDATORY REQUIREMENTS.	17
4.3 QUALIFICATIONS AND EXPERIENCE.	51
4.4 ORAL PRESENTATIONS.....	57
SECTION V: ATTACHMENTS	58



Section II: SIS Overview

Headquarters Location:	Lexington, Kentucky
Company Name:	Software Information Systems, LLC (d/b/a SIS, a Converge Company)
Short Name:	SIS or SIS, A Converge Company
Year Established:	1982
Address:	165 Barr Street · Lexington, KY 40507-1321
Website:	http://www.thinksis.com
Phone:	(859) 977-4747
Fax:	(859) 977-4750
Regional Offices:	

Farmington Hills, MI

32605 West Twelve Mile Road · Suite 195 · Farmington Hills, MI 48334
(248) 522-9820

Louisville, KY

4965 U.S. Highway 42 · Suite 1000 · Louisville, KY 40222
(502) 228-3133

Cincinnati, OH

8805 Governor's Hill Drive · Suite 210 · Cincinnati, OH 45249
(513) 791-7777

Charleston, WV

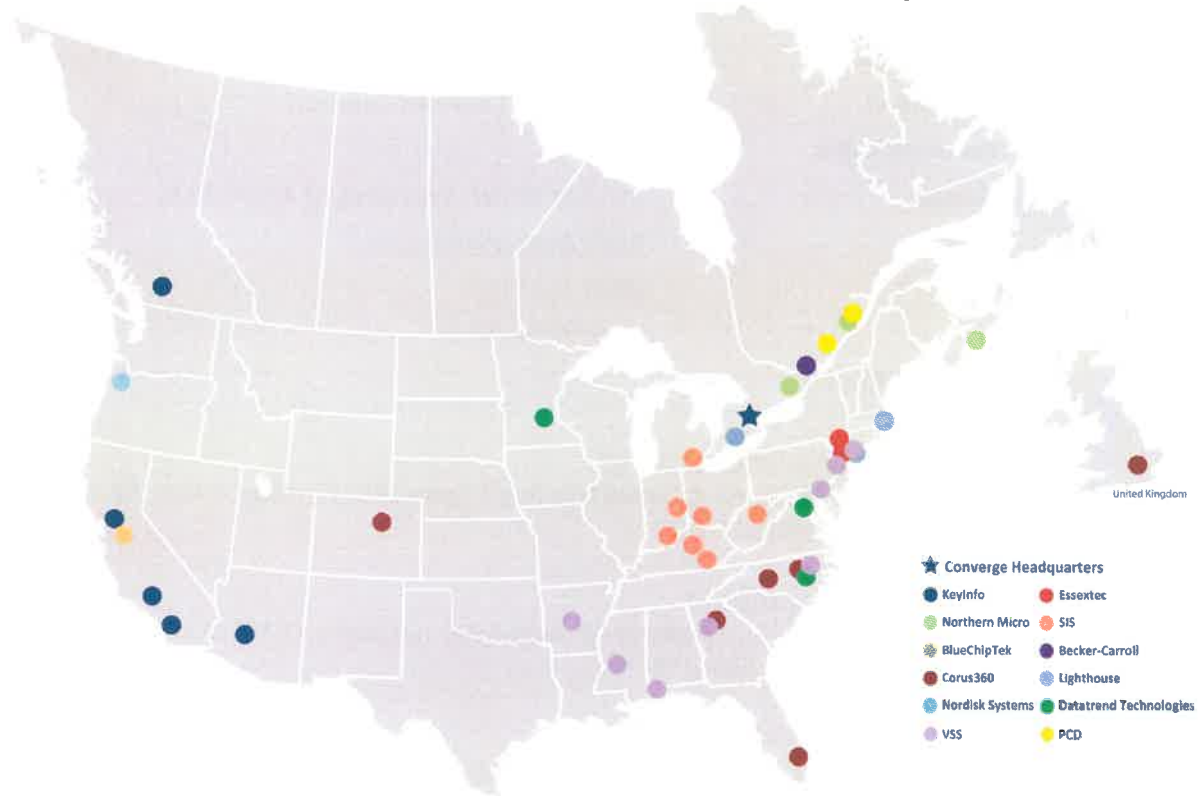
NorthGate Business Park · 200 Association Dr. · Charleston, WV 25311
(304) 768-1645

Indianapolis, IN

10650 North Bennett Parkway · Suite 400 · Zionsville, IN 46077
(317) 733-4870



SIS is a wholly owned subsidiary of publicly traded company, Converge Technology Solutions, Corp. (“Converge”). The below figure expresses the geographical footprint of Converge:

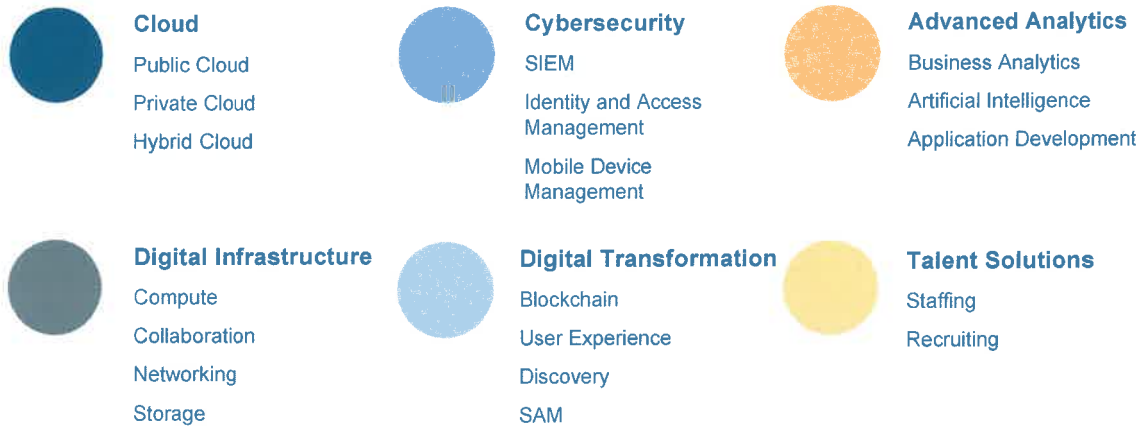


Range of Services

SIS is proud to maintain a wide variety of service competencies, delivered by our team of trained and experienced engineers and consultants. A sample list of our service capabilities is provided below:

- Assessment/Health Check Services
- Architecture and Pre-Sales Consulting
- Installation and Configuration Services
- Data Migration Services
- Staff Augmentation
- Post-Installation Break/Fix and Upgrade Services
- Project Management Services
- Knowledge Transfer Services
- Cloud Services via the SIS Managed Solution Center (“MSC”)
 - Hosting and High Availability
 - Managed Services
 - Disaster Recovery
- Business Intelligence and Data Warehouse Development
- Information Security Services
- Database Administration
- Software Analysis and Development

Hybrid IT – Solution Level & Practices



Confidential and Proprietary Copyright © 2020 Converge Technology Solutions Corp.



SIS Company Overview

In business since 1982, SIS, a Converge company is an IBM Platinum Business Partner, Veeam Platinum Reseller and Veeam Platinum Cloud Service Provider, Microsoft Gold Datacenter Partner, VMware Premier Partner, Cisco Gold Partner and Dell EMC Gold Partner. SIS is headquartered in Lexington, KY, with regional offices in Louisville, KY; Cincinnati, OH; Charleston, WV; Indianapolis, IN; and Farmington Hills, MI.

Customers rely on SIS's consultative engagement model where we serve as business partners, advisors and strategists. Our teams deliver a full range of technology infrastructure and managed IT services to help customers achieve measurable business results. SIS is organized into business units that work collaboratively to provide total solutions to our clients.

Our proven methodology, experienced professionals and innovative technologies help customers infuse technology into a clear strategy to drive results in system availability, recovery, performance and efficiency. Every solution is customized to customers' unique business requirements, leveraging existing IT investments while keeping scalability and TCO top of mind.



Data Center Solutions

SIS Data Center Solutions are comprehensive and state-of-the-art solutions designed and deployed by SIS, with technology from SIS strategic partners.

SIS Cloud Solutions

SIS Cloud Solutions are a combination of SIS technology, vendor technology, and SIS services. This combination is an outcome-based solution vs. the technology or service itself. SIS Cloud Solutions include on-premise, public, and hybrid cloud solutions.

SIS Insights

SIS Insights is an overlay of all solutions offered by SIS. Each engagement has the insights of SIS's brightest technical resources. Each product has SIS Insights included in the services. SIS Insights leverages our strongest asset: our people.

Market Awards

SIS gained national recognition by earning the IBM Leadership Award three times. SIS also has the designation of being one of few VMware Authorized Consultants in the region and was recognized by IBM as the first partner globally to be certified as a Cloud Infrastructure Partner.

SIS has received numerous certifications, designations, and recognitions from third parties. The data behind third-party recognition offers our company in-depth information, which we can apply to strengthen our products, services, and internal operations. Such recognition also enables SIS to measure ourselves against national benchmarks of our competitors; thereby, ensuring we are utilizing best practices to become a leader in the IT industry.

Below represents a few of the many recognitions SIS has received throughout the years:

- Inaugural Veeam Innovation Award Winner



- IBM Platinum Business Partner
- Avnet/TechData Analytics and Data Award
- IBM Choice Award – North American Top Strategic Partner
- IBM “Big Data” Partner of the Year
- Lane Report Top Technology Services Companies of Kentucky
- CRN Solution Provider 500
- Eight Time Best Places to Work Kentucky Award Winner
- Named as SOC2 (Service Organizational Control) Provider
- Selected as Partner for Veeam Availability Suite
- Talking Cloud 100 Ranking
- IBM Edge Winner
- Named to CRN’s Solution Provider 500 List
- Microsoft US Central Region Renewal Partner of the Year
- IBM Collaboration Solutions Award (Winner)
- Microsoft Central Region SMB Partner Award for VAR Champion Partner of the Year
- FINALIST: IBM Best Industry Solution for Health Care
- IBM Global Financing Leadership Award
- Veeam #1 ProPartner – Ohio Valley Region
- CRN Top 100 Healthcare VARS
- Microsoft Gold Datacenter Partner
- Inc. 500 “Fastest Growing, Privately Held Companies in America”
- IBM “Leadership Award”
- VAR500 winner
- CRN Technology Elite 250
- Leadership Award for Healthcare – Trusted Advisor Award Avnet
- Finalist for IBM Beacon Award – Best Industry Solution for Healthcare
- Outstanding PureFlex-Flex Specialty Partner in North America



Section III: Solution Overview

In response to CRFP 0231 2000000001 (the “RFP”), SIS is pleased to present this Technical Proposal to the State of West Virginia (the “State”). In accordance with the State’s requirements, SIS is providing the following required documents along with this proposal:

1. West Virginia Office of Technology “On-Premise Infrastructure” RFP signed by SIS
2. Addendum Acknowledgement Form signed by SIS
3. Purchasing Affidavit signed by SIS

Pursuant to Section 5 “Vendor Proposal” of the RFP, SIS has additionally fulfilled the following requirements:

- ✓ SIS has constructed a simple, economical, and concise response for the State’s consideration, referencing online URLs within its response where appropriate to incorporate relevant information for the State’s review.
- ✓ SIS is prepared to accept financial responsibility for all expenses incurred by SIS in responding to this RFP, including by not limited to preparation, delivery, and travel.
- ✓ SIS is submitting this Technical Proposal and a separate Cost Proposal to the State. This Technical Proposal contains no cost information; all cost information is contained in the Cost Proposal.
- ✓ The title page of this proposal reflects SIS’s corporate contact information, name of the SIS contact person, signature on behalf of SIS, and the date of submission.
- ✓ The table of contents is located at the beginning of this proposal for the State’s convenience.
- ✓ The structure of this proposal is such that SIS’s responses clearly correlate to the State’s requests in Section 4 of the RFP. Please see the below section “SIS Responses to Section 4 of the RFP.”
- ✓ SIS understands the need for timely presentation of its response before the bid opening time and is submitting a copy of its Technical Proposal and its Cost Proposal to 2019 Washington Street East, Charleston, WV 25305-0130.

SIS, in partnership with NetApp, IBM, and Zerto, have architected the enclosed solution to meet the requirements outlined in the RFP for Data Center 2.0 for the State of West Virginia Office of Technology. The solution is designed be upwardly scalable and several tiers of support for compute, availability, storage, and recoverability have been included in the design to meet the State’s needs for servicing various workloads. All included products can be configured to support the various cybersecurity requirements as an infrastructure component for a broader overall plan. A combination of managed services and cloud services are included as part of the solution to help the State support the designed infrastructure throughout the life of the solution deployment. The proposal also includes detail regarding staff augmentation for the defined skills outlined in the RFP.

Introduction



Figure 1 Introduction

Figure 1 above provides a high-level overview of the components included to support the various aspects of the RFP requirements. SIS has designed a solution consisting of offerings from various best of breed technologies.

NetApp offerings in compute, storage, and networking are included in the response to provide the building blocks for the on-premise infrastructure component of the solution. NetApp HCI compute nodes in combination with FAS storage and high-performance network switching provide the building blocks to host the x86 based workloads. The infrastructure can start small and scale up to very large size with the architecture design planned.

To support the replication and availability requirements of the various tiers, Zerto or NetApp-based replication will be used. Zerto can replicate and manage the availability of the “hot” standby requirements at a per VM level. NetApp provides storage-based replication for a more “cold” failover, as needed. Both of these solutions can be configured to support various levels of Recovery Point and Time Objectives.

IBM offerings including IBM Power systems, IBM Fibre Channel Switches, IBM Spectrum Protect software, and NetApp ESeries storage are utilized in the solution to meet the requirements outlined in for Enterprise Data Backup. Here, the solution provides the most thorough coverage for applications and operating systems as well as a scalable architecture to meet the needs of the State today and long into the future.

For the Infrastructure Operations Monitoring component of the RFP response, SIS is leveraging IBM QRadar and HCL BigFix. This solution allows for a cloud-based service offering to monitor and manage the entire environment for the State.

SIS has looked to its parent company, Converge Technology Solutions Corp., to provide the On-Demand Professional Services as part of the overall solution. The staffing team within Converge has extensive experience and can find and provide skilled resources across all the requested skillsets.

The combination of these services designed by SIS to meet the needs of the RFP will also be augmented by a Service Delivery Manager. This individual will be the State’s primary point of contact for all the additional content and details requested as part of the RFP requirements.

All these components come together to deliver a scalable solution for the State of West Virginia to help with their desire to build a new hosted data center architecture for the Office of Technology.

On-Premise Infrastructure



Figure 2 On-Premise Infrastructure Components

The SIS proposal provides for a tiered approach to consumption of resources. Compute and memory resources are the same regardless of the tier consumed. This need is provided by the NetApp HS410 compute nodes. Each node is configured as reflected below:

- 16-core 2.8GHz CPU or greater
- 512GB memory
- 4x 10Gb Network ports

For the initial deployment, a minimum of two nodes (preferably three) would be used to ensure failover capability of the desired workload. An N+1 model is desired to be run at all times, however, that decision will ultimately be up to the State to ensure redundancy during a potential node planned or unplanned outage.

A node expansion can be provisioned through an additional node with the below configuration:



- 16-core 2.8Ghz CPU or greater
- 512GB of memory
- 4x 10Gb Network ports

As for the storage needs, NetApp FAS storage will provide the needed storage capacity and performance to meet the defined Volume Storage and/or the Performance Storage requirements. The SIS design includes FAS 8200 controllers with the below specifications for the Volume Storage requirements:

- FAS8200 HA Pair (or equivalent)
- 24x4TB HDD
- 4x 10Gb Network Ports

The Performance Storage needs will be fulfilled with a NetApp A300 All Flash controller and storage. This system will have the below specifications as part of the SIS proposal:

- A300 HA Pair (or equivalent)
- 12x3.8TB SSD
- 4x10Gb Network Ports

The two storage controllers and architectures are designed specifically to service storage needs. For the Performance Tier, All Flash storage and controllers are being utilized to maximize performance and support fast data retrieval. For the Volume Tier storage, high capacity spinning disk is used to reduce cost and maximize capacity available for the storage need. Storage can be assigned to hosts in either iSCSI or NFS for the needs of the VMware Hypervisor design. The NetApp Storage can also support SMB protocol should the State decide to deploy Hyper-V for the hypervisor layer. Fibre Channel, while supported on the proposed storage models, is not part of the design put forth within this response.

The interconnection of storage and compute is to be facilitated with Cisco 5K switches priced and sold through NetApp. The network switches will be able to connect into the State of West Virginia's network through 100Gb uplinks as defined in the RFP response. As various resources are added to the compute or storage, new switches may need to be implemented as part of the scaling architecture.

Various levels of availability have also been defined for the associated Tiers of compute consumption. At the lowest, Tier 0, level, none of the deployed compute resources would be replicated. If a data backup of the workload is needed, the Enterprise Data Backup solution could be leveraged to support this availability need. For Tier 1 and Tier 2 workloads, Zerto replication software will be utilized to manage the off-site replication as well as the RPO/RTO required by the specific Tier. Zerto performs write mirroring within the Hypervisor for defined workloads and replicates to an offsite cluster. The workload can be configured to support the RPO's and RTO's defined within the RFP. It should be noted that additional storage consumption as well as small replication appliances are required to be deployed within the environment on each node (per best practice). Should the State desire not to leverage Zerto replication, the State can leverage NetApp Storage replication to meet the needs of a "cold" failover scenario.

Throughout the lifetime of the deployment of the On-Premise Infrastructure, SIS will engage with the State to support semi-annual code upgrade and maintenance on the environment. This will be funded through a fixed monthly price that will scale alongside the additional consumption of hardware and software resources. Should the State wish to perform urgent changes outside of this schedule, an ad hoc Statement of Work will need to be scoped for the specific services requested.

As the environment grows in scope, services will be provided within the monthly cost to support the deployment and configuration of the new assets. Should hardware fail within the environment, the original equipment manufacturer will perform onsite replacement to ensure optimal availability.

All software licensing required to support the functionality required as described in the RFP will be included as part of the paid engagement.

Overall, the SIS proposed solution provides a scalable architecture to support the compute, storage, availability, and support requirements specified in the RFP. The solution can be configured to meet the most stringent security requirements. Also, the scalability of the solution will grow with the needs of the State.

Enterprise Data Backup

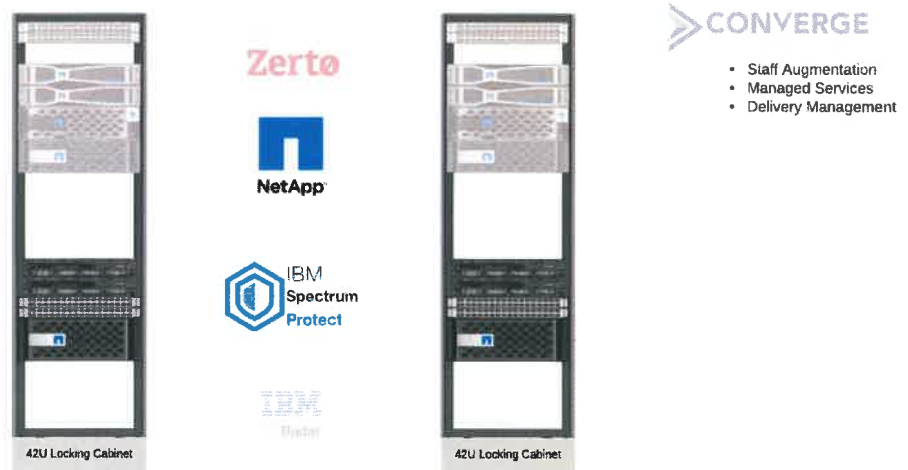


Figure 3 Enterprise Data Backup Components

SIS has designed an Enterprise Data Backup solution that is supported by decades of development and provides for some of the most thorough protection a solution can provide. The IBM Spectrum Protect Software stack is an industry leading offering. It supports a wide range of operating systems, applications, and architectures. It can scale to support petabytes of backed up data and with the combined Predatar offering, it is extremely easy to use and manage. The software will be deployed on industry leading IBM Power systems with NetApp ESeries storage as the back-end repository for the data. IBM Spectrum Protect supports multisite replication to ensure even a site removal will not stop the solution from restoring needed data to the business.

SIS has extensive experience on Spectrum Protect and will be best suited to assist the State with a quick transition to the new platform. Depending upon the scope of data to be protected, the solution can be deployed and ready to start receiving backup data from clients in short order. Industry best practice for data protection, indexing, and retrieval is at the core of the Spectrum Protect solution. File level or full

volumes can be protected and restored to the same or alternate targets in a quick and efficient manner. To reduce costs of the solution, techniques like client-side data reduction can be leveraged to reduce backup window impacts as well as storage needs for the backed-up data. Cost efficient NetApp ESeries storage is also part of the solution to ensure a cost-effective solution is deployed.

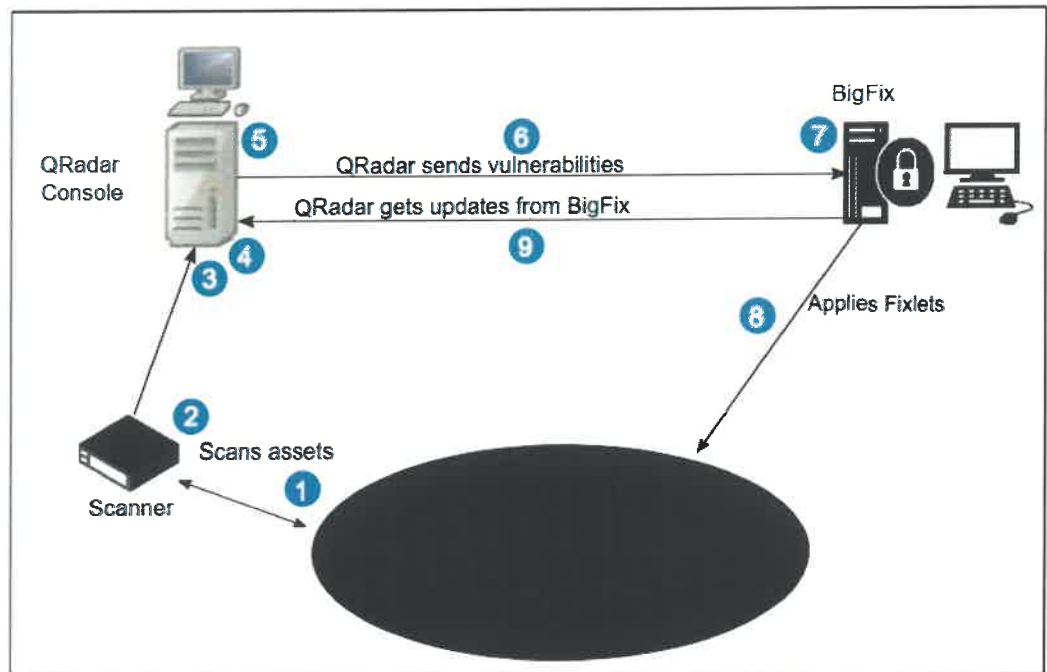
As the solution scales, any services required to support the add on capacity to the environment will be included in the additional monthly cost of the overall solution. As for initial deployment, a one-time charge will be made to support the startup and training of the Enterprise Data Backup Solution as per the requirements within the RFP.

Infrastructure Operations Monitoring

SIS has designed an enterprise-level security and monitoring solution which is leveraging both IBM QRadar and HCL Big Fix (formerly owned by IBM.) Both pieces of the monitoring solution are mature in the industry and have been rated in the top quadrant from Gartner for many, many years.

For the monitoring solution, SIS has taken the State of West Virginia’s requirements, applied best practices for not only monitoring, but also security, and brought forth a hybrid solution that is flexible, fluid and easily scalable. The solution will provide the highest-level enterprise network security as well as up-down monitoring. The flexibility of this solution will enable the State of West Virginia to predict current and future costs, automate processes (security, reporting remediation and control of nodes) thereby reducing the security risks and the labor intensive and error prone manual processes. Because this solution is automated and crosses heterogeneous environments, the State will have a single dashboard visibility. The processes are automated, eliminating the need for resources to physically monitor, protect, report on and control the environments.

The compatibility between Qradar and BigFix combines two powerful solutions to bring forward a robust and world-class addition to Infrastructure Operations Monitoring at the State of West Virginia.



On-Demand Professional Services

TALENT SOLUTIONS >>> **CONVERGE TALENT SOLUTIONS** > **CONVERGE**

WHO WE ARE

The Talent Solutions team, a part of Converge Technology Solutions, Corp., works with clients to deliver continuous results with people. Our in-house team carefully vets candidates for their technical skills and professional values to make sure our clients get the right person for their organization. The proven methodology that we employ has resulted in a 98% retention rate.



REAL PEOPLE USING DATA TO FIND THE PERFECT TALENT



The Converge Talent Solutions team is comprised of a dedicated team that works to deliver exceptional technology staffing services to customers by finding the most talented resourced across the North America. Offering traditional staff augmentation (contract to full time placements) as well as specializing in project-based work, we strive to place the best resources with our clients. Traditional staffing services (staff augmentation) include contract, contract to perm and full-time placements. Our team can place people in entry level roles up to C-Level executives. Additionally, we specialize in project-based work, utilizing known and recruited resources to compliment the professional services that our companies offer.

Summary

SIS has worked hard to build a plan to support the needs of the State for the RFP for the Datacenter 2.0 project. The solution is upwardly scalable, serves the needs of the State, is backed by industry-leading providers and expertise, and ultimately provides the groundwork for a very productive relationship between the State, SIS, and the supporting original equipment manufacturers.

Section IV: RFP from the State of West Virginia

REQUEST FOR PROPOSAL WV Office of Technology On-Premise Infrastructure

SECTION 4: PROJECT SPECIFICATIONS

4.1 Background and Current Operating Environment: The West Virginia Office of Technology, under the West Virginia Department of Administration, and its Chief Technology Officer (CTO), sets goals to develop an organized approach to information resource management for the State, while providing technical assistance to State entities in the design and management of information systems.

The State of West Virginia's strategic technology goals (digital government, technology optimization & value, enterprise services, and cybersecurity) interrelate to the strategic initiative known as Data Center 2.0. The Data Center 2.0 initiative strives to accomplish the following:

- Establish a centralized on-premise infrastructure contract enabling the WVOT to support a myriad of applications in a multitenant environment.
- Leverage a co-location model to ensure the cybersecurity, privacy, redundancy, and resiliency standards of the State data center locations adhere to acceptable levels;
- Drive data center consolidation and the server virtualization;
- Improve the cybersecurity and privacy posture of the State infrastructure leveraging a risk and compliance-based model;
- Through a centralized, managed enterprise contract, the on-premise infrastructure can be expanded or contracted (technology infrastructure acquisitions, allocation, and provisioning), greatly improving the time to deploy or retract resources, in support of technology projects and initiatives;
- Reduce financial overhead expense and cyber risk in the maintenance and management of multiple on-premise infrastructures with aged and in some cases unsupported infrastructure; and
- Set the stage for a hybrid data center architecture, ensuring proper design and implementation to support leveraging cloud resources for the greatest return on investment for cloud- appropriate workloads.



WVOT provides highly reliable, protected, and cost-effective technology services to approximately 25,000 computers and 20,000 network users. Services are delivered by approximately 200 full-time and temporary employees and supplemented by specialized contract services and staff on an as-needed basis. There are approximately 210 entities total within the executive branch where services are provided. Funding for the Office of Technology is derived from a fee for services model.

Current Data Center Infrastructure Summary: WVOT's current server and storage environment consists of approximately 1400 servers with 1.3PB of total storage, of which approximately 750TB is in use. This storage feeds approximately 780 virtualized servers with the rest being physical servers. We currently use the VMware vSphere 6.7 platform for our virtualization environment.

The operating systems in production include Microsoft Windows Servers, HP-UX 11.31, AIX 5.3 through 6.1, and Red Hat Enterprise Linux (RHEL) 5 through 6.

The current storage environment consists predominantly of EMC and NetApp storage arrays including VNX 5400, VNX 5200, VNXe 3150, VMAX, etc.

Most of the equipment in the current data center is reaching capacity or end of life status (or both). The current data center space is also limited in terms of physical space, power, and cooling.

WVOT is looking to replace these disparate units/services with a single enterprise-class, fully integrated infrastructure. We are expecting to grow approximately 5% - 7% in capacity and/or services year over year during the lifetime of this contract

Current Enterprise Backup Service Summary: WVOT provides an enterprise backup service to supported executive branch agencies.

- EMC IOPA with Data Domain
- DDBoost and Avamar
- EMC Avamar (handles 70% of the total backup load)
- IBM Tivoli

Current Infrastructure Operations Monitoring Summary: WVOT maintains a limited infrastructure operation monitoring capability.

- Capability is stretched across various tools, across the different IT support functions providing a limited operational monitoring capability.
- Tools: Solarwinds & What's Up Gold

Note the State's strategy is to continually seek cost optimization and modernization in technology management, which could include leveraging a multi-source integrator model (MS/).



4.2 Project Goals and Mandatory Requirements: The purpose of this RFP is to establish a contract for on-premise data center infrastructure capable of scalability, flexibility, and elasticity. The RFP defines the service expectations and services scope. Vendor's are highly encouraged to review the entire RFP to ensure proper scoping in their proposal. Vendor should provide its approach and methodology to providing the solution or solving the problem described by meeting the goals/objectives identified below. Vendor's response should include any information about how the proposed approach is superior or inferior to other possible approaches, outline project deliverables, and provide supporting documentation.

NOTE: If, as part of its proposal, the Vendor submits appendices or other supplemental materials, the Vendor should denote specifically in those materials where the relevant information is located.

4.2.1 Goals and Objectives - On-Premise Infrastructure -The primary goal of this solicitation is to establish on-premise infrastructure contract to enable WVOT to provide virtualized x86 computer and storage resources to executive branch agencies who fall under the purview of the West Virginia Office of Technology (WVOT). The solution should be designed with the capability to expand and shrink the physical infrastructure and associated operational expense, under a scalable infrastructure architecture. There are four (4) components to this RFP; On-Premise Infrastructure, Enterprise Data Backup, Infrastructure Operations Monitoring and On-Demand Professional Services. The overarching goals for each component are outlined below.

4.2.1.1 On-Premise Infrastructure:

4.2.1.1.1 Tiered Solution. The State seeks a tiered pricing model for the proposed infrastructure solution. The tiering delineation is established by business objectives.

Each solution tier should be designed to leverage a three (3) line item structure as outlined below. Please also see mandatory minimum specifications for below tiers and expansions in sections 4.2.4.3.5 , 4.2.4.3.6, and 4.2.4.3.7.

→**Response:** SIS understands that the State desires a three-tier solution within one data center. As such we are proposing NetApp storage which has the capability of a three data tiers on premise as well as the capability to add a cloud tier if desired at a later point in time.

4.2.1.1.1.1 Tier Base

The base line item is intended to provide the complete solution of the associated tier solutions at one (1) data center location.



The base line item can also be leveraged by the state to implement an offsite data backup and/or disaster recovery capability of the associated tier.

The base line item should include all required components (hardware, software, middleware, equipment, networking, licensing, support, implementation & firmware management services) to successfully operate the associated tiers.

→**Response:** SIS understands that the State desires a complete solution of the associated tier solutions at one (1) data center location which can also be leveraged by the State to implement an offsite data backup and/or disaster recovery capability of the associated tier with all components included. As such we are proposing NetApp storage in combination with IBM Spectrum Protect which combined and separately each have the ability to provide the desired functionality.

4.2.1.1.1.2 Tier Node Expansion

The tier node expansion line item provides the ability to expand or contract the processing capability (cores & volatile memory) of an existing base solution of the same tier.

→**Response:** SIS is proposing NetApp HCI compute capability which allows for scalability within tiers as well as combining compute across tiers to provide the most cost effective and granular solution for the State. Additional information on NetApp HCI is provided as supplementary material to this proposal.

4.2.1.1.1.3 Tier Storage Expansion

The tier storage expansion line item provides the ability to expand or contract the storage capability of an existing base solution of the same tier. Multiple storage types can be provided as options but should be scoped/sized to align to the single, per tier, line item pricing.

→**Response:** SIS is proposing NetApp OnTap Storage which allows for scalability within tiers as well as combining compute across tiers to provide the most cost effective and granular solution for the State. We are offering multiple storage types as options which could be scoped/sized to align to the single, per tier, line item pricing. Additional information on NetApp OnTap storage is provided as supplementary material to this proposal.

4.2.1.1.1.4 Tier Level: 0

Tier Type: Limited Performance Tier Primary Business Driver: Cost



Tier Goals: Tier 0 is the intended service:

- When lowest cost operational expense is the primary business driver.
- For hosting non-critical (deferrable services) applications with reduced performance requirements.
- For applications with limited backup requirements.
- For applications with limited to no disaster recovery objectives.
- When best-effort hardware service support levels are acceptable.

→**Response:** SIS understands that the State of West Virginia desires a tier 0 solution for which cost is the primary factor and performance is not critical. The NetApp Hybrid storage solution proposed has this capability and can be coupled or not coupled with the IBM Spectrum Protect backup solution to allow for a desired level of back and disaster recovery options.

4.2.1.1.1.5 Tier Level: 1

Tier Type: Balanced Performance Tier

Primary Business Driver: Balanced combination between cost and performance

Tier Goals: Tier 1 is the intended service:

- For hosting both deferrable and important applications with standard performance capabilities requirements.
- For applications with standard data backup requirements.
 - Deferrable services: twelve (12) hours RPO
 - Important services: one (1) hour RPO
- For applications with standard disaster recovery objectives.
 - Deferrable services: twelve (12) hours RTO
 - Important services: four (4) hours RTO
- When standard hardware service support levels are acceptable.

→**Response:** SIS understands that the State of West Virginia desires a tier 1 solution for which the cost factor and performance are balanced. The NetApp Hybrid storage solution proposed has the capability of using internal snapshots and can be coupled or not coupled with the IBM Spectrum Protect backup solution to allow for a desired level of back and disaster recovery options which can easily meet or exceed the desired RPO and RTO objectives. Additional information on NetApp OnTap Hybrid storage is provided as supplementary material to this proposal.

4.2.1.1.1.6 Tier Level: 2

Tier Type: High Performance Tier



Primary Business Driver: High performance/Disaster Recovery

Tier Goals: Tier 2 is the intended service:

- For hosting both important and critical applications with high performance capabilities requirements.
- For applications with critical data backup requirements.
 - Important services RPO of approximately one (1) hour
 - Critical services RPO of less than 15 minutes
- For applications with critical disaster recovery objectives.
 - Important services RTO less than four (4) hours
 - Critical services RTO of less than two (2) hours
- When premium hardware service support levels are required.

→ **Response:** SIS understands that the State of West Virginia desires a tier 2 solution for which the performance and disaster recovery capabilities are at the highest tier. The NetApp All Flash storage solution proposed has both the performance and disaster recovery capability of using internal snapshots and can be coupled or not coupled with the IBM Spectrum Protect backup solution to allow for a desired level of back and disaster recovery options which can easily meet or exceed the desired RPO and RTO objectives. Additional information on NetApp OnTap all Flash is provided as supplementary material to this proposal.

4.2.1.1.2 Managed Services Scope. The managed-services scope of the on- premise infrastructure is specifically limited to the infrastructure provided under this contract. The State's existing infrastructure is not included within the scope of the managed services scoping goals described below:

4.2.1.1.2.1 Physical Layer: services and support of the physical layer of the provided infrastructure.

→ **Response:** All physical layer support and services for the provided infrastructure will be provided by the original equipment manufacturer ("OEM"). As new equipment is installed, or physical layer components need replaced, OEM engineers will be engaged to provide the necessary services.

4.2.1.1.2.2 Firmware Layer: services and support of the firmware layer of the provided infrastructure.

→ **Response:** All firmware layer support and services for the provided infrastructure will be provided by the OEM. On a semi-annual basis, the OEM will provide the required upgrade services. For any off-schedule upgrades that WVOT and the OEM determine to be required, a Statement of Work would be created to provide these services.



4.2.1.1.2.3 Licensing & Hardware Support: licensing relating to the support of the physical infrastructure, ensuring equipment is properly supported by the provider.

→ **Response:** All licensing and hardware support will be provided by the OEM.

4.2.1.1.2.4 The following aspects of services are NOT included in the scope: operating system, virtualization, software, and applications serviced and supported by WVOT.

→ **Response:** SIS acknowledges that items in this Section 4.2.1.1.2.4 are not included within the scope of this RFP.

4.2.1.1.3 Network Infrastructure.

4.2.1.1.3.1 Vendor should provide all components necessary to physically interconnect and enable logical interconnection of the infrastructure to the boundary edge of the provided infrastructure.

→ **Response:** Compliant – SIS’s solution shall include all components necessary for physical and logical connectivity for the proposed on-premise infrastructure. WVOT shall be responsible for ensuring that their data center(s) is equipped with sufficient internet connectivity, heating/cooling, power, and LAN network drops.

4.2.1.1.3.2 WVOT has a separate contract with other providers to procure hardware, software and services to provide network infrastructure connectivity from the edge of the on-premise infrastructure solution(s) to the internal state network, and therefore are NOT included within the scope of this contract.

→ **Response:** SIS acknowledges that we shall not be responsible for providing the network infrastructure connectivity described in this Section 4.2.1.1.3.2.

4.2.1.1.3.3 Data transport services, as it pertains to MPLS, site-to-site, and cloud interconnect connections are NOT included in the scope of the solution.



→**Response:** SIS acknowledges that we shall not be responsible for providing the data transport services described in this Section 4.2.1.1.3.3.

4.2.1.1.4 Architecture and Design. Vendor's solution architecture should be designed to have accommodate future growth without requiring a major redesign during the contract.

→**Response:** Compliant – SIS has designed its solution to take into account WVOT's estimated year-over-year growth rate of 5%-7% for the life of the contract. The solution we have proposed also includes the capability of expanding to the cloud at a later point in time, if desired. In the event future growth significantly outpaces WVOT's provided estimate during the contract, SIS would expect to collaborate with WVOT to determine and document mutually agreeable updates to the solution.

4.2.1.1.5 Physical Data Center Locations. The scope of the contract is to provide the on-premise infrastructure for on-premise data center location(s) within the State of West Virginia or any location on the United States East Coast. The data center locations are outside the scope of this contract and will be managed by the State or through a separate contract. The initial location for physical equipment provided through this contract is intended to be *West Virginia Regional Technology Park, 2020 Union Carbide Drive, Building 6000, South Charleston, Kanawha County, West Virginia, USA*

→**Response:** SIS acknowledges the initial location data center location specified in this Section 4.2.1.1.5 and has taken this information into account for its solution. After award of the final contract to SIS, the on-premise infrastructure would be shipped to West Virginia Regional Technology Park, 2020 Union Carbide Drive, Building 6000, South Charleston, Kanawha County, West Virginia, USA. (Please note that ship times will vary. Due to COVID-19 measures at the time of this response submission, current ship times could range between 60-90 days from the date of the order.)

4.2.1.1.6 Data Center Footprint. Any solution proposed by the Vendor should make use of the smallest footprint (e.g. rack space) possible. WVOT has a finite number of racks in the initial lease of our data center space and making efficient use of the racks is going to be a factor in our award decision. Vendor should include the total number of racks needed for their solution in the response to this RFP. WVOT's co-located lease defines the rack size requirements to be a standard 42U (either 2-post or 4-post) rack.

→**Response:** Compliant – SIS has selected rack dense products which, combined with their data efficiency, limit the footprint of the solution as much as technically possible. We have included the total number of racks needed for initial phase of the solution in the response to this RFP and have proposed standard 42U 4-post racks.



4.2.1.1.7 Rack Specifications. Vendor's racks used for their solution should have dual power distribution feeds that are connected to separate US standard 220V 30A twist-lock receptacles (L630P plugs should be needed to mate to L630R receptacles) at the data center location. All equipment should have redundant power supplies that can absorb the entire electrical load for that piece of equipment should one fail. Vendor should install power and network connectivity from the bottom of the rack to the top of the rack using standard methods for ensuring the wiring within the rack is kept neat and organized.

→**Response:** Compliant – The proposed solution meets the specification outlined in 4.2.1.1.7.

4.2.1.1.8 Physical Cabinets Access Control. Vendor's solution should address physical security controls as it relates to cabinets. Vendor should provide documentation on how their proposed physical cabinet solution is auditable with respect to security controls.

→**Response:** SIS has proposed standard 42U 4-post racks which include key locking doors for physical security as part of the solution.

4.2.1.1.9 Infrastructure Ownership. The State does not stipulate the solution model as it pertains to the ownership of the on-premise infrastructure provided by the vendor. The vendor should describe the concept of ownership within their proposal and explain how the model supports the goals and objectives of this solicitation.

→**Response:** In this RFP response, SIS is utilizing a lease to meet the scale-up requirements of the requested environment. All physical equipment would be leased to the State of WV by a third-party leasing company (e.g. NetApp Capital Solutions). As new equipment is requested to be added to the environment, the new equipment would be added to the existing lease for a duration to support a co-terminus end date of the lease with the initial equipment deployed. A monthly fee for managed services requested as a part of this RFP would also be provided from SIS to the State. The monthly managed services fee will scale in cost along with the scaling of the equipment within the WVOT environment. At the end of the initial lease term, the State of WV will have the option to buy out the lease, and thus own the equipment after the lease has expired. All cloud-based services and subscriptions will end upon the expiration of the contract unless a new contract is put in place with the provider.

4.2.1.1.10 On-Premise Infrastructure Proposal. Vendor should provide documentation outlining how their solution helps the State achieve the goals and objectives outlined in this RFP for on-premise infrastructure. In



addition, the documentation should specifically seek to address the following:

4.2.1.1.10.1 Enhancing the State's ability to conduct data center consolidation.

→**Response:** The proposed solution will provide a single architecture to standardize the consumption of IT infrastructure resources. Through infrastructure standardization, a more directed consolidation of IT resources will be possible for hosted workloads.

4.2.1.1.10.2 Enabling opportunity to address the various business drivers, while seeking cost efficiencies and optimization.

→**Response:** The proposed solution builds a platform for deploying workloads in a single architecture designed to support the business requirements of the various tiers defined within this RFP.

4.2.1.1.10.3 Enabling agility and flexibility in data center resources.

→**Response:** The solution provided allows for independent scaling of compute and storage infrastructure to support the consolidation effort of the State. The ability to scale compute and storage independently provides for consuming of the desired resource without the need to consuming other resources.

4.2.1.1.10.4 For each tier, provide a comprehensive outline of the technical specifications of their solution.

→**Response:** Please refer to Section III: Solution Overview in the SIS proposal.

4.2.1.1.10.5 Explain how the performance storage is designed to address data retrieval as the primary driver.

→**Response:** For the performance storage, SIS has proposed NetApp All Flash storage which offers the highest level of performance for enterprise class storage in the industry. This is exemplified in multiple #1 SPC benchmarks and will give the State of West Virginia the confidence that their workload is hosted on the highest performing enterprise class storage in the industry. Additional information on NetApp OnTap all Flash storage is provided as supplementary material to this proposal.

4.2.1.1.10.6 Explain how volume storage is designed to address data volume as the primary driver.



→ **Response:** For the volume storage, SIS has proposed NetApp hybrid storage which offers the industry's best balance of performance and capability. This is exemplified by NetApp storage being ranked #1 in the Gartner Magic Quadrant for General Purpose storage, scoring first in four out of five Gartner critical capabilities and in various IDC analysis. Additional information on the Gartner and IDC reports is provided as supplementary material to this proposal.

4.2.1.1.10.7 Explain how your storage offerings are specifically designed to balance performance and cost efficiencies.

→ **Response:** For all storage, SIS has proposed NetApp storage which is natively designed to be both high-performing and efficient. All NetApp storage proposed is based on the world's #1 Storage Operating System Data OnTap. The OnTap operating system has multiple #1 benchmarks which are run with both deduplication and compression storage efficiencies turned on. Most other vendors turn their efficiencies off while running benchmarks, because their efficiency considerably affects their performance. In addition, the NetApp storage provides native multi-protocol capability allowing for the same system to provide both block and NAS storage vs. other solutions that would need two separate devices to accomplish this task. As an added feature, NetApp storage provides secure multi-tenancy which allows data from multiple State agencies to share storage while maintaining separate security for that data in their own Active Directory, if desired. This is the same functionality the US Federal Government utilizes to protect classified data. NetApp storage efficiencies and capabilities create negligible performance impact and as such SIS believes that the proposed NetApp storage solution provides the best combination of performance and efficiency for WVOT's needs. Additional information on NetApp OnTap storage operating system as well as its efficiency, security and multi-tenancy features is provided as supplementary material to this proposal.

4.2.1.2 Enterprise Data Backup. The State seeks an enterprise data backup solution for this contract. The following specifications provide the goals and services included in this solicitation:

4.2.1.2.1 Vendor's proposed solution should include applicable, supported hardware, software, middleware, technical dependencies and managed services (as scoped) to enable an enterprise data backup capability.

→ **Response:** SIS's proposed Enterprise Data Backup solution will leverage IBM POWER Systems, known for industry-leading reliability, backing up to high-performance NetApp E-Series storage. The IBM Spectrum Protect Suite of software (see the products listed at <https://www.ibm.com/support/pages/ibm-spectrum-protect-suite-v81-information-portal>) deployed on the IBM POWER Systems platform would provide scalable data protection for physical file servers, applications, and virtual environments. Technical dependencies for the Enterprise Data Backup solution require that WVOT's data center meet all the requirements stated in SIS's response to Section 4.2.1.1.3.1. Please refer to SIS's responses to Section 4.2.1.2.7 for information concerning the management of the Enterprise Data Backup environment.



4.2.1.2.2 The solution should be capable of providing industry best practices in enterprise data backup capabilities.

→ **Response:** IBM Spectrum Protect (formerly Tivoli Storage Manager/ADSTAR Distributed Storage Manager) has been an industry leader in data protection for over 25 years. IBM has continued to innovate and modernize this product throughout the years to include support for new application and infrastructure platforms that are market-leaders. All WVOT specified platforms are supported in Spectrum Protect, via one of its many included APIs and client-agent products. For additional information, please see the IBM Spectrum Protect data sheet at <https://www.ibm.com/downloads/cas/L9MD4MEZ>, which is also provided as supplementary material to this proposal.

4.2.1.2.3 The solution should include capabilities designed to provide enhanced cybersecurity protection, such as protection against ransomware cyber-attacks.

→ **Response:** IBM Spectrum Protect provides security notifications for potential ransomware attacks. Two key authorization for administrator commands offers tighter security and requires dual authorization to prevent data loss. After client backup sessions, statistics are analyzed for signs of ransomware infection. If signs are present, administrators are notified, and a warning message is displayed in the Operations Center.

4.2.1.2.4 The solution should include capabilities designed to enable cost efficiencies in data storage requirements.

→ **Response:** IBM Spectrum Protect includes a wide variety of data reduction methods, including client and/or server-side compression and de-duplication. These features can be enabled and disabled depending on workload, to optimize system utilization and improve capacity efficiency, or throughput needs, depending on requirements.

4.2.1.2.5 **Transition Timeline:** The vendor should be capable of implementing a transition from the existing enterprise data backup to the Vendor's solutions within sixty (60) days of the contract award.

→ **Response:** Due to the nature of backup software, implementation of the server-side and repository components can be completed well under 60 days. However, full client deployment and integration across all WVOT client systems may exceed 60 days.

4.2.1.2.6 **Transition Plan:** A transition plan should be provided to the State for approval that outlines the transition from the existing enterprise backup to the Vendor's solution. This should be accomplished within thirty (30) days of contract award.



→ **Response:** SIS will include a transition plan as part of the deployment service. This will include a client migration strategy that provides a break-less backup flow, leveraging existing and new data protection platforms.

4.2.1.2.7 Managed Services Scope: The enterprise data backup scope is **NOT** limited to the data located on infrastructure provided under this contract. The State seeks to leverage this component of the contract to backup data in both the provided infrastructure and existing, state-owned, on-premise infrastructure requiring data backup. The solution should include the following:

- Physical Layer: Services and support of the physical layer of the Enterprise Data Backup & Protection Service.
- Firmware Layer: Services and support of the firmware layer of the Enterprise Data Backup & Protection Service.
- Application Layer: License(s), services, and support for installation, configuration, documentation, training, and operational hand-off to the State of an enterprise-class data backup capability.

→ **Response:** This solution will include capacity growth services for the infrastructure hardware and necessary software changes to leverage that growth, as additional capacity beyond the initial deployment is required. Storage and host devices will be maintained with periodic checks and updates of firmware (6 months). Support and licenses will be included along with the software. Documentation for implementation and maintenance will be accessible for ongoing administration. Training for ten (10) individuals is also included within SIS's proposed solution.

4.2.1.2.8 Enterprise Data Backup Proposal. Vendor should provide documentation outlining how their solution helps the State achieve the goals and objectives outlined in this RFP for enterprise data backup. In addition, the documentation should specifically seek to address the following:

4.2.1.2.8.1 The Vendor's ability to quickly transition from the existing solution to their proposed solution.

→ **Response:** Utilizing a combination of agent-less backup and application-integrated APIs, the implementation will be designed to provide fast on-boarding of backup workloads.

4.2.1.2.8.2 How the Vendor's solution provides industry best practices in data protection.

→ **Response:** IBM Spectrum Protect has been identified as a leader in data protection for multiple decades by many independent agencies. Technologies like PROGRESSIVE INCREMENTAL file backups,



VADPI functionality, DB2 HP DB for indexing and inventory, and leveraging enterprise-level AIX/Power systems hosts provides one of the best solutions available for data backup and recovery.

4.2.1.2.8.3 How the Vendor 's solution provides cost-effective data backup enabling an adherence to compliance requirements.

→ **Response:** The provided solution leverages NetApp’s high-performance block-based ESeries storage that is scalable and cost-effective, along with IBM’s premier hardware platform providing the scale needed to allow for capacity and growth the WVOT expects to need over the life of this solution.

4.2.1.2.8.4 How the Vendor's solution provides flexible capability enabling cost optimization.

→ **Response:** Due to the highly configurable nature of IBM Spectrum Protect, the multiple tiers of requirements for WVOT can be integrated with the use of custom policies, retention rules, and client agents rules.

4.2.1.3 Infrastructure Operations Monitoring. The State seeks an infrastructure operation monitoring solution for this contract. The following specifications outline the goals and services for infrastructure operations monitoring :

4.2.1.3.1 Vendor's proposed solution should provide supported hardware, software, middleware, technical dependencies and/or managed services (where applicable) to enable network and system monitoring that is accessible to both the State and the Vendor.

→ **Response:** Compliant – SIS’s proposed solution for Infrastructure Operations Monitoring would be a hosted SaaS service and would be accessible to both the State of West Virginia and SIS.

4.2.1.3.2 Vendor's system should have the ability to monitor any system (including but not limited to physical servers, virtual servers, storage arrays, databases) and/or any network equipment (including but not limited to switches, routers, etc.).

→ **Response:** Compliant – SIS’s proposed solution meets the requirements of this Section 4.2.1.3.2.

4.2.1.3.3 The monitoring system should be able to create and respond to alerts by notification of appropriate persons via Email, SMS, or other such means

when set thresholds are exceeded. The system should also be able to do basic remediation (e.g. restart services based on triggers).

→ **Response:** Compliant – SIS’s proposed solution meets the requirements of this Section 4.2.1.3.3.

4.2.1.3.4 System should also be able to produce automated reports on a set schedule or on demand about all nodes that are under monitoring. These reports should indicate the health of the system(s).

→ **Response:** Compliant – SIS proposed solution meets the requirements of this Section 4.2.1.3.4.

4.2.1.3.5 Vendor should explain how their proposed monitoring service is both cost effective and uses the least amount of system resources to provide monitoring and supporting the infrastructure.

→ **Response:** The Infrastructure Operations Monitoring offering that SIS proposes is cost effective and efficient because it:

- Leverages a SaaS Environment, eliminating the need for additional on-premise system resources
- Enables the State of West Virginia to predict current and future costs
- Automates:
 - Processes
 - Security
 - Reporting
 - Remediation and control of nodes
- Drastically reduces security risks
- Eliminates labor intensive and error prone manual processes

4.2.1.3.6 Managed Services Scope: The infrastructure operations monitoring scope is NOT limited to the infrastructure provided under the contract. The State seeks to leverage this component of the contract operationally monitoring both the provided infrastructure as part of this contract and for existing, state- owned, on-premise infrastructure, where needed. The solution should include the following:

- Physical Layer: services and support of the physical layer of the infrastructure operations monitoring.
- Firmware Layer: services and support of the firmware layer of the Infrastructure Monitoring & Management Service.
- Application Layer: license(s), services, and support to install, configure, document, training, and operational hand-off to the State of an enterprise-class infrastructure monitoring tool.



→ **Response:** Because SIS's Infrastructure Operations Monitoring is a SaaS-based service, all physical components of the platform are hosted and maintained by the SaaS provider as part of the service; maintenance of the physical layer is, therefore, baked into the subscription cost. Similarly, support for the firmware layer of SaaS Infrastructure Operations Monitoring would be addressed by the SaaS providers (IBM and HCL) as part of the service offering and would be inherently included within the subscription cost. SIS is pleased to include application layer services and support for the Infrastructure Operations Monitoring service. Training for up to ten (10) individuals is also included within SIS's proposal.

4.2.1.3.7 Infrastructure Operations Monitoring: Vendor should provide documentation outlining how their solution helps the State achieve the goals and objectives outlined in this RFP for infrastructure operations monitoring. In addition, the documentation should specifically seek to address the following:

4.2.1.3.7.1 How the Vendor's solution provides industry best practices in infrastructure management.

→ **Response:** For 10 Years, QRadar has ranked in Gartner's Top Quadrant. Please see Attachment #1. Gartner rankings are based on industry best practices and the solution's sustained results (see <https://www.gartner.com/en/research/methodologies/magic-quadrants-research>)

4.2.1.3.7.2 How the Vendor's solution has been scoped and balanced to provide critical capabilities of infrastructure management, while considering cost control.

→ **Response:** For the monitoring solution, we have taken the State's requirements, applied best practices for not only monitoring, but also for security and brought forth a cloud-based solution that is flexible, fluid and scalable. The flexibility of this solution will enable the State to predict current and future costs, automate processes (security, reporting remediation and control of nodes) thereby reducing the security risks and the labor intensive and error-prone manual processes.

4.2.1.3.7.3 How the Vendor's solution provides flexibility in its implementation, enabling the State to maintain visibility on critical resources, but not requiring the capability for resources where the primary business driver is cost.

→ **Response:** Because this solution is automated and crosses heterogeneous environments, the State will have a single dashboard visibility. The processes are automated, eliminating the need for resources to physically monitor, protect, report on and control the environments.



4.2.1.4 On-Demand Professional Services. Vendor should be capable of providing technical professional services, on an as needed basis.

4.2.1.4.1 The State seeks to leverage a statement of work model in utilizing the on-demand professional services.

4.2.1.4.2 The State may leverage these on-demand professional services to perform various technology support functions related to this contract. Those functions could include, but are not limited to, staff augmentation, project work requiring specialization, server provisioning, and application migration.

→ **Response:** Please see SIS's responses to Sections 4.2.1.4.3 and 4.2.1.4.4. below.

4.2.1.4.3 Professional Services Definitions.

4.2.1.4.3.1 Application Migration Specialist. Ability to conduct application and system analysis for the evaluation of application migration. Ability to provide application dependency mapping and documented migration proposal plans. At least seven (7) years of experience. Bachelor's Degree or equivalent work experience.

4.2.1.4.3.2 Data Backup and Disaster Recovery Specialist. Ability to design, maintain and audit backup solutions including achievement of RPO and RTO requirements. Ability to design, maintain and test of disaster recovery capabilities of data center infrastructure. Ability to maintain documentation and processes related to DR and building test plans for DR test scenarios. At least seven (7) years of experience. Bachelor's Degree or equivalent work experience.

4.2.1.4.3.3 Data Migration Specialist. Ability to conduct system, data, and operations analysis, requirements and systems development analysis and design. Able to apply formal, established engineering and management principles to specifications and documentation of systems developed, with an emphasis on business process identification, mapping, and analysis. Can formulate, defines, validates, and documents system scope and objectives, user



requirements or stories, system use cases, business process workflows, enterprise architectures, system specifications and design based on user needs and specifications, research, and fact-finding. At least seven (7) years of experience. Bachelor's Degree or equivalent work experience.

- 4.2.1.4.3.4** Database Specialist. Ability to plan and coordinate the development of data structures and access strategies in alignment with business and mission requirements. Knowledge of and ability to monitor databases and to analyze and organize data and apply new technology designs and programs. At least seven (7) years of experience. Bachelor's Degree or equivalent work experience.
- 4.2.1.4.3.5** Project Manager. Ability to manage all aspects of a technology project while applying best practice PM processes. At least five (5) years of experience. Bachelor's Degree or equivalent work experience.
- 4.2.1.4.3.6** Storage Specialist. Ability to provide system engineering & systems architecture support for enterprise class storage systems. Knowledge of Storage array, SAN network and Infrastructure systems trouble shooting experience. At least seven (7) years of experience. Bachelor's Degree or equivalent work experience.
- 4.2.1.4.3.7** System Administrator Specialist. Ability to design, configure, maintain, and test application servers. At least seven (7) years of experience. Bachelor's Degree or equivalent work experience.
- 4.2.1.4.3.8** Technical Writer. Ability in writing technical documentation to include framework documents, operating instructions, how-to manuals, and assembly instructions to help technical support staff, consumers, and other users understand complex technical systems. At least four (4) years of experience. Bachelor's degree or equivalent work experience.

→ **Response:** SIS has read the requirements in this Section 4.2.1.4.3.8 and it able to supply resources with these levels of skill and experience.



4.2.1.4.4 On-Demand Professional Services Proposal. Vendor should provide documentation outlining how their solution helps the State achieve the goals and objectives outlined in this RFP for on-demand professional services. In addition, the documentation should specifically seek to address the following:

4.2.1.4.4.1 How the Vendor's solution enables the Statement of Work (SOW) model to identify, scope and define deliverables in the drafting of the SOW.

→ **Response:**

Statement of Work Model

To help ensure that SIS and WVOT have a mutual understanding of the required On-Demand Professional Services, SIS would fully expect to create SOWs capturing the scope of work, deliverables, assumptions, and estimates of effort as requests for such services arise. Rates for the professional services would align with the prices documented within the final contract between WVOT and SIS. Authorized points of contact within WVOT would send requests for new SOWs to the assigned SIS Project Manager (during implementation and initial setup of the solution) or to the SIS Service Delivery Manager (post-implementation of the solution), who would then contact the SIS Contract Manager to begin the SOW drafting process. Upon completion of the initial draft, the Project Manager or Service Delivery Manager would present the SOW to WVOT for evaluation and would facilitate negotiation between WVOT and the SIS Contract Manager, if required. Once the SOW has been finalized, it would need to be signed by authorized representatives at the State and SIS prior to becoming actionable. Following the mutual execution of the SOW, SIS would engage with WVOT to begin scheduling and project initiation activities.

Staff Augmentation

SIS carefully screens potential resources by reviewing resumes to select candidate with the desired skills, testing those skills (currently via a web-based testing service) followed by on-site interviews with technical staff and management in cooperation with our client. To augment our staff, SIS has strategic alliances with vendors, partner firms, and local recruiters to provide skills required by our clients. Once a resource is found for WVOT's needs, SIS will draft a SOW to identify the resource, hourly rate, term of engagement, deliverables, and any other relevant or pertinent information that is required for the engagement.

Staffing is a core competency of SIS's parent company, Converge Technology Solutions Corp. As a result, one of our key services is supplying clients with recruiting expertise regarding IT professionals. We have built our reputation by attracting and recruiting high quality, technical candidates that meet the most stringent client demands. We shall provide services as outlined in this RFP on a customized, collaborative basis. Our approach to IT recruiting is disciplined and comprehensive. SIS will spend quality time to get to know the State's needs, requirements, concerns, and current strategies and we will utilize this knowledge



to successfully identify high-caliber candidates that fit well within the State organization's culture. The recruiting methodology is designed for each individual client; therefore, we lean towards a tailored methodology. Our approach for IT recruitment will include thoughtful analysis and thorough background and reference checks. The steps of the recruitment process are detailed in Attachment #2.

In-House Expertise

SIS follows the same extensive vetting process for internal resources as we do for our clients. SIS has employees that have tenure spanning multiple years with SIS. Additionally, our employees attend training and certifications to ensure their skills and knowledge remain current. Every member of SIS's technical consulting team possesses one or more certifications. SIS is a total *Technology Solution Provider*, working with best of breed technologies and employing best practices as defined by the industry. The SIS employees are evaluated extensively prior to onboarding, and these individuals stand up as leaders in their chosen technology. SIS strives to hire the best of breed in IT.

4.2.2 Solution Support Documentation - Vendor should agree to create planning documents outlining all necessary elements of solution management that should be updated continuously during the lifetime of the contract.

4.2.2.1 Vendor's proposal should provide an example of a similar government-owned or managed implementation plan outlining key objectives, dependencies, and timeline for the initial design and implementation of the service. Vendor should, no later than 30 days post-award, submit to WVOT an implementation plan for approval.

→ **Response:** Please refer to the implementation plan that SIS provided for the wvOASIS Production and Disaster Recovery Infrastructure Upgrade (CRFQ ERP2000000002) for the State of West Virginia, enclosed as Attachment #3. SIS is prepared to construct and deliver an implementation plan outlining the key objectives, dependencies, and timeline for the deployment and initial setup of SIS's proposed solution for WVOT within thirty (30) days of final contract award to SIS.

4.2.2.2 Vendor's proposal should provide an example of a guide for on-going operations outlining key objectives, dependencies, and timeline for the on-going management and maintenance of the solution. Vendor should, no later than 30 days post-award, submit to WVOT an on-going operations guide for approval.

→ **Response:** On-going operations and definitions of roles will be a key to making this engagement a success, and SIS is prepared to develop an on-going operations guide within thirty (30) days post-award. This document will need to be maintained throughout the life of the contract. The assigned SIS Service Delivery Manager will own this document as part of their interaction with the State.

At a high-level, this document will set forth the below details to ensure a clear level of understanding between SIS and the State:



- Definition of terms
 - This will ensure a common language is used and understood between the organizations
 - Will be reviewed and edited as needed and agreed upon between the State and SIS as new terms are identified
- Client Support Model
 - Contains detailed instructions concerning procedures for contacting the right resource to support various aspects of the solution
 - Provides an escalation plan for the State and SIS
- Work Order Model
 - Description of what needs to happen in the event of a work order needs to be completed
 - Includes initiation, execution, and sign-off phases of the work order
- Client Communication Plan
 - A description documenting how to notify the State of any communication
 - A tiering system of notification will be used to denote plans for Executive Only, Urgent, Warning, and Informational communications
- Support Schedule
 - Lists and describes normal business operations from an SIS/OEM standpoint
 - Lists response time objectives for the various components of the solution, as applicable

Ultimately, this plan needs to be built in conjunction with the State. SIS will work with the State to include any additional content areas they feel is necessary to support the engagement and on-going operations of the environment.

- 4.2.2.3** Vendor's proposal should provide an example of a solution transition and contract exit plan for another entity of similar size and scope as part of their bid response. The plan should outline key objectives, dependencies, and tasks necessary to disentangle the Vendor from the agency. An official solution transition and contract exit plan should be provided to WVOT by the end of year one (1) of the contract.

→ **Response:** In the event the State desires to transition the solution to another vendor, SIS is committed to helping make the transition as smooth as possible. Because the new vendor may have new and different processes, procedures and requirements, the solution transition plan must be carefully customized to ensure that the solution is effectively and thoroughly transitioned while minimizing adverse impacts to the State. Therefore, any transition plan constructed by SIS would need to be developed with an understanding of the specific vendor that will be taking over management of the solution. In general, SIS would expect to include the following high-level components in the transition plan:

- Current Solution Review
 - Includes making available all documentation created as part of the engagement
 - A review session with the new vendor or State to address any questions they may have
 - Asset listing including end of lease information
 - List of any on-going financial responsibilities
- Transition Team
 - Provide a list of named individuals within SIS responsible for managing the transition



- tasks required for the duration of three (3) months after the decision to transition is made
- o Goal of the team is to ensure a smooth transition is achieved
- Consultation Option
 - o Additional time to assist with the transition can be consumed as a billable engagement with either the State directly or the new vendor assuming responsibilities of the environment, depending upon the scope and specific expertise needed to provide further assistance

Please refer to Attachment #4 for a sample contract exit plan. SIS expects that the contract exit plan constructed for the State would be reviewed and refined periodically during the life of the contract to take new risks and requirements into account. The assigned SIS Service Delivery Manager along with the SIS Contract Manager would be responsible for arranging reviews of the contract exit plan with WVOT to ensure that appropriate updates are made to the action items, designated tasks, and timeframes.

- 4.2.2.4 Vendor's proposal should explain how they would support the State relating to cybersecurity and privacy audits when components of the contract fall within the scope of audits. The State leverages NIST 800-53 to map all controls to a common framework.

→ **Response:** SIS is subject to SOC2 Type 2 annual security audits, maintains its own quarterly self-assessment, and follows the guidelines of NIST 800-53 in the management of its own data center in Lexington, KY. While SIS cannot make any representations beyond those provided by the OEMs with respect to cybersecurity and privacy for the solution proposed to WVOT, SIS would fully expect to collaborate during WVOT's security audits, and would provide the data SIS is reasonably able to obtain in order to assist in those efforts; in certain circumstances, some data may need to be provided in a redacted format in order to prevent inadvertent disclosure of proprietary information.

- 4.2.2.5 Lifecycle Model: Vendor's proposal should submit an example of an on-premise infrastructure lifecycle management plan explaining how the Vendor's proposal will address the lifecycle stages of the on-premise infrastructure. This plan should be updated and submitted to WVOT for review and approval at least every twelve (12) months.

→ **Response:** The SIS response supports ongoing lifecycle management through depreciation of the assets with a termed lease agreement. At the end of the lease term, a new lease can be undertaken with new upgraded equipment and a phase-out effort of the existing infrastructure can be undertaken.

All hardware included as part of the SIS response is new hardware from the OEM. The hardware includes maintenance and support for a full 48 months. Having these contracts in place will ensure that the State's infrastructure in the environment will always be under maintenance. SIS's solution is also built such that, as the equipment ages, new equipment can be implemented to replace any equipment that reaches end of life during the contract term, while keeping the same pricing intact for consumption.



Every 12 months, the SIS Service Delivery Manager would provide an asset review report. This report will show all the equipment at end of service life, end of support life, and end of contract. This effort will ensure all equipment is tracked and ensured to be fully functional with active support and maintenance contracts in place.

4.2.2.6 The State desires regularly scheduled meetings and/or calls to discuss the following areas:

- Architecture and Design
- Implementation
- Ordering and Billing
- Service and Support
- Project Management

Please describe your company's ability to hold monthly meetings on each of these topics, as well as your company's implementation plans for starting these discussions.

Vendor should provide an example of a maintenance plan outlining the roles and responsibilities of the vendor as it relates to the scoped managed services outlined. The maintenance plan should outline maintenance requests and the approval process.

→ **Response:** The assigned Service Delivery Manager will conduct regular touchpoints with the customer to review the various elements of service being provided. All bullet points listed above would be considered in scope for those discussions. Not all topics will be covered as part of a standard agenda, but each meeting can be adjusted as needed.

4.2.2.7 If the Vendor's work requires them to be at a State site, the Vendor should provide the Agency at least seventy-two (72) hours' notice before arriving at the site. Vendor should comply with all Agency policies, State laws, and background checks for contractors, Vendor's, and visitors. Vendor should describe their approach to this requirement.

→ **Response:** SIS, OEM's, and contractors performing under the contract, shall comply with all laws applicable to their performance and obligations.

SIS and OEM personnel undergo background checks as a part of routine employee onboarding procedure. Contractors supplying the On-Demand Professional Services shall also be required to undergo background checks per WVOT's specifications.

The initial implementation of the proposed solution will require onsite visits for physical setup and installation; once equipment is accessible remotely, SIS expects that the remaining work can be done via remote (VPN) connection. Unless otherwise instructed or approved by WVOT personnel, SIS shall adhere



with the 72-hour advanced onsite notice guideline specified in this Section 4.2.2.7 for the initial implementation services as well as for the On-Demand Professional Services. Any OEM-provided maintenance services performed onsite shall follow any response time standards documented in the OEM maintenance contracts and associated materials.

4.2.3 Contract Management

4.2.3.1 Contract Management: Vendor's proposed solution should provide applicable, supported hardware, software, middleware and technical dependencies that enables contract management from the business management perspective of centralized ordering, billing, financial auditing, and reporting.

→ **Response:** SIS's solution is composed such that SIS would be the State of West Virginia's centralized contact for all ordering for the proposed solution. The State's reporting needs may be met in a variety of ways depending upon what types of reports are required, but SIS would generally be the State's primary contact for this aspect of the solution, as well. For instance, the SIS Project Manager and/or Service Delivery Manager would be responsible for providing time reports for the On-Demand Professional Services as reasonably requested. Please also see the SIS response to Section 4.3.1.7. for additional information about the SIS Project Manager and Service Delivery Manager's role in contract management.

Billing and financial auditing responsibilities would be shared between SIS (for all services) and the leasing company (for all infrastructure components and maintenance under lease). As a full-owned subsidiary of a publicly traded company, SIS would expect that its obligations with respect to financial auditing would be limited to providing the publicly available financial records of SIS's parent company (Converge Technology Solutions Corp.) and/or the financial transaction records between SIS and the State of West Virginia, unless otherwise required by law.

4.2.3.2 Included Professional Services: Vendor should provide professional services for configuration and management of the solutions, as well as training for no less than ten (10) persons. Vendor should also produce documentation (either vendor or manufacturer created) showing how the systems work and how changes can be made if needed.

→ **Response:** SIS's proposal includes professional services for the initial implementation of the solution, as well as training for IBM Spectrum Protect, IBM QRadar, and HCL BigFix for ten (10) individuals apiece. On-Demand Professional Services would also be made available should the State require professional services assistance from time to time during the term of the contract.

Standard documentation (such as system manuals and as-built configurations) pertaining to the functionality and setup of the solution components shall be provided to the State after the initial implementation of the solution. Additional resources providing guidance on troubleshooting and other administration tasks are also available online, such as at the sites shown here:

- NetApp: <https://mysupport.netapp.com/documentation/productsatoz/index.html>
- IBM Spectrum Protect:



https://www.ibm.com/support/knowledgecenter/en/SSEQVQ_8.1.0/srv.solutions/c_tsm_concept_s.html

- IBM QRadar: <https://www.ibm.com/support/knowledgecenter/en/SS42VS>
- HCL BigFix: https://support.hcltechsw.com/csm?id=bigfix_support
- Zerto: <https://www.zerto.com/myzerto/knowledge-base/>

4.2.3.3 Billing: Vendor's proposed solution should provide billing capabilities designed to simplify the procedures of a chargeback model, as well as, provide a holistic view of service. The state desires the billing detail to include but not be limited to billing by agency, consumption usage by agency, inventory, and disaster recovery services. Vendor should provide an example of billing capabilities designed to simplify the procedures of a chargeback model, as well as, provide a holistic view of service. (Example: Department of Transportation charges broken down as specified above)

→ **Response:** SIS's proposed solution contains the reporting tools and resources necessary to assist WVOT with simplifying the procedures of a chargeback model, provided that WVOT and SIS closely collaborate to achieve this goal. Without the input of WVOT, SIS will not be able to understand which State agency is consuming which portion of the infrastructure. While there are many ways to calculate cost of resource consumption, SIS expects that the simplest method would be by standardizing based on Virtual Machine profile(s).

Standard Virtual Machine profiles are common in the public and private cloud industry. By defining the characteristics of each Virtual Machine profile, along with the cost to support one instance of the profile, WVOT can provide a catalog of profiles to be consumed by the end users or agencies. The main problem some users experience is that standardized profiles put too stringent of a rule set to support various workloads. It also often requires over-provisioning of resources to ensure the workload is able to support it as a client of the Private Cloud.

SIS can work with WVOT to develop a pricing catalog that is accurate, and flexible to meet the needs of the State and the agencies. It would be an on-going collaborative effort, but not an impossible task.

4.2.3.4 Financial Reporting: Vendor's proposed solution should develop and provide financial reporting to meet the State's reporting obligations and the State's goals of transparency and technology optimization.

→ **Response:** SIS would expect to work with WVOT to develop a financial reporting process pertaining to the finally awarded contract. Per SIS's response to Section 4.2.3.1, financial reporting may require the involvement of leasing company for information pertaining to the leased infrastructure and maintenance components of the solution.



- 4.2.3.5 **Third Party Terms and Conditions:** Vendor should limit pass-through of third-party terms and conditions; Vendor should describe how their proposal meets this goal.

→**Response:** The solution proposed by SIS incorporates substantial components provided by third-party OEMs. Any and all goods and services provided by OEM's under this contract shall be subject to the applicable terms and conditions provided by such OEM. The below terms and conditions would supersede any additional or different terms presented by the State (including, without limitation, any standard terms and conditions incorporated into the State's RFP) with regard to each respective component of the solution unless otherwise negotiated between the parties in writing.

Terms and conditions applicable to NetApp component(s) of the solution are available here: <https://www.netapp.com/us/how-to-buy/stc.aspx>

Terms and conditions applicable to IBM QRadar component(s) of the solution are available here: https://www.ibm.com/software/passportadvantage/pa_agreements.html

Terms and conditions applicable to HCL component(s) of the solutions are available here: <https://www.hcltechsw.com/wps/portal/resources/master-agreements>

Terms and conditions applicable to Zerto component(s) of the solution are available here: <https://www.zerto.com/zerto-terms-and-conditions-product/>

Terms and conditions applicable to the Predatar software(s) is included in Attachment #5.

Terms and conditions applicable to the On-Demand Professional Services and implementation services performed by SIS can be found here: <http://thinksis.com/wp-content/uploads/2018/08/master-service-agreement.pdf>

The leasing company selected to finance the infrastructure and maintenance components of the solution would also be likely to require the State's adherence to certain terms and conditions.

- 4.2.4 **Mandatory Project Requirements** - The following mandatory requirements relate to the goals and objectives and must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it will comply with the mandatory requirements and include any areas where its proposed solution exceeds the mandatory requirement. Failure to comply with mandatory requirements will lead to disqualification, but the approach/methodology that the vendor uses to comply, and areas where the mandatory requirements are exceeded, will be included in technical scores where appropriate. The mandatory project requirements are listed below.

- 4.2.4.1 **General Mandatories**

- 4.2.4.1.1 The State of West Virginia reserves the right to move, change or add additional Data Center locations.



→**Response:** Compliant – The proposed solution shall permit the State of West Virginia to move, change, or add additional Data Center locations. All such requested changes would need to be documented in writing between SIS and the State and may result in additional charges (e.g. for transportation for equipment, reinstallation services, and additional infrastructure costs).

4.2.4.1.2 WVOT will not accept penalties for scaling down any tier solution, expansion node, expansion storage or infrastructure monitoring node(s).

→**Response:** The SIS proposed solution is being delivered through an operational lease. The State shall be able to cease use of any infrastructure they no longer need to consume at any time; however, lease payments for all infrastructure shall still be required for the duration of the contract.

4.2.4.1.3 The Vendor must agree that the State owns all data gathered under the scope of this contract. The Vendor must produce and/or return the data upon the State's request in an editable format mutually agreeable to both parties. If any component (e.g. disk drive) fails, the Vendor must ensure any data on said component is destroyed in accordance with WVOT policies and certify, either in writing or some other mutually agreeable format, that any data on said component was destroyed.

→**Response:** SIS acknowledges and agrees that the State owns all data gathered under the scope of this contract; SIS does not expect any ownership rights with respect to such data. Please also see SIS's response to Section 4.2.4.2.6 for more information.

4.2.4.1.4 Vendor shall provide the State full access to any and all encryption keys the Vendor may generate in support of this contract.

→**Response:** SIS and OEMs will not own any encryption keys as part of the final contract. It is the sole responsibility of the WVOT to own and maintain all encryption keys.

4.2.4.1.5 Vendor shall ensure all solution expenses associated with this contract are captured within the pricing sheet.

→**Response:** Compliant – SIS is including all solution expenses within its Cost Proposal.

4.2.4.2 Cybersecurity Mandatory Requirements

4.2.4.2.1 Vendor proposed solution must be capable of adherence to federal and state law.

→**Response:** Please see the SIS response to Section 4.2.2.7 and 4.2.4.2.2.



4.2.4.2.2 Vendor's proposed solution must adhere to the State of West Virginia's Cyber Security & Privacy policies, procedures, and standards; these can be viewed at the following link:

<https://technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx>

→**Response:** SIS's proposed solution incorporates substantial components provided by third-party OEMs, including maintenance support. SIS is not able to make any warranty or representation regarding the proposed solution's adherence with the State of West Virginia's Cybersecurity & Privacy policies, procedures and standards beyond the representations provided by the respective OEMs. Resources regarding the OEMs' cybersecurity and privacy policies are provided below for WVOT's review:

- Information concerning IBM QRadar's cybersecurity features can be found here: https://exchange.xforce.ibmcloud.com/hub/extension/6ecaea38823253d1bba05637d5d0bea5?_ga=2.209832981.1625512216.1586266404-955976318.1586266404&cm_mc_uid=67004545056915862664042&cm_mc_sid_50200000=80337601586271154844&cm_mc_sid_52640000=32534381586271627129 and here: <https://www.ibm.com/downloads/cas/RLXJNX2G> (see also Attachment #6).
- Information concerning HCL's compliance capabilities can be found here: <https://support.bigfix.com/documents/HCL%20BigFix%20-%20Datashet%20-%20Patch%20-%20v1.2.pdf> (see also Attachment #7) and HCL's Privacy Statement can be found here: <https://www.hcltechsw.com/wps/portal/resources/master-agreements>
- NetApp is the largest provider of storage to the US Federal Government with 50% market share in Civilian Agencies and 70% market share in Secure Federal (Classified) agencies. NetApp storage secures some of the most highly classified data in the world. Please see Attachment #8 for additional information concerning NetApp OnTap's data security features. NetApp's Privacy Policy can be found here: <https://www.netapp.com/us/legal/privacypolicy/index.aspx>
- Information concerning Zerto's cybersecurity features is available in Attachment #9. Zerto's Privacy Policy can be found here: <https://www.zerto.com/privacy-policy/>

4.2.4.2.3 Vendor proposed solution must be capable of adherence to all applicable security and privacy standards that are subject to the following:

- Health Insurance Portability and Accountability Act (HIPAA) requirements as outlined in the attached Business Associate Addendum (BAA);
- Federal Information Security Management Act (FISMA), National Institute of Standards Technology's Special Publication (NIST SP) 800- 53, NIST SP 800-17 which serve as the baseline;
- Family Education Rights and Privacy Act (FERPA) requirements;
- Criminal Justice Information System (CJIS) requirements;



- Payment Card Industry Data Security Standards (PCI-DSS) requirements;
- Federal tax Information (FTI) and Internal Revenue Service publication 1075 (IRS 1075) requirements;
- Centers for Medicare & Medicaid (CMS) Services Information Security Policy requirements.

→**Response:** While all the infrastructure provided as part of this RFP response can be configured to support the applicable security and privacy standards, it is incumbent upon the State to instruct SIS how they would like the infrastructure deployed to ensure it meets these requirements. The data security and privacy are the responsibilities of the State. SIS does not make any claim of responsibility as to adherence to security and privacy standards the State must meet. Please also see SIS's response to Section 4.2.4.2.2.

4.2.4.2.4 The Vendor must adhere to personnel security requirements for background checks in accordance with state law. The vendor is liable for all costs associated with ensuring their staff meets all requirements.

→**Response:** Compliant - SIS conducts background checks for all of its employees and shall ensure that contractors performing the On-Demand Professional Services undergo background checks, as well. SIS shall take responsibility for all costs it incurs in ensuring that its staff meets the requirements under this Section 4.2.4.2.4. Third-party OEMs performing under this contract also conduct background checks for their personnel.

4.2.4.2.5 The Vendor must implement and strictly adhere to physical equipment inventory policy and procedures that are designed to ensure data protection.

→**Response:** SIS is willing to work with the state to physically track the equipment (asset tags and asset database entries) for purposes of inventory tracking. Please see SIS's response to Section 4.2.4.2.2. for additional information regarding data protection procedures.

4.2.4.2.6 The Vendor must adhere to industry-standard data destruction measures and provide the state with written attestation of data destruction. This includes failed hardware where State data may reside.

→**Response:** Spectrum Protect equipment retirement will include encryption key deletion procedures and US DoD 5220.22-M level data wipe prior to any equipment leaving WVOT facilities. The data wipe process may take several weeks to complete, depending upon the quantities of data erased. The NetApp storage solution proposed includes a secure erase functionality that can be utilized to meet the requirements of this Section 4.2.4.2.6 and data stored via the IBM QRadar platform is capable of being destroyed, as well.



4.2.4.2.7 All Vendor's must ensure that any equipment or software used is not at manufacturer's specified "end of life" (EOL) or "end of support" (EOS) dates and will be supported by the original manufacturer. Maintenance and Support contracts shall be maintained by the vendor on all equipment and software for the life of this contract. Copies of such contracts should be provided to the State with Vendor's response.

→**Response:** Compliant - SIS understands and will comply with the requirement in this Section 4.2.4.2.7. Copies of the maintenance contracts can be found at the following locations:

Maintenance terms and conditions applicable to IBM components of the solution can be found here: https://www.ibm.com/software/passportadvantage/pa_agreements.html

Maintenance terms and conditions applicable to HCL components of the solution can be found here: <https://www.hcltechsw.com/wps/portal/resources/master-agreements>

Maintenance terms and conditions applicable to Zerto components of the solution can be found here: <https://www.zerto.com/zerto-terms-and-conditions-product/>

Maintenance terms and conditions applicable to NetApp components of the solution can be found here: <https://www.netapp.com/us/media/support-services-terms.pdf>

4.2.4.3 On-Premise Infrastructure Mandatory Requirements: Pricing for Vendor's proposed solution must provide supported hardware, software, middleware, technical dependencies and/or managed services (where applicable) to ensure that all the goals/objectives of this RFP are met. The price for each solution, node expansion and storage expansion must be entered on the pricing sheet (Attachment "A").

4.2.4.3.1 Virtualization. The on-premise infrastructure solution must be compatible with industry-standard virtualization software. The State currently leverages VMWare. The Operating System (OS) and virtualization licensing are outside the scope of the on-premise infrastructure component.

→**Response:** Compliant – SIS's proposed solution is compatible with industry-standard virtualization software. SIS understands that the operating system and virtualization licensing are outside the scope of the on-premise infrastructure component.

4.2.4.3.2 Networking. The on-premise solution must include all components to enable the internal networking of the on-premise infrastructure. The State will provide boundary networking capability enabling the network connection of the infrastructure to the state's internal network and to the Internet.



→**Response:** Compliant – SIS’s proposed solution contains all components to enable the internal networking of the on-premise infrastructure.

4.2.4.3.3 Active Directory Domain. The on-premise solution must be capable of integrating with the WVOT's Active Directory (AD) domain.

→**Response:** Compliant – SIS’s proposed on-premise solution is capable of integrating with the WVOT’s Active Directory domain.

4.2.4.3.4 Domain Name Service (DNS). The on-premise solution must be capable of integrating with WVOT's DNS.

→**Response:** Compliant – SIS’s proposed on-premise solution is capable of integrating with WVOT’s DNS.

4.2.4.3.5 The Base Solution for all tier levels must have the ability, to be provisioned by the State, with the following minimum specifications:

- 24 vCPU cores at a minimum of 2.6GHz processing speed
- 512 GB RAM
- 500 GB Performance Storage
- 1 TB of Volume Storage

→**Response:** Compliant – SIS understands the requirements and has designed the solution to meet or exceed these requirements. Additional information about NetApp HCI is provided as supplementary material with this proposal.

4.2.4.3.6 The Node Expansion for all tier levels must have the ability, to be provisioned by the State, with the following minimum specifications:

- 12 vCPU core expansion
- 256GB RAM

→**Response:** Compliant – SIS understands the requirements and has designed the solution to meet or exceed these requirements. Additional information about NetApp HCI compute is provided supplementary to this proposal.

4.2.4.3.7 The Storage Expansion for all tier levels must have the ability, to be provisioned by the State, with the following minimum specifications:

- Performance Storage of 10TB
- Volume Storage of 25TB



→ **Response:** Compliant – SIS understands the requirements and has designed the solution to meet or exceed these requirements. Additional information on NetApp OnTap is provided supplementary to this proposal.

4.2.4.4 Enterprise Data Backup Mandatory Requirements - Pricing for Vendor's proposed solution must provide supported hardware, software, middleware, technical dependencies and/or managed services (where applicable) to ensure that all the goals/objectives of this RFP are met. The price for the solution must be entered on the pricing sheet (Attachment "A").

4.2.4.4.1 Pricing Structure. The pricing structure will account for the following components.

4.2.4.4.1.1 Data Backup Initial Installation. The initial installation line item is designed to include all aspects to scope, design, architecture, implement, configure, test, train, and operational hand-off the capability to the State.

→ **Response:** Compliant – SIS would provide all aspects stated in this Section 4.2.4.4.1.1 as part of the initial implementation.

4.2.4.4.1.2 Data Backup Solution. The data backup solution provides the monthly cost for base level solution. The data backup solution must include:

4.2.4.4.1.2.1 Data backup for one-hundred fifty (150) TB.

→ **Response:** Compliant – SIS's proposed solution will include 150TB of storage per site. This can be used as active/passive, active/active, or a combination of the two. The 150TB is post-data-reduction capacity, meaning logical capacity will exceed this number in most circumstances.

4.2.4.4.1.2.2 Data backup capability at two (2), physically separate locations for redundancy.

→ **Response:** The solution will include two (2) physical deployments of Spectrum Protect, with replication established between the two locations, allowing data to be electronically transmitted from site-to-site for data resiliency.

4.2.4.4.1.3 Data Backup Expansion. The data backup expansion line item is designed to include costs associated with the



storage expansion of the solution. The data backup expansion must include:

4.2.4.4.1.3.1 Minimal backup storage expansion of fifty (50) TB.

→ **Response:** Expansion options for this solution will entail a 50-60TB expansion option (per site) as needed, with minimal configuration changes. Storage can be added with zero downtime and scalability to 1PB (initially) following this model is planned in the design.

4.2.4.4.2 Physical Infrastructure Location. Any physical infrastructure should be installed at a State-owned or State-leased data center location. Any change of location for the physical infrastructure is a decision held solely by the State.

→ **Response:** The solution will be installed at the State's designated data center location, providing data protection services for its respective site (local backups) with data-reduced replication services to the alternate location (compression/deduplication before transmission).

4.2.4.5 Infrastructure Operational Monitoring Mandatory Requirements - Pricing for Vendor's proposed solution must provide supported hardware, software, middleware, technical dependencies and/or managed services (where applicable) to ensure that all the goals/objectives of this RFP are met. The price for each monitored system (or group of monitored systems) must be entered on the pricing sheet (Attachment "A").

4.2.4.5.1 Pricing Structure:

4.2.4.5.1.1 Infrastructure Monitoring Initial Installation. The initial installation line item is designed to include all aspects to scope, design, architecture, implement, configure, test, train, and operational hand-off the capability to the State.

→ **Response:** Compliant – Pricing in SIS's Cost Proposal for the Infrastructure Operational Monitoring includes all of the requirements in this Section 4.2.4.5.1.1.

4.2.4.5.1.2 Infrastructure Monitoring Solution. The solution line item provides the monthly cost for base level solution. The infrastructure monitoring solution must, minimally, include the ability to operationally monitor two-hundred fifty



(250) components. A component consists of a physical device or a software instance.

→ **Response:** Compliant – The cost presented in SIS’s Cost Proposal represents the monthly price for the base level solution. The Infrastructure Operational Monitoring solution that SIS proposes is a SaaS service and is capable of monitoring over 1,400 components.

4.2.4.5.1.3 Infrastructure Monitoring Expansion. The expansion line item is designed to include costs associated with component expansion of the solution. The expansion must, minimally, include a component volume expansion of fifty (50) components.

→ **Response:** Compliant – SIS has included pricing for an expansion option within its Cost Proposal.

4.2.4.6 On-Demand Professional Services Mandatory Requirements - Pricing for any professional services must be fully "loaded" to capture all direct and overhead expenses, travel, per diem, and any other travel-related expenses. Prices for all positions included in this RFP must be entered on the pricing sheet (Attachment "A").

4.2.4.6.1 Vendor must agree to an open-end contract method, where prior to each potential engagement of professional services, a Statement of Work will be drafted and mutually agreed upon by both parties. After a SOW is finalized, each engagement will be initiated by the State via Delivery Order that incorporates the SOW. This applies to all professional service positions listed in Specification 4.2.1.4. No statement of work will be permitted to include work unrelated to Data Center 2.0.

→ **Response:** Compliant – The pricing rates listed within SIS’s Cost Proposal are fully loaded and SIS expects to leverage Statements of Work to document each requested engagement for On-Demand Professional Services. SIS acknowledges that no Statements of Work will be permitted to include work unrelated to Data Center 2.0.

4.2.4.7 Contract Management Mandatory Requirements

4.2.4.7.1 The successful Vendor must assign an experienced and skilled Project Manager who will provide a high-level project management plan including key components such as a project charter, issue tracking, statements of work (SOW), work breakdown structures (WBS), implementation schedules, etc. in accordance with the Project Management Body of Knowledge (PMBOK) or



other industry standard project management methodology stated in West Virginia State Code (§5A-6-4b). The link can be found at: <http://www.legis.state.wv.us/WVCODE/Code.cfm?chap=05A&art=6#06>. The project management plan must be submitted to and approved by the State prior to implementation.

→ **Response:** SIS will assign a Project Manager for all onboarding and implementation activities in scope for installation of hardware/software and delivery of services. Additionally, SIS will construct a project management plan and submit to the State for approval post-award. Upon completion of onboarding and implementation activities, SIS will assign a Service Delivery Manager to oversee delivery of services, contract change management, and customer satisfaction for the life of the agreement.

4.2.4.7.2 The successful Vendor's Project Manager must track and report (via written status reports) the following: schedule, scope, budget, issues, risks, specified performance indicators, and other metrics determined appropriate throughout the project and each site implementation.

→ **Response:** Compliant – SIS Project Managers maintain these project artifacts as part of every engagement with customers.

4.2.4.7.3 Vendor billing errors must be credited back to the State from the effective date of the error. The State reserves the right to withhold payment until credit is received.

→ **Response:** SIS shall promptly credit back the State of West Virginia for any billing errors pertaining to SIS's invoicing. However, any billing errors pertaining to the infrastructure and maintenance under lease would need to be corrected by the leasing company.

4.2.4.7.4 For auditing, billing, and support purposes, the State requires any service with an associated rate to be identified on its monthly bill. As such, the State must be provided, at a minimum, the following:

- Billing Period
- Billed Entity Name
- Customer Name/Account (if different from billed entity)
- Itemized Cost for Individual Billing Components
- Total Cost

The cost identified in the bill must match the contract rates for the specified services.



→ **Response:** Compliant - SIS shall include the information specified in this Section 4.2.4.7.4 on its monthly services invoices to the State of West Virginia.

4.2.4.7.5 The Vendor must invoice on a consistent monthly billing cycle across all services. Increases or decreases for a partial month must be prorated based on the date of the service increase or decrease.

→ **Response:** SIS shall invoice the State on a regular, monthly basis for the services components of the proposed solution. Invoicing pertaining to the infrastructure and maintenance would come from the leasing company and is only upwardly scalable in price.

4.2.4.7.6 All tier Base Solution(s), Expansion Node(s), Expansion Storage, Enterprise Data Backup, and Infrastructure Operations Monitoring pricing must include the cost of delivery, physical installation, and initial physical configuration by the Vendor. The Vendor 's unit price should be inclusive of all hardware maintenance and support costs.

→ **Response:** Compliant – SIS’s unit pricing within its Cost Proposal aligns with the requirements of this Section 4.2.4.7.6.

4.2.4.7.7 Vendor must input pricing for each tier Base Solution(s), Expansion Node(s), Expansion Storage, Enterprise Data Backup, and Infrastructure Operations Monitoring in the pricing page. These costs will be a per month charge and include all costs for providing that service as indicated elsewhere in this RFP. Vendor must also input a per hour charge for those professional services positions listed on the pricing page.

→ **Response:** Compliant – SIS has input the pricing in its Cost Proposal in accordance with the instructions in this Section 4.2.4.7.7.

4.2.4.7.8 Vendor must input percent discount to the corresponding Asset in Service year periods on the pricing page. (Cells G4 through M4). Enter a whole number (e.g. 4) or fraction of a number (e.g. 7.5) corresponding to the percentage discount. The spreadsheet will automatically treat the number as a percentage.

→ **Response:** SIS acknowledges the State’s instructions in this Section 4.2.4.7.8.

4.2.4.7.9 The Vendor's price in Asset in Service will be used by the State to calculate the cost of all orders. Orders placed in billing status in Year 1 will be billed at



the subsequent Year's monthly unit price beginning in subsequent year. For example, a tier 0 solution ordered in month 1 of Year 1, will be invoiced at the Year 2 unit price beginning in Month 1 of Year 2.

→ **Response:** SIS acknowledges the State's calculation method represented in this Section 4.2.4.7.9.

4.2.4.7.10 The State expects full, complete, and timely cooperation in disentangling the relationship if the Agreement expires or terminates for any reason. In the event of expiration or termination, the State expects that the Vendor shall, among other things: return all State data and documentation to the State, including but not limited to configuration information and allow the State or the replacement provider(s) continued view (read-only) access to all billing, previously placed orders, and previously opened trouble ticket system, and document processes that have been employed in servicing the State and provide the state a copy, in accordance with methods and procedures to be agreed upon and established in the Agreement. **Please acknowledge your acceptance of this.**

→ **Response:** SIS acknowledges and accepts the State's requirements in this Section 4.2.4.7.10. The process for completing these requirements is expected to take at least ninety (90) days.

4.3 Qualifications and Experience: Vendor should provide information and documentation regarding its qualifications and experience in providing services or solving problems like those requested in this RFP. Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives were and how they were met), references for prior projects, and any other information that vendor deems relevant to the items identified as desirable or mandatory below.

4.3.1 Qualification and Experience Information: Vendor should describe in its proposal how it meets the desirable qualification and experience requirements listed below.

4.3.1.1 Vendor should specify previous experience in providing an on-premise infrastructure, preferably with government organizations. Vendor should include the scope of programs implemented. Vendor should also include any contacts at the specified entity who can be contacted for verification.

→ **Response:**

SIS has previously conducted on-premise infrastructure deployments for the State of West Virginia. Below are some of the latest examples with references and project summaries for the State's review:



Reference	Solution Summary
<p>Tim Conzett Senior Administrator Office of Data Management and Information Systems 1900 Kanawha Boulevard, East Building 6 Suite 750 Charleston, WV 25305 Phone: 304-558-8869 tim.conzett@k12.wv.us wvde.state.wv.us</p>	<p>SIS assisted the West Virginia Department of Education (“WVDOE”) to procure and install new compute infrastructure at WVDOE’s premises in 2019. As a part of this solution, SIS successfully migrated WVDOE off of their old compute systems and configured the new systems for high availability.</p>
<p>Matt Ellison Chief Information Officer/Chief Technology Officer West Virginia OASIS Phone: 304-741-8565 1007 Bullitt Street Charleston WV 25301 matt.ellison@wvoasis.gov</p>	<p>In late 2019 and early 2020, SIS engaged with the West Virginia OASIS (“wvOASIS”) team to complete an on-premise storage, compute, and networking infrastructure refresh for the wvOASIS production and disaster recovery locations. SIS architected a solution consisting of industry-leading technologies to replace wvOASIS’s aging hardware and deployed its skilled and experienced personnel to conduct implementation, migration, and knowledge transfer professional services prior to successfully handing off the solution to the wvOASIS team.</p>
<p>Kin Richardson Director of Network Operations West Virginia State Treasurer’s Office 322 70th Street S.E. Charleston, WV 25304 Phone: 304-341-0727 richardson@wvsto.gov</p>	<p>In 2018 and early 2019, SIS engaged with the West Virginia State Treasurer’s Office (“WVSTO”) team to complete an on-premise storage, compute, and networking infrastructure refresh for the WVSTO production and disaster recovery locations. SIS architected a solution consisting of industry-leading technologies to replace WVSTO’s end of life hardware. SIS deployed its skilled and experienced personnel to conduct implementation, migration, and knowledge transfer professional services prior to successfully handing off the solution to the WVSTO team.</p>

4.3.1.2 Vendor should describe its experience and process for supporting cybersecurity requirements associated with the components of this RFP.

→ **Response:** Please refer to SIS’s response in Section 4.2.4.2.2.

4.3.1.3 Vendor should describe its experience and capabilities in supporting their customers during compliance audits when the vendor-supplied solution is within the scope of audit.

→ **Response:** Please refer to SIS’s response in Section 4.2.2.4.



4.3.1.4 Vendor should describe its policies and procedures for conducting sub-contractor assurance, validating both the capability of the vendor to fulfill contracted responsibilities and adhere to all applicable security & privacy policies.

→ **Response:** Please see Attachment #2 for SIS’s recruitment process relating to staffing services. Components of the solution which are not performed via SIS’s own personnel or staffing would be conducted by an OEM.

4.3.1.5 Vendor should list all references and/or examples for previous experiences in providing on-premise infrastructure services. Vendor should include any applicable documentation pertaining to the services outlined within this solicitation.

→ **Response:** SIS has conducted numerous on-premise infrastructure deployments over the years and our expertise and dedication has earned the trust and repeat business of many clients. SIS’s parent company, Converge Technology Solutions Corp., is a NetApp Gold Partner and IBM Platinum Partner with dozens of employees holding certifications from both NetApp and IBM.

Below are some references provided as examples for the State’s evaluation:

Reference	Solution Summary
Chad Hanson Senior Vice President, Director of IT Phone: 740-374-6119 Peoples Bank 138 Putnam St Marietta OH 45750 chad.hanson@pebo.com	SIS deployed Production and Disaster Recovery infrastructure for Core Banking Applications for over 90 Branches and 1000 employees.
Brian Broyles Chief Technology Officer First Community Bank One Community Place Bluefield, VA 24605 Phone: 304-323-6400 bbroyles@fcbinc.com	SIS deployed Production and Disaster Recovery infrastructure for Core Banking Applications for over 80 Branches and 900 employees.
Kim Ennis, PMP Senior Director IT HealthSmart Benefit Management, LLC 602 Virginia Street, East Charleston, WV 25301 Phone: 304-353-8884 kim.ennis@healthsmart.com	SIS deployed Production and Disaster Recovery infrastructure for third-party administration of healthcare claims by self-insured companies. Infrastructure provided from the SIS Managed Solution Center (SIS Cloud).



<p>Fred Cash ITS Manager of Computer Services City of Cleveland 205 W. Saint Clair Ave, 4th Floor Cleveland, OH 44113 Phone: 216-664-7008 fcash@city.cleveland.oh.us</p>	<p>NetApp deployed Production and Disaster Recovery infrastructure for Cleveland’s ERP System, similar to WV Oasis.</p>
<p>Rich Lemmon Infrastructure Manager Monongalia General Hospital 1200 J. D. Anderson Drive Morgantown, WV 26505 304 598-1655 lemmonr@monhelthsys.org</p>	<p>SIS provided Production Compute and Storage for infrastructure onsite and live DR site at the SIS Managed Solution Center (SIS Cloud).</p>
<p>Christopher Delaney Vice President, Information Technology Wyndham Destinations 9998 North Michigan Road Carmel, IN 46032 1-317-805-9090 Christopher.delaney@wyn.com</p>	<p>SIS has assisted with:</p> <ul style="list-style-type: none"> • The design, provision and implementation of enterprise storage and compute architectures • Software Asset Management services for multiple software publishers • Virtualization, migration and management of server environments • Private cloud hosting • Engagements around public cloud migration, Cloud Native and automation best practices.
<p>Joe Pregnotato IT Manager Wakefern Food Corp 230 Raritan Center Parkway Edison, NJ 08837 732-512-6625 joe.pregnotato@wakefern.com</p>	<p>Converge, via its subsidiary, Essex Technology Group, has supported Wakefern in the following projects:</p> <ul style="list-style-type: none"> • The design, implementation, and support of their internal and external corporate communications Portal (for employees, members, and retailers). • The migration of email, instant messaging and collaboration tools from on-premise to a cloud hosted service. • Supported numerous other application development, system engineering, enterprise architecture efforts.

4.3.1.6 Vendor's should hire staff that have the appropriate background, education, and experience to address all tiers and services of the contract.



→ **Response:** Please refer to SIS’s response to Section 4.2.1.4.4. for information concerning SIS’s hiring policies. Staff employed by OEMs are subject to the hiring standards and policies implemented by such OEMs.

4.3.1.7 The State desires an Account Team (including Account Support Representative, Technical Support Representative, Solution Implementation Support Representative, Contract Manager, Billing Support Representative, Security/Compliance Specialist, and Project Manager) for the winning solution and life of the contract. Vendor should describe in detail the responsibilities of key roles and staff’s experience in working in these roles.

→ **Response:** The Account Team that SIS assigns for the management of this engagement will involve the collaboration of multiple, experienced SIS team members. Fulfillment of the roles and responsibilities that WVOT requests in this Section 4.3.1.7. would be addressed as described below. SIS has identified members that would possibly be assigned to the project team; however, other team members with similar skills and knowledge could be assigned in place of members listed below.

Service Delivery Manager – The SIS Service Delivery Manager would be responsible for overseeing delivery of managed services, contract change management, and customer satisfaction for the life of the contract. This individual would be WVOT’s primary point of contact with respect to the post-implementation solution operations and would therefore be considered the *Account Support Representative*. Adjacent to their role as the Account Support Representative, the SIS Service Delivery manager would also be considered the primary *Technical Support Representative* who would be available to facilitate resolution of WVOT’s support needs with the respective OEM’s as needed, and also the primary *Billing Support Representative* who will be responsible for fielding questions and reporting billing information related to the On-Demand Professional Services. Given the complexity of this solution, SIS would expect to assign a Service Delivery Manager with multiple years of related experience to WVOT. Steve Staten has over sixteen years of experience as a Sales and Service Delivery Manager. His primary focus is on the larger, Tier 3 clients that require an elevated level of service and attention to billing and customer advocacy.

Lead Architect – The Lead Architect would fulfill the role of a *Solution Implementation Support Representative* who will provide the necessary technical coordination for the deployment and initial setup of the On-Premise Infrastructure, Enterprise Data Backup, and Infrastructure Operations Monitoring components of the solution, as well as contributing to the construction of the solution transition plan requested under 4.2.2.3. Michael Vannette, the SIS Technical Design Authority Director, has over 18 years of experience as a Solution Architect. His experience covers Storage, Compute, Virtualization, Data Protection, and Private Cloud. He has planned and participated in many onsite and remote engagements spanning various technologies and is intimately familiar with the requirements of a service-based infrastructure.

Contract Manager – The SIS Contract Manager would be responsible for participating in any necessary legal negotiation of the final contract with the State, owning the Statement of Work creation process for the On-Demand Professional Services, executing requisite documents on behalf of SIS, and approving the official contract exit plan required under Section 4.2.2.3. Karen Smallwood, the SIS Contracts and Compliance Director, has over six years of experience as a Contract Manager and thirteen years of



experience as an IT Augmented Staff Buyer. Due to her dual perspectives (as a client and a supplier), Karen has the ability to both empathize with clients' concerns and mitigate risk by addressing concerns up front.

Security/Compliance Specialist – The Security/Compliance Specialist would be available to receive and respond to questions from WVOT regarding cybersecurity and, if necessary, coordinate conversations with the respective OEM's regarding the security controls of OEM-provided components of the solution. Andy Nuxoll, the SIS Director of Information Security, holds CISSP, CCSP, CISM, and CGEIT certifications and would be WVOT's primary contact with respect to compliance.

Project Manager – The SIS Project Manager would be responsible for constructing the implementation plan requested under Section 4.2.2.1. and would be responsible for coordinating scheduling, overseeing resources, and applying best practice PM skills to facilitate the deployment and initial setup of the On-Premise Infrastructure, Enterprise Data Backup, and Infrastructure Operations Monitoring components of the solution. As required, the SIS Project Manager could also be involved in certain Statements of Work requested for On-Demand Professional Services where such Statements of Work require the involvement and experience of a Project Manager for successful delivery. The SIS Project Manager shall be responsible for facilitating a smooth hand-off to the SIS Service Delivery Manager for post-deployment operations and will collaborate as needed with the Service Delivery Manager to construct the on-going operations guide required under Section 4.2.2.2. Jason Coffey is a Project Management Professional with over 12 years of experience delivering technology solutions for customers in a wide variety of industries.

4.3.2 Mandatory Qualification/Experience Requirements -The following mandatory qualification/experience requirements must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it meets the mandatory requirements and include any areas where it exceeds the mandatory requirements. Failure to comply with mandatory requirements will lead to disqualification, but areas where the mandatory requirements are exceeded will be included in technical scores where appropriate. The mandatory qualifications/experience requirements are listed below.

4.3.2.1 Vendor must have provided on-premise infrastructure hardware and/or services within an organization of similar size and complexity or larger.

→**Response:** Please refer to SIS's response to Section 4.3.1.5. for examples of infrastructure solutions that SIS has provided which are comparable in size to this solicitation.

4.3.2.2 Vendor must provide at least two (2) on-premise infrastructure hardware and/or service contract summaries for in-progress or completed contracts within the past five (5) years that are similar in size and scope to this solicitation.

→**Response:** Please refer to SIS's response to Section 4.3.1.5. for contract summaries comparable in size to this solicitation.



- 4.4 Oral Presentations:** The Agency has the option of requiring oral presentations of all Vendor's participating in the RFP process. If this option is exercised, it would be listed in the Schedule of Events (Section 1.3) of this RFP. During oral presentations, Vendor's may not alter or add to their submitted proposal, but only clarify information. A description of the materials and information to be presented is provided below:

Materials and Information Requested at Oral Presentation:

- 4.4.1** A Summary of the Vendor's solution, including product and support offerings, ability to deliver the solution in the specified timeframes, and experience in providing managed and hosted Infrastructures.
- 4.4.2** The vendor will discuss each phase or major milestone listed in sections 4.2.1 and 4.2.2 of this document.
- 4.4.3** The State will ask clarifying questions regarding the Vendor's submitted technical response.
- 4.4.4** Oral Presentations will be conducted at the Agency's facility provided by the Agency. Vendor's should plan to provide their own media and demonstration hardware and, if preparing handouts, should prepare a number equal to the number of convenience copies of their proposals supplied on the Bid Opening Date, unless specifically advised by the Agency otherwise.

→**Response:** Upon request, SIS and the supporting OEMs will be able to present the solution in an oral presentation. A minimum of at least two (2) weeks is requested to accommodate schedules of required personnel to deliver the presentation.

Section V: Attachments

Attachment #1

Magic Quadrant

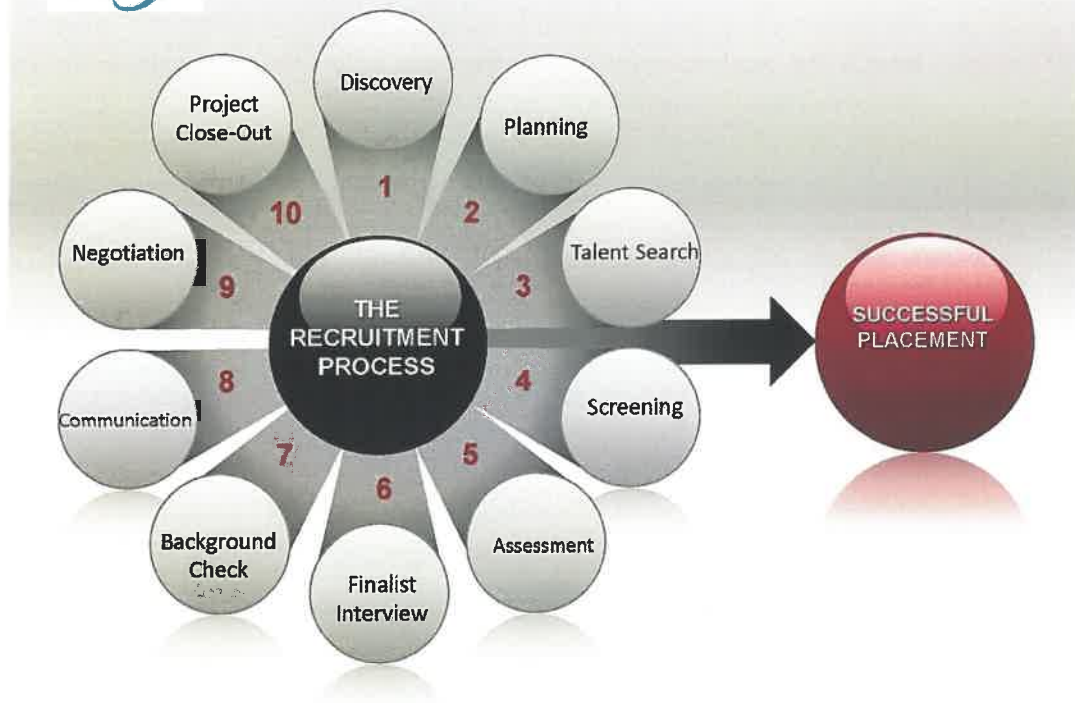
Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (February 2020)



Attachment #2

SIS RECRUITMENT PROCESS



Step 1: Initial Consultation/ Discovery – During the initial phase of the On-Demand Professional service request, SIS shall work with State of West Virginia to determine the following:

- Initial consultation for SIS to fully understand the strategic goals, culture, concerns, and upcoming changes of State of West Virginia
- Confirm or expand the position description outlining the responsibilities, expectations, and desirable qualifications for the position
- Identify the Search Committee (comprised of both SIS and State of West Virginia resources)
- Develop a Successful Candidate Profile
- Develop initial interview questions for all phases of the Recruitment process (telephone/remote or on-site)

Step 2: Planning (in collaboration with State of West Virginia)

- Develop the timeline – SIS will begin with a target date for onboarding of the resource and working backwards to determine expectations for events (e.g. candidate presentation, phone interviews, on-site interviews, etc.)
- Each task or event shall be documented and have a projected start and finish date
- Develop the Search and Advertising Strategies
- Create an “attraction” folder to present to potential candidates to provide information about State of West Virginia, the position, and general information about the assignment/job location



- Document the timeline, search and advertising strategies, and other pertinent information into a project plan

Step 3: Talent Search

- An exhaustive search is conducted to identify a pool of candidates. SIS utilizes a variety of sources (e.g., advertisement, industry contacts, social media, professional associations, our own database, and other recruitment tools/database)
 - The SIS Contract Manager, in conjunction with the SIS Recruiters shall maintain spreadsheets of all candidates and can forward to State of West Virginia upon request or both parties can determine preset submission of reports in timeline
 - SIS shall submit detailed summaries of candidates it recommends to be interviewed
 - SIS shall comply with State of West Virginia’s Equal Opportunity policy during the recruitment process

Step 4: Screening

- SIS shall set up preliminary screening of those candidates who are desirable based upon their qualifications, compatibility, and other relevant traits
- SIS shall be responsible for coordinating interviews with the candidates
- SIS shall be responsible for sending communications and feedback to candidates regarding search process

Step 5: Assessment and Initial Background Check

- From the candidates in the initial screening process (Step 4), SIS shall assist State of West Virginia in developing a “short list” of semifinalist candidates
- SIS shall research the background of any candidates on the “short list” utilizing such resources as, Facebook, LinkedIn, Google, LexisNexis, and public court records
- For each recommended semi-finalist, SIS shall certify educational credentials and obtain two or more initial professional references
- During this phase, the “attraction” folder may be given to the semi-finalist for recruitment purposes
- SIS shall prepare a written report on each semi-finalist reflecting employment and salary history, education, technical knowledge, communication skills, and potential issues with organizational fit

Step 6: On-Site Finalist Interview

- SIS shall coordinate on-site interviews for the finalist
- The Search Committee shall conduct a panel interview of the finalist
- Behavior-based interview questions and procedures are developed to ensure thoroughness and legal requirement adherence

Step 7: Formal Background Check

- SIS shall verify of previous employment to ensure that is no complaints on record against the candidate



- SIS shall conduct formal in depth personal and professional reference checks of finalist candidate

Step 8: Communications to Finalist and State of West Virginia

- SIS shall be responsible to notify the final candidate in writing that any hiring decision shall be contingent on State of West Virginia required national background check and a pre-employment screen
- The results of the background checks shall be reported to State of West Virginia
- SIS shall maintain contact with State of West Virginia to report progress and to assure work is satisfactory throughout the project

Step 9: Negotiations

- SIS may assist in the negotiations with any finalist candidate as requested by State of West Virginia
 - State of West Virginia reserves the exclusive right to announce the hiring of the new employee
 - SIS shall keep all information regarding the resource recruitment confidential
 - All offers to finalist candidate shall be made by State of West Virginia

Step 10: Close-Out and Follow-Up

- SIS is committed to a smooth transition for State of West Virginia and the new resource – guidance is provided to enable an efficient learning curve and social transition
- SIS will reach out to State of West Virginia to gain feedback regarding performance of the new resource (performance evaluations shall take place on the 30th, 60th, and 90th day of resource's tenure with your organization)
- SIS shall retain records of its search activities and shall share those as requested
- SIS shall retain the associated records for three (3) years after final payment by State of West Virginia



165 Barr Street, Lexington, KY 40507 | www.thinksis.com | (859) 977-4747
Document#: 5275Tv1

Attachment #3

Please see the sample implementation plan on the following page.

Task #	Task Name	Resource Names	Predecessors	Estimated Duration	% Complete
36	Pre-Implementation				
37	Inventory equipment	Michael Vanette			
38	Verify cables for connectivity	Jarelle Marshall, George Shearer			
39	Validate Rack space (is all equipment going in the same rack?)				
40	Confirm power wips are in place	Charles Swiger			
41	Determine if there are access prerequisites for SIS personnel	Lisa Hicks			
42	Implementation				
43	Production Site Implementation				
44	Network Deployment Services	Keith Jones			
45	Assist Agency w/ connecting & configuring to the environment and	Keith Jones		1 day	
46	Hardware Installation	BJ Schwein			
47	Inventory shipment to verify that all components have been delivered	BJ Schwein			
48	Rack, stack, cable & conduct base configuration for the following:	BJ Schwein			
49		BJ Schwein			
50		BJ Schwein			
51		BJ Schwein		1 day	
52	Power on all equipment to validate that hardware is operational	BJ Schwein			
53	Hardware Installation	BJ Schwein			
54	Configuration	BJ Schwein			
55	Assist Agency with upgrading firmware to latest recommended version at the time of install	BJ Schwein			
56	Assist Agency with configuring to	BJ Schwein			
57	Assist Agency and with connecting and configuring access to	NetApp, BJ Schwein		2 days	
58	Assist Agency with configuring and templates to support up to	BJ Schwein			
59	Assist Agency with configuring and templates to support up to	BJ Schwein			
60	Assist Agency with testing and validating	BJ Schwein			
61	services				
62	Assist Agency with installing on up to	BJ Schwein			
63	Assist Agency with adding into existing	BJ Schwein			
64	Assist Agency with configuring and	BJ Schwein		2 days	
65	Assist Agency with deploying and testing up to	BJ Schwein			
66	Assist Agency with testing and validating	BJ Schwein			
67	Assist Agency with migrating up to	BJ Schwein			
68	Assist Agency with and replication deployment for	Jarelle Marshall, BJ Schwein		2 days	
69	Services	Keith Jones			
70	Rack, stack, and cable	Keith Jones			
71	Power on the to validate that hardware is operational	Keith Jones		2 days	
72	Configure in an HA cluster	Keith Jones			
73		Keith Jones			
74		Keith Jones			
75		Keith Jones			
76		Keith Jones			
77		Keith Jones			
78		Keith Jones			
79		Keith Jones			
80		Keith Jones			
81	DR Site implementation				
82	Network Deployment Services	Keith Jones			
83	Assist Agency with connecting and configuring to the and	Keith Jones		1 day	
84	Hardware Installation	BJ Schwein			
85	Inventory shipment to verify that all components have been delivered	BJ Schwein			

86	Rack, stack, cable and conduct base configuration for the following:	BJ Schwein		1 day	
87		BJ Schwein			
88		BJ Schwein			
89		BJ Schwein			
90	Power on all [redacted] to validate that hardware is operational	BJ Schwein		2 days	
91	Configuration	BJ Schwein			
92	Assist Agency with upgrading [redacted] to latest recommended version at the time of install	BJ Schwein			
93	Assist Agency with configuring [redacted] to [redacted]	BJ Schwein			
94	Assist Agency and [redacted] with connecting and configuring access to [redacted]	NetApp, BJ Schwein			
95	Assist Agency with configuring [redacted] and templates to support up to [redacted]	BJ Schwein			
96	Assist Agency with configuring [redacted] and templates to support up to [redacted]	BJ Schwein			
97	Assist Agency with testing and validating [redacted]	BJ Schwein			
98	Services			2 days	
99	Assist Agency with installing [redacted] on up to [redacted]	BJ Schwein			
100	Assist Agency with adding [redacted] into existing [redacted]	BJ Schwein			
101	Assist Agency with configuring [redacted]	BJ Schwein			
102	Assist Agency with deploying and testing up to [redacted]	BJ Schwein			
103	Assist Agency with testing and validating [redacted]	BJ Schwein			
104	Assist Agency with [redacted] and replication deployment for [redacted]	Jarelle Marshall, BJ Schwein		1 day	
105	Services	Keith Jones		2 days	
106	Rack, stack, and cable [redacted]	Keith Jones			
107	Power on the [redacted] to validate that hardware is operational	Keith Jones			
108	Configure a single [redacted]	Keith Jones			
109	[redacted]	Keith Jones			
110	[redacted]	Keith Jones		2 days (remote)	
111	[redacted]	Keith Jones			
112	[redacted]	Keith Jones			
113	[redacted]	Keith Jones			
114	[redacted]	Keith Jones			
115	[redacted]	Keith Jones			
116	[redacted]	Keith Jones			
117	[redacted]	Keith Jones			
118	[redacted]	Keith Jones			
119	Documentation				
120	Warranty documentation from the original equipment manufacturer (OEM)				
121	OEM operating manuals, information/instructions for the solution components				
122	Contact information, online web portal site for OEM maintenance support and customer service needs				
123	As-built documentation and Visio's for [redacted] deployment	BJ Schwein		1 day	
124	Network diagram of [redacted] connectivity				
125	Copies of OEM software license documentation, as required				
126	Knowledge Transfer and/or Training				
127	Knowledge transfer of [redacted]	SIS			
128	Training Credits	Charlie Arnett			
129	[redacted]	[redacted]			
130	[redacted]	[redacted]			
131	[redacted]	[redacted]			

Attachment #4

Sample Exit Plan

Introduction

1. This Exit Plan (the “Plan”) is intended to outline the roles and responsibilities of the Client and Provider concerning termination or expiration of the Contract.
2. The parties shall periodically review the Plan over the life of the Contract and make revisions as appropriate to accommodate changing needs.
3. The activities under this Plan shall commence promptly following Provider’s receipt of Client’s written termination notice with ninety (90) days’ advance notice, or not less than ninety (90) days from the expiration of the Contract where Client has notified Provider in advance of Client’s decision not to renew.
4. The Client and Provider shall each designate a single technical point of contact to respond to questions and receive information during the exit process.
5. Until the tasks described within this Plan are completed, Client shall continue to supply Provider with access to all necessary environments, personnel, and information required to perform Provider’s exit activities.

Exit Strategy

Action Item	Details of Tasks to be Undertaken	Timeframe	Responsible Party (Provider/Client/Mutual)
Issue notice of non-renewal or intent to terminate	Must be issued in writing by authorized Client representative.	At least ninety (90) days prior to intended termination or at least ninety (90) days before expiration of the Contract	Client
Conduct initial exit strategy call	Review Client’s context and reasons for termination; refine exit plan to account for new risks, if required.	Within five (5) days after Provider’s receipt of termination/non-renewal notice	Mutual
Review Asset List	Review and discuss list of equipment on lease including any coming upon end of life	Within fourteen (14) days after Provider’s receipt of termination/non-renewal notice	Mutual
Identify leased equipment to be returned/bought out	Send Provider detailed email documenting Client’s intention to (1) buy out all leased equipment, (2) buy out certain leased equipment items, or (2) return all leased equipment.	Within thirty (30) days after Provider’s receipt of termination/non-renewal notice	Client
Validation of Client backups	Verify that Client has migrated their data off of leased equipment that is being returned or made sufficient backup copies of such data.	Within forty-five (45) days after Provider’s receipt of termination/non-renewal notice	Client (with Provider’s assistance, if required)



Coordinate buy-out	Contact lessor concerning any equipment for buy-out.	Within forty-five (45) days after Provider's receipt of termination/non-renewal notice	Client
Transfer of configuration documentation to Client	Conduct call with Client technical point of contact and his/her selected technical staff to discuss configuration documentation and answer questions.	No later than seven (7) days prior to the official termination or expiration date	Provider
Transfer of support ticket records	Run an export of all support tickets entered by Client; deliver to Client technical point of contact via email.	No later than seven (7) days prior to the official termination or expiration date	Provider
Return or destruction of all Client data, materials, and Confidential Information	Conduct DoD wipe of all hard drives on leased equipment to be returned, after Client has validated backups; shred confidential papers; ship tangible Client-owned materials to address designated by Client; conduct best effort purge of Confidential Information from Provider email systems.	Within thirty (30) days after Client's validation of backups	Provider
Return leased equipment that is not purchased	Package and ship to lessor's designated address.	Within ten (10) days after completion of hard drive data wipe	Provider
Return or destruction of all Provider materials and Confidential Information	Shred confidential papers; ship tangible Provider-owned materials to address designated by Provider; conduct best effort purge of Confidential Information from Client email systems.	No later than thirty (30) days after the official contract termination or expiration date	Client
Final review and validation	Conduct call with Client and Provider technical points of contact to discuss any remaining action items and path to completion.	No later than seven (7) days prior to the official termination or expiration date	Mutual
Issue final invoice for services	Invoice shall align with the rates and fees specified in the Contract.	Within seven (7) days following the termination date/contract expiration date	Provider
Final payment for services	Payment may be made by ACH or by check.	Within the payment term specified in the Contract	Client



Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

State of West Virginia
 Request for Proposal
 21 – Info Technology

Proc Folder: 655755

Doc Description: Addendum 10-Data Center 2.0 RFP (OT20023)

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2020-03-20	2020-04-10 13:30:00	CRFP 0231 OOT2000000001	11

BID RECEIVING LOCATION

BID CLERK
 DEPARTMENT OF ADMINISTRATION
 PURCHASING DIVISION
 2019 WASHINGTON ST E
 CHARLESTON WV 25305
 US

VENDOR

Vendor Name, Address and Telephone Number:

Software Information Systems, LLC
 165 Barr Street
 Lexington, KY 40507
 859.977.4796

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers
 (304) 558-0246
 jessica.s.chambers@wv.gov

Signature X *Karen Smallwood*

FEIN # 61- 1371685

DATE 04/06/2020

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION:

Addendum No.10

The purpose of this Addendum is to extend the Bid Opening Date to 4/10/2020, bid opening time remains at 1:30 PM (EDT) per the request of the donor community.

*** Please note electronic responses to this solicitation via wvOasis have been prohibited. You must submit your proposal via hard copy prior to the bid opening date and time.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US		WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Data Center 2.0	1.00000	LS	<i>see Cost Proposal</i>	

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description :

Data Center 2.0 pricing per Exhibit A pricing page total.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Mandatory PreBid Conference at 1:00 PM (EST)	19-12-06
2	Technical Question Deadline at 12:00 PM (EST)	19-12-13
3	2nd Technical Question Deadline at 9:00 AM (EST)	02-04
4	Please see revised specifications and Pricing Page	02-26

REQUEST FOR PROPOSAL

WV Office of Technology

On-Premise Infrastructure

Example:

Proposal 1 Cost is \$1,000,000
Proposal 2 Cost is \$1,100,000
Points Allocated to Cost Proposal is 30

Proposal 1: Step 1 – $\$1,000,000 / \$1,000,000 = \text{Cost Score Percentage of 1 (100\%)}$
Step 2 – $1 \times 30 = \text{Total Cost Score of 30}$

Proposal 2: Step 1 – $\$1,000,000 / \$1,100,000 = \text{Cost Score Percentage of 0.909091 (90.9091\%)}$
Step 2 – $0.909091 \times 30 = \text{Total Cost Score of 27.27273}$

- 6.8. Availability of Information:** Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-11(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Software Information Systems
(Company)

Charles D. Arnett, Sr. Chief Executive
(Representative Name, Title)

304 549-7698 Cell 304 768-1645 office 304 768-1671 Fax
(Contact Phone/Fax Number)

4-18-2020
(Date)

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

CONSTRUCTION CONTRACTS: Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

ALL CONTRACTS: Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceeds five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (W. Va. Code §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: Software Information Systems, LLC

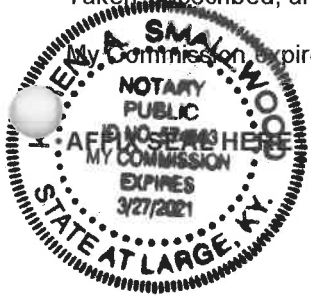
Authorized Signature: *[Signature]* Date: April 6, 2020th

State of Kentucky

County of Fayette, to-wit:

Taken, subscribed, and sworn to before me this 6th day of April, 2020.

My Commission Expires March 27, 2021.



NOTARY PUBLIC *[Signature]*

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: _____

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

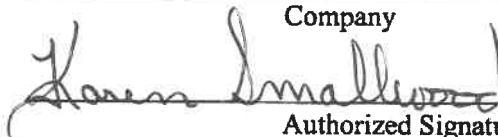
(Check the box next to each addendum received)

- | | |
|--|---|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input checked="" type="checkbox"/> Addendum No. 6 |
| <input checked="" type="checkbox"/> Addendum No. 2 | <input checked="" type="checkbox"/> Addendum No. 7 |
| <input checked="" type="checkbox"/> Addendum No. 3 | <input checked="" type="checkbox"/> Addendum No. 8 |
| <input checked="" type="checkbox"/> Addendum No. 4 | <input checked="" type="checkbox"/> Addendum No. 9 |
| <input checked="" type="checkbox"/> Addendum No. 5 | <input checked="" type="checkbox"/> Addendum No. 10 |

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Software Information Systems, LLC

Company



Authorized Signature

April 6, 2020

Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.
Revised 6/8/2012

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Name, Title)
Karen Smallwood - Director, Contracts & Compliance

(Printed Name and Title)
165 Barr Street, Lexington, KY 40507

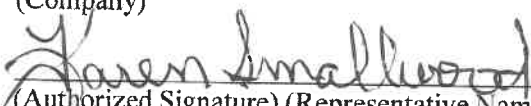
(Address)
859.977.4796

(Phone Number) / (Fax Number)
ksmallwood@thinksis.com

(email address)

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that I have reviewed this Solicitation in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

Software Information Systems, LLC

(Company)


(Authorized Signature) (Representative Name, Title)

Karen Smallwood - Director, Contracts & Compliance

(Printed Name and Title of Authorized Representative)

4/6/2020

(Date)

859.977.4796

(Phone Number) (Fax Number)

REQUEST FOR PROPOSAL

WV Office of Technology
On-Premise Infrastructure

Example:

Proposal 1 Cost is \$1,000,000
Proposal 2 Cost is \$1,100,000
Points Allocated to Cost Proposal is 30

Proposal 1: Step 1 – $\$1,000,000 / \$1,000,000 = \text{Cost Score Percentage of } 1 (100\%)$
Step 2 – $1 \times 30 = \text{Total Cost Score of } 30$

Proposal 2: Step 1 – $\$1,000,000 / \$1,100,000 = \text{Cost Score Percentage of } 0.909091 (90.9091\%)$
Step 2 – $0.909091 \times 30 = \text{Total Cost Score of } 27.27273$

6.8. Availability of Information: Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-11(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Software Information Systems, LLC
(Company)

Karen Smallwood - Director, Contracts & Compliance
(Representative Name, Title)

859.977.4796
(Contact Phone/Fax Number)

4/6/2020
(Date)

Why NetApp?

NetApp is the current market and technology leader in unified storage, and one of the fastest growing SAN vendors

NetApp is also the largest provider of storage to the US Federal Government with 50% market share in civilian agencies and 70% market share within secure federal agencies. This should provide piece of mind to the State of West Virginia that the solution proposed will meet and exceed any requirements the State may have.

Gartner has ranked NetApp as a leader for mid-range disk and NAS in its *Magic Quadrant*. Gartner also recognizes NetApp's merit in other storage-related markets, including storage resource management, data protection services, storage implementation services, and backup and recovery.

NetApp customers have recognized us as the industry leader in providing flexible, efficient, and future-ready storage architecture.

ONTAP is the Number One Storage Operating System

International Data Corporation (IDC) 2017 Q4 Storage Hardware and Software Market Share shows that NetApp ONTAP® is the number one storage operating system.¹

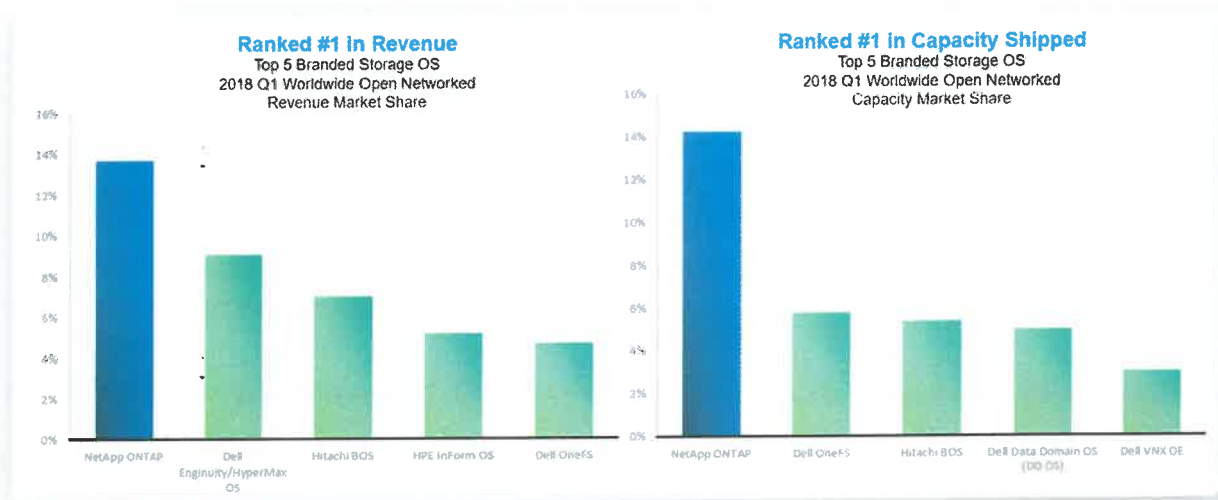


Figure 1: NetApp ONTAP is the #1 Open Networked Branded Storage OS – The latest IDC Enterprise Storage Systems Tracker confirms that NetApp ONTAP was ranked #1 based on sales of Open Networked Enterprise Storage Systems (for both revenue and terabytes).

The following table highlights the features and functions that set NetApp ONTAP solution apart from other storage platforms.

¹ Source: IDC, Worldwide Quarterly Enterprise Storage Systems Tracker - Q1 2018, June 5, 2018.

Table 1: NetApp ONTAP features and functions.

NetApp ONTAP	
Universal Data Platform	<ul style="list-style-type: none"> • All protocols: CIFS, FCoE, FCP, iSCSI, NFS • All disk types: SSD, SAS, NL-SAS, SATA • All workload types: Small or large block, random or sequential • Maximum simplicity: One system to learn and support, for all your needs
Flexible Scalability	<ul style="list-style-type: none"> • Expandable performance: Scale up and out, controllers and disk • Expandable capacity: Scale up and out • Operational efficiency: Grow without adding points of management
Integrated Data Protection	<ul style="list-style-type: none"> • Native zero-impact, space-efficient snapshots • Deep application integration (application-consistent snapshots, and so on) • Native disaster recovery replication: SnapMirror® • Native optional disk-to-disk backup: SnapVault®
Open and Extensible Platform	<ul style="list-style-type: none"> • Robust APIs that support third-party and custom integration • Several supported tools and environments • Designed to scale from small to massive environments
Zero-downtime Lifecycle Maintenance	<ul style="list-style-type: none"> • Replace all components without downtime or costly migrations • Add performance, connectivity, and capacity without disruption
Secure Multi-tenancy	<ul style="list-style-type: none"> • Shared storage to maximize efficiency, while maintaining secure separation • Secure, scalable, and fully-functional multi-tenant solution • Robust QoS and role-based access control to achieve service level success
Business-empowering Efficiency	<ul style="list-style-type: none"> • Highly-granular 4KB block-level deduplication of NAS and SAN primary data • Cache amplification with deduplication-aware SSD Flash Pools • Zero-cost near-instantaneous clones revolutionize dev/test and VM build-out
Complete Data Portability	<ul style="list-style-type: none"> • The ability to move data anytime, without disruption to any type of disk • The flexibility to move data in and out of private, hybrid, and public clouds • Highly efficient, deduplication-enabled replication

Leading Provider of Storage Efficiency Capabilities

NetApp is a leading provider of storage efficiency capabilities such as thin provisioning and deduplication. Our unique approach delivers a universal platform, which provides a challenge to the legacy unified storage offered by competitors. The flexibility and efficiency of NetApp architecture directly translates into better operation and significantly improves total cost of ownership.

NetApp is differentiated by our ability to:

- Enable automation that matches pre-defined service levels
- Unify heterogeneous environments under a single, highly capable, management umbrella
- Deliver application-consistent point-in-time copies, as well as integrate storage operations into the application environments
- Provide functional, capable data protection and disaster recovery with our disk arrays—not just deliver what amounts to checkmark boxes for such functionality
- Deliver capabilities such as secure multi-tenancy and a comprehensive SRM environment that easily plugs into existing system frameworks

NetApp recognized as a Leader in 2019 Gartner Magic Quadrant for Primary Storage

This Magic Quadrant was published as part of a larger research note and should be evaluated in the context of the entire report. The full report is available from NetApp.

<https://www.netapp.com/us/campaigns/gmq-primary-storage-report/index.aspx>

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from NetApp. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Figure 1. Magic Quadrant for Primary Storage



IDC Also shows NetApp AFF/FAS was #1 in scale-out NAS
IDC WW Quarterly Enterprise Storage Systems Tracker, 2019 Q1, June 6, 2019 – Vendor Revenue

IDC PERSPECTIVE

A New NetApp Is on the Rise

Eric Burgener

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: NetApp – Delivering Value for Enterprises Undergoing Digital Transformation

Enterprise storage customers that have not dealt with NetApp in the past few years may not even recognize the vendor. In the past year in particular, the vendor has undergone a significant and broad-reaching evolution that positions it to cater to the needs of enterprises undergoing digital transformation in ways that differentiate it from its competitors in meaningful ways. This document summarizes those changes, presenting a "new" NetApp whose offerings mesh well with industry trends and customer needs.

Key Takeaways

- NetApp has undertaken significant positive change in five key areas: hybrid cloud integration, storage consumption models, customer experience (CX), the pursuit of a primarily software-defined infrastructure strategy, and the planting of its stake in the ground as a leader in SAN (block-based workloads) in addition to retaining its crown as the leader in enterprise NAS.
- NetApp is leveraging leading-edge technologies for enterprise use in a variety of areas, including NVMe, persistent memory, and artificial intelligence/machine learning (AI/ML).
- With its public cloud-based offerings, NetApp can now provide true enterprise storage capabilities to a variety of new customer types starting at well under \$100/month (for 50GB).

Recommended Actions

- IT organizations undertaking technology refreshes that are moving toward a hybrid multicloud strategy should at least familiarize themselves with what NetApp offers in this area as its portfolio represents the leading edge at the intersection of enterprise storage and hybrid cloud.
- New constituencies like cloud architects and DevOps managers should take note of Azure NetApp Files, a cloud-based enterprise file offering that is quick to provision, low risk, and low cost and is available directly from first-party public cloud providers like Microsoft.
- Regardless of whether customers look at NetApp or not, they should be evaluating enterprise storage vendors capabilities in the same areas that have been instrumental to NetApp's evolution (hybrid cloud, consumption models, CX, NVMe technology, use of AI/ML to drive business value, etc.).

Source: IDC, 2019

SITUATION OVERVIEW

In the past 10 years, the enterprise storage industry has undergone significant evolution. Those large established vendors that lead in one era do not necessarily evolve effectively when major new technologies drive major change. One of the hallmarks of a truly great company (and a great long-time partner to its customers) is its ability to adapt to these types of changes while maintaining industry leadership. NetApp, a \$6+ billion vendor of information technology (IT) infrastructure, rose to prominence in the 1990s with its high-performance, highly available, and easy-to-deploy filers but has evolved as the storage industry has evolved over the past two decades to establish and maintain leadership in other technology areas as well like unified storage and all-flash arrays (AFAs). The vendor is currently undergoing another major evolution, and there was significant discussion of steps the vendor has taken to evolve their business at the recent NetApp Insight event (NetApp's annual end-user conference, which was held in late October 2019).

The major changes in the enterprise storage industry in the past few years have revolved around several key areas:

- The IT organizations of most successful, growing businesses have started the process of digital transformation (the move to much more data-driven business models) and are deploying new artificial intelligence- and machine learning (AI/ML)-driven workloads to help inform better business decisions.
- The new data-driven business model requires significantly more agility on the part of IT organizations, a fact which has led to rapid growth in the use of cloud-based services, the deployment of more software-defined infrastructure, the domination of primary external storage revenue by solid state technologies, and significant interest in subscription-based consumption models.
- As organizations evolve their IT infrastructure to meet changing performance, availability, scalability, and agility requirements, they are looking to cloud technologies to increase agility and provide access to newer technologies needed in the burgeoning big data analytics arena such as accelerated compute, AI/ML, and massively scalable cold storage. They are also looking to cloud technologies to offload IT infrastructure management responsibilities and move more infrastructure and workloads to operational expenditure (opex) models. Overall, cloud-based spend (public and private) is moving from 42% of total information and communications technology spend in 2018 to 50% by 2023, and 52% of IT organizations already had a hybrid cloud environment in place in 2019.

In 2019, the enterprise storage market exhibited a revenue growth slowdown. Coming off of a banner year in 2018, the slower industry revenue growth in 2019 appeared even more pronounced, and many of the top enterprise storage vendors (in terms of market share by revenue) were affected by this slowdown. In response to this, NetApp has made a number of changes – so much so that many prospective customers that have not dealt with NetApp in the past 12-18 months may not even recognize the vendor. Some of these changes were in fact implemented as early as 2018, based on the vendor's understanding of the evolving enterprise storage market direction, and have in fact already started to bear fruit. The "new" NetApp is a very different company than it was just two short years ago, and the company's adjusted direction meshes well with both industry trends and evolving enterprise customer needs. Based on IDC's analysis of these changes over the past 18 months, this document calls out five key aspects of the vendor's new offerings, areas of focus, and business strategy that traditional IT customers (as well as new constituencies for enterprise storage purchases like cloud architects and DevOps managers) may find both surprising and appealing.

So You Think You Know NetApp ...

Most IT personnel who have managed storage over the past 20 years or so are familiar with NetApp as a company. Based on the most recently released quarterly revenue, the vendor holds the number 2 market share position in external enterprise storage and the number 2 market share spot in AFAs. But unless IT executives have been engaging with NetApp over the past 12-18 months, they likely have a dated view of the vendor's offerings, capabilities, and strengths. At the recent NetApp Insight event, this dichotomy was readily apparent and was made all the more important by the fact that the capabilities of the "new" NetApp are strongly keyed to where the IT infrastructure market is going. Here are some important things in this new era of digital transformation that IT executives may not be aware of about NetApp today:

- **First, NetApp was the first established storage provider to understand the importance of the evolution to hybrid cloud (back in late 2015) and it has maintained leadership in this area since then.** The company announced the NetApp Data Fabric at that time and has energetically expanded the hybrid cloud capabilities of its entire portfolio over the past four years. Since 2016, NetApp has had the most complete (in IDC's opinion) hybrid cloud offering encompassing multipublic cloud capabilities, extensive hybrid cloud integration points with its on-premises IT infrastructure, unified AI/ML-infused control planes that provide single-pane-of-glass management for hybrid cloud environments, and enterprise-class web-scale infrastructure offerings for on-premises and private cloud environments. These capabilities provide "public cloud" advantages while overcoming common public cloud challenges (performance, availability, governance, compliance, etc.). NetApp has been first to market with many hybrid cloud integration capabilities over the years and, despite the fact that many of its competitors have introduced similar offerings, continues to innovate at a rate sufficient to keep them the industry leaders in this arena.

Over the past year, the vendor continued to push the envelope on hybrid cloud capabilities with new NetApp Data Fabric announcements. With the introduction of Azure NetApp Files (ANF), NetApp is making an enterprise-class file service available on public cloud environments as a first-party offering with a low entry price point. Microsoft sells this, not NetApp, giving the product significantly more reach, particularly into smaller accounts that may not yet know NetApp. ANF is based on NetApp's venerable ONTAP storage operating environment but purchased and paid for as a Microsoft Azure-based subscription service, and its availability as a true enterprise-class first-party file-based service directly from a major public cloud provider differentiates it from other public cloud-based offerings in the market to date. Turbocharged by the introduction of ANF, NetApp is becoming one of the largest and fastest-growing provider of file services in the public cloud: its cloud data services business experienced 167% year-over-year growth (a growth rate tied with number 2 provider Microsoft, according to IDC data), and end users spent well over \$100 million with cloud providers for NetApp's data services (which includes ANF, Cloud Volumes Service, and Cloud Volumes ONTAP) in 2019.

NetApp is pursuing a multipublic cloud strategy; has introduced a number of offerings across Amazon Web Services, Microsoft Azure, and Google Cloud Platform (most recently with support for Google's Anthos open application modernization platform); and is working toward extending its common, feature-rich "public cloud experience" with unified management and true enterprise capability across both on-premises and off-premises environments (regardless of public cloud provider). To enable automation that spans on-premises and public cloud-based infrastructure, NetApp has strongly committed to the use of Kubernetes with the NetApp Kubernetes Service (NKS) and has introduced new tools (Cloud Insights, Fabric Orchestrator, FabricPool, etc.) that make it easier to manage and drive business value with hybrid multicloud

environments. NetApp also introduced NetApp HCI (software-defined, enterprise-scale hybrid cloud infrastructure) to give customers an option for traditional or private cloud deployments that delivers the advantages of the "public cloud experience" for on-premises infrastructure.

As part of NetApp's strong emphasis on hybrid cloud integration, the ONTAP operating environment gives traditional on-premises storage administrators ample opportunity to work with and leverage cloud technologies and ultimately repurpose themselves as cloud specialists. This is based on the vendor's extensive hybrid multicloud functionality, ability to access full ONTAP functionality for cloud-based storage services, and the availability of cloud-based tools that provide single-pane-of-glass administration and management for both on-premises and off-premises storage infrastructure.

- **Second, in the past year, NetApp has made major changes in its product and sales strategies to make the company agnostic as to whether its customers buy on-premises or public cloud-based infrastructure from them.** This removes the tension that still exists in many enterprise storage vendors' sales forces between on-premises and cloud-based infrastructure sales. It also gives customers more freedom to locate workloads in the optimal location (on premises or off premises) based on their requirements rather than sales account team preference for a particular consumption model type.
- **Third, NetApp has made significant investments to improve its ability to deliver a consistently superior customer experience (CX) across its entire customer base, despite the fact that many of its core customers already view NetApp as offering industry-leading CX.** CX goes beyond just the quality of technical support – it focuses on the entire storage life-cycle experience of the customer from initial short list creation through purchase, deployment, management, expansion, technical support, technology refresh and, ultimately, retirement, taking into account the ease of doing business with the vendor, the ability of the vendor to become a trusted advisor to its customers, and the willingness of customers to recommend the vendor to their peers.

In 2018, the vendor created a central group, headed by a NetApp executive, to define and coordinate a consistent approach to CX across the entire company. That group established baseline metrics for CX that applied companywide and has been evolving the vendors' products, services, and workflows to improve these metrics over time. Extensive primary research into CX-related areas performed both by NetApp and by outside contractors helped this group define areas for improvement for NetApp, and many of the announcements in 2H19 specifically leveraged these results. NetApp's coordinated efforts in the CX arena have resulted in key changes in how they do business:

- At the October NetApp Analyst Insight conference, NetApp introduced Keystone to further simplify the customer experience. It includes a broad-reaching subscription-based consumption model that makes it much easier to buy, consume, and operate IT infrastructure. Customers make three simple decisions – where do they want to operate (in the cloud or on premises), what type of data services do they want (block/file/object), and who should manage it (NetApp or the customer) – and NetApp does the rest. Keystone allows IT services to be provisioned more quickly, reduces the cost of managing storage, and increases IT stability and predictability while at the same time allowing customers to move IT infrastructure assets off the balance sheet.
- NetApp introduced a Cloud Customer Group that is specifically focused on understanding how its customers want and need to leverage cloud-based services so that the vendor can continue to innovate to maintain its hybrid multicloud leadership. Since this organization was launched in 2019, it has grown NetApp's online community sixfold (an outcome that indicates the value this drives for customers).

- NetApp has gone all-in on the use of AI/ML to drive value for customers and improve overall CX. The vendor's cloud-based predictive analytics platform (Active IQ) is one of the most mature in the industry, and the vendor has been extending the platform's coverage to include more storage systems and offerings (including public cloud services) in its portfolio. Data collected by Active IQ is used to expose risk factors and prevent problems before they affect operations, improve the efficiency of storage system resource utilization, speed trouble ticket issue resolution, and help automate routine operations. Data collected across all of NetApp's customer touch points (over 200 billion data points per day) is now being analyzed using AI/ML to make its customers' lives better in a systematic manner, driving higher performance and availability, easier administration, and lower cost.
- NetApp has put a number of guarantees in place for its enterprise storage customers that are intended to further improve the overall CX. These include guarantees on performance, 100% data availability, storage efficiency (data reduction) ratios, predictable maintenance pricing, and solid state media endurance.
- **Fourth, at this point, NetApp is more of a software rather than a hardware company.** Yes, the company does still sell hardware associated with appliances but it has been moving functionality out of hardware into software for years, more broadly enabling the use of lower-cost commodity hardware technologies while still providing its enterprise-class functionality differentiation. This is important for customers that are looking for increased deployment flexibility and agility, for easier technology refresh, and for better hybrid cloud integration capabilities. And customers should also note that NetApp is not just a storage vendor – through reference architectures and channel partners, it offers validated IT infrastructure solutions with converged (with Cisco) and hyperconverged infrastructure as well as accelerated compute (for AI/ML and other big data analytics workloads [with NVIDIA]) platforms.

With its software-centric strategy, NetApp provides a variety of software-defined datacenter options. Through a long-standing relationship with VMware, NetApp offers deep integration with virtualized infrastructure technologies from VMware (a key vendor in software-defined datacenter). NetApp's hyperconverged infrastructure offerings (NetApp HCI) support the ability to scale compute and storage resources independently, giving VMware customers the option to scale storage capacity as necessary without having to purchase additional VMware software (which is licensed based on the number of cores in a CPU rather than storage capacity). For those customers interested in open source-based software-defined datacenter options, NetApp offers fully verified and supported reference architectures that leverage Red Hat OpenShift, Google Anthos, and related technologies like Kubernetes and Docker.

The vendor's strategic orientation has also shifted from being a storage provider to being a data services provider. Messaging around new offerings from the vendor emphasizes how it provides data services for digitally transformed (or transforming) companies that are looking to better leverage data to drive their own business growth and how NetApp's Data Fabric strategy makes it easier to deploy and manage data in hybrid multicloud environments to drive business value.

- **Fifth, NetApp should not be thought of as just a NAS vendor.** NetApp originally started as a NAS vendor in the mid-1990s. By 2002, it had pioneered the concept of the "unified storage" platform – an enterprise-class storage system that could simultaneously support both block- and file-based storage. Today, NetApp has tens of thousands of systems deployed in production, with 42% of them running mission-critical block-based applications like Oracle, SQL Server, SAP, and other key strategic workloads (as of January 2020). Many of these systems only support block-based workloads (despite their unified storage capabilities).

NetApp's block-based performance, availability, and scalability are on par with that of its most capable block-based competitors.

In recent years, NetApp has noted an increasing percentage of customers that buy and use its systems as a "dedicated" platform for their most mission-critical block-based enterprise workloads. Through the end of 2019, NetApp was one of the fastest-growing "SAN vendors" (by revenue) among the established enterprise IT infrastructure vendors. Based on customer demand, in late 2019, NetApp introduced the NetApp All SAN Array (ASA), an ONTAP-based storage platform that is specifically optimized to run only block-based workloads. This all-flash system features performance and other optimizations (like symmetric active/active controllers that support virtually instantaneous failover recovery and more intuitive management of block-based environments), giving customers that want to keep block- and file-based workloads on separate dedicated platforms anyway additional options. The availability of the ASA puts NetApp on a more even footing with its block-based competitors and will ultimately give customers more block-based options as NetApp rolls the ASA into its converged infrastructure offerings.

Two Additional Aspects to the "New" NetApp

Despite all the offerings from NetApp that extend its capabilities beyond just storage, the vendor continues to innovate in that arena as well. NetApp is a leader in the emerging persistent memory and NVMe technologies that will become increasingly important to next-generation workloads in "digitally transformed" IT organizations over the next several years. NetApp began shipping NVMe-based versions of its flagship all-flash FAS (AFF) systems in mid-2018 and was one of the first established enterprise IT infrastructure vendors to support NVMe over Fabrics (NVMe-oF) host connections on these enterprise-class systems. The vendor's July 2018 acquisition of PlexiStor led to the announcement of MAX Data, a persistent memory-based software solution that, by leveraging Intel Optane DC persistent memory, provides applications with storage latencies under 10 microseconds while offering all the enterprise-class capabilities of ONTAP-based storage. That is the lowest latency available from any enterprise-class, shared storage platform in the industry today.

Finally, the vendor also spoke publicly about changes it has been making in 2H19 to increase the emphasis on new customer acquisition. This document has already mentioned cloud-based offerings like Azure NetApp Files, Cloud Volumes Service, and Cloud Volumes ONTAP that provide multiple entry points to NetApp technology for constituents (like Cloud Architects and DevOps Engineers) that have not been traditional NetApp customers. These offerings have very low price points, are quick and easy to deploy, and exhibit none of the "risk" associated with traditional enterprise storage purchases yet they showcase differentiating NetApp capabilities in the areas of performance, availability, scalability, and functionality.

In October, the vendor announced a new chief marketing officer (CMO), James Whitmore, who had come over with the SolidFire acquisition in 2016. Whitmore had been acting CMO for most of 2019 and was instrumental in NetApp's efforts to market to "new" customers (those defined as having spent less than \$50,000 with the vendor over the past four years). NetApp is attending cloud, developer, and other trade shows it had not been attending in the past to explain how its offerings make the lives of these constituencies better. Additional investments have been made in "hunter" sales resources (that have been prevalent in NetApp's competitors for years) while at the same time expanding account team composition to include resources focused on CX much earlier in the purchase process. According to data shown at the NetApp Analyst Insight conference, these efforts are demonstrably increasing the percentage of quarterly revenue NetApp generates from new customers.

ADVICE FOR THE TECHNOLOGY BUYER

IDC has noted that, on a purely functional basis, there are many enterprise storage vendors that can meet customer requirements for performance, availability, scalability, and manageability. As a result, many enterprise storage vendors are investing in other areas to generate meaningful differentiation that drives business value for customers. These areas include hybrid cloud integration strategies and capabilities, the overall quality of CX vendors deliver, and how they leverage AI/ML to drive value in the areas of performance, availability, capacity utilization, infrastructure efficiency, and cost. Initial purchase prices are important, but total cost of ownership is more important, particularly as equipment depreciation life cycles increase due to newer technologies like scale-out architectures, software-defined infrastructure, and the ability to support nondisruptive technology refresh.

Customers looking to deploy new workloads and/or refresh IT infrastructure as they digitally transform their companies should consider NetApp, particularly if hybrid cloud integration is a key strategic concern. Customers will see a company driving industry leadership in new storage technologies like NVMe, persistent memory and/or storage class memory, and hybrid cloud integration, as well as a company that is proliferating the CX that keeps its core customers committed to NetApp across a much broader set of constituencies. This is clearly no longer the NetApp that you may have known from the past, and the company is very intelligently making strategic investments in those areas of differentiation that are key to digital transformation.

LEARN MORE

Related Research

- *Worldwide All-Flash Array Market Shares, 1H19: Share Percentages Are Evolving But Share Ranking Remains Stable Among Top Vendors* (IDC #US45620819, November 2019)
- *The Evolving Market for Enterprise Storage: Hybrid Cloud, NVMe, and Software Defined Are the Next Wave* (IDC #US45598619, November 2019)

Synopsis

This IDC Perspective analyzes NetApp's transformation in the past 18 months. In the past 12-18 months, the NetApp executive team has driven significant change within the vendor to optimize its offerings and presentation to customers undergoing digital transformation. These changes were very evident at the NetApp Analyst Insight conference held in late October 2019. Many prospective customers that have not dealt with NetApp in the past 12-18 months may not even recognize the vendor, and the vendor's new direction meshes well with both industry trends and evolving enterprise customer needs. This document reviews those changes, offering an introduction to the "new" NetApp for prospective customers.

"Established enterprise storage vendors that want to stay in business as the industry transitions to enable digital transformation need to change their business models as well," said Eric Burgener, research vice president, Infrastructure Systems, Platforms and Technologies at IDC. "NetApp has been very open about discussing its own evolution as an enterprise vendor, and it is clear how it is changing the company and how it deals with customers to drive improvements in the overall customer experience."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights.

Copyright 2020 IDC. Reproduction is forbidden unless authorized. All rights reserved.



NetApp storage infrastructure technologies have been architected to deliver an average of six 9s (99.9999%). Recent IDC studies show that most NetApp customers achieve greater than six 9s availability when utilizing best practices.¹ NetApp® ONTAP® 9 software, AFF8000 and AFF A-Series systems as well as FAS2500, FAS2600, FAS8000, FAS8200, and FAS9000 systems offer such extreme levels of performance and capacity scaling that The State of West Virginia can expect to achieve six 9s availability—that's roughly six seconds of downtime on an annual basis.

IDC survey data indicates that the average cost of unplanned downtime varies from \$60,433 per hour for small enterprises (1,000–4,999 employees) to \$79,385 per hour for large enterprises (more than 10,000 employees). 63.3% of enterprises have recovery point objectives of less than an hour, and 39.2% of them have recovery time objectives of less than 30 minutes for critical application environments. Strict service-level agreements demand a highly available, highly resilient storage infrastructure.

Over the past four and a half years, NetApp's installed base of tens of thousands of enterprise storage systems has proven that it can meet "six-nines" availability requirements (based on IDC's in-depth review of uptime statistics collected by NetApp's cloud-based predictive analytics platform). Customers looking for flash-optimized, highly scalable storage solutions that can deliver the kind of uptime expected by today's internet-savvy end users should consider NetApp's portfolio of ONTAP 9-based (NetApp's mature and very feature-rich storage operating system) storage platforms.

— IDC, *Enterprise Storage: The Foundation for Application and Data Availability White Paper*, October 2018

¹ IDC, October 2018

NetApp Scored first in 4 out of 5 Gartner 2019 Critical Capabilities for Hybrid Array Storage Systems: customer use cases

NetApp FAS Hybrid-Flash Arrays

In Gartner 2019 Critical Capabilities for Hybrid Array Storage Systems:

- FAS Series received the highest scores for:
 - OLTP – 4.22 out of 5
 - Server Virtualization – 4.23 out of 5
 - Analytics – 4.25 out of 5
 - VDI – 4.30 out of 5
- FAS Series received the second highest score for:
 - HPC – 4.24 out of 5



Image Source: NetApp

Source: Gartner 2019 Critical Capabilities for Hybrid Arrays Storage Systems, 26 September 2019, Santhosh Rao, John Monroe, Roger W. Cox. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

All Flash FAS

NetApp® All Flash FAS (AFF) is an all-flash array that delivers high performance, flexibility, low latency, and superior data management without sacrificing enterprise capabilities. AFF enables a smooth transition to flash for your data center, built on NetApp ONTAP® data management software.

As businesses go through digital transformation, they must modernize their IT infrastructure to improve speed and responsiveness to support critical business operations. Although all-flash storage systems have been widely adopted to accelerate typical enterprise applications, newer workloads such as data analytics, artificial intelligence (AI), and deep learning—demand higher performance that first-generation flash systems cannot deliver.

In addition, as more organizations adopt a “cloud first” strategy, it is critical to offer enterprise-grade data management capabilities for a shared environment across on-premise data centers and the cloud. Many all-flash array solutions available today lack robust data management, integrated data protection, seamless scalability, new levels of performance, deep application, and cloud integration.

Cloud-Connected All-Flash Storage Powered by ONTAP

NetApp® All Flash FAS (AFF) is a robust scale-out platform built for virtualized environments, combining low-latency performance with comprehensive data management, built-in efficiencies, integrated data protection, multiprotocol support, and nondisruptive operations.

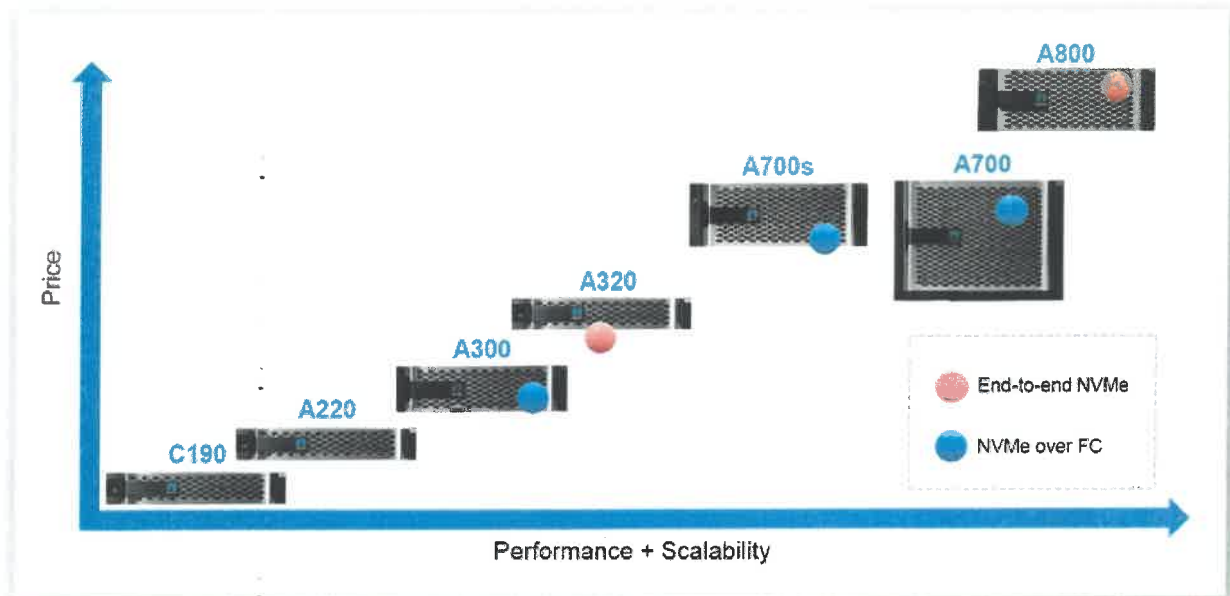


Figure 1: AFF portfolio – Modernize with cloud connected flash; provides solutions to modernize IT for small to large enterprises.

“We’re able to fit a whole lot more in a smaller amount of space and still provide more performance than we had before.”

— CI Engineer, financial services firm

NetApp AFF A-Series systems are designed to help businesses accelerate infrastructure transformation and fuel data-driven strategies. Powered by NetApp ONTAP® data management software, AFF systems accelerate, manage, and protect business-critical data and give you an easy and smooth transition to flash for your digital transformation in the hybrid cloud. With AFF systems, you can:

- Increase operational efficiency
- Accelerate applications and future-proof your infrastructure
- Keep business-critical data available, protected, and secure.

Increase Operational Efficiency

AFF offers the broadest application ecosystem integration for enterprise application, such as virtual desktop infrastructure (VDI), database, and server virtualization—supporting Oracle, Microsoft SQL Server, VMware, SAP, MySQL, and more. Infrastructure management tools simplify and automate common storage tasks so that you can:

- Provision and rebalance workloads by monitoring clusters and nodes
- Use one-click automation and self-service for provisioning and data protection
- Import LUNs from third-party storage arrays directly into an AFF system to seamlessly migrate data

In addition, with the NetApp Active IQ® intelligence engine you can optimize your NetApp systems with predictive analytics and proactive support tool, provide real-time insights and recommendations to prevent problems and optimize your data infrastructure.

“With the NetApp solution, we can slash the time needed to create an environment from 6 hours to 5 minutes regardless of scale, while provisioning additional environments simultaneously. That translates to a time savings of 70% for each product line.”

— Sandrine Kalk | Director of Global DevOps and Operations, Verint

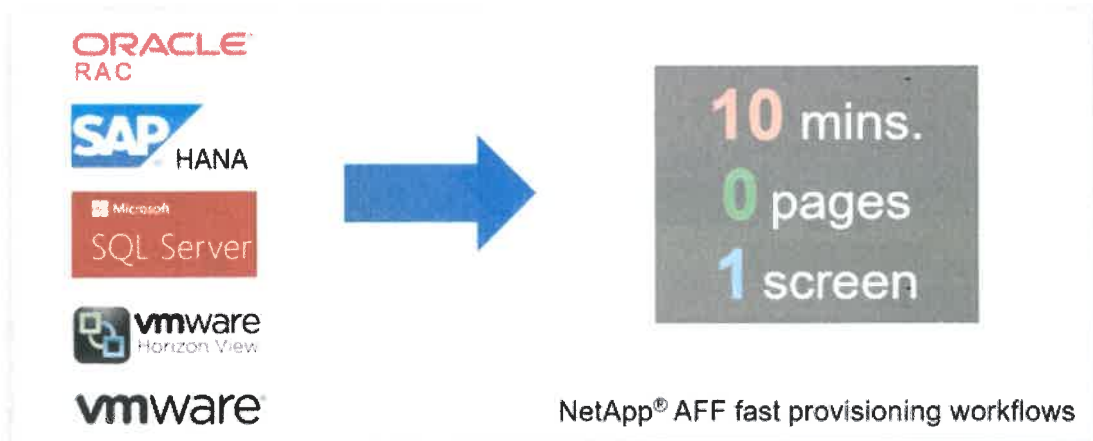


Figure 2: Application-aware data management – Deploy key workloads in less than 10 minutes with ONTAP System Manager.

Achieve Storage Savings, Backed by the Industry's Most Effective Guarantee

With AFF, reduce your data center costs with the best effective capacity for any workload, backed by the industry's most effective guarantee. We guarantee in writing:

- 3:1 guarantee across all workloads
- 4:1 for VVOL and 8:1 for VDI
- Use snapshots and get 10x higher efficiency

AFF system's support for solid state drives (SSDs) with multistream write technology, combined with advanced SSD partitioning, provides maximum usable capacity, regardless of the type of data that you store. Thin provisioning; NetApp Snapshot™ copies; and inline data reduction features, such as deduplication, compression, and compaction, provide additional space savings—without affecting performance—so you can purchase the least amount of storage capacity possible.

Build your Hybrid Cloud with Ease

The NetApp Data Fabric helps you simplify and integrate data management across cloud and on-premises to meet business demands and gain a competitive edge. With AFF, you connect to more clouds for more data services, data tiering, caching, and disaster recovery. FabricPool gives you the ability to move data automatically between AFF and the cloud storage tiers to maximize performance and reduce overall data management cost. Simplify hybrid cloud backup and recovery with cloud-resident NetApp Data Availability Services and accelerate read performance for data that is shared throughout your organization and across hybrid cloud deployments.

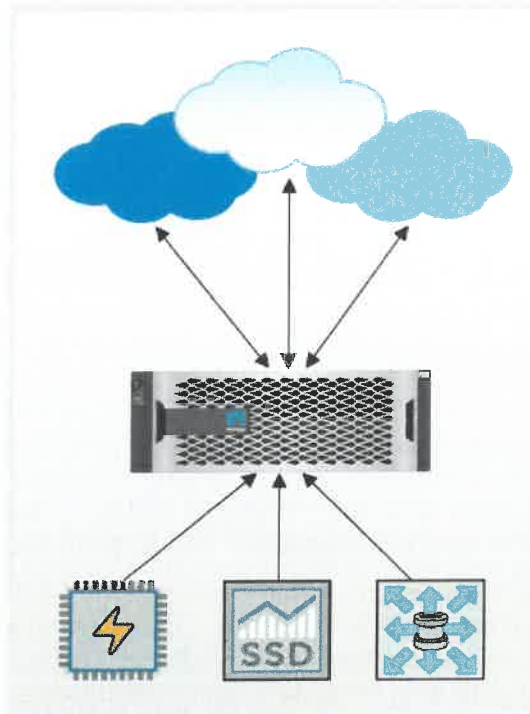


Figure 3: Future-proof your infrastructure with the most cloud-connected all-flash array – Designed for the cloud era to connect to more clouds, in more ways, and to more services—to virtually any service provider or private cloud.

Accelerate Applications and Future-Proof Your Infrastructure

NetApp AFF systems deliver industry-leading performance proven by SPC-1¹ and SPEC SFS industry benchmarks, making them ideal for demanding, highly transactional applications such as Oracle, Microsoft SQL Server, MongoDB databases, VDI, and server virtualization. The AFF A800 system achieved:

- 2,401,000 SPC-1 IOPS at 0.590 SPC-1 IOPS Response Time in a new SPC-1v3 result
- Lowest latency and \$/GB among the top 5 results
- Predictable and consistent latency
 - ~0.4ms latency @ 80% load
 - 0.351ms SPC-1 Overall Response Time
- Highest storage capacity utilization
 - 66% versus ~30% from most others

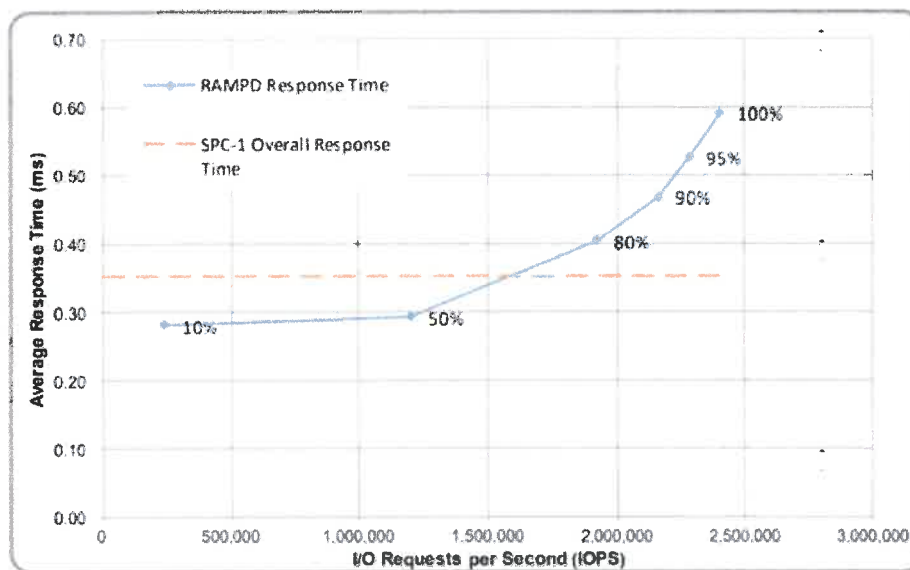


Figure 4: AFF A800 Places in the Top 4 of SPC-1v3 – Best performance and value among major vendors who publish benchmarks.

Accelerate Demanding Workloads

Accelerate the most demanding workloads with an AFF A800 and AFF A320 system. The AFF A800 combines NVMe SSDs and NVMe/FC connectivity to provide an ultrafast end-to-end data path to your applications. The midrange AFF A320 system supports NVMe/RoCE connectivity on the backend to the NVMe drive shelf and NVMe/FC on the front-end to the host. The AFF A320 leads the market with the best combination of NVMe-oF technologies.

Consolidate all workloads on AFF systems, which deliver up to 11.4 million IOPS at 1ms latency in a cluster with a truly unified scale-out architecture. You can manage a scalable NAS container of up to 20PB and 400 billion files with a single namespace by using NetApp FlexGroup volumes, while maintaining consistent high performance with adaptive quality of service (QoS) and resiliency. NetApp FlexCache[®] software improves the speed and productivity

¹ Link to SPC-1 report: <http://spcresults.org/benchmarks/results/spc1-spc1e#A32007>.

of collaboration across multiple locations and increases data throughput for read-intensive applications.

The NVMe-ready AFF A800s awarded the Product of the Year award for Enterprise Storage from CRN.

Modernize with Advanced NVMe

Designed specifically for flash, the AFF A-Series all-flash systems deliver industry-leading performance, capacity density, scalability, security, and network connectivity in dense form factors. AFF A-Series systems support NVMe/FC host connectivity, so you can gain twice the IOPS and cut application response time in half compared with traditional FC. These systems support a range of ecosystems, including VMware, Microsoft Windows 10, and Linux, with storage path failover. For most customers, integrating NVMe/FC into an existing SAN is a simple, nondisruptive software upgrade.

In addition, integrate new technologies and private or public cloud into your infrastructure nondisruptively. AFF is the only all-flash array where you can combine different controllers, SSD sizes, and new technologies—protecting your investment.

Keep Important Data Available, Protected, and Secure

Support backup and disaster recovery needs through our complete suite of integrated data protection and replication features. NetApp Integrated Data Protection technologies protect data and accelerate recovery; for easier management they integrate with leading backup applications. Benefit from features and capabilities such as NetApp Snapshot™ copies, cloning, encryption, and both synchronous and asynchronous replication for backup and disaster recovery. Key capabilities and benefits include:

- Reduced data management costs with native space efficiency with cloning and NetApp Snapshot copies. Up to 1,023 copies are supported.
- Unified, scalable platform and plug-in suite for application-consistent data protection and clone management with NetApp SnapCenter®.
- Reduced overall system costs with NetApp SnapMirror® replication software, which replicates to any type of FAS/AFF system: all-flash, hybrid, or HDD, on the premises or in the cloud.
- Synchronous replication with NetApp MetroCluster™ software, a capability in the all-flash-array market that delivers zero RPO and low to zero RTO for mission-critical workloads.
- Regulatory compliance with NetApp SnapLock® technology, which is enabled with Integrated Data Protection and storage efficiency.

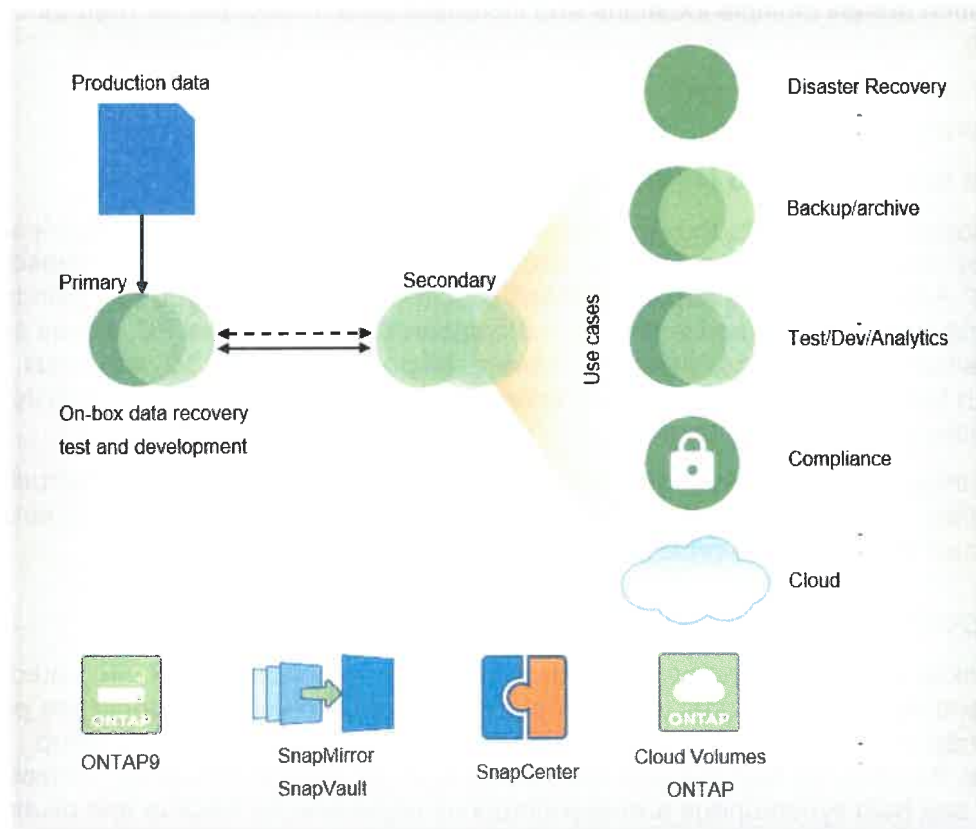


Figure 5: NetApp integrated data protection – Offers one data management flexible platform that provides data availability to keep applications running, mitigate risk, control costs, and improve data protection processes.

In addition, flexible encryption and key management help guard sensitive data on the premises, in the cloud, and in transit. With the simple and efficient security solutions, you can:

- Achieve FIPS 140-2 compliance (Level 1 and Level 2) with self-encrypting drives and use any type of drives with software-based encryption.
- Meet governance, risk, and compliance requirements with security features such as secure purge; logging and auditing monitors; and write once, read many (WORM) file locking.
- Protect against threats with multifactor authentication, role-based access control, secure multitenancy, and storage-level file security.

“NetApp's multiprotocol capability was a major draw for our colleges. With NetApp, we can enable our colleges to retain their skillsets. They don't have to learn something new or put in a mix of products just to accommodate their protocols.”

— Daniel Black | Director of Engineering, Technical College System of Georgia

Future-Proof Your Investment with Maximum Flexibility

NetApp solutions establish a seamless, well-integrated hybrid cloud architecture or Data Fabric that easily ties together private cloud, service providers, and hyperscale cloud providers along with their data management environments. This Data Fabric gives you the ability to implement the hybrid cloud on its own terms. Move data and applications to an AFF system, on commodity hardware with software-defined storage, or in the cloud. The Data Fabric offers a broad set of application ecosystem integration for database, VDI, and server virtualization.

With AFF, which is Data Fabric ready, your investment is protected as performance and capacity needs change or your cloud strategy evolves:

- AFF systems eliminate performance silos. Seamless integration with hybrid FAS systems means that workloads can transparently move between high-performance tiers and low-cost capacity tiers.
- Seamlessly adapt to changing needs with the only all-flash array that offers the ability to intermix different controllers, SSD sizes, and next-generation technologies.
- AFF is data fabric ready, with proven cloud connectivity. FabricPool enables you to move data automatically between AFF and the cloud storage tiers to maximize performance and reduce overall data management cost.
- Optimize data management for enterprise workload environments with leading application integration with Oracle, Microsoft, VMware, SAP, OpenStack, and many more.

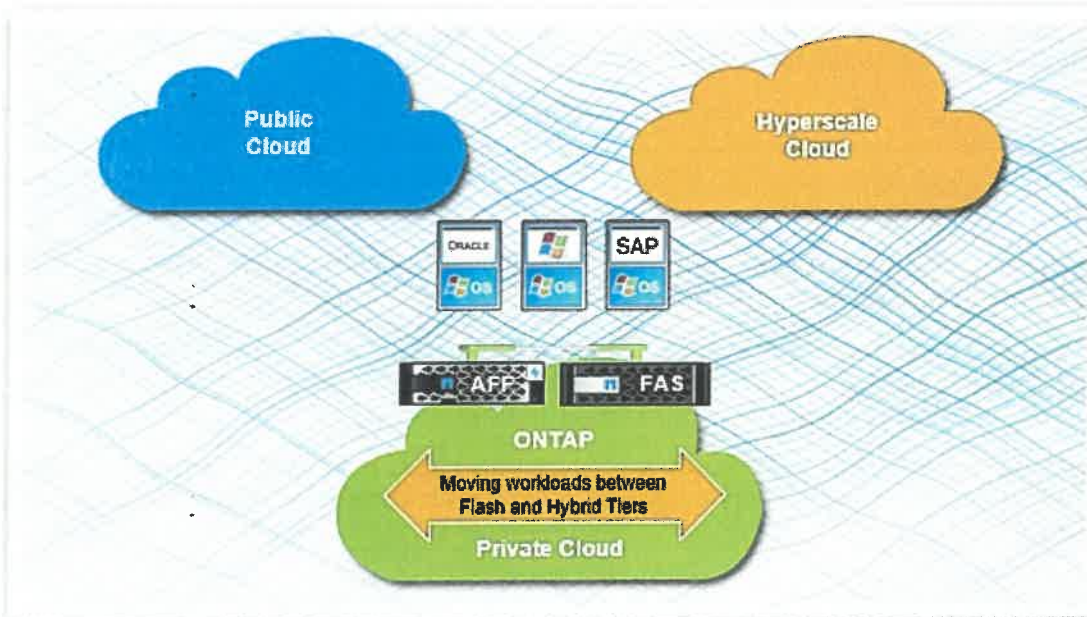


Figure 6: AFF is Data Fabric ready—moving data between tiers and different clouds.

“With NetApp All Flash FAS, we can improve the quality of healthcare in our own hospitals and others throughout the region by offering high-performing electronic patient records and virtual desktops to healthcare providers.”

— Reinoud Reynders, IT Manager, Infrastructure and Operations at UZ Leuven

All-Flash Performance Powered by End-to-End NVMe Technology

AFF systems are excellent for performance-demanding applications and mixed-workload environments that consist of, for example, Oracle, Microsoft SQL Server, MongoDB databases, VDI, and server virtualization. With NVMe-based AFF A800, AFF is also a great choice for AI and deep-learning environments:

- Combined with ONTAP cloud integration and software-defined capabilities, AFF enables the full range of the data pipeline that spans the edge, the core, and the cloud for AI and deep learning, leveraging the same ONTAP data management.
- The end-to-end NVMe-based AFF A800 delivers 1.3 million IOPS at below 500µs latency.
- Built-in adaptive QoS safeguards SLAs in multiworkload and multitenant environments. It optimizes performance control dynamically with superior scalability of up to 40,000 workloads per cluster at LUN, file, and VVol levels.
- With the latest ONTAP release, AFF delivers up to 90% performance increase for Microsoft SQL Server with multichannel SMB.

Storage Efficiency Technologies

NetApp is known for its superior storage efficiency technologies, such as inline deduplication, inline compression, thin provisioning, and space-efficient Snapshot copies. These technologies apply to AFF systems and further reduce your total cost of ownership by lowering cost per effective gigabyte of storage:

- Performance-efficient inline data reduction technologies provide an average of 5 to 10 times space savings for a typical use case.
- Space-saving inline data compaction technology places multiple logical data blocks from the same volume into a single 4KB block. Space savings as high as 67:1 from this feature have been observed when using inline data compaction and inline compression with an Oracle database.
- There is a near-zero performance impact with inline compression. Incompressible data detection eliminates wasted cycles.
- You can increase space savings by eliminating redundant blocks using inline deduplication—effective for operations such as VDI OS patches in which this deduplication can achieve 70:1 reduction rates.
- As the first all-flash array to support SSDs with MSW technology, and combined with advanced SSD partitioning in ONTAP, AFF further increases usable capacity by up to 42%.

NetApp Simplifies Management

NetApp management software provides automated tools to further simplify management of storage operations:

- Set up and configure AFF quick and easy with preconfigured systems for SAN and NAS deployments. It takes less than 10 minutes with ONTAP System Manager.
- OnCommand Workflow Automation automates common storage tasks such as provisioning and data protection. It provides fast one-click automation and self-service.

- To optimize storage for peak performance and to keep everything running smoothly, OnCommand Performance Manager provisions and rebalances workloads by monitoring clusters and nodes to assure performance headroom.
- Import LUNs from storage arrays that are not based on ONTAP software directly into an AFF system to seamlessly migrate data from older storage arrays.

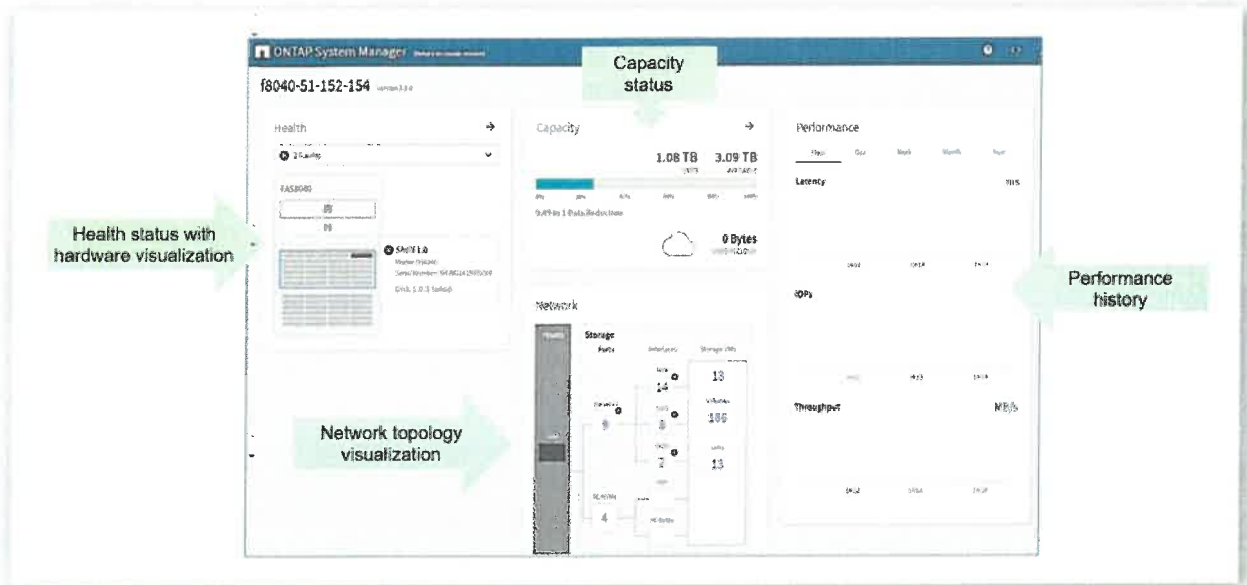


Figure 7: Intuitive ONTAP System Manager –Based on REST APIs, the new System Manager dashboard is more intuitive and displays richer information in a more actionable view.

Get More Business Value with Services

To help you fully realize the benefits of NetApp solutions, NetApp Services and our NetApp certified services partners will collaborate with you through a full portfolio of services that covers the company's IT lifecycle. NetApp offers:

- Assessment services to evaluate the performance and efficiency of workloads across heterogeneous environments
- Advisory services to determine the best workload candidates to move to flash
- Deploy and optimize services to prepare your environment and deliver continuous operation of AFF systems
- Managed upgrade services to secure your storage environment and to protect your investment by ensuring your ONTAP software is the most current version.

NetApp Support offerings, such as the NetApp Active IQ® cloud-based predictive cloud-based analytics and proactive support tool, provide real-time insights and recommendations to prevent problems and optimize your data infrastructure. Learn more at netapp.com/services.

AFF A-Series Systems

NetApp AFF systems help you meet your enterprise storage requirements with the following AFF A-Series Systems:

AFF A800

The AFF A800 is designed for the most demanding workloads requiring ultra-low latency and is the first flash array on the market to support NVMe SSDs and NVMe over Fabrics (NVMe-oF). It provides end-to-end NVMe connectivity between storage arrays and host servers for maximum bandwidth, high IOPS, and the lowest possible latency. Each 4U chassis accommodates dual controllers for high availability (HA) and includes 48 slots for NVMe SSDs. In addition to 32Gb and 16Gb FC, network options include the storage industry's first 100GbE connectivity, as well as 40GbE and 10GbE. An NVMe-powered SAN scale-out cluster supports up to 12 nodes (6 HA pairs) with 1,440 drives and nearly 160PB of effective capacity. NAS scale-out clusters support up to 24 nodes (12 HA pairs). The AFF A800 future-proofs your data infrastructure with NetApp ONTAP 9 the industry's leading data management software.

"NetApp once again hits it out of the park with the enterprise focused A800. The performance profile is very strong, taking its position at the top of the ONTAP family."

— *StorageReview Editors' Choice, May 2019*

AFF A700

The AFF A700 is a high-end NetApp storage controller designed for performance-driven workloads and data centers requiring a modular design. The AFF A700 can dramatically enhance performance and high-performance I/O density in a new 8U HA form factor and it includes options for 40GbE and 32Gb FC along with the latest in SAS connectivity, the SAS 3.0 standard with 12Gb speeds. This controller also provides the most versatile I/O interface available, the UTA2 connections that support 10GbE and 16Gb FC and that can be easily changed between these two protocols in the field. AFF A700 controllers support up to 12 nodes for SAN deployments and up to 24 nodes in NAS deployments.

AFF A700s

The AFF A700s is an integrated high-end all-flash array and best for performance-driven workloads and data centers requiring a small footprint. The AFF A700s comes in a compact form factor with dual controllers and 24 internal SSDs in a single 4U chassis. A700s provides data center efficiencies and excellent performance with reduced power and cooling. AFF A700s performance is comparable to that of AFF A700; however, they offer different connectivity and capacity options to address different solutions and customer requirements.

AFF A320

The AFF A320 midrange end-to-end NVMe NetApp AFF storage controller is a modern NVMe Flash storage system. It provides application performance improvements with lower latencies compared to the AFF A300. For enterprise applications that require the best performance at value, the AFF A320 includes dense 2U form factor with two HA controllers, extreme bandwidth with 16 onboard 100GbE ports and four expansion slots in an HA pair, adapter support includes 100GbE, 32Gb FC, 25GbE, and 10GbE support, NVDIMMs for persistent write cache of data received but not yet committed to flash media, and host-side NVMe/FC support for low-latency, high-performance remote direct memory access (RDMA) connectivity to the NVMe SSDs.

AFF A300

The A300 firmly targets enterprise applications that require best balance of performance and cost. It is more powerful than the AFA A220 for users that need additional capacity and performance. The AFF A300 is easy to set up and runs the latest version of ONTAP and supports SSDs up to 30TB. It requires just 12 SSDs to start but scales to over 140PB raw (560PB effective) in NAS config and 70PB raw (280PB effective) as SAN. The A300 supports 10GbE, 40GbE as well as Fibre Channel up to 32Gb and NVMe/FC with the 32Gb FC adapter.

The midrange AFF A300 recently won the Editor's Choice Award from StorageReview, which bestows this award for "performance in excess of competitive offerings, a feature set that is innovative and sets a new bar for competitive offerings or for defining a new category or space within enterprise IT". Through Storage Review's independent testing with Oracle, SQL, VDI workloads, AFF A300 stands out with its impressive performance and feature set.

— StorageReview Editors' Choice, November 2018

AFF A220

The AFF A220 is ideal for mid-size business and small enterprises that require simplicity and best value. With the AFF A220 you can accelerate business insights and demanding workloads. This 2U array enables enhanced storage efficiency based on the types of workloads. With a potential maximum raw capacity of up to 48.3 PB and maximum memory of 768 GB, NetApp ensures the effectiveness of its inline data reduction technologies, including compression, deduplication and data compaction. It offers 4x 10 GbE cluster interconnect channels for distribution of the processing across an array of nodes in the clusters, and high-data rate and low-latency communication between node processes.

"In addition to accelerating every application without disruption, the NetApp AFF A200 dramatically improves data center economics and enables data-driven enterprises to modernize their infrastructures with confidence. Editor's Choice award for the NetApp AFF A200 for phenomenal performance at sub-millisecond latencies."

— StorageReview Editors' Choice, November 2017

AFF C-Series Systems

NetApp AFF C-Series offers entry-level all-flash systems with enterprise-grade features.

AFF C190

The NetApp AFF C190 offers an enterprise-class flash system for an affordable price. It is designed for IT generalists to meet business requirements with comprehensive data services, seamless scalability, new levels of performance, and cloud integration. With the C190 you can effortlessly connect to public clouds and automatically tier cold data or back up to the cloud to reduce overall storage costs. It delivers industry-leading hybrid cloud integration, supporting all major public clouds including Google Cloud, Amazon Web Services (AWS), Microsoft Azure, IBM Cloud, and Alibaba Cloud.

Table 1: All Flash FAS A-Series Systems technical specifications.

AFF Technical Specifications						
	AFF A800	AFF A700s	AFF A700	AFF A320	AFF A300	AFF A220
Maximum scale-out	2–24 nodes (12 HA pairs)					
Maximum SSD	2,880	2,529	5,760	576	4,608	1,728
Max effective capacity ²	316.3PB	316.3PB	702.7PB	35PB	562.2PB	193.3PB
Per-System Specifications (Active-Active Dual Controller)						
Controller form factor	4U with 48 SSD slots	4U with 48 SSD slots	8U	2U	3U	2U with two 24 SSD slots

Table 2: AFF A-Series software.

AFF A-Series Software	
Features and software included with ONTAP software	<p>Efficiency: NetApp FlexVol[®], inline deduplication, inline compression, inline compaction, and thin provisioning</p> <p>Availability: Multipath I/O and active-active HA pair</p> <p>Data protection: NetApp RAID DP[®], NetApp RAID TEC[®], and Snapshot technology</p> <p>Whole cluster synchronous replication: MetroCluster</p> <p>Performance control: Adaptive QoS and balanced replacement</p> <p>Management: OnCommand Workflow Automation, ONTAP System Manager, and Active IQ Unified Manager</p> <p>Scalable NAS container: NetApp ONTAP FlexGroup</p> <p>Storage protocols supported: NVMe/FC, FC, FCoE, iSCSI, NFS, pNFS, and SMB</p>
Flash bundle	<p>NetApp SnapRestore[®] software: Restore entire Snapshot copies in seconds</p> <p>NetApp SnapMirror software: Simple, flexible backup and replication for disaster recovery</p> <p>NetApp FlexClone[®] technology: Instant virtual copies of files, LUNs, and volumes</p> <p>NetApp SnapCenter[®]: Unified, scalable platform and plug-in suite for application-consistent data protection and clone management</p> <p>NetApp SnapManager software: Application-consistent backup/recovery for enterprise applications</p> <p>Go to NetApp.com for information on additional software available from NetApp.</p>

² Effective capacity is based on 5:1 storage efficiency ratios with the maximum number of SSDs installed. The actual ratio can be higher depending on workloads and use cases.

AFF A-Series Software

Extended-value software (optional)

NetApp OnCommand Insight: Flexible, efficient resource management for heterogeneous environments

NetApp SnapLock: Compliance software for write once, read many (WORM) protected data

NetApp Volume Encryption (free license): Granular, volume-level, data-at-rest encryption

NetApp FabricPool feature: Automatic data tiering to the cloud

SnapMirror Synchronous: Synchronous data replication with zero recovery point objective

NetApp Data Availability Services: Cloud native backup solution for ONTAP storage

NetApp FlexCache: Acceleration for data access for single or multisite deployment

Table 3: All Flash FAS C-Series Systems technical specifications.

AFF C190 Technical Specifications for Active-Active Dual Controller

Drives and Capacity	Connectivity	Protocols and Operating Systems
Max. effective capacity 50TiB ³	4 ports—12Gb/6Gb SAS	ONTAP 9.6 GA or later
Max. SSD 24 drives	1GbE management port, USB port	Protocols: FC, FCoE, iSCSI, NFS, pNFS, SMB
Drive type: 960GB SSD	8 ports—FC target (16Gb) 8 ports—FCoE target, UTA2 12 ports—10GbE ports, UTA2 12 ports—10GBASE-T	Host OS version: Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Linux, Oracle Solaris, AIX, HPE UX, macOS, VMware, ESX

³ Effective capacity is based on 3:1 storage efficiency ratios with the maximum number of SSDs installed. The actual ratio can be higher depending on workloads and use cases

Table 4: AFF C-Series software.

Software Included with AFF C190

Features and software included with ONTAP software	<p>Efficiency: NetApp FlexVol[®], inline deduplication, inline compression, inline compaction, and thin provisioning</p> <p>Availability: High availability (HA) pair and multipath I/O</p> <p>Data protection: NetApp RAID DP[®], NetApp RAID TEC[®], and Snapshot technology</p> <p>SnapMirror Synchronous replication</p> <p>Performance acceleration: NetApp FlexCache[®] software</p> <p>Management: OnCommand Workflow Automation, ONTAP System Manager, and Active IQ Unified Manager</p> <p>Scalable NAS container: NetApp ONTAP FlexGroup</p> <p>Storage protocols supported: FC, FCoE, iSCSI, NFS, pNFS, and SMB</p> <p>NetApp SnapRestore[®] software: Restore entire Snapshot copies in seconds</p> <p>NetApp SnapMirror software: Simple, flexible backup and replication for disaster recovery</p> <p>NetApp FlexClone[®] technology: Instant virtual copies of files, LUNs, and volumes</p> <p>NetApp SnapCenter[®]: Unified, scalable platform and plug-in suite for application-consistent data protection and clone management</p> <p>NetApp SnapManager software: Application-consistent backup/recovery for enterprise applications</p>
Extended-value software (optional)	<p>NetApp OnCommand Insight: Flexible, efficient resource management for heterogeneous environments</p> <p>NetApp SnapLock[®]: Compliance software for write once, read many (WORM) protected data</p> <p>NetApp Volume Encryption (free license): Granular, volume-level, data-at-rest encryption</p> <p>NetApp FabricPool: Automatic data tiering to the cloud</p> <p>NetApp Data Availability Services: Cloud native backup solution for ONTAP storage</p>

Disaggregated Hyper Converged Infrastructure

NetApp® HCI is an enterprise-scale, hyper converged infrastructure for hybrid clouds that gives you a public cloud experience from your private cloud. Deliver an as-a-service experience to your users while maintaining complete control over performance, availability, and costs.

Faced with rapidly evolving business needs and unbridled data growth, today's enterprises must maintain a proactive, agile environment to be competitive and grow business. Public cloud providers are appealing because they make it easy for business to quickly spin up new services and make them immediately and globally available in today's digital sphere. Although this approach may address immediate needs, it can result in loss of control from financial, regulatory, and management standpoints.

To contain costs and regain control of company data, IT departments must deliver applications and workloads with the same simplicity, efficiency, and flexibility offered by major public cloud providers. However, traditional data centers are straining under web applications, mobile users, and an influx of data that they were not designed to handle. The complexity of traditional data centers makes it more difficult for IT to launch new, agile applications quickly enough to meet developer demand and the business value they provide.

Today IT is faced with disparate environments between public clouds and private clouds. They have to contend with legacy applications on-prem, cloud native app development, and support the expectations of public clouds including easy to consume and fast to deploy user experiences.

Command Your Cloud—with Disaggregated Hyperconverged Infrastructure for Hybrid Clouds

NetApp® HCI is an enterprise-scale, disaggregated hyper converged infrastructure designed for hybrid, multiclouds that consists of software-defined compute, network, and storage. It delivers a public cloud consumption experience with simplicity, dynamic scale, and operational efficiency. With NetApp HCI, The State of West Virginia's infrastructure and cloud architects can seamlessly access services from their on-premises or from any third-party cloud provider and mix and match these services to optimize resources for specific workloads and applications.

NetApp HCI gives you the ability to consolidate and easily manage multiple applications with guaranteed workload performance that your users and customers demand. Scale compute and storage resources independently so you can grow on your terms and never pay for more than you need. Deploy in minutes with a turnkey cloud infrastructure that eliminates the complex management of traditional three-tier architectures.

"For virtually every application that we have moved to the new system, our users have noted a performance improvement. Some things are definitely running twice as fast. Also, we did pay a sizeable set of maintenance fees on the old array—so basically, we're getting new performance for what we were paying to keep the status quo."

— Sean Henry Senior Manager, American Showa

In addition, NetApp HCI is integrated into your data fabric. You can use the full potential of your applications, with their associated data and the services they require, across any cloud. With the

NetApp HCI future-proof environment you can seamlessly add multiple new workloads such as Splunk, SAP, VDI, SQL Server, MongoDB, and more, to support your business transformation.

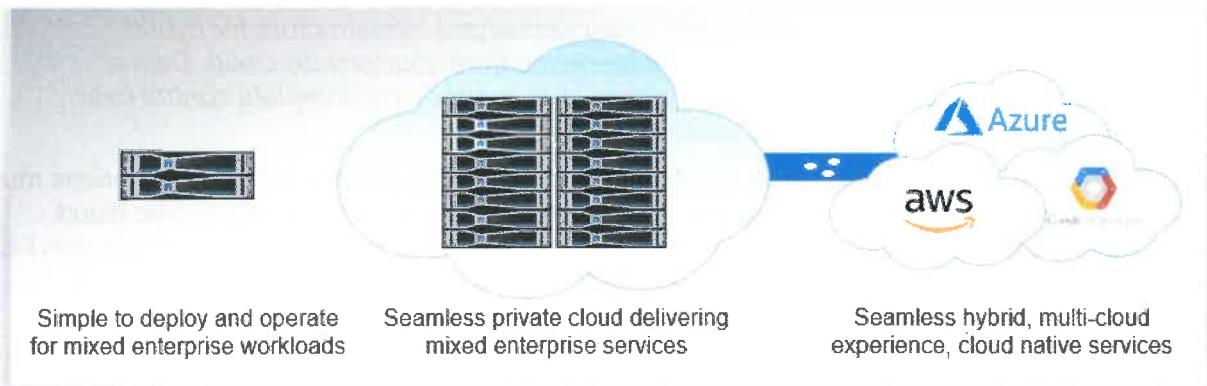


Figure 1: NetApp HCI: A seamless hybrid multicloud experience – From hyperconverged infrastructure to hybrid-cloud infrastructure.

With NetApp HCI The State of West Virginia can:

- Scale on your terms
- Choose the right cloud for any workload
- Achieve a competitive advantage

Scale on Your Terms

NetApp HCI delivers a hybrid cloud infrastructure that addresses enterprise-class multicloud agility, scale, and services. It brings together NetApp Element[®] software with all-flash storage core processing for system-critical applications; graphical processing units for virtualized desktops; and networking. All parts of the infrastructure are fully architected and managed as an appliance, enabling unique efficiencies.

Increase productivity with guaranteed, predictable performance across all your applications with the SolidFire[®] Element software's innovative three-dimensional Quality of Service (QoS). Future-proof your investment with an agile, scale-out architecture that lets you independently scale compute and storage resources on demand, without disruption from generation to generation.

Choose the Right Cloud for Any Workload

Enterprises must harness the current wealth of data and apply it to create new value across the entire organization—all with limited time, skills and budget. NetApp gives you the ability to build a data fabric that unleashes the full potential of your data across any cloud—public, private, or hybrid. NetApp HCI integrates into your data fabric for enhanced data services, including file services through NetApp ONTAP[®] Select, object services through NetApp StorageGRID[®], replication services through NetApp SnapMirror[®], data visibility through NetApp Cloud Insights, and backup and recovery services through NetApp Cloud Backup.

NetApp HCI with NetApp Kubernetes Service and NetApp Cloud Volumes

IT is emerging with a new set of expectations—Cloud-native, DevOps, infrastructure-as-a-service consumption, and self-service have all become baseline expectations. A private cloud

on the premises is expected to have all of the efficiencies and abilities of the public cloud. More and more IT needs extensive hybrid cloud and even multicloud capabilities for efficient development and workload portability.

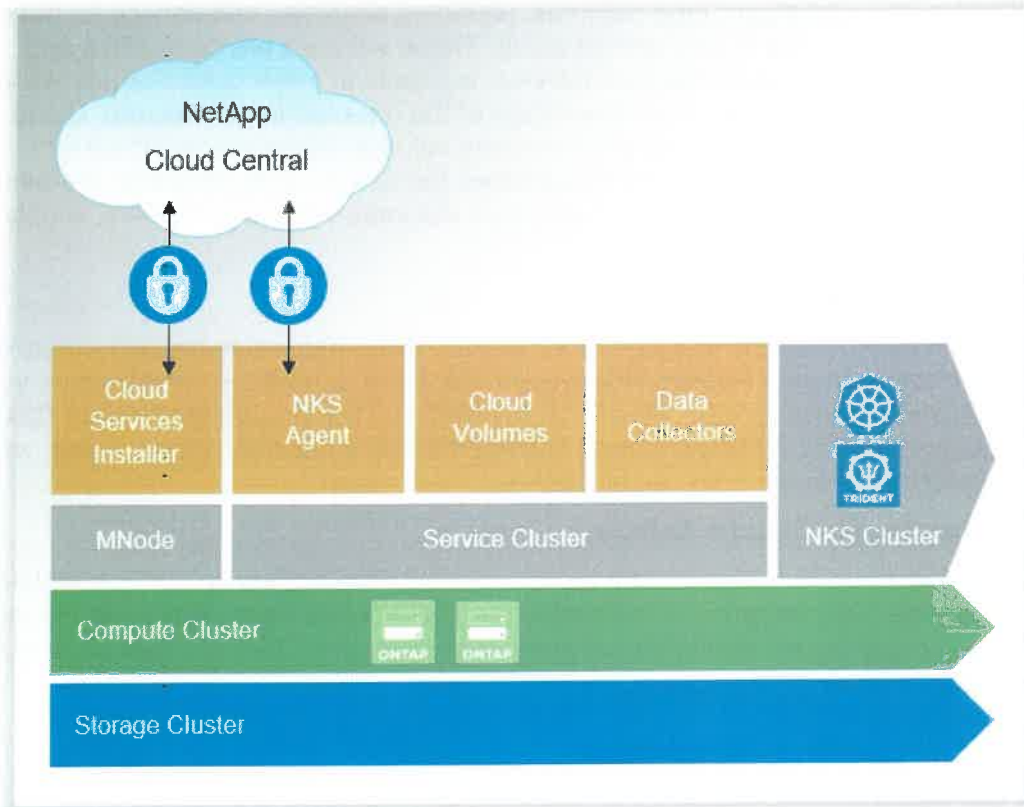


Figure 2: Solution architecture overview – Architecturally, all of this new functionality is deployed in a service cluster on your NetApp HCI system, which is then managed centrally by NetApp.

“NetApp has showed us the power of its comprehensive suite of solutions, from All Flash Storage Systems to HCI, to all opportunities offered by NetApp Cloud Data Services. The company has helped us capitalize on today’s business opportunities while we innovate for tomorrow.”

— *Konstantin Kosternarov, Chief Technology Officer, Ducati Motor Holding*

In addition to meeting modern consumption and orchestration requirements, any enterprise-grade private cloud must also be robust. It must offer production-grade qualities such as scalability, predictable and guaranteed performance, and availability. NetApp offers solutions to deploy an efficient, cloud-native control plane. These solutions include hybrid multicloud capabilities and advanced storage services that support efficient consumption models, enable cloudlike provisioning on your premises, and offer a way into the data fabric.

NetApp Kubernetes Service

With a NetApp HCI-based private cloud, you can choose how you deploy your control plane. NetApp Kubernetes Service (NKS) gives you the ability to easily deliver cloud-native capabilities on your premises by using a Kubernetes service hosted and managed by NetApp. You can also

choose to deploy a VMware-based or Red Hat-based private cloud, instead of or in addition to using NetApp Kubernetes Service. There's no lock-in—just more options.

NetApp Cloud Volumes

NetApp HCI also offers NetApp Cloud Volumes, providing simplified self-service for deploying enterprise-grade file volumes in your private cloud. These volumes are compatible and interoperable with NetApp Cloud Volumes Service, available in major public clouds, so you can replicate data between clouds and take advantage of the data fabric architecture. Cloud Volumes includes Trident, which facilitates persistent volume claims management for containers, provisioned either by NetApp Kubernetes Service or other popular Kubernetes-based packages. You can also choose to use Cloud Volumes without containers, simply provisioning file shares to virtual machines.

Deploy a Cloud Region, On Premises

NetApp makes it easy to deploy and keep your NetApp Kubernetes Service and Cloud Volumes environments current on your NetApp HCI system. We have built all the infrastructure you need and automated the process for you. Simply deploy NetApp HCI through the NetApp Cloud Central portal, and your cloud infrastructure becomes a fully functioning cloud region, with updates and patches managed directly by NetApp.

NetApp HCI for Google Cloud's Anthos

Anthos is a hybrid cloud Kubernetes data center solution. Run Anthos on NetApp HCI and get an easy-to-manage, enterprise-scale foundation for DevOps and PaaS. Build and manage your virtualized and containerized workloads on a single platform and Optimize data performance while effectively controlling your data in any environment.

Achieve a Competitive Advantage

The more you can automate routine tasks, the more you can eliminate the risk of user error associated with manual operations, while also freeing resources to focus on higher value assignments that drive business.

NetApp HCI streamlines installation through an intuitive deployment engine that has automated over 400 inputs to fewer than 30 to get you up and running in about 45 minutes. Simple centralized management through VMware gives you control of NetApp HCI through tools you already use, so you can focus valuable resources on higher priorities that drive business growth. A robust suite of API's enables seamless integration into higher-level management, orchestration, backup, and disaster-recovery tools.

Enterprise-Scale Infrastructure

NetApp HCI delivers IT simplicity and business efficiency, security, and flexibility. NetApp HCI is deployed and maintained as a single appliance with compute and storage nodes that can scale independently. Independent node architecture gives you the ability to intermix product generations to unlock new capabilities without forklift upgrades. Once you meet the minimum configuration requirements, you can mix and match storage and compute nodes and sizes that integrate seamlessly to scale your environment non-disruptively.

"NetApp HCI allows me the flexibility to scale. It allows me to increase performance, increase storage, based on my needs on demand. It allows me to adjust my technology solution based on the constantly changing needs of hospitals like ours."

— David Chou VP, CIO and CDO, Children's Mercy Hospital

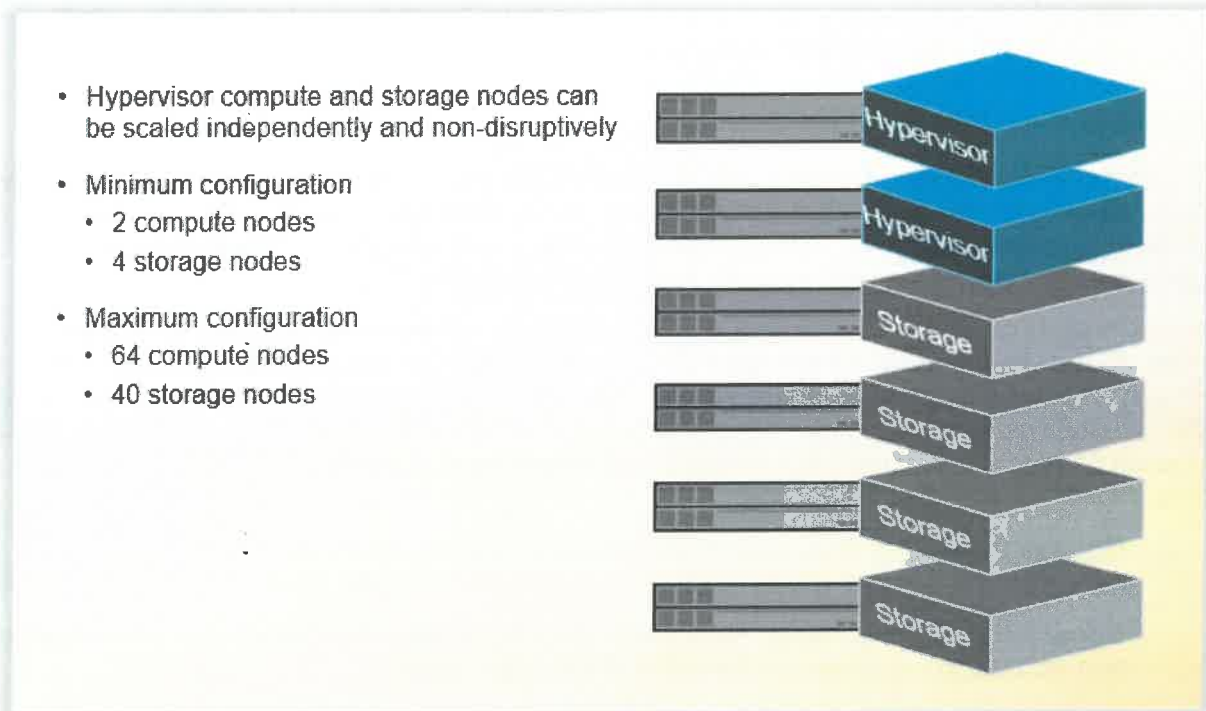


Figure 3: Enterprise scale minimum HCI configuration – Once you meet the minimum configuration requirements, you can mix and match storage and compute nodes and sizes.

Get [guaranteed storage efficiency](#) with global, always-on duplication and compression across all workloads. NetApp HCI is backed by world-class support, with a single point of contact for both hardware and software. Support includes 24/7/365 worldwide availability, with 4-hour on-site response for critical system issues.

Element Capacity Licensing

Capacity licensing is a pricing model that gives you the ability to purchase data storage based on how much capacity is provisioned on your storage infrastructure. It decouples purchasing Element software from the underlying NetApp HCI.

Capacity licensing gives you economic benefits across an entire data center footprint to better align with ever-changing needs. Purchase only the software you need today and “pay as you grow”. It also passes through hardware at cost, eliminating the need to source, validate, and integrate your hardware. With capacity licensing you can:

- Benefit from licenses that are transferable and not locked to a particular hardware
- Pool capacity across your enterprise to eliminate stranded capacity and enable geographic flexibility

- Scale hardware and software independently; only buy what you need, when you need it
- Use pricing based on provisioned capacity to reduce dependency on data reduction efficiency rates
- Realize the long-term time value of money by delaying the purchase of hardware or software packs until you are ready to utilize each
- Use volume discounts to drive down the cost of software as storage capacity grows, creating a more predictable purchasing model

NetApp Keystone: Cloud Consumption for NetApp HCI

NetApp Keystone is a new financial program that allows you to minimize risk while building new infrastructure and managing your digital transformation. With Keystone, you can lessen the complexities associated with IT infrastructure and lifecycle management. Keystone gives IT buyers a clear, easy-to-understand path forward for managing IT.

Cloud Consumption for NetApp HCI is a month-to-month, on-premises flexible deployment model. Cloud Consumption for NetApp HCI delivers economical and operational efficiencies with a public cloud experience that is simple, fast, and easy to deploy in your own private cloud. With Cloud Consumption you can rapidly innovate, manage, scale, and consume NetApp HCI at the pace of your use with radically simple contract terms and monthly billing. With Cloud Consumption for NetApp HCI you can:

- **Manage regulatory risk.** Maintain jurisdiction over regulatory compliance and data security while bringing the benefits of the public cloud to your on-premises private cloud.
- **Boost economic flexibility.** Remove or reduce the capex burden of your infrastructure and achieve the pay-per-use flexibility of the public cloud.
- **Scale on your own terms.** Lower barriers to entry and scale on your own terms by paying per node, per month, without the exposure of asset ownership.

Build Your Data Fabric

Data is at the heart of every business. New technologies impact every discipline, every economy, and every industry. Technologies like artificial intelligence (AI) and the Internet of Things (IoT) are going mainstream and they generate and depend on vast amounts of data and capabilities. As data drives digital transformation, harnessing that data is key to competitive advantage. To be successful, you must have the ability to move fast, innovate, react, and be nimble. You also must be able to access data and resources that live anywhere, and everywhere.

It is likely you have efforts underway to transform with cloud, add new cloud-like capabilities to your current IT environment, or run your IT environment better—quite possibly all at the same time. When you work with NetApp to accomplish any of these goals, you are, by default, building a data fabric. You are ensuring your data and applications are in the right place at the right time with the right characteristics and capabilities to achieve new insights and accelerate innovation.

“Data fabric enables frictionless access and sharing of data in a distributed data environment. It enables a single and consistent data management framework, which allows seamless data access and processing by design across otherwise siloed storage.”

— Gartner, *Top 10 Data and Analytics Technology Trends for 2019*¹

IT Priorities that Unite with Data Fabric

Data fabric provides a common framework to simplify the integration and orchestration of data services across your choice of clouds. When you build a data fabric with NetApp, you unleash the power of data to meet business demands and gain a competitive edge.

We have learned that building a data fabric is typically an outgrowth of another major IT initiative, rather than a goal in itself. We take a strategic approach to help you with your cloud and IT initiatives while building your data fabric.

If you are looking to transform with cloud. Only NetApp offers data services across the world's biggest clouds: Microsoft Azure, Amazon Web Services (AWS) and Google Cloud Platform—plus many other cloud and colocation providers, including Alibaba, IBM, Equinix, and BT. Choose the cloud resources that are best for your workloads and simplify the complexities of managing data across multiple clouds and on premises.

If you are looking to grow by adding new capabilities, speed, and agility to your current environment. NetApp provides private cloud capabilities. This gives you the ability to deliver new applications and services faster and run existing workloads more efficiently. You gain real cloud, real performance, at scale, and on premises.

If you are looking to run your current application environment more efficiently. NetApp provides high-performing, cloud-integrated technologies and converged and hyper-converged infrastructures. This includes a highly differentiated portfolio of all-flash and hybrid array offerings. You get simplicity, speed, and automation across core, edge, and cloud.

In all these cases, we help you move from building data centers to building data fabrics.

¹ Gartner Identifies Top 10 Data and Analytics Technology Trends for 2019, See Gartner press release [here](#).

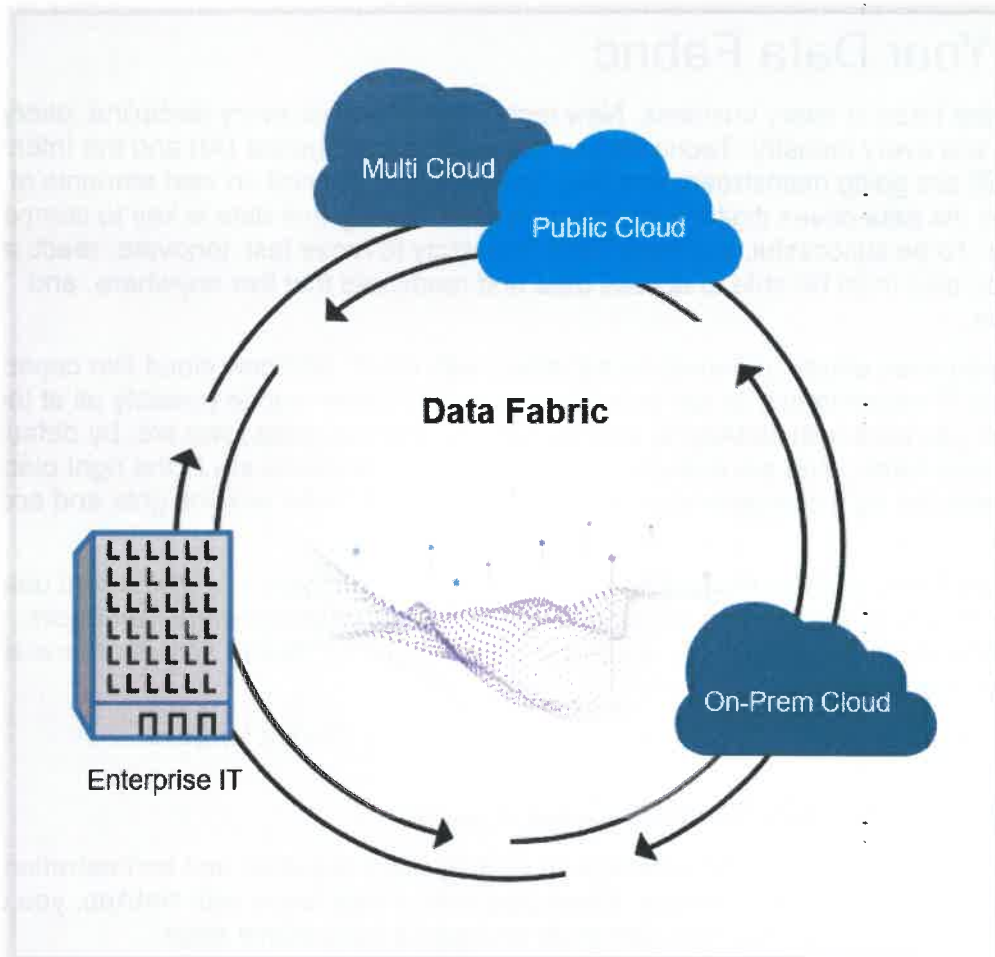


Figure 1: Data fabric connectivity through hybrid multicloud – Data fabric connects everything, across diverse platforms and incompatible data silos with virtually no down time.

A data fabric delivered by NetApp provides:

- Software-defined data management that runs anywhere—on our engineered systems, on third-party hardware, or natively on various public cloud providers.
- Embedded data protection software that enables an efficient backup and disaster recovery strategy, including to the public cloud.
- Cloud integration and migration tools to make public cloud a seamless and efficient extension of your on-premises data center environment.

Data Fabric Building Blocks

Only NetApp offers the full range of capabilities to build and manage your unique data fabric. With NetApp you can:

- **Discover.** Understand the state of your data, applications, systems, and services.
- **Integrate.** Stitch everything together to gain control.
- **Automate.** Define your rules so the fabric can take care of itself.

- **Optimize.** Monitor the state of your fabric and react.
- **Protect.** Back up and restore data for business continuity.
- **Secure.** Simplify compliance, preserve integrity, and control access.

When you build your data fabric with NetApp, you can consume, manage, and pay for services the way you want.

“The continued survival of any business will depend upon an agile, data-centric architecture that responds to the constant rate of change.”

— *Donald Feinberg, vice president and distinguished analyst at Gartner, Gartner Data & Analytics Summit, Sydney Australia, February 18, 2019*

Fabric Orchestrator

NetApp’s Fabric Orchestrator provides an extensible cloud service that gives you the ability to create and manage your data across your hybrid multicloud environment.

It is a data service connecting all points of data production with all points of data consumption. Fabric Orchestrator brings the building blocks described previously into a single user interface and unified data fabric API. It enables you to discover your data, applications, and services by securely connecting to public, private, and on-premises providers including ONTAP® systems, Cloud Data Services, and NetApp HCI. You can invite your teams to collaborate on data, organize it, protect it, secure it, orchestrate and integrate it—all through a rich metadata tagging and labeling solution.

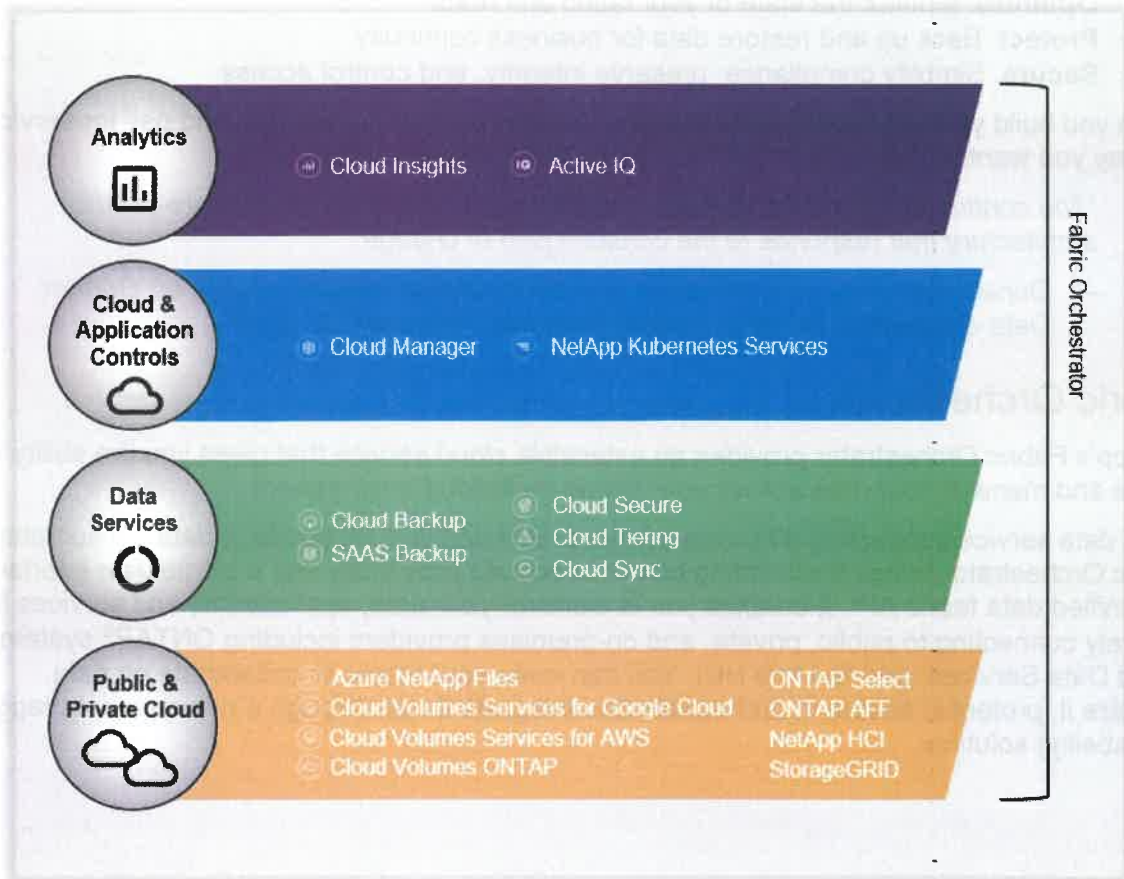


Figure 2: Manage your data fabric with the right capabilities.

Using Fabric Orchestrator, you can:

- Easily scale processes and policies across an entire data estate
- Apply access controls automatically to new datasets according to established policy
- Organize data by using simple concepts like tags and labels
- Automate the proximity of data according to usage patterns and applications
- Enforce data deletion policies across all applications without relying on busy administrators to remember to remove data

“Deriving value from analytics investments depends on having an agile and trusted data fabric.”

— Gartner, *Top 10 Data and Analytics Technology Trends That Will Change Your Business*. April 11, 2019

Business Priorities Accelerated by Data Fabric

With a data fabric established, you can accelerate the missions vital to your business:

- Realize the promise of public cloud: drive flexibility speed, cost savings, and innovation
- Deliver a public cloud experience on premises: simplify and automate infrastructure for virtualized workloads and new application development

- Fuel enterprise applications: accelerate new projects, simplify operations, future-proof IT
- Develop and deploy applications faster: streamline software development and DevOps deployment pipelines
- Accelerate the journey to AI: leverage AI to stay competitive, drive growth, and decrease expenses

Your Path to the Data Fabric

The benefits of the data fabric are tangible, and we have many real-world examples that illustrate how enterprises are building their data fabric with NetApp today. Enterprises everywhere are now using their unique data fabrics to create new customer touchpoints, capture innovative business opportunities, and optimize operations.

One principle guides our innovation: enabling our customers to fully realize the business value of data across the cloud, whether public, private, or hybrid.

Protect Sensitive Data in Data Storage Systems with No Disruption to Operations

The ability to protect and store critical data is a major focus for today's organizations. Networked storage streamlines accessibility to mission-critical information, but it can leave data vulnerable. Firewalls, intrusion-prevention systems, and other next generation network security solutions can secure assets at the perimeter. However, data at the storage core can still be exposed to both internal and external attacks. With the appropriate data protection technologies integrated throughout the data fabric, organizations can guard against potential malicious attacks and attempts to steal confidential data.

NetApp takes a multi-layered and immersion approach to embed and uphold the integrity and confidentiality of The State of West Virginia's most valued assets: your data. With the appropriate data security solutions deployed, you can guard against potential malicious attacks and attempts to steal confidential data. NetApp and our technology partners, provide an extended portfolio of security solutions that have been tested with NetApp storage systems.

NetApp Flexible Encryption Solutions

NetApp offers several encryption solutions that meet a variety of customer requirements.

- **NetApp Storage Encryption.** NSE uses self-encrypting disk drives for full disk encryption (FDE) of data with NetApp® ONTAP®. NSE enables you to benefit from NetApp's leading storage efficiencies such as compression and deduplication while also leveraging industry standard 256-bit AES encryption on FIPS 140-2 Level 2 validated drives. NSE is a simple way to automatically encrypt all data. It removes the complexity of keeping track of where the most sensitive data resides and reduces the risk of data being outside an encrypted volume. As data is written to the drive, it is automatically encrypted. When data is read, it is automatically decrypted. NSE mitigates several threats; including preventing unauthorized access to encrypted data at rest on powered-off disk drives. This capability prevents unauthorized users from removing a shelf or drives for use with unsanctioned systems. In addition, NSE includes cryptographic shredding of data through disk destroy commands that render the disk completely unusable. This feature greatly simplifies disposal of drives and eliminates the need for costly, time-consuming physical drive shredding.

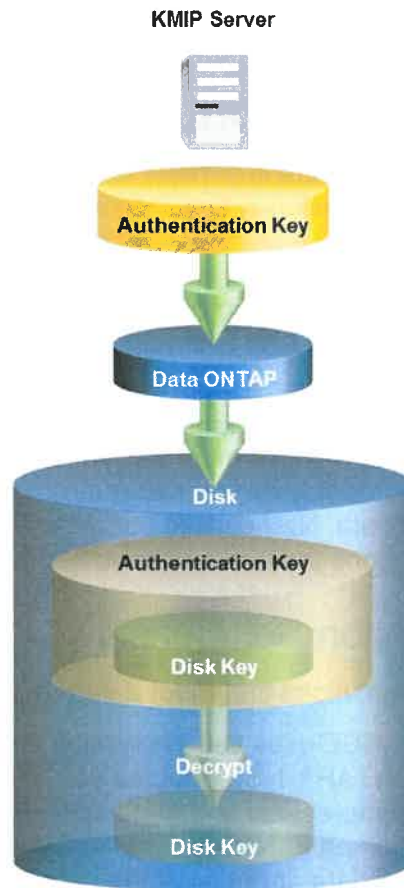


Figure 1: How the KMIP server works with NSE.

NSE supports the entire suite of storage efficiency technologies from NetApp, including deduplication and compression, giving you the efficiency savings you see with unencrypted volumes. Array-based AV scanning is also supported.

- **NetApp Volume Encryption.** NVE is a software-based, data-at-rest encryption solution available starting with ONTAP 9.1 management software. NVE allows ONTAP to encrypt data, per volume for granularity, and to have that data be stored on disk without requiring self-encrypting drives. NVE gives The State of West Virginia the ability to leverage storage efficiency features that would be lost if you decided to encrypt at the application layer. You can use any existing disk with NVE, which also includes NSE drives for “double” or “layered” encryption.

Note: NSE and NVE can be used together to provide customers two distinct layers of encryption; NSE can use onboard or external key management; NVE uses onboard key management only; reference the NSE and NVE datasheet for more details (release pending).

- **Gemalto SafeNet Key Secure.** Provides centralized and consistent enterprise key management that integrates with existing infrastructures. The State of West Virginia can protect confidential data with a unified key lifecycle management solution that secures data across multi-tenant or cloud environments with isolation and granular access to data.

SafeNet KeySecure solutions can manage keys across heterogeneous encryption platforms, offering support for the OASIS Key Management Interoperability Protocol as well as for proprietary interfaces. In addition, Keys are stored in a FIPS 140-2 Level 3 compliant hardware module. Security teams can uniformly view, control, and administer cryptographic policies and keys for all their sensitive data—whether it resides in the cloud, in storage, in databases, or on virtual platforms anywhere else.

Gemalto is a leading global provider of data protection, serving more than 25,000 customers in more than 100 countries, across both commercial and government agencies. Many of the world's leading global organizations rely on Gemalto to secure their high-value data throughout the information lifecycle, from the data center into the cloud:

- Protect over 80% of the world's intra-bank fund transfers and nearly \$1 trillion per day.
 - Monetize the most high-value software—more than 100 million license keys protect and manage on-premise, embedded, and cloud applications globally.
 - The de facto root of trust—deploying more than 86,000 key managers and protecting up to 750,000,000 encryption keys.
 - Control access to the most sensitive corporate information—more than 35 million identities protected via tokens, smartcards, and mobile devices managed on-premise and in the cloud.
- **NetApp® Cloud Backup Encryption.** Helps The State of West Virginia securely back up data to any cloud (private or public) at up to 90% less cost compared to on-premise solutions. You can now include the public and private cloud as part of backup and recovery, and archiving strategies for cost-effective data protection. Cloud Backup can achieve faster recovery, reduce data loss, and deliver ironclad security, all with minimal management overhead. The Cloud Backup solution provides data at rest encryption using FIPS 140-2 with the AES-256 standard for both cloud and local cached data. In addition, the Cloud Backup solution retains all NetApp storage efficiencies by encrypting data after deduplication and compression further enhancing the effectiveness of the solution. Moreover, onbox (OKM) and external key management solutions are supported.
 - **NetApp® SolidFire®.** Provides the agility to deploy new applications and capabilities faster with all flash storage arrays. It increases security by leveraging always on data at-rest encryption using FDE drives with AES 256-bit drive based encryption and onboard key management for ease of deployment. In addition, the SolidFire solution leverages local and LDAP based authentication and secure control plane access with TLS and SSHv2.
 - **Cloud Volumes ONTAP.** Leverages the power of the ONTAP software solution to deliver enterprise class data storage management across cloud vendors, while ensuring security through the use of software based data at-rest encryption (using the XTS-AES algorithm) and external key management with Cloud Volumes ONTAP or via Amazon EBS.
 - **NetApp® SANtricity® Full Disk Encryption.** Provides a powerful and simple-to-administer tool for securing critical information and protecting against the constant threats to data at rest. SANtricity FDE utilizes AES 256-bit encryption, FIPS 140-2 level 2 manufacturer validated drives, and combines local key management with FDE-capable drives, protecting data from unauthorized access or modification resulting from theft, loss, or repurposing of the disk drives. And the simple and intuitive configuration menus offer an easy way to manage this added security. As disk drives will inevitably be removed from the data center,

E-Series systems with FDEs mitigate the risks associated with data loss: returning spares, upgrades, moving, decommissioning, and breaches.

- **NetApp® StorageGRID®.** Provides the ability to protect object storage across heterogeneous platforms, address hardware refreshes, and tiering to tape and cloud. The StorageGRID solution does this while encrypting objects with AES-256 software based encryption. In StorageGRID each object is encrypted by a unique symmetric key and the symmetric key is encrypted by the “grids” public key providing a robust security posture.

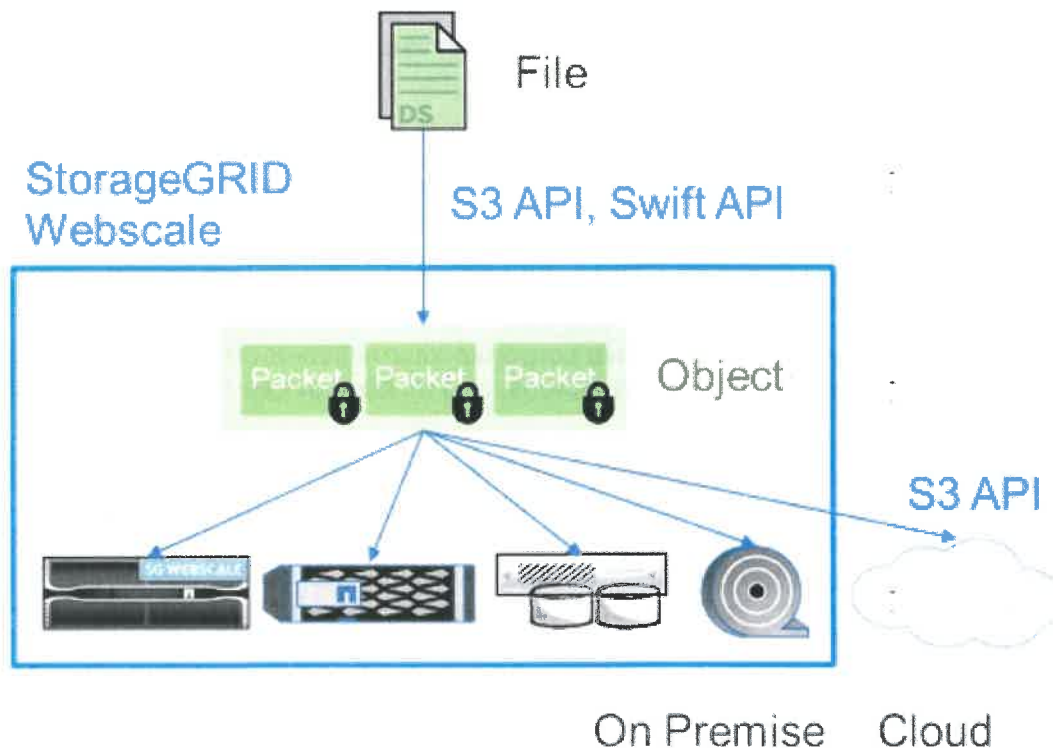


Figure 2: A typical StorageGRID architecture.

- **NetApp Security Services.** NetApp and our partners offer a large number of security services, including design and implementation of key management appliances for enterprise key management, including SafeNet KeySecure, Vormetric DSM, and others. In addition, the security services team is continually designing and deploying secure solutions throughout the NetApp portfolio, including NSE, NVE, Cloud Backup, StorageGRID, SANtricity with FDE, Cloud Volumes ONTAP, select, and SolidFire solutions.

Additional security and data migration services are also available. Please contact your account team for a Security Services engagement to address the needs and requirements of your organization.

ONTAP 9: Harness the Power of the Hybrid Cloud

NetApp ONTAP simplifies data management for any application, anywhere. Accelerate and protect data across the hybrid cloud; and future-proof your data infrastructure. The latest version, ONTAP 9.7, offers a number of enhancements, including a new management user interface and synchronous mirroring with MetroCluster.

The State of Est Virginia's transformation into a digital business brings with it pressures to be more efficient, respond quickly to new opportunities, and improve the customer experience. This might require modernizing your IT infrastructure, integrating new types and uses of data into your existing environment, and managing data on premises as well as in the cloud—yet operations must be simplified, costs reduced, and security increased.

NetApp® ONTAP 9® unifies data management across flash, disk, and cloud. It bridges current enterprise workloads and new emerging applications providing unmatched versatility, comprehensive data protection, and leading storage efficiency. NetApp ONTAP 9.7 is the latest generation of the leading data management software that delivers the performance, data resiliency, protection, and scalability that you need for your data infrastructure. ONTAP 9.7 continues to build the foundation for a modern data fabric. You can easily harness the power and agility of the hybrid cloud to get the most value from your data wherever you need it—at the edge, in the data center, or in the cloud. This latest release of ONTAP software is well suited for enterprise business applications and for artificial intelligence (AI) and real-time analytics.

Leverage ONTAP 9 to:

- Simplify operations and reduce cost
- Adapt to changing business needs
- Protect and secure data across the hybrid cloud

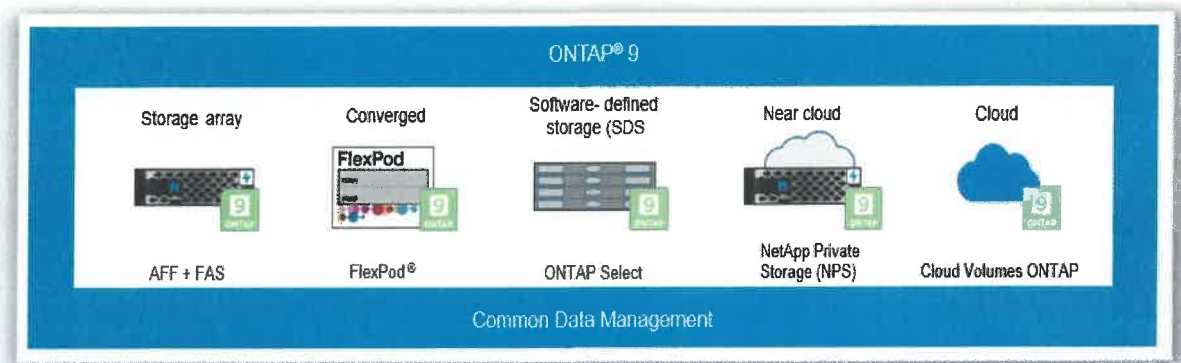


Figure 1: Standardize data management across architectures with a rich set of enterprise data services.

"Ease of use is the most valuable feature for us....With ONTAP we have more shelves, more disks, and aggregates."

— Peggy Baladera, Storage Tec, General Dynamics Mission Systems Inc.

Simplify Operations and Reduce Costs

Although storage might double in size, it no longer means there is twice as much work required. ONTAP has a common set of features across deployment architectures that simplify complex tasks so your staff can be more productive.

Receive Proven Storage Efficiency

With ONTAP, you can reduce costs with one of the most comprehensive storage efficiency offerings in the industry. You get NetApp Snapshot™ copies, thin provisioning, as well as replication and cloning technologies. You also get inline data compression, inline deduplication, and inline compaction that work together to reduce data management costs and maximize effective capacity. In addition, FabricPool automates the cost-efficient tiering of cold data to both public and private clouds.

Deploy Workloads in Less Than 10 Minutes

Fast provisioning workflows enable the deployment of key workloads such as Oracle, SQL Server, SAP HANA, VDI, and VMware in less than 10 minutes from power-on to serving data. Years of NetApp experience and best practices are integrated into the System Manager wizard and factory configurations, so you can quickly set up new configurations by answering a few questions. As new workloads are deployed, ONTAP 9 gives you the visibility to know which node has the most performance capacity available for optimal deployment.

Save Time with the New Management User Interface

ONTAP System Manager has been redesigned with new dashboard page views and simpler workflows that are based on REST APIs. The new management user interface gives you the ability to easily see the status of your cluster and to take quick actions to complete management tasks or mitigate risks before they become problems. ONTAP System Manager will save you time by showing key system information about capacity, hardware health, networking, and performance history with up to one year of data. Only one screen is needed for provisioning LUNs or NAS volumes.

Simplify Operations and Unify Data Management

Simplify your operations by unifying data management across a hybrid cloud that can span flash, disk, and cloud running SAN and NAS workloads. Increase the efficiency of your staff and easily move data between nodes to where it is most needed. ONTAP is the foundation for a data fabric that gives freedom, choice, and control across your storage environment.

Automatically Tier to Cloud

You can deliver high performance to your applications and reduce storage costs by automatically tiering cold data from the performance tier to a private or public cloud. FabricPool frees up space on your existing NetApp All Flash FAS (AFF) infrastructure, so you can consolidate more workloads.

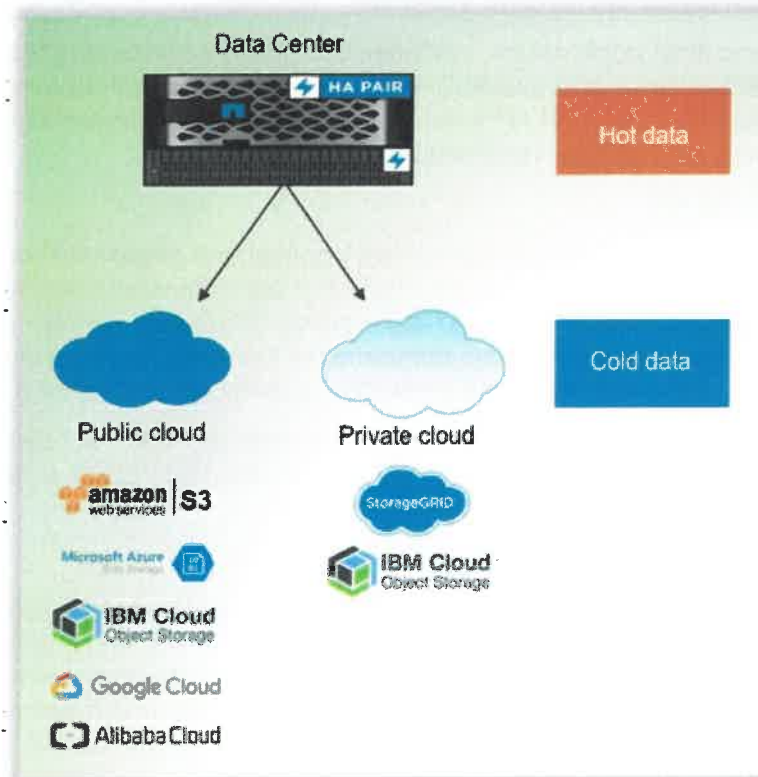


Figure 2: Automatic cloud tiering of cold data – ONTAP 9.7 enables mirroring of tiered, cold data to multiple cloud buckets, either in public clouds or in on the premises. This feature increases your flexibility to change cloud-tiering providers or locations and gives you an additional level of resiliency if one cloud tier location goes offline.

Maximize Investment Protection

ONTAP gives you the flexibility to create an integrated, scalable storage environment by clustering storage controllers from different families—AFF and FAS—as well as from different generations. Grow with the latest hardware and continue to use your older hardware. When it is time to retire a storage system, simply upgrade the controllers and keep data in place on the existing disk shelves.

Gain Simple, Powerful Management Capabilities

NetApp data management infrastructure software manages hybrid clouds. You can centrally monitor the health of your environment by viewing metrics on capacity utilization, performance, availability, and data protection. It can also help automate your storage processes and integrate them into your data center orchestration platform for end-to-end service delivery for your private and hybrid cloud services.

NetApp Active IQ® intelligence provides predictive analytics and actionable insights based on machine learning and artificial intelligence. This intelligence helps optimize your NetApp investment, simplify and automate operations, and achieve data center efficiencies.

“ONTAP has really reduced our costs because we learned that we could use our storage with fewer machines and drive down data center costs.”

— Oliver Fuckner, Systems Administrator, Strato AG

Adapt to Changing Business Needs

To support your critical applications, you need a storage environment that cost-effectively delivers high performance and availability that can also scale with business growth and protect your valuable data. ONTAP 9 delivers on all these requirements with highly efficient flash performance for scalable, nondisruptive operations.

Optimized for Flash

ONTAP 9 delivers the horsepower that critical applications require without compromising on rich data services. AFF systems running ONTAP 9 are optimized specifically for flash, including AFF systems with NVMe solid-state drives (SSDs) and NVMe over Fabrics, providing up to twice the performance compared to the same workloads running on prior ONTAP releases, while still delivering consistent submillisecond latency.

ONTAP 9 also enables FAS hybrid-flash systems to deliver flash-accelerated performance that is balanced with hard disk drives (HDD) economies. Hot data is automatically cached in flash to accelerate application performance.

Consistent Performance

Quality of service (QoS) workload management allows you to control the resources that each workload can consume, to better manage performance spikes and improve customer satisfaction. Adaptive QoS can be used to set both maximum and minimum resource levels, which is especially important for business-critical workloads, and it automatically adjusts storage resource levels to respond to changes in workloads and deliver consistent performance.

Seamless Scalability

Storage systems that run ONTAP can transparently scale from a few terabytes up to 176PB. You can scale up by adding capacity. Or scale out by adding additional storage controllers to seamlessly expand your cluster up to 24 nodes as your business needs grow. Rebalance capacity to improve service levels by redeploying workloads dynamically and avoiding hot spots. You can also isolate workloads and offer levels of service by using different controller technologies, storage tiers, and QoS policies.

In addition, ONTAP supports massive NAS containers that are easy to manage. With FlexGroup, a single namespace can grow to 20PB and 400 billion files while maintaining consistent high performance and resiliency.

Future-proof Your Data Infrastructure

ONTAP 9 provides the flexibility you need to design and deploy your storage environment across the widest range of architectures, so you can match the approach that is best for your evolving business needs:

- NetApp hardware systems: AFF all flash systems and FAS hybrid-flash systems
- Converged infrastructure: FlexPod®
- On commodity servers as software-defined storage (SDS): ONTAP Select
- Next to the cloud: NetApp Private Storage (NPS) for Cloud
- In the cloud: Cloud Volumes ONTAP

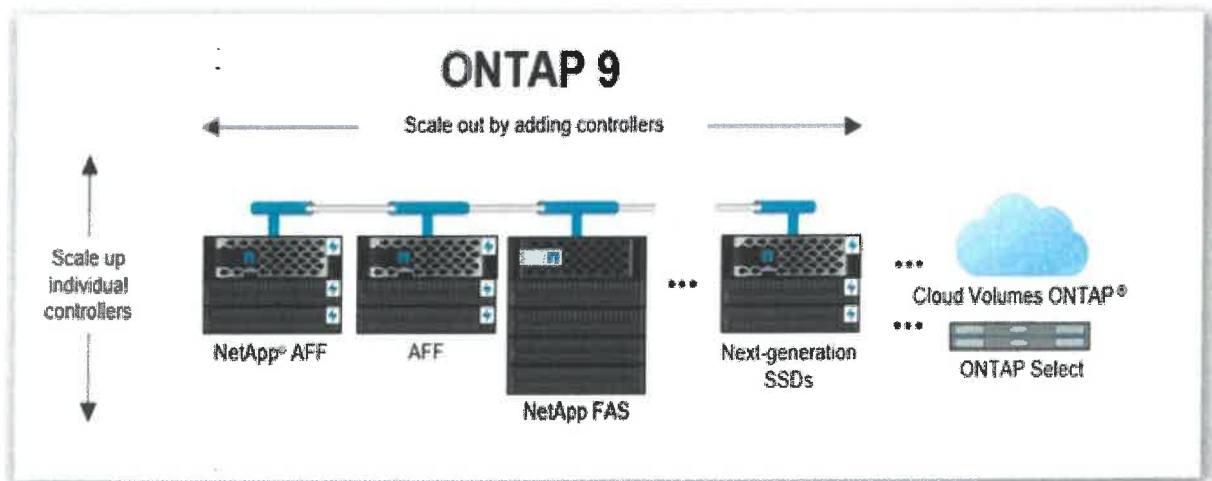


Figure 3: Scale seamlessly – Scale out by intermixing your choice of flash and hybrid-flash nodes, upgrade hardware/software or scale up without disrupting users, incorporate software-defined, cloud, and future-generation flash.

Flexibly consolidate both NAS and SAN workloads onto any ONTAP environment while delivering consistent data services. You can also seamlessly move your data between architectures to get your data onto the optimal environment for performance, capacity, and cost efficiency.

Protect and Secure Your Data Across the Hybrid Cloud

ONTAP provides comprehensive data protection so you can protect your data seamlessly across the hybrid cloud.

Integrated Data Protection and Nondisruptive Operations

NetApp offers a complete suite of Integrated Data Protection (IDP) to safeguard your operations and keep them running smoothly. You can:

- Meet your requirements for local backup with near-instant recovery by using space-efficient NetApp Snapshot copies. Application-created Snapshots that are used by third-party data protection software are replicated, as well as LUN clones.
- Achieve remote backup/recovery and disaster recovery with SnapMirror® asynchronous replication.
- Get zero data loss protection (RPO=0) for your NVMe environment with SnapMirror Synchronous replication.

NetApp MetroCluster™ technology delivers business continuity by synchronously mirroring between locations for continuous data availability. A MetroCluster storage array, leveraging FC or IP connectivity, can be deployed at a single site, across a metropolitan area, or in different cities. With the release of ONTAP 9.7, you can use your existing network infrastructure for synchronous mirroring with MetroCluster. Simultaneously mirror your tiered data out to multiple clouds. You get the flexibility to store your data at multiple cloud providers for added resiliency and it simplifies the process for changing cloud providers.

ONTAP gives you the ability to perform critical tasks without interrupting your business by dynamically assigning, promoting, and retiring storage resources without downtime over the lifecycle of an application. Data can be moved between controllers without application interruption, so you can get the data on the node that delivers the optimal combination of speed, latency, capacity, and cost.

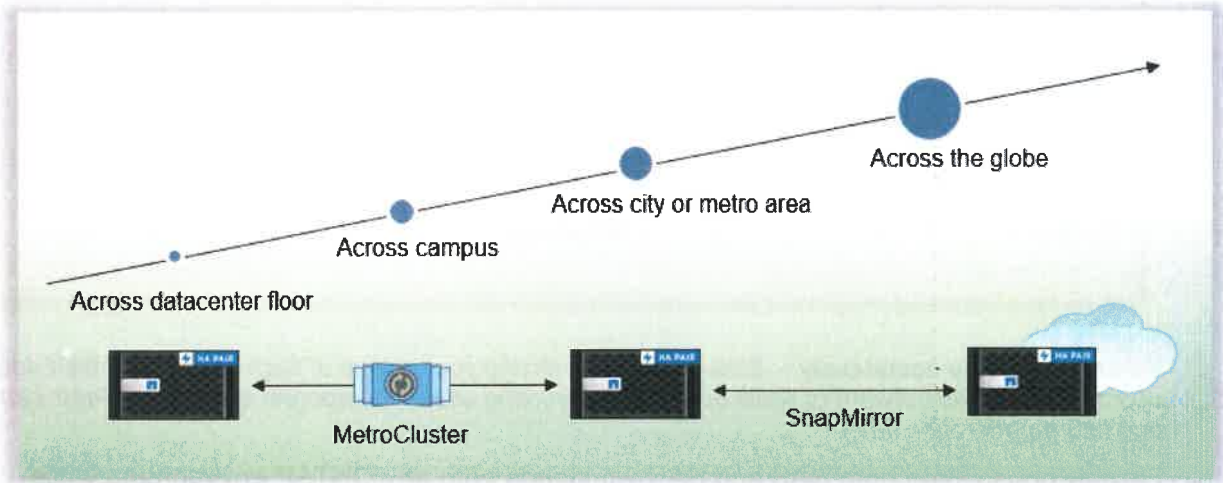


Figure 4: SnapMirror extends data protection across the globe.

“Since implementing NetApp® MetroCluster™ in 2009, Jack Wolfskin hasn’t experienced a single second of downtime or any data loss. Another advantage of MetroCluster software is that we manage upgrades from anywhere instead of coming in on the weekends.”

— Severin Canisius, Senior IT Manager

Robust Security

Security capabilities in ONTAP help you integrate data security across your hybrid cloud and avoid unauthorized data access. You can easily and efficiently protect at-rest data by encrypting any volume on an AFF or FAS system with NetApp Volume Encryption—a feature that is built in to ONTAP. It does not require special encrypting disks. In-flight encryption for backup and replication protects data in transit. Plus, other features such as multifactor authentication (MFA), role-based access control (RBAC), and onboard and external key management increase the security of your data. With ONTAP 9.7, it is simpler to protect your data by automatically enabling data at-rest encryption for new volumes when an encryption key manager is configured on the cluster. Included with ONTAP 9.7, Active IQ Unified Manager now provides a security dashboard that highlights where you can improve cluster-wide security based on best practices.

Secure Consolidation

ONTAP gives you the ability to save time and money by sharing the same consolidated infrastructure for workloads or tenants that have different performance, capacity, and security requirements without fear that the activity in one tenant partition will affect another. With multitenancy, a storage cluster can be subdivided into secure partitions governed by rights and permissions.

Rigorous Compliance

To meet stringent compliance and data retention policies, NetApp SnapLock® software enables write once, ready many (WORM) protected data for your ONTAP environment. NetApp also provides superior integration with enterprise backup vendors and leading applications. Our IDP solutions include integrated and unified disk-to-disk backup and disaster recovery in a single process for VMware and Microsoft virtualization. In addition, cryptographic shredding enables General Data Protection Regulation (GDPR) compliance.

“The secure multitenancy built into ONTAP is key to our cloud business model.”

— Frank Bounds, Senior Storage Engineer, TCDI

Simple, Straightforward Transition to ONTAP 9

No matter what your starting point, NetApp streamlines your move to ONTAP 9. You can:

- Upgrade from ONTAP 8.3 with a simple update of your ONTAP software—no disruption and zero downtime.
- Make a smooth transition from ONTAP 7-Mode with proven tools and best practices, including 7-Mode Transition Tool (7MTT) and Copy Free Transition (CFT).
- Use straightforward import processes from third-party storage to ONTAP 9.

Consult our experts to plan and implement your transition and gain the latest ONTAP advantages from day one. You can use either NetApp Services or NetApp Certified Services Partners, do it yourself using our proven tools and processes, or choose a combination of approaches.

“Using the brand-new copy-free transition process to achieve both the hardware refresh and upgrade to ONTAP with minimal business disruption was the perfect option. It reduced risk, slashed migration time, and cut costs and was something we were able to fully justify.”

— Andrew Bentley, Infrastructure Lead, Repsol Sinopec Resources UK

ONTAP Technical Highlights

The building blocks for ONTAP scale-out storage configurations are high-availability (HA) pairs in which two storage controllers are interconnected to the same set of disks. If one controller fails, the other takes over its storage and continues serving data.

With ONTAP, each storage controller is referred to as a cluster node. Nodes can be different models and sizes of AFF and FAS systems. Disks are made into aggregates, which are groups of disks of a type that are composed of one or more RAID groups protected by using NetApp RAID DP® and RAID TEC technology.

A key differentiator in an ONTAP environment is that numerous HA pairs are combined into a cluster to form a shared pool of physical resources that are available to applications, SAN hosts, and NAS clients. The shared pool appears as a single system image for management purposes. This means that there is a single common point of management, whether through the graphical user interface or command-line interface tools, for the entire cluster.

Although the members of each HA pair must be the same controller type, the cluster can consist of heterogeneous HA pairs of AFF all-flash arrays as well as FAS hybrid-flash arrays. Over time, as the cluster grows, and new controllers are released, it is likely to evolve into a combination of several different node types. All cluster capabilities are supported, regardless of the underlying controllers in the cluster.

To improve data access in NAS applications, NetApp virtualizes storage at the file-system level. This enables all client nodes to mount a single file system, access all stored data, and automatically accommodate physical storage changes that are fully transparent to the clients. Each client or server can access a huge pool of data residing across the ONTAP system through a single mount point.

Meet High-Availability Requirements

The proven reliability features in NetApp hardware and software result in data availability of more than 99.9999% as measured across the NetApp installed base. Backup and replication technologies integrated in the NetApp ONTAP data management software help keep your applications and data continuously available to users.

Nondisruptive Operations to Eliminate Downtime

Nondisruptive operations (NDO) are fundamental to the superior scale-out architecture of NetApp ONTAP. NDO is achieved as the storage infrastructure remains up and serving data throughout the execution of hardware and software maintenance operations as well as during other IT lifecycle operations. The goal of NDO is to eliminate downtime—whether it is preventable, planned, or unplanned—and to allow changes to your systems to occur at any time.

ONTAP allows you to transparently move data and network connections anywhere within the storage cluster. The capability to move individual data volumes or LUNs allows you to redistribute across a cluster at any time and for any reason. It's transparent and nondisruptive to NAS and SAN hosts, and it enables the storage infrastructure to continue to serve data throughout these changes. This is helpful to rebalance capacity usage, to optimize for changing performance requirements, or to isolate one or more controllers or storage components when it becomes necessary to execute maintenance or lifecycle operations.

Table 1: Hardware and software maintenance operations can be performed nondisruptively with ONTAP.

Operation	Details
Upgrade software	Upgrade from one version of ONTAP to another
Upgrade firmware	System, disk, switch firmware upgrade
Replace failed controller or component within a controller	Network interface cards (NICs), host bus adapters (HBAs), and power supplies
Replace failed storage components	Cables, drives, shelves, and I/O modules

Table 2: Lifecycle operations can be performed nondisruptively with ONTAP.

Operation	Details
Scale storage	Add storage (shelves or controllers) to a cluster and redistribute volumes for future growth
Scale hardware	Add hardware to controllers to increase scalability, performance, or capability (HBAs, NICs, NetApp Flash Cache™ or Flash Pool™ caching)
Refresh technology	Upgrade storage shelves, storage controllers, back-end switch
Rebalance controller performance and storage utilization	Redistribute data across controllers to improve performance
Rebalance capacity	Redistribute data across controllers to account for future capacity growth
Rebalance disk performance and utilization	Redistribute data across storage tiers within a cluster to optimize disk performance

On-Demand Scalability—Expand as you Build

The ONTAP architecture is key to delivering maximum on-demand scalability for your shared IT infrastructure, offering performance, price, and capacity options.

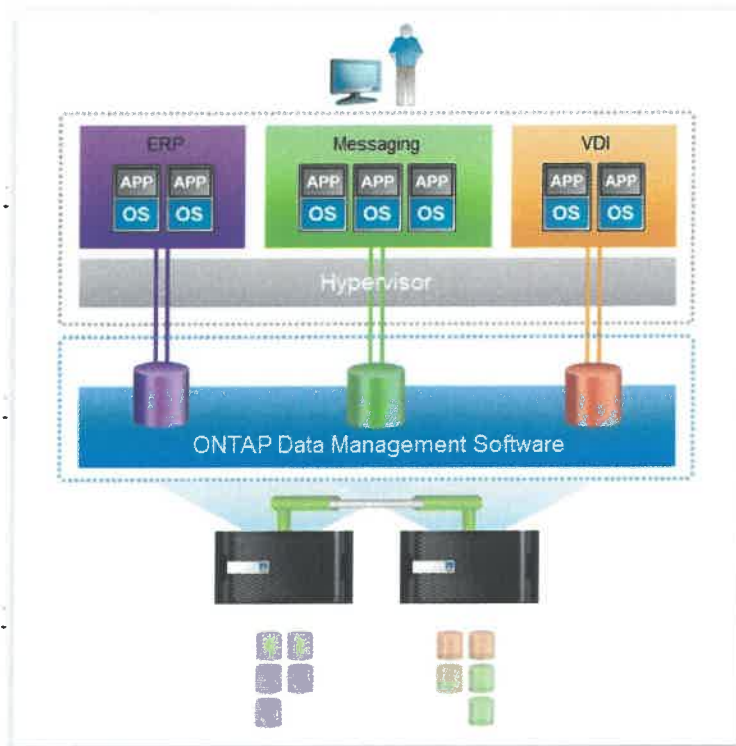


Figure 5: Expand as you build – Start with a two-node cluster and expand controllers and capacity when you need to, nondisruptively.

There are several approaches for leveraging flash in NetApp FAS hybrid-flash systems to accelerate workloads and reduce latency. Flash Cache can increase read performance for frequently accessed data. Plus, Flash Pool aggregates combine SSDs with traditional hard drives for delivering optimal performance and efficiency.

NetApp AFF all-flash systems offer the advantage of scalable performance with consistent low latency for SAN and NAS workloads. Customers can start with deploying AFF in an HA pair configuration to deliver enterprise-grade data management and high performance for a dedicated workload. If additional performance is required, AFF can scale out in a cluster—up to 24 nodes, delivering millions of IOPS at submillisecond latency and a total of over 88PB of SSD capacity.

The extra value of AFF shines when it is used as a high-performance node combined with hybrid-flash FAS systems in an ONTAP environment. This becomes a single storage repository for all workloads. And it enables nondisruptive movement of workloads to the node that best meets your performance and price/performance requirements at different points in time.

Multiprotocol Unified Architecture

A multiprotocol unified architecture provides the capability to support several data access protocols concurrently in the same overall storage system across a range of controller and disk storage types. ONTAP protocol support includes:

- SMB 1, 2, 2.1, 3, 3.1.1 (CIFS)
- NFS v3, v4, and v4.1, including pNFS
- iSCSI
- FCP (Fibre Channel Protocol)
- FCoE (Fibre Channel over Ethernet)
- NVMe over FC (NVMe/FC), starting with ONTAP 9.4

Data replication and storage efficiency features in ONTAP are seamlessly supported across all protocols.

SAN Data Services

With the supported SAN protocols (FC, FCoE, iSCSI, and NVMe/FC), ONTAP provides LUN services. This is the capability to create LUNs and make them available to attached hosts. Because the cluster consists of numerous controllers, there are several logical paths to any individual LUN. A best practice is to configure at least one path per node in the cluster. Asymmetric Logical Unit Access is used on the hosts so that the optimized path to a LUN is selected and made active for data transfer. Support for multipath I/O is also available from leading OS and third-party driver vendors.

NAS Data Services

ONTAP can provide a single namespace with the supported NAS protocols such as SMB [CIFS] and NFS (NAS clients can access a very large data container by using a single NFS mount point or CIFS share). Each client, therefore, needs only to mount a single NFS file system mount point or access a single CIFS share, requiring only the standard NFS and CIFS client code for each operating system.

The namespace of ONTAP is composed of potentially thousands of volumes joined by the cluster administrator. To the NAS clients, each volume appears as a folder or subdirectory,

nested off the root of the NFS file system mount point or CIFS share. Volumes can be added at any time and are immediately available to the clients, with no remount required for visibility to the new storage.

The clients have no awareness that they are crossing volume boundaries as they move about in the file system, because the underlying structure is completely transparent.

ONTAP can be architected to provide a single namespace, yet it also supports the concept of several securely partitioned namespaces, called Storage Virtual Machines or SVMs. This accommodates the requirement for multi-tenancy or isolation of particular sets of clients or applications.

Opex and Capex Efficiency—Grow Your Business, Not IT Expense

NetApp storage solutions operating with ONTAP 9 deliver the industry's leading storage efficiency capabilities with features such as inline compression, inline deduplication, inline data compaction, thin provisioning, and thin clones. With these features coupled with space-efficient NetApp Snapshot copies, RAID DP, and RAID TEC, you can enjoy significant reductions in required disk capacity (varies by workload) when compared with traditional storage technologies.

Table 3: ONTAP 9 offers a robust set of standard and optional features.

NetApp Software and Features		
	Function	Benefits
Data compaction	Packs more data into each storage block for greater data reduction.	Works with compression to reduce the amount of storage that you need to purchase and operate.
Data compression	Provides transparent inline and postprocess data compression for data reduction.	Reduces the amount of storage that you need to purchase and maintain.
Deduplication	Performs general-purpose deduplication for removal of redundant data.	Reduces the amount of storage that you need to purchase and maintain.
FabricPool	Automates data tiering to the cloud (public and private).	Decreases storage costs for cold data.
Flash Pool™ Caching	Creates a mixed-media storage pool by using SSDs and HDDs.	Increases the performance and efficiency of HDD pools with flash acceleration.
FlexCache®	Caches datasets within a cluster and at remote sites.	Accelerates read performance for hot datasets by increasing data throughput within a cluster and improves the speed and productivity of collaboration across multiple locations. FlexGroup volumes can now be cached with FlexCache, enabling data volumes larger than 100TB to be cached.

NetApp Software and Features

	Function	Benefits
FlexClone®	Instantaneously creates file, LUN, and volume clones without requiring additional storage.	Saves you time in testing and development and increases your storage capacity.
FlexGroup	Enables a single namespace to scale up to 20PB and 400 billion files.	Supports compute-intensive workloads and data repositories that require a massive NAS container while maintaining consistent high performance and resiliency. For enhanced security and locking, NFSv4.0 and NFSv4.1 are now supported.
FlexVol®	Creates flexibly sized volumes across a large pool of disks and one or more RAID groups.	Enables storage systems to be used at maximum efficiency and reduces hardware investment. To enable higher performance and to scale capacity, you can now convert a FlexVol volume to a single-member FlexGroup volume without copying data.
MetroCluster	Combines array-based clustering with synchronous mirroring to deliver continuous availability and zero data loss; up to 700km distance between nodes.	Maintains business continuity for critical enterprise applications and workloads if a data center disaster occurs.
Performance capacity	Provides visibility of performance capacity that is available for deploying new workloads on storage nodes.	Simplifies management and enables more effective provisioning of new workloads to the optimal node.
QoS (adaptive)	Simplifies setup of QoS policies and automatically adjusts storage resources to respond to workload changes (number of TB of data, priority of the workload, etc.).	Simplifies operations and maintains consistent workload performance within your prescribed minimum and maximum IOPS boundaries.
RAID-TEC™ and RAID DP® technologies	Provides triple parity or double-parity RAID 6 implementation that prevents data loss when three or two drives fail.	Protect your data without the performance impact of other RAID implementations; reduce risks during long rebuilds of large-capacity HDDs.
SnapCenter®	Provides host-based data management of NetApp storage for databases and business applications.	Offers application-aware backup and clone management; automates error-free data restores.

NetApp Software and Features

	Function	Benefits
SnapLock	Provides WORM file-level locking.	Supports regulatory compliance and organizational data retention requirements.
SnapMirror	Provides integrated remote backup/recovery and disaster recovery with incremental asynchronous data replication; preserves storage efficiency savings during and after data transfer.	Provides flexibility and efficiency when replicating data to support remote backup/recovery, disaster recovery, and data distribution.
SnapMirror Synchronous	Delivers incremental, volume-granular, synchronous data replication; preserves storage efficiency savings during and after data transfer.	Achieve zero data loss protection (RPO=0).
SnapRestore®	Rapidly restores single files, directories, or entire LUNs and volumes from any Snapshot copy.	Instantaneously recovers files, databases, and complete volumes from your point-in-time Snapshot copy.
Snapshot	Makes incremental data-in-place, point-in-time copies of a LUN or a volume with minimal performance impact.	Enables you to create frequent space-efficient backups with no disruption to data traffic.
Volume encryption	Provides data-at-rest encryption that is built into ONTAP.	Easily and efficiently protect your at-rest data by encrypting any volume on an AFF or FAS system; no special encrypting disks are required.

Attachment #8

ONTAP 9 Security Features

NetApp® ONTAP® storage management software continues to evolve, with security as an integral part of the solution. The State of West Virginia can simplify and strengthen your security posture by integrating data security throughout your hybrid cloud. You can help meet governance, risk, and compliance requirements such as HIPAA, PCI-DSS, and GDPR and cost effectively secure your NetApp ONTAP environment by incorporating industry-standard, built-in security that meets FIPS 140-2 compliance.

The latest release, ONTAP 9, contains many new security features and functions that are invaluable for protecting your security posture and helping your organization adhere to industry best practices. These new features make data confidentiality, integrity, and availability top priorities. As an example, the State of West Virginia can easily and efficiently protect at-rest data with NetApp Storage Encryption (NSE)—that uses self-encrypting drives. Or encrypt any volume and any disk across FAS, AFF, and ONTAP Select deployments with NetApp Volume Encryption (NVE)—that does not require special encrypting disks. Key management can be delivered in a self-contained encryption solution using Onboard Key Manager, included with ONTAP, or with external key management solutions that provide separation of duties and a centralized key repository. The new and existing security features and functions in the ONTAP 9 solution give The State of West Virginia the ability to:

- **Enhance data confidentiality, integrity, and availability.** Apply the NetApp ONTAP 9 Data Fabric security constructs to solidify the confidentiality, integrity, and availability of the State of West Virginia’s most important resource: data.
- **Create a security posture for your environment.** Establish a secure foundation in your organization’s data fabric and understand the visibility and security functions that create a secure infrastructure.
- **Apply NetApp and industry best practices for security.** Establish a vetted security footprint with help from NetApp expertise, industry knowledge, and common practices.
- **Satisfy governance and compliance requirements.** Apply established security best practices to adhere to and support industry regulation and security compliance.

The following table outlines the function and impact of ONTAP security features.

Table 1: ONTAP security features.

New Security Features in ONTAP 9		
Software or Feature	Function	Impact
NetApp Volume Encryption	NVE is a software-based encryption mechanism that enables The State of West Virginia to encrypt data on any type of disk.	Data encryption at rest continues to be an industry focus. NVE maintains a strong security posture across the full breadth of the NetApp Data Fabric.
SMB encryption uses Advanced Encryption Standard (AES)-New Instructions (NI) acceleration	Intel AES NI improves on the AES algorithm and accelerates data encryption with supported processor families.	Accelerating security functions provides efficiency. Efficient use of resources is pivotal to providing successful security solutions.
NetApp Cryptographic Security Module (NCSM)	NCSM provides FIPS 140-2–compliant cryptographic	Dedicated security modules improve resource efficiency. In addition,

New Security Features in ONTAP 9

	operations for select SSL-based management services.	FIPS 140-2 is the recognized industry standard for cryptography products and solutions,
SHA-2 (SHA-512) support	To enhance password security, ONTAP 9 supports the SHA-2 password hash function and defaults to using SHA-512 for hashing newly created or changed passwords.	SHA-2 has become the industry standard for hash functions because of its improved security posture relative to the often-infiltrated SHA-1 standard.
Secure Log Forwarding (Syslog over Transport Layer Security [TLS])	The log forwarding function enables administrators to provision targets or destinations so that they can receive syslog and audit information. Because of the secure nature of syslog and audit information, ONTAP can send this information securely through TLS using the TCP-encrypted parameter.	Log and audit information is invaluable to an organization for support and availability. In addition, the information contained in logs (syslogs) and audit reports and outputs is typically sensitive in nature. To maintain security controls and posture, you must manage log and audit data in a secure manner.
TLS v1.1 and TLS v1.2	ONTAP applies TLS v1.1 and TLS v1.2 for secure communication and administration functions.	NetApp does not recommend using TLS v1.0 because its significant vulnerabilities make it incompatible with compliance standards such as PCI-DSS. NetApp recommends using TLS v1.1 and TLS v1.2 because of their strength and integrity.
Onboard Key Manager (OKM)	OKM in ONTAP 9 provides a self-contained encryption solution for data at rest. OKM works with NVE, which offers a software-based encryption mechanism that enables The State of West Virginia to encrypt data and use any type of disk. OKM also works with NSE, which performs full-disk encryption by using self-encrypting drives.	OKM provides key management for NSE and NVE. The use of this encryption technology in ONTAP enables The State of West Virginia to secure data at rest, which is critical for any security solution.
Enhanced file system auditing	ONTAP 9 increases the number of auditing events and details that are reported across the solution. The following key details are logged with the creation of events: <ul style="list-style-type: none"> • File • Folder • Share access 	NAS file systems have increased their footprint in today's threat landscape. Therefore, the visibility provided by audit functions remains critically important and the increased audit capability in ONTAP 9 provides more CIFS audit details than ever before.



New Security Features in ONTAP 9

- Files created, modified, or deleted
- Successful file read access
- Failed attempts to read fields or write files
- Folder permission changes

CIFS SMB signing and sealing

SMB signing helps protect the security of The State of West Virginia's data fabric by protecting the traffic between storage systems and clients from replay or man-in-the-middle attacks. SMB signing also makes sure that SMB messages have valid signatures. In addition, ONTAP supports SMB encryption, also known as sealing.

A common threat vector for file systems and architectures lies within the SMB protocol. Signing and sealing enables unadulterated validation of traffic in addition to secure data transport on a share-by-share basis.

Kerberos 5 and Krb5p support

ONTAP supports 128-bit and 256-bit AES encryption for Kerberos. The privacy service includes the verification of received data integrity, user authentication, and data encryption before transmission.

Krb5p authentication protects against data tampering and snooping by using checksums to encrypt all traffic between client and server.

Lightweight Directory Access Protocol (LDAP) SMB signing and sealing

ONTAP 9 supports signing and sealing to protect session security on queries to an LDAP server.

Signing confirms the integrity of the LDAP payload data using secret-key technology. Sealing encrypts the LDAP payload data to avoid transmitting sensitive information in clear text.

Ed25519 and NIST curves in SSH (updated algorithms and hmacs)

ONTAP 9 provides updated SSH ciphers and key exchanges, including AES, 3DES, SHA-256, and SHA-512.

As the threat landscape evolves, the strength of the protocol algorithm, cipher, and key exchanges is vital to the integrity of the protocol and product function.

NetApp SnapLock® technology with NSE

ONTAP 9 supports NSE with the SnapLock feature, which provides administration and storage for write once, read many (WORM) data.

SnapLock technology creates special-purpose volumes in which files can be stored and committed to a nonerasable, nonrewritable state. This state can be preserved indefinitely or for a designated retention period while maintaining the secure posture (encryption) of the NSE solution.

Table 2: ONTAP security features.

Existing ONTAP Security Features		
Software or Feature	Function	Impact
NetApp Storage Encryption	NSE is the NetApp implementation of full-disk encryption using self-encrypting drives. NSE provides a nondisruptive encryption implementation that supports the entire suite of NetApp storage efficiency technologies.	Data encryption at rest continues to be an industry focus. NSE provides full-disk encryption and makes sure that the full breadth of the NetApp Data Fabric maintains a strong security posture from end to end.
Role-based access control (RBAC)	RBAC in ONTAP gives administrators the ability to limit or restrict users' administrative access to the level granted for their defined role. It allows administrators to manage users by their assigned role.	Access control is a foundational element for creating a security posture. Functions such as RBAC give The State of West Virginia the ability to determine who has data access and to what extent they have such access. This capability limits vulnerabilities and exploits, including data exfiltration and escalation of privileges.
Aggregate encryption for Cloud Volumes ONTAP	Cloud Volumes ONTAP creates an encryption key for each aggregate on the system and sends it to the key managers. Administrators can view the ID for these keys from Cloud Manager. Keys must be deleted by the administrator because they are not automatically deleted.	The individual encryption keys for each aggregate improve secure-key management, which is critical for a secure solution.
Antivirus connector (virus scanning)	Virus scanning is performed on Vscan servers that run the antivirus connector and antivirus software. Typically, the system running ONTAP is configured to scan files when they are modified or accessed by a client.	Threat and attack vectors continue to grow. Inline virus scanning of accessed or modified files protects the integrity of an organization's files.
Login and message of the day banners	Login banners are printed in the output prior to authentication. These banners allow organizations and administrators to communicate with system users.	Login banners enable organizations to present operators, administrators, and even miscreants with terms and conditions of acceptable use for a system. The banners also indicate who has permission to access the system.
Logging	Log and audit information is invaluable to an organization for support and availability. In addition, the information and	The offloading of syslog information is necessary to limit the scope or footprint of a breach to a single system or solution.



Existing ONTAP Security Features

	<p>details contained within logs (syslogs) and audit reports or outputs are generally of a sensitive nature. Organizations must manage log and audit data in a secure manner to maintain security controls and posture</p>	
External key management	<p>External key management is handled with a 3rd party system in the storage environment that securely manages authentication keys used by encryption features in the storage system, such as NSE. The storage system uses an SSL connection to contact the external key-management server and store and retrieve authentication keys with the Key Management Interoperability Protocol.</p>	<p>External key management centralizes an organization's key management functions and also stores keys away from system assets, reducing the likelihood of compromise.</p>
KRB5i	<p>The krbp5 authentication mode is secure and protects against data tampering and snooping by using checksums to encrypt all traffic between the client and server. ONTAP supports 128-bit and 256-bit AES encryption for Kerberos. This privacy service verifies the integrity of received data, authenticates users, and encrypts data before transmission.</p>	<p>Krbp5 integrity checksums are an evolution in Kerberos authentication. These checksums verify that authentication communications were not edited or altered.</p>
SMBv3 signing and sealing	<p>ONTAP 9 supports signing and sealing to enable session security on traffic between the storage system and the client.</p>	<p>Signing confirms the integrity of the SMB payload data using secret-key technology. Sealing encrypts the SMB payload data to avoid transmitting sensitive information in clear text.</p>
Sanitizing a disk	<p>Disk sanitization enables The State of West Virginia to remove data from a disk or set of disks so that the data can never be recovered.</p>	<p>Security protocols often require you to make data unrecoverable from a disk. The sanitize disk function provides this capability.</p>
NetApp FPolicy® technology	<p>FPolicy is an infrastructure component of ONTAP that enables partner applications to monitor and set file access permissions. File policies can</p>	<p>Access control is a key security construct. As such, visibility and the ability to respond to file access and file operations is critical for maintaining your security posture.</p>



Existing ONTAP Security Features

be set based on file type. FPolicy determines how the storage system handles requests from individual client systems for operations such as create, open, rename, and delete. Note: Beginning with ONTAP 9, the FPolicy file access notification framework is enhanced with filtering controls and resiliency against short network outages.

To provide visibility and access control to files, the ONTAP solution uses the FPolicy feature.

IBM Spectrum Protect

Trusted backup and recovery software solutions

Highlights

- Multi-workload data protection lowers operational costs
- Tremendous scalability to support massive data growth
- Storage efficiency with incremental forever backups and compression
- Cyber resiliency support provides always-on data monitoring
- Data retention options including cloud and on-premises storage
- Leverage for data retention and disaster recovery

It can be challenging for organizations to manage the cost, complexity and capabilities of their backup systems, especially when they collect, process and store more information than ever before. Backup administrators feel pressure of increasingly stringent compliance demands such as multi-modal delivery models, growing infrastructure complexity, flat IT budgets, and increasing regulation and compliance requirements, such as those stemming from the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and the General Data Protection Regulation (GDPR).

IBM Spectrum Protect™ provides scalable data protection for physical file servers, applications, and virtual environments. Organizations can scale up to manage billions of objects per backup server. They can also reduce backup infrastructure costs with built-in data efficiency capabilities and migrate data to tape, public cloud services and on-premises object storage. IBM Spectrum Protect can also be a data offload target for IBM Spectrum Protect Plus, providing ability to leverage your existing investment for long-term data retention and disaster recovery.

Simplified backup administration

Backups can be managed by IBM Spectrum Protect Operations Center, VMware vSphere Client or third-party software. IBM Spectrum Protect Operations Center delivers breakthrough visibility and ease of use for backup administrators, reducing the level of expertise required. Server administrators can restore individual virtual machines from the VMware vSphere Client or launch the IBM Spectrum Protect VMware graphical user interface to schedule, monitor and perform backups.

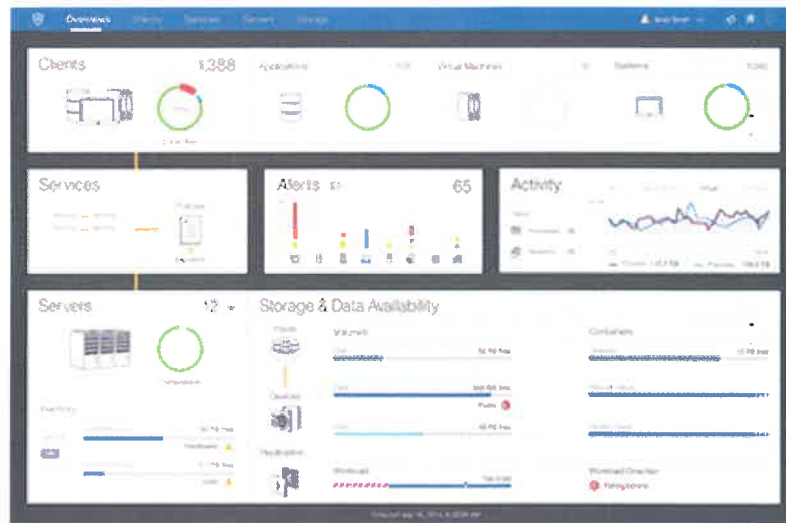
IBM [Spectrum Protect blueprints and configuration scripts](#) are designed to help reduce deployment time and guesswork by automating deployment steps and integrating best practices for small, mid-sized and large environments.

Simplified solution bundles—such as IBM Spectrum Protect Suite and IBM Spectrum Storage Suite—help clients get up and running fast with easy-to-manage licensing for IBM Spectrum Protect that includes snapshots and popular backup agents for virtual environments, databases, email and enterprise resource planning.

Built-in cloud integration

Backup to the cloud or backup in the cloud is simple, secure and cost-effective with IBM Spectrum Protect. IBM Spectrum Protect container storage pools enable external cloud and object storage without additional hardware or gateways on popular cloud environments such as IBM SoftLayer, IBM Cloud Object Storage, Amazon Simple Storage Service (Amazon S3), and now Microsoft Azure Blob storage. These container storage pools include in-line deduplication for efficient use of space and bandwidth as well as encryption to ensure that your data is secure.

IBM Spectrum Protect also provides Representational State Transfer (REST) application programming interfaces (APIs) and OpenStack backup drivers. Front-safe portal software, available from IBM, enables multi-tenancy, on-boarding and billing for IBM Spectrum Protect. IBM Resiliency Services and IBM Business Partners offer a number of cloud-based data protection solutions for pay-as-you-go backup and recovery in the cloud.²



IBM Spectrum Protect Operations Center provides an advanced visual dashboard, built-in analytics and integrated workflow automation features to dramatically simplify backup administration.

Reduced backup infrastructure costs

IBM Spectrum Protect can help users save up to 53 percent¹ in backup infrastructure costs. Savings are typically found in storage media, backup servers, data center floor space, power and cooling. IBM Spectrum Protect high-performance deduplication, compression and incremental forever capabilities work together to reduce backup storage requirements.

IBM Spectrum Protect efficiency capabilities are enabled entirely in software. Additional hardware-based appliances aren't needed for deduplication, encryption, network acceleration or cloud access.

For maximum cost flexibility, IBM Spectrum Protect enables a broad choice of storage options for backup data, including flash, disk, tape, object stores and public clouds.

Scalable performance

Organizations of all sizes need advanced data-protection capabilities. Organizations with fewer than 50 managed servers or less than 100 terabytes of backup data can choose specially priced IBM Spectrum Protect entry-level solution bundles.

IBM Spectrum Protect servers can expand to manage billions of objects per server, so there is less disruption and complexity as backup workloads grow.

As data grows, IBM Spectrum Protect backups can be augmented with advanced agents and snapshots that can reduce backup and restore times for large applications and virtual machines. For example, IBM Spectrum Protect Snapshot can back up 500 VMware virtual machine images

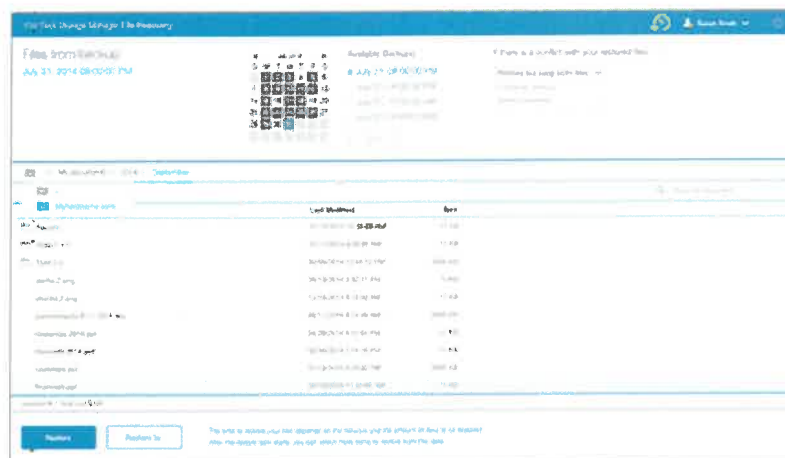
in as little as seven minutes.³

Backup information can also be replicated between IBM Spectrum Protect servers, either on-premises or hosted in the cloud. IBM Spectrum Protect Extended Edition includes policy-driven remote replication, which can significantly reduce storage space requirements at primary backup sites. Organizations needing faster data transfer can enable the IBM Spectrum Protect High Speed Data Transfer option, which uses patented IBM Fast, Adaptive and Secure Protocol (IBM FASP) technology to transfer data faster than TCP over high-latency or high-loss networks.

Optimized data protection

IBM Spectrum Protect is a complete solution. It enables advanced data protection for current and next-generation environments, including cloud, virtualized and software-defined environments; core applications; and remote facilities. Data managed by IBM Spectrum Protect is easily replicated to off-site recovery facilities for safekeeping.

Backups are important, but restores are essential. IBM Spectrum Protect solutions enable fast, flexible restores from primary and remote recovery sites. IBM Spectrum Protect helps recover individual items, complex systems and entire data centers. Recovery simulators provide assurance that systems can be recovered as expected.



A self-service restore portal enables data, server and application owners to easily recover their data.

Virtualized, software-defined infrastructures

IBM Spectrum Protect for Virtual Environments and IBM Spectrum Protect Snapshot can back up and restore data residing in virtual, software-defined environments without negatively impacting applications and operations that share the underlying physical resources. IBM offers a choice in data protection options, including incremental “forever” backups and hardware-assisted snapshots.

Flexible restores

Flexible recovery options in IBM Spectrum Protect are designed to simplify common restore requests, including:

- Self-service restore portal, initially for VMware data
- Individual item, database, volume-level, and data store restores from snapshots
- Near-instant access to backup data for Microsoft Windows and Linux Intel-based servers and Windows workstations
- Snapshot copying, browsing and recovery
- Automatic restores from an alternate backup server, if the primary backup server is unavailable
- Simplified disaster-recovery audits, recovery simulators and guided recovery from disasters

Multi-site replication

IBM Spectrum Protect Extended Edition enables backup data to be replicated on an incremental, scheduled or per-client basis from one IBM Spectrum Protect server to another. Replication is policy-driven, so on-site and off-site retention policies can be different. Plus, replication can be performed with deduplicated data, which improves network efficiency. It can also be scheduled during relatively quiet times to help reduce the impact on production applications.

In replicated environments, a remote IBM Spectrum Protect server can be used as a hot standby. Alternatively, two active IBM Spectrum Protect servers can replicate to each other. A single replication target can be used to consolidate data from multiple active IBM Spectrum Protect backup servers.

¹ Based on IBM assessments using Butterfly Software.

² IBM Cloud Managed Backup services can be found here: ibm.com/services/us/en/it-services/business-continuity/cloud-managed-backup; IBM Business Partners offering IBM Spectrum Protect-based cloud services can be found here: ibm.com/partnerworld/wps/servlet/ContentHandler/isv_com_dvm_techval_tivoli_BackupByTSM

³ Performance based on IBM measurements in a controlled environment.

Advantages of IBM data protection for virtual machines

Feature	Benefits	VMware	Hyper-V
Auto-discovery of new virtual machines	Helps ensure that all data in the virtualized environment is protected	•	•
Self-service restore portal	Enables data, server and application owners to easily recover their data	•	
Item-level recovery	Enables fast recovery of individual files, Microsoft Exchange mailboxes, emails and Microsoft SQL Server databases	•	•
Application-consistent backup and recovery	Helps ensure complete application backups and simplifies restore processes	•	•
Copy management	Enables a single virtual-machine snapshot to be used for data recovery, testing, development, etc.	•	•
Integration with hardware snapshots	Enables faster snapshots with less impact on application performance	•	
Incremental forever backups	Reduces the need for extra backup system capacity	•	•
Data deduplication	Enables high-performance space reduction on the virtual machine or backup server	•	•
Nondisruptive, single-pass backups	Helps increase application performance during backups	•	•
Agentless support	Helps simplify deployment	•	•
Tape support	Helps reduce costs for long-term storage	•	•
Instant access/instant restore	Helps reduce the user impact during virtual machine restores	•	
Single-pass, full datastore recovery	Provides near-instant recovery of an entire datastore, including all virtual machines*	•	
* Near-instant recovery for virtual machines is enabled by IBM Spectrum Protect for Virtual Environments; near-instant recovery for Windows desktops and laptops is enabled by IBM Spectrum Protect for Workstations.			

IBM integration with VMware tools and APIs

Feature	Benefits
VMware vSphere Web Client support	Allows VMware administrators to easily perform data protection and recovery operations, powered by IBM Spectrum Protect, and launched within the familiar vSphere interface
VMware vSphere Web Client Native HTML5 support	Enables VMware administrators to use a consistent UI built on new VMware Clarity UI standards, cross-browser and cross-platform independent and with no browser plug-ins to install/manage
VMware vCenter integration	Enables VMware administrators to easily configure, schedule, and monitor backups and snapshots
VMware vStorage API support	Helps reduce compute, storage and network overhead

IBM Spectrum Protect at a glance

<p>Backup server components</p> <ul style="list-style-type: none"> • IBM Spectrum Protect - Automates data backup and restore functions, supports a broad range of platforms and storage devices, reduces the data storage footprint and maintains a catalog of protected data • IBM Spectrum Protect Plus - Provides near-instant recovery, replication, reuse, and self-service for virtual machines, databases, and applications in hybrid multicloud environments • IBM Spectrum Protect Extended Edition - Adds disaster-recovery management, node replication, network data management protocol (NDMP) backup and large tape library support • IBM Spectrum Protect Operations Center - Provides an at-a-glance view of the IBM Spectrum Protect environment, which simplifies reporting and enables faster problem resolution; included with IBM Spectrum Protect • IBM Spectrum Protect High Speed Data Transfer - Improves throughput over high latency, high-packet-loss wide area networks • IBM Spectrum Protect for Data Retention - Enables long-term record retention with flexible hold and release processing • IBM Spectrum Protect for SAN - Enables SAN-attached IBM Spectrum Protect servers and user systems to use Fibre Channel connections to storage systems for data backup • Front-safe Cloud Portal - Enables multi-tenancy, on-boarding, and billing for IBM Spectrum Protect
<p>Backup agent for virtual environments and core applications—Enables high-performance, online backups and flexible restores, which can increase application availability</p> <ul style="list-style-type: none"> • IBM Spectrum Protect for Virtual Environments - Works with VMware and Microsoft Hyper-V virtual servers and hosted applications • IBM Spectrum Protect for Mail - Works with IBM Domino and Microsoft Exchange • IBM Spectrum Protect for Databases - Works with Oracle and Microsoft SQL Server; IBM DB2 and IBM Informix include IBM Spectrum Protect backup agents • IBM Spectrum Protect for Enterprise Resource Planning - Works with SAP and SAP HANA • DocAve Backup and Restore for Microsoft SharePoint Backup - Works with Microsoft SharePoint • OpenStack IBM Tivoli Storage Manager backup driver—Included in OpenStack distribution
<p>Snapshot management</p> <ul style="list-style-type: none"> • IBM Spectrum Protect Snapshot - Enables application-aware, virtual machine-aware, hardware-assisted snapshot backup and recovery management for most major IBM and non-IBM storage systems • Rocket Device Adapter Pack for IBM Tivoli Storage FlashCopy Manager - Expands IBM Spectrum Protect Snapshot platform support to include several EMC, Hitachi and HP storage devices and NetApp clusters connected to UNIX servers
<p>Bare machine recovery and recovery simulators</p> <ul style="list-style-type: none"> • IBM Tivoli Storage Manager for System Backup and Recovery - Offers a comprehensive system backup, restore and reinstallation tool with bare-metal restore capabilities for IBM AIX • Cristie Bare Machine Recovery software for Tivoli Storage Manager, TBMR - Provides rapid recovery from IBM Spectrum Protect backups, without having to perform any other backup of the operating system files • Recovery Simulator for TBMR - Tests whether a machine can be successfully recovered from backups created by Cristie TBMR and IBM Spectrum Protect • Recovery Simulator for Tivoli Storage Manager for Virtual Environments - Tests whether a machine can be successfully recovered from backups created by Cristie TBMR and IBM Spectrum Protect for Virtual Environments
<p>Continuous data protection</p> <ul style="list-style-type: none"> • IBM Spectrum Protect for Workstations - Provides continuous, automated backup of desktop and laptop workstations running Windows operating systems
<p>Hierarchical space management (HSM) - Enables policy-based migration of inactive data to tape, leaving the directory structure on disk so users don't have to change the way they access their files</p> <ul style="list-style-type: none"> • IBM Spectrum Protect HSM for Windows - Works with Windows data • IBM Spectrum Protect for Space Management - Works with AIX and Linux data

IBM Spectrum Protect solution bundles at a glance

	IBM Spectrum Protect Suite - Front End	IBM Spectrum Protect Suite
Available components		
IBM Spectrum Protect	Extended Edition	Extended Edition
IBM Spectrum Protect Snapshot	•	•
IBM Spectrum Protect for Virtual Environments	•	•
IBM Spectrum Protect for Mail	•	•
IBM Spectrum Protect for Databases	•	•
IBM Spectrum Protect for Enterprise Resource Planning	•	•
IBM Spectrum Protect backup-archive client for file systems	•	•
IBM Spectrum Protect for Storage Area Networks	•	•
IBM Spectrum Protect for Space Management	•	•
Entry option	•	•
IBM Spectrum Protect Plus	•	•
Archive option		•
IBM ProtecTIER option		•
IBM Cloud Object Storage		•
License plan		
Per component	Unlimited	Unlimited
Per capacity	License by capacity protected by the products in the bundle	License by capacity used for managed backup data, measured after deduplication and other efficiency features are used
Entry offerings (some restrictions apply)		
	IBM Spectrum Protect Suite Entry - Front End	IBM Spectrum Protect Suite Entry
Capacity	100 TB of managed backup data, measured by capacity protected by the products in the bundle	100 TB of managed backup data, measured after deduplication and other efficiency features are used

Why IBM?

IBM data protection solutions offer a simplified user experience that helps deliver superior business outcomes. IBM is using applied analytics to make backup and storage management software more intelligent, so users can deliver global data availability. IBM continues to innovate, bringing first-to-market capabilities—built on a solid foundation of trusted technology—to increasingly complex backup and recovery environments.

For more information

To learn more about IBM Spectrum Protect, including platforms supported and system requirements, contact your IBM representative or IBM Business Partner, or visit:

ibm.com/systems/storage/spectrum/protect

© Copyright IBM Corporation 2020.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at <https://www.ibm.com/legal/us/en/copytrade.shtml>, and select third party trademarks that might be referenced in this document is available at https://www.ibm.com/legal/us/en/copytrade.shtml#section_4.

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:

IBM®, IBM SoftLayer®, IBM FASP®, IBM Domino®, IBM DB2®, IBM Informix®, IBM Tivoli®, IBM Tivoli Storage FlashCopy®, IBM AIX®, IBM ProtecTIER®, IBM Power®, IBM Spectrum Protect™, IBM Spectrum Storage™, IBM Resiliency Services™



Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.



Highlights

- Gain comprehensive visibility into security data from a single console
 - Reduce thousands of events into a manageable list of prioritized offenses
 - Analyze network, endpoint, asset and user data to quickly detect threats
 - Simplify compliance with automated data ingestion, correlation and reports
 - Integrate threat intelligence from IBM® and third-parties using STIX/TAXII
 - Achieve a quick time-to-value with over 450 default setting integrations
 - Deploy a scalable platform on-premises, in the cloud or as a hybrid model
-

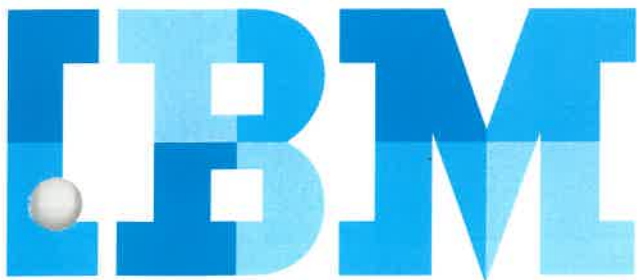
IBM QRadar SIEM

Today's networks are more complex than ever before, and protecting them from increasingly malicious and sophisticated attackers is a never-ending task. Organizations seeking to protect their customers' identities, safeguard their intellectual property and avoid business disruption need to proactively monitor their environment so that they can rapidly detect threats and accurately respond before attackers are able to cause material damage.

IBM QRadar® Security Information and Event Management (SIEM) is designed to provide security teams with centralized visibility into enterprise-wide security data and actionable insights into the highest priority threats. As a first step, the solution ingests a vast amount of data throughout the enterprise to provide a comprehensive view of activity throughout on-premises and cloud-based environments. As data is ingested, QRadar applies real-time, automated security intelligence to quickly and accurately detect and prioritize threats. Actionable alerts provide greater context into potential incidents, enabling security analysts to swiftly respond to limit the attackers' impact. Unlike other solutions, only QRadar is purpose-built to address security use cases and intentionally designed to easily scale with limited customization effort required.

Gain comprehensive, centralized visibility

Enterprise networks can span across traditional on-premises IT, cloud-based and operational technology (OT) environments, all of which require some level of oversight to effectively protect assets, accurately detect threats and maintain compliance. Before security teams can start analyzing data to detect and manage threats, they must first have centralized visibility into disparate security data. QRadar enables organizations to gain centralized, comprehensive visibility into siloed environments by collecting, parsing and normalizing both log and flow data.



The solution includes more than 450 pre-built Device Support Modules (DSMs), which provide default setting integrations with commercial off-the-shelf technologies. Customers can simply point logs to QRadar, and the solution can automatically detect the log source type and apply the correct DSM to parse and normalize the log data. As a result, QRadar customers can get up and running much faster than customers of alternative solutions. Additional integrations can easily be added via apps in the IBM Security App Exchange. QRadar also offers a simple DSM Editor with an intuitive graphical user interface GUI that enables security teams to easily define how to parse logs from custom applications.

To help easily establish the asset database, which enables organizations to define critical assets or network segments, QRadar can inspect network flow data to automatically identify and classify valid assets on the network based on the applications, protocols, services and ports they use.

QRadar supports a wide variety of technologies, applications and cloud services to help customers gain comprehensive visibility into enterprise-wide activity. Once this data is centralized, it can be automatically analyzed to identify known threats, anomalies that may indicate unknown threats and critical risks that may leave sensitive data exposed.

Automate security intelligence to rapidly detect threats

QRadar SIEM is designed to automatically analyze and correlate activity across multiple data sources including logs, events, network flows, user activity, vulnerability information and threat intelligence to identify known and unknown threats.

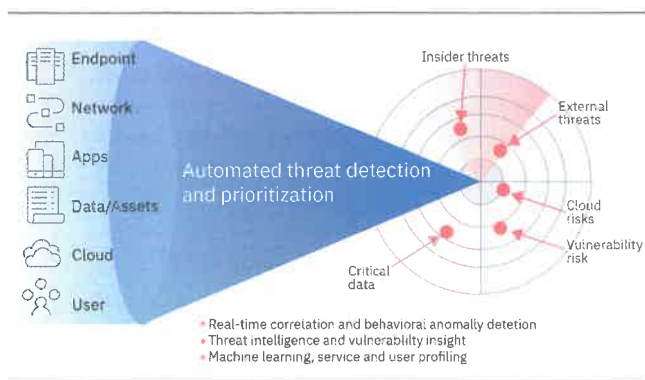


Figure 1: QRadar SIEM collects, analyzes and correlates data from a wide variety of sources to detect and prioritize the most critical threats that require investigation.

QRadar SIEM intelligently correlates and analyzes a variety of information, including the following activities:

- Security events: From firewalls, virtual private networks, intrusion detection systems, intrusion prevention systems, databases and more
- Network events: From switches, routers, servers, hosts and more
- Network activity context: Layer 7 application context from network and application traffic
- Cloud activity: From SaaS and Infrastructure as a Service (IaaS) environments, such as Office365, Salesforce.com, Amazon Web Services (AWS), Azure and Google Cloud
- User and asset context: Contextual data from identity and access management products and vulnerability scanners
- Endpoint events: From the Windows event log, Sysmon, EDR solutions and more
- Application logs: From enterprise resource planning (ERP) solutions, application databases, SaaS applications and more
- Threat intelligence: From sources such as IBM X-Force®

QRadar includes hundreds of pre-built security use cases, anomaly detection algorithms, rules and real-time correlation policies to detect known and unknown threats. As threats are discovered, the solution aggregates related security events into single, prioritized alerts known as “offenses.” Offenses are automatically prioritized based on both the severity of the threat and the criticality of the assets involved.

Within each offense, security analysts can see the full chain of threat activity from one single screen. From here, analysts can easily drill down into specific events or network flows to start an investigation, assign the offense to a specific analyst or close it out. Offenses are automatically updated as new related activity occurs so that analysts can see the most up-to-date information at any given time. This unique approach helps security analysts easily understand the most critical threats in the environment by providing end-to-end insight into each potential incident while simultaneously reducing the total alert volume.

Detect anomalous network, user and application activity

As attackers become more sophisticated in their techniques, known threat detection is no longer sufficient on its own. Instead, organizations must also have the ability to detect slight changes in network, user or system behavior that may indicate unknown threats, such as malicious insiders, compromised credentials or fileless malware.

QRadar contains a variety of anomaly detection capabilities to identify changes in behavior that could be indicators of an unknown threat. And the unique ability of QRadar to monitor and analyze Layer 7 application traffic enables it to more accurately identify anomalies that other solutions may miss.

By optionally using QRadar Network Insights as part of the SIEM deployment, organizations can gain insight into which systems communicated with each other, which applications were involved and what information was exchanged in the packets. By correlating this information with other network, log and user activity, security analysts can uncover abnormal network activity that may be indicative of compromised hosts, compromised users or data exfiltration attempts.

While QRadar ships with numerous anomaly and behavioral detection rules as default settings, security teams can also create their own rules, tailor anomaly detection settings and download over pre-built 160 apps from the IBM Security App Exchange to augment their deployment.

Better manage compliance with pre-built content, rules and reports

QRadar provides the transparency, accountability and measurability critical to an organization's success in meeting regulatory mandates and reporting on compliance. The solution's ability to correlate and integrate threat intelligence feeds yields more complete metrics for reporting on IT risks for auditors. Hundreds of pre-built reports and rule templates can help organizations more easily address industry compliance requirements.

Profiles of network assets can be grouped by business function—for example, servers that are subject to Health Insurance Portability and Accountability Act (HIPAA) compliance audits—to help teams more easily report on relevant activity as needed.

QRadar has the experience and resources needed to help organizations address risk and regulatory exposure by providing default setting compliance packages for General Data Protection Regulation (GDPR), the Federal Information Security Management Act (FISMA), Sarbanes-Oxley (SOX), HIPAA, ISO 27001, Payment Card Industry Data Security

Standard (PCI DSS) and more. These packages are included free of charge with a QRadar SIEM license and are available in the IBM Security App Exchange.

Easily scale with changing needs

The flexible, scalable architecture of QRadar is designed to support both large and small organizations with a variety of needs. Smaller organizations can start with a single all-in-one solution that can be easily upgraded into a distributed deployment as needs evolve. Larger enterprise organizations can deploy dedicated components to support global, distributed networks with high data volumes. The QRadar SIEM solution includes the following components: event collectors, event processors, flow collectors, flow processors, data nodes (for low cost storage and increased performance) and a central console. All components are available as hardware, software or virtual appliances. Software and virtual appliance options can be deployed on-premises, in IaaS environments or distributed across hybrid environments.

Regardless of deployment model, organizations can optionally add in high availability and disaster recovery protection where and when needed to help to ensure continuous operations. For organizations seeking business resiliency, QRadar delivers integrated automatic failover and full-disk synchronization between systems without the need for additional third-party fault management products. For organizations seeking data protection and recovery, QRadar disaster recovery solutions can forward live data, such as flows and events, from a primary QRadar system to a secondary parallel system located at a separate facility.

About IBM QRadar

IBM QRadar SIEM sits at the core of the IBM QRadar Security Intelligence Platform, which applies automated, intelligent analytics to a vast amount of security data to provide security analysts with actionable insight into the most critical threats, enabling them to make better, faster triage and response decisions.

This comprehensive platform brings together log management SIEM, network analysis, vulnerability management, user behavior analytics, threat intelligence and AI-powered investigations into one single platform managed from a single interface.

Components of the solution are fully integrated, enabling customers to start as small or large as they choose and easily scale up or down as their needs change. Learn more at: ibm.com/qradar.

Why IBM Security?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitoring greater than 60 billion security events per day in more than 130 countries, and the corporation holds more than 3,700 security patents.



© Copyright IBM Corporation 2019

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
February 2019

IBM, the IBM logo, ibm.com, IBM QRadar, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.



Please Recycle

IBM QRadar

Sense and detect modern threats with the most sophisticated security analytics platform



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

- Analyze security data
- Understand context
- Profile usage

Use cases

- Advanced threat detection
- Critical data protection
- Insider threat monitoring
- Risk and vulnerability management
- Unauthorized traffic detection
- Forensics investigation and threat hunting

Why IBM?

- Your security dashboard
- The power to act—at scale
- IBM Security App Exchange
- One platform, global visibility

For more information

Conquer the unknown

Security professionals live in a world of constant suspense. Threats and attacks hit their organizations from every angle, every minute of every day. When persistent attackers break in, they move slowly and quietly. They hunt for valuable data and they cover their tracks. In fact, a recent survey found that the mean time to identify an attack was 256 days, while the mean time to contain it was 82 days.¹ Consequently, life in a Security Operations Center (SOC) is stressful; many teams just don't know what they don't know.

Gone are the days when security teams could just lock down the perimeter, ban many forms of Internet access and fight the latest fire. Today's organizations demand near-ubiquitous connectivity in order to keep the business moving while simultaneously stopping advanced threats, identifying fraud and rogue insiders, and ensuring continuous compliance. New requirements call for analyzing as much information as possible to detect threatening activities that lurk under the surface—and respond more rapidly. SOC analysts must develop a keen ability to detect deviations from normal activities, and the solutions they choose must be able to scale, reaching every nook and cranny of the enterprise with a single, cohesive platform.



Attackers can lurk within an organization for **8 to 9 months** before they're discovered.¹

¹ "2015 Cost of a Data Breach Study: Global Analysis," Ponemon Institute Research Report, May 2015.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

- Analyze security data
- Understand context
- Profile usage

Use cases

- Advanced threat detection
- Critical data protection
- Insider threat monitoring
- Risk and vulnerability management
- Unauthorized traffic detection
- Forensics investigation and threat hunting

Why IBM?

- Your security dashboard
- The power to act—at scale
- IBM Security App Exchange
- One platform, global visibility

For more information

Sense threats and act

To stay ahead, organizations need to be able to “sense” chains of malicious activities in the same way that people sense danger when they see, hear, smell or feel troublesome conditions. They need a security platform that can:

- Deploy rapidly across an entire network, including cloud-based resources
- Detect subtle differences in the environment, such as lurking intruders or rogue insiders
- Discover attacks without depending upon a few highly trained specialists
- Collect, normalize and correlate billions of events, prioritized to a handful of issues
- Identify the important vulnerabilities and risks to prevent a breach

On the bright side, today’s SOC analysts no longer have to go it alone. Just as the attackers have banded together to share their insights and techniques, the security community has responded with similarly shared resources. The emergence of these new threat intelligence and application sharing facilities helps limit the effectiveness of new malware and exploit kits, and the impact of zero-day or one-day vulnerabilities. Yet many SOC analysts are still limited by aging log management systems or basic security information and event management (SIEM) solutions that generate excessive alerts using a single instance of suspicious behavior.



Making sense of millions of security events is nearly impossible with basic SIEM tools.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

- Analyze security data
- Understand context
- Profile usage

Use cases

- Advanced threat detection
- Critical data protection
- Insider threat monitoring
- Risk and vulnerability management
- Unauthorized traffic detection
- Forensics investigation and threat hunting

Why IBM?

- Your security dashboard
- The power to act—at scale
- IBM Security App Exchange
- One platform, global visibility

For more information

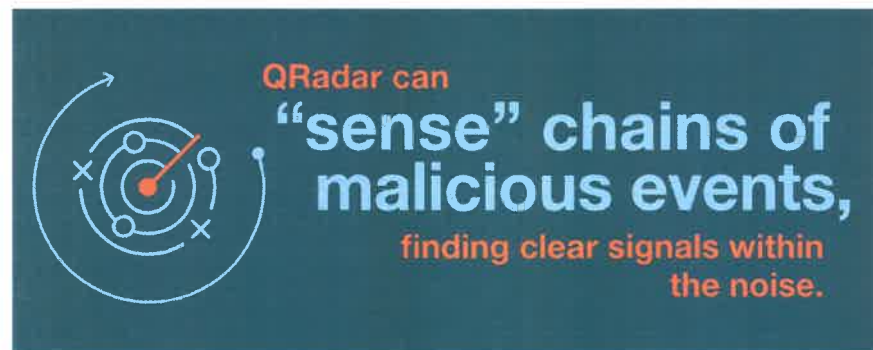
Use analytics to eliminate threats

The most serious security breaches don't begin with a big bang. Instead, cybercriminals launch "low and slow" attacks that can persist for months. Wouldn't it be great if you could identify subtle and related changes in the environment, and then alert security teams when weird stuff starts to occur?

IBM® QRadar® Security Intelligence Platform is the only security solution powered by IBM Sense Analytics™, which can:

- Develop user and asset profiles to baseline legitimate activities
- Detect abnormal behaviors across people (including insiders, partners, customers and guests), networks, applications and data
- Relate current and historical suspicious activities, increasing the accuracy of identified incidents
- Retrieve and replay network activity and investigate packet content in its original form
- Find and prioritize weaknesses before they're exploited

Point products that perform moment-in-time analyses are unreliable; they can't associate new network activity with "risky" users, such as those who are known to have previously visited websites with poor reputations. Sense Analytics helps eliminate threats by matching user behavior with log events, network flows, threat intelligence, vulnerabilities and business context. It enables organizations to focus on their most immediate and dangerous threats by finding clear signals within the noise—and guides them through remediation efforts to minimize any potential damage.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

Analyze security data

Understand context

Profile usage

Use cases

Advanced threat detection

Critical data protection

Insider threat monitoring

Risk and vulnerability management

Unauthorized traffic detection

Forensics investigation and threat hunting

Why IBM?

Your security dashboard

The power to act—at scale

IBM Security App Exchange

One platform, global visibility

For more information

How does Sense Analytics work?

Without data, analytics are useless, and without lots of data, they're simply weak. Some of this data comes from the operation of your network, some of it is stored in applications, some of it is derived from previous analyses, and some of it arrives as a feed from an external source. QRadar collects raw security data from every device, application and user within the network—whether on an organization's premises or hosted within a cloud environment.

Sense Analytics can:

- [Analyze security data](#)
- [Understand context](#)
- [Profile usage](#)

Once the data is collected, QRadar appliances perform real-time analyses to search for immediate signs of danger, and then further infuse the results with other stored intelligence about any of the involved network, user or file metadata. QRadar allows security teams to understand how current activities are related to what's occurred in the past, and one key aspect of sensing change is having the right parameters for baseline activity.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

[Analyze security data](#)

Understand context

Profile usage

Use cases

Advanced threat detection

Critical data protection

Insider threat monitoring

Risk and vulnerability management

Unauthorized traffic detection

Forensics investigation and threat hunting

Why IBM?

Your security dashboard

The power to act—at scale

IBM Security App Exchange

One platform, global visibility

For more information

Analyze security data to sense threats

Powered by Sense Analytics, QRadar uses advanced, state-based analysis to transform current security data into meaningful insights. Security teams can define multiple types of conditions to help them sense potentially malicious activity, including:

- Behavioral changes to catch deviations from regular patterns
- Anomalies that can uncover new network traffic or traffic that suddenly ceases
- Threshold violations to find occurrences of an activity that exceeds a defined level

A change in the regular behavior of users or identities is often one of the first signs that the network's been breached and, perhaps, someone's credentials have been compromised. Sense Analytics not only compares real-time activity to historical patterns, but it also detects new application usage, new website visits and new file-transfer activities. It can also help rule out false-positive results by pulling data from organizational identity systems, allowing SOC analysts to see a recent reporting or role change for the individual.



Using QRadar, an international energy company can analyze **two billion events per day—** correlating data in real time—to identify the 20 to 25 potential offenses that pose the greatest risk.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

Analyze security data

Understand context

Profile usage

Use cases

Advanced threat detection

Critical data protection

Insider threat monitoring

Risk and vulnerability management

Unauthorized traffic detection

Forensics investigation and threat hunting

Why IBM?

Your security dashboard

The power to act—at scale

IBM Security App Exchange

One platform, global visibility

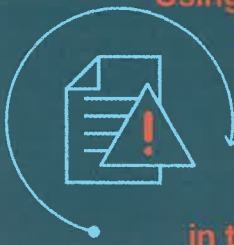
For more information

Understand context by analyzing events to flows to packets

One powerful and often overlooked source of context can be derived from native network flow data—the data that identifies IP addresses, ports, protocols, and even application or “payload” content crisscrossing the network—all captured through immediate deep-packet inspections or the post-incident recovery of full packets. This enables security teams to:

- Profile “normal” network traffic and get alerts when conditions change
- Find new or compromised hosts communicating with malicious IPs
- Detect new security threats without the use of signatures
- Replay the step-by-step actions of a detected intruder or malicious user
- Get visibility into the application layer and detect suspicious content or inappropriate use

Sense Analytics uses network data to provide context for every event, incident or correlated offense. It can detect if a web server stops responding to communications, identify a significant change in the activity level of commonly used services, and generate alerts when new services or protocols appear on the network. This analysis also reveals application types and identifies port and protocol mismatches—which can help expedite investigations.



Using QRadar, a major healthcare provider detected **unencrypted patient data** being passed in the clear. Thanks to rapid detection, it quickly remediated the risk and avoided potential penalties.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

Analyze security data

Understand context

Profile usage

Use cases

Advanced threat detection

Critical data protection

Insider threat monitoring

Risk and vulnerability management

Unauthorized traffic detection

Forensics investigation and threat hunting

Why IBM?

Your security dashboard

The power to act—at scale

IBM Security App Exchange

One platform, global visibility

For more information

Profile usage to store insights and help manage risk

A security solution designed to quickly search through real-time data is going to miss a lot of incidents that require prior knowledge of key applications, the people who use them, their typical performance levels, their associated hosts, and when they experience fast and slow periods of activity. Knowledge of these parameters is crucial for actionable intelligence.

The ability to store knowledge by profiling assets and individuals is a foundational characteristic of Sense Analytics. QRadar automatically discovers assets and creates asset profiles, using network flow data and vulnerability scans. Profiles define what an asset is, identify how it communicates with other assets, list the permissible applications and outline the presence of any known vulnerabilities. QRadar then uses all of this context to reduce noise and provide highly accurate incidents.

Building knowledge about what network users are doing is equally valuable for attack and breach detection. QRadar can track IP and MAC addresses, email IDs and chat handles, for example, and it can leverage other IBM or third-party identity and access management programs to provide valuable context to incident investigations. It can use all of these associations to qualify the scope of its analytics, and include or exclude individuals or personas associated with suspect activity—happening currently or observed in the recent past.



QRadar can help a credit card firm protect its critical data and infrastructure from advanced threats—while also achieving deployment, tuning and maintenance cost savings up to 50 percent.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

Analyze security data

Understand context

Profile usage

Use cases

Advanced threat detection

Critical data protection

Insider threat monitoring

Risk and vulnerability management

Unauthorized traffic detection

Forensics investigation and threat hunting

Why IBM?

Your security dashboard

The power to act—at scale

IBM Security App Exchange

One platform, global visibility

For more information

Explore use cases that show the power of Sense Analytics

In many environments, complacency and lapses in security practices mean that critical assets aren't necessarily as secure as they can—or should—be. Organizations need to limit the downside of an inevitable breach. They need solutions that cover the complete environment without any blind spots.

From the moment it's installed, QRadar begins building actionable security intelligence that can help strengthen an organization's defenses. The use cases in which the solution delivers rapid value include:

- [Advanced threat detection](#)
- [Critical data protection](#)
- [Insider threat monitoring](#)
- [Risk and vulnerability management](#)
- [Unauthorized traffic detection](#)
- [Forensics investigation](#)



QRadar takes

the mystery
out of security
investigations,

helping security teams identify attackers, their
tactics and where the initial breach occurred.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

Analyze security data

Understand context

Profile usage

Use cases

Advanced threat detection

Critical data protection

Insider threat monitoring

Risk and vulnerability management

Unauthorized traffic detection

Forensics investigation and threat hunting

Why IBM?

Your security dashboard

The power to act—at scale

IBM Security App Exchange

One platform, global visibility

For more information

Use cases:

Advanced threat detection

Using real-time analytics, security teams can detect if a host visits a potentially malicious domain, but an alert might not be required for just a visit. However, if that same host starts demonstrating beaconing behavior—detected by using historical long-term analysis—and it also starts transferring abnormally high data volumes deviating from behavioral baselines, the combination of all three conditions enables QRadar to produce a single, heightened alert.

QRadar can also sense a sudden change in network traffic, such as the appearance of a new application on a host or the termination of a typical service, capturing it as an anomalistic condition. Anomalies are not easily spotted by security teams as they search through system logs—unlike malware signatures or other defined attacks against known vulnerabilities. By definition, an anomaly is an oddity, and is only discoverable by a security solution that monitors and profiles the actions of all users and entities.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

Analyze security data

Understand context

Profile usage

Use cases

Advanced threat detection

Critical data protection

Insider threat monitoring

Risk and vulnerability management

Unauthorized traffic detection

Forensics investigation and threat hunting

Why IBM?

Your security dashboard

The power to act – at scale

IBM Security App Exchange

One platform, global visibility

For more information

Use cases:

Critical data protection

Overnight, a new application begins operating on a network host. This activity might be the result of a new business requirement or someone simply installing a chat application. But if that host has access to critical data, and also has a known vulnerability associated with it, QRadar can create a high-priority alert to prompt security teams to investigate the incident.

QRadar quickly detects when event traffic exceeds a specific activity level and generates an alert. The threshold or limit can be based on any data that is collected in QRadar, such as network device configurations, servers, network traffic telemetry, applications, and end users and their activities. And like a behavioral change or anomaly, QRadar can enrich the alert with the context of user identities, ports and protocols in use, IP reputations and reported threat activities to provide security teams with a deeper perspective about the incident.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

Analyze security data

Understand context

Profile usage

Use cases

Advanced threat detection

Critical data protection

Insider threat monitoring

Risk and vulnerability management

Unauthorized traffic detection

Forensics investigation and threat hunting

Why IBM?

Your security dashboard

The power to act—at scale

IBM Security App Exchange

One platform, global visibility

For more information

Use cases: Insider threat monitoring

A customer service representative suddenly begins downloading twice the normal amount of data from a client information system, which might be part of some new sales analysis activity. But if QRadar knows that representative recently visited a potentially suspicious website, and is now seeing small amounts of data being sent to a competitor's site, the security staff can be informed before a large amount of information is leaked.

By profiling entities and individuals, QRadar stands out from other security products. The combination of a comprehensive set of data, business context and threat intelligence—coupled with the ability to detect deviations from normal behavior as well as recognize what behavior is not allowed or is inappropriate—provides for an extremely powerful incident detection capability.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

Analyze security data

Understand context

Profile usage

Use cases

Advanced threat detection

Critical data protection

Insider threat monitoring

Risk and vulnerability management

Unauthorized traffic detection

Forensics investigation and threat hunting

Why IBM?

Your security dashboard

The power to act—at scale

IBM Security App Exchange

One platform, global visibility

For more information

Use cases:

Risk and vulnerability management

When a new entity appears on the network, QRadar automatically senses its existence through passive profiling of logs and flow data. With its seamlessly integrated vulnerability scanner, QRadar can trigger a scan of this new entity to discover if it has any urgent or high-risk vulnerabilities that are exposed to potential threat sources.

For example, when a new server is added to the network, QRadar can detect if it is missing critical patches or has default administrative credentials. QRadar can then notify the appropriate team to remediate and/or schedule a patch, and then escalate the issue if that task hasn't been performed in a timely manner.

What's more, new vulnerability disclosures are automatically correlated with existing data without needing a rescan, which helps improve the speed and accuracy of detection. The resulting operational savings also allows security analysts to spend more time focused on proactive tactics, such as risk analysis and vulnerability patching activities.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

Analyze security data

Understand context

Profile usage

Use cases

Advanced threat detection

Critical data protection

Insider threat monitoring

Risk and vulnerability management

Unauthorized traffic detection

Forensics investigation and threat hunting

Why IBM?

Your security dashboard

The power to act—at scale

IBM Security App Exchange

One platform, global visibility

For more information

Use cases:

Unauthorized traffic detection

With most organizations now supporting bring-your-own-device (BYOD) endpoints, security teams are seeing more network traffic associated with social media applications. Users often access their corporate email systems and stay connected with friends through Facebook, LinkedIn, Twitter and other services—all with the same device. QRadar collects and analyzes this data, and notices when, for example, Internet chat sessions start connecting through port 80, the port normally reserved for HTTP traffic. Further connections with known botnet servers quickly verify the injection of malware and prompt the security team to take action.

QRadar collects and analyzes data from mobile and BYOD devices both from the network layer and from endpoint management systems. It can detect potential threats—such as a jailbroken device, suspicious applications installed on a device, or potentially malicious Internet communications—and then trigger quarantining of the device and/or escalation to the appropriate security team for action.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

Analyze security data

Understand context

Profile usage

Use cases

Advanced threat detection

Critical data protection

Insider threat monitoring

Risk and vulnerability management

Unauthorized traffic detection

Forensics investigation and threat hunting

Why IBM?

Your security dashboard

The power to act—at scale

IBM Security App Exchange

One platform, global visibility

For more information

Use cases:

Forensics investigation and threat hunting

During the investigation of an offense, a security analyst discovers that one or more employees have succumbed to a phishing scam and the attacker has latched on and expanded to an internal server host. The pattern matches one identified by X-Force and is known to inject remote-access Trojan (RAT) software, which is difficult to detect.

With a few mouse clicks, QRadar recovers all network packets associated with the incident and reconstructs the step-by-step movements—showing the security analyst with crystal-clear clarity exactly where and when the RAT software was installed. The forensics workflow enables the analyst to quickly and easily build a rich profile of the malicious software and piece together the infection paths through link analysis to identify “patient zero” and any other infected parties. As a result, the security team can quickly remediate the damage and help minimize recurrences.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

Analyze security data

Understand context

Profile usage

Use cases

Advanced threat detection

Critical data protection

Insider threat monitoring

Risk and vulnerability management

Unauthorized traffic detection

Forensics investigation and threat hunting

Why IBM?

Your security dashboard

The power to act—at scale

IBM Security App Exchange

One platform, global visibility

For more information

IBM delivers actionable intelligence for an active offense and stronger defense

Information security is a boardroom priority, but many organizations still depend upon dozens of point products for moment-in-time insights. Highly trained personnel are using search engines to comb through mountains of data, but more and more often, attackers evade detection by switching IPs, protocols, ports and applications to latch on, expand and gather valuable data after a successful breach.

IBM QRadar is different. It deploys rapidly regardless of a network's scale and begins delivering results in mere hours. Its cognitive-like capabilities and stored intelligence can associate related attacks emanating from the same source or corresponding to the same targeted data. QRadar delivers these actionable insights to meet both current and future needs—from advanced threat detection to insider threat monitoring, fraud detection, risk and vulnerability management, forensics investigations, and compliance reporting.

Key reasons why security leaders choose QRadar include:

- [An easy-to-use security dashboard](#) that highlights the most important threats and supports fast, effective investigation and remediation workflow
- [Near-limitless scalability](#), backed by X-Force threat intelligence and the collaborative power of IBM X-Force Exchange
- [The IBM Security App Exchange](#), featuring IBM and partner-developed applications (apps) that extend the capabilities of QRadar without added complexity
- [The single, integrated platform with global visibility](#), providing insights about network, application and user activity



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

- Analyze security data
 - Understand context
 - Profile usage
-

Use cases

- Advanced threat detection
 - Critical data protection
 - Insider threat monitoring
 - Risk and vulnerability management
 - Unauthorized traffic detection
 - Forensics investigation and threat hunting
-

Why IBM?

Your security dashboard

- The power to act—at scale
 - IBM Security App Exchange
 - One platform, global visibility
-

For more information

Bring the most important threats to life

Once the threat, attack or breach is detected, then it's time to take action. QRadar empowers security teams with a web-based user interface that has a common look and feel across the entire platform. Switching between monitoring log activity, watching network activity, reviewing highly correlated offenses, running risk and vulnerability analyses, or performing forensics analysis is as easy as clicking on a tab to display an

information-rich dashboard screen. Each dashboard has extensive security intelligence information, organized into highly visual displays of recent activity that's easily investigated with just a few mouse clicks.

Spend a few minutes looking at the spikes or drilling down into the details underlying a reported offense. Security teams can quickly understand the nature of the highlighted problem; any vulnerabilities exploited; the injection of any botnet, RAT or other malware programs; and the extent of any lost data. Now it's time to act before any real damage is done.



Many of the world's largest companies rely on QRadar to help

**keep them
out of the news.**



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

Analyze security data

Understand context

Profile usage

Use cases

Advanced threat detection

Critical data protection

Insider threat monitoring

Risk and vulnerability management

Unauthorized traffic detection

Forensics investigation and threat hunting

Why IBM?

Your security dashboard

The power to act—at scale

IBM Security App Exchange

One platform, global visibility

For more information

Gain the power to act—at scale

Using the greater QRadar platform, security teams can clearly understand both what has happened and what's at stake if they don't act—quickly. Key capabilities such as threat monitoring, risk and vulnerability management, and compliance reporting are typically a click away, and can pass relevant data to each other. Plus, QRadar includes tight integration with X-Force threat intelligence for hourly updates on global attack techniques and malware strains.

In the event of a breach, QRadar integrated forensics technology provides SOC analysts with packet data for an associated offense, detailing the step-by-step actions of intruders with exact clarity. Defeating some threats simply requires blocking communications with an external IP address, but others require the mobilization of emergency response teams to isolate and reconfigure hosts, disable malware and patch vulnerabilities. But what if your team doesn't know exactly what to do? It's time to ask for help, collaborate with peers, seek a solution or even hire a professional services team.

The QRadar open framework—as well as the [IBM Security App Exchange](#)—helps facilitate tighter integrations with IBM and third-party solutions. For example, one of the apps on the site passes QRadar offense data to Resilient Systems' Incident Response Platform for immediate action. Another app provides a similar data sharing capability with the Carbon Black Enterprise Response endpoint management solution.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

Analyze security data

Understand context

Profile usage

Use cases

Advanced threat detection

Critical data protection

Insider threat monitoring

Risk and vulnerability management

Unauthorized traffic detection

Forensics investigation and threat hunting

Why IBM?

Your security dashboard

The power to act—at scale

IBM Security App Exchange

One platform, global visibility

For more information

Expand capabilities with the IBM Security App Exchange

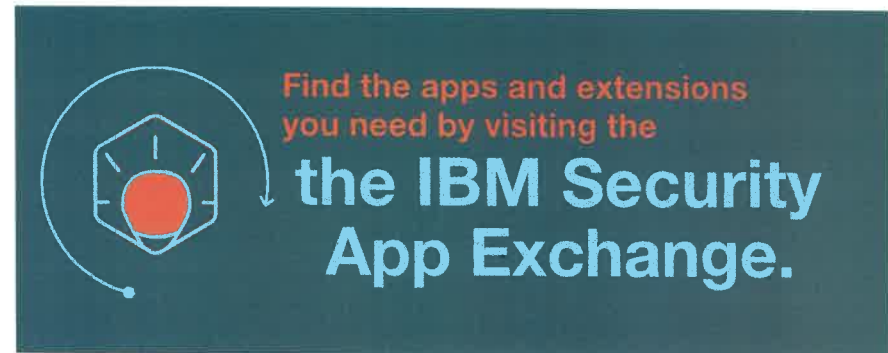
The [IBM Security App Exchange](#) expands the flexibility of QRadar exponentially. This premier collaboration site allows customers, developers and business partners to share apps, security app extensions and enhancements to IBM Security products.

With the IBM Security App Exchange, organizations can:

- Obtain apps that extend the capabilities of IBM Security solutions
- Share best practices and learn from others
- Find solutions and use cases that enhance the strategic value of security operations

All code is reviewed by IBM against set criteria before it appears on the site. And security teams can download and install the solutions independently—outside of official product release cycles. This way, they can apply new security use cases without adding unnecessary solution complexity.

In particular, QRadar users can download industry-, threat-, device- and vendor-specific content from the IBM Security App Exchange. Plus, they can access custom reports, dashboards, specialty analytics and threat information.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

Analyze security data

Understand context

Profile usage

Use cases

Advanced threat detection

Critical data protection

Insider threat monitoring

Risk and vulnerability management

Unauthorized traffic detection

Forensics investigation and threat hunting

Why IBM?

Your security dashboard

The power to act—at scale

IBM Security App Exchange

One platform, global visibility

For more information

Deploy one platform with global visibility

Today's security environments are full of complexity—often, security data is distributed across multiple offerings from different vendors, all with different interfaces and data storage formats. To effectively detect existing and emerging threats, security teams need a consolidated view of this data, combined with comprehensive threat detection analytics and response capabilities. QRadar uses a single, federated database for all security data that is specifically designed for scalable collection from on-premises and cloud systems, storage, reporting and very fast investigation search performance. In addition, QRadar is optimized for real-time and historical incident analysis, detecting incidents in a matter of seconds after they occur—not hours, days or weeks.

QRadar also provides a highly integrated set of security use cases, with additional ones available via the IBM Security App Exchange. Security teams can use a single, dashboard-based console for all functions, including real-time security monitoring; proactive risk and vulnerability management; and incident detection, forensics and remediation. This one hub for security operations and response fuses intelligence from IBM and third-party products—backed by a consistent user interface and workflow—making your security operations team far more effective.



Home

Conquer the unknown

Sense threats and act

QRadar Sense Analytics

How does it work?

Analyze security data

Understand context

Profile usage

Use cases

Advanced threat detection

Critical data protection

Insider threat monitoring

Risk and vulnerability management

Unauthorized traffic detection

Forensics investigation and threat hunting

Why IBM?

Your security dashboard

The power to act—at scale

IBM Security App Exchange

One platform, global visibility

For more information

For more information

To learn more about [IBM QRadar Security Intelligence Platform powered by Sense Analytics](#), please contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

© Copyright IBM Corporation 2016

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
April 2016

IBM, the IBM logo, ibm.com, QRadar, Sense Analytics, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

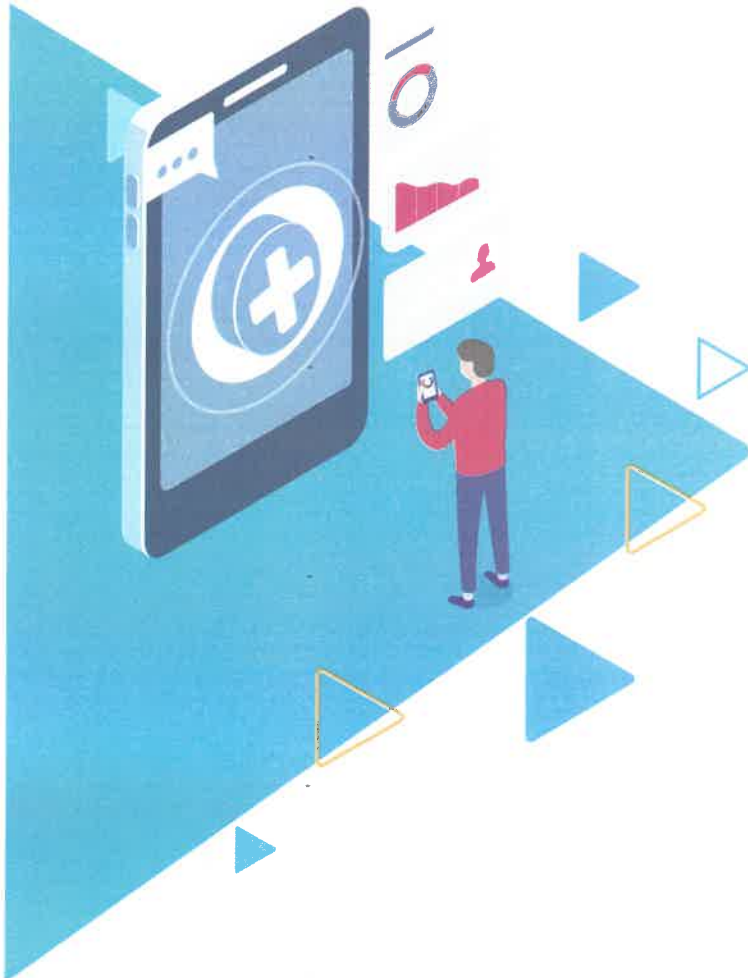
The client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.





BigFix Patch

Continuous patch compliance, visibility and enforcement

With software—and the threats against that software—constantly evolving, organizations need an effective way to assess, deploy and manage a constant flow of patches for the myriad operating systems and applications in their heterogeneous environments. For system administrators responsible for potentially tens or hundreds of thousands of endpoints running various operating systems and software applications, patch management can easily overwhelm already strained budgets and staff. BigFix Patch balances the need for fast deployment and high availability with an automated, simplified patching process that is administered from a single console. BigFix Patch gives organizations access to comprehensive capabilities for delivering patches for Microsoft Windows, UNIX, Linux and Apple Macintosh operating systems; third-party applications from vendors including Adobe, Mozilla, Apple and Java; and customer-supplied patches to endpoints—regardless of their location, connection type or status.

Endpoints can include servers, laptops, desktops and specialized equipment such as point-of-sale (POS) devices, ATMs and self-service kiosks. In addition, virtual machines can be patched so that virtual and cloud environments have the same level of security as physical systems.

Highlights

- Automatically manage patches for multiple operating systems and applications across hundreds of thousands of endpoints—regardless of location, connection type or status
- Fixlet® messages, delivered regularly by the BigFix development team, wrap the update with policy information (such as patch dependencies, applicable systems and severity level) which is read by an intelligent agent so only the relevant updates for that specific endpoint are downloaded and installed
- Reduce security and compliance risk by slashing remediation cycles from weeks to days or hours
- Gain greater visibility into patch compliance with flexible, real-time monitoring and reporting

Addressing security needs across the organization

One approach to patch management is to create large patch files with a large update "payload" and distribute them to all of the endpoints, regardless of whether they already have all of the patches. BigFix Patch takes a different approach, automatically creating patch policies, called Fixlet® messages, which wrap the update with policy information such as patch dependencies, applicable systems and severity level. An intelligent agent recognizes which patches are required for the machine on which it is installed based on the endpoint's unique hardware, operating system, configuration settings, applications and installed patches. The agent then automatically retrieves and applies only the relevant updates for that specific endpoint.

Accelerate and automate the patch management process

BigFix Patch automates the entire patch management process and enhances security while saving organizations money, time and effort.

Research—BigFix acquires, tests, packages and distributes many patch policies directly for users, removing considerable patch management overhead. This largely automated process provides a consistent, high-quality patch in a timely manner.

Assess—The BigFix intelligent agent continuously monitors and reports the endpoint status, including patch levels, to a management server. This intelligent agent also compares endpoint compliance against defined policies, such as mandatory patch levels.

Remediate—An organization can quickly create a report showing which endpoints need updates and then distribute those updates to the endpoints within minutes. IT administrators can safely and rapidly patch Windows, Linux, UNIX and Mac operating systems with no domain-specific knowledge or expertise, and the solution stores audit information that tracks who ordered which updates to be applied to which endpoints.

Confirm—Once a patch is deployed, BigFix automatically reassesses the endpoint status to confirm successful installation and immediately updates the management server in real time. BigFix automatically validates all patches not by looking at exit codes; but by using the same process used to determine patch relevance to accurately reflect patch status. This step is critical in supporting compliance requirements, which require definitive proof of patch installation. With this solution, operators can watch the patch deployment process in real time via a centralized management console to receive installation confirmation within minutes of initiating the patch process. By closing the loop on patch times, organizations can ensure patch compliance in a way that is smarter and faster.

Enforce—The BigFix intelligent agent provides continuous endpoint enforcement and ensures that endpoints remain updated. If a patch is uninstalled for any reason, the agent can be configured to automatically reapply it to the endpoint as needed.

Report—Integrated web reporting capabilities allow end users, administrators, executives, management and others to view dashboards and receive up-to-the-minute reports. Dashboards and reports indicate which patches were deployed, when they were deployed, who deployed them, and to which endpoints. Special "click-through" dashboards show patch management progress in real time.

With BigFix, the remediation cycles are short and fast, which enables an industry-leading, rapid-response capability for addressing malware and security exposures.

Achieve continuous compliance

Many organizations need to establish, document and prove compliance with patch management processes in order to comply with governmental regulations, service level agreements (SLAs) with other organizations and internal constituents, and corporate policies. Regulations such as Sarbanes-Oxley, Payment Card Industry (PCI) Data Security Standard (DSS) and Health Insurance Portability and Accountability Act (HIPAA) require that a regular, fully documented patch management process be in place, and proof of continuous compliance is necessary in order to pass audits. BigFix's ability to enforce policies and quickly report on compliance can help improve an organization's audit readiness.

Simple to use, vast in scope

A single patch management server can support up to 250,000 endpoints, shortening patch times and updates with no loss of endpoint functionality, even over low-bandwidth or globally distributed networks. The solution features patented bandwidth-throttling technology that manages network traffic and minimizes congestion.

Customers using BigFix have achieved 95+ percent first-pass success rates—up from the conventional 60 to 75 percent rate—not only increasing the effectiveness of the patch process but cutting operational costs and reducing staff workloads by as much as 20 to one. BigFix can patch endpoints on or off the network—including devices using Internet connections—with minimal endpoint impact. This means laptops using a public Internet connection at a coffee shop and other "roaming" devices can still receive patches.

BigFix Platform Requirements	
Server	<ul style="list-style-type: none"> Windows Server 2008/2008R2, 2012/2012R2, 2016 Microsoft SQL Server 2008-2017 RedHat Enterprise Server 6, 7 DB2 10.x
Console	<ul style="list-style-type: none"> Windows 7,8,10/Server 2008 -2019 Adobe Flash Player 12+
Agent	<ul style="list-style-type: none"> Windows Vista-10 Windows Server 2008-2019 Windows 10 IoT Windows Embedded 7/2009, POSReady 7/2009 RHEL: 5, 6, 7 CentOS: 5.3, 6, 7 Debian:7, 9, 8 Oracle Enterprise Linux: 6, 6.7, 7, 7.1, 7.2 Raspbian 9 SLES: 10, 11, 12 Ubuntu: 12.04 LTS - 18.04LTS Solaris: Mac: OSX 10.8 - macOS 10.14 AIX 6.1, 7.1, 7.2 HP-UX 11.11, 11.23, 11.31 + End-of-life platforms managed by previous versions of the BigFix Agent!
Hypervisor Extenders:	<ul style="list-style-type: none"> PowerVM VMWare ESXi 5.5, 6, 6.5

Why BigFix?

The BigFix Family includes:

- **BigFix Lifecycle**—This easy-to-manage, quick-to-deploy solution provides unified, real-time visibility and management of endpoints including asset discovery, patch management, software distribution, operating system deployment, and remote desktop control.
- **BigFix Compliance**— This easy-to-manage, quick-to-deploy solution provides unified, real-time visibility and enforcement to help organizations both protect endpoint assets and assure regulators that systems are meeting security compliance standards.
- **BigFix Inventory**—This software enables users to discover and analyze applications installed on desktops, laptops and servers. Drill-down information about software

For more information

To learn more about BigFix, contact your HCL Software representative, HCL Business Partner, or visit: www.BigFix.com.

About HCL Software

HCL Software is a division of HCL Technologies that develops and delivers a next-generation portfolio of enterprise-grade software-based offerings with flexible consumption models, spanning traditional on-premises software, Software-as-a-Service (SaaS), and bundled managed services. We bring speed, insights and innovations (big and small) to create value for our customers. HCL Software areas include DevOps, Security, Automation, Application Modernization, Data and Integration Infrastructure, and several Business Applications. HCL embraces the real-world complexity of multi-mode IT that ranges from mainframe to cloud and everything in between while focusing on customer success and building 'Relationships Beyond the Contract.'



© Copyright 2019 HCL

HCL Corporation Pvt. Ltd.
Corporate Towers,
HCL Technology Hub,
Plot No 3A, Sector 126,
Noida - 201303. UP (India)

Produced in the United States of America.

HCL, the HCL logo, hcl.com, bigfix.com, BigFix, and Fixlets are trademarks of HCL Corporation., registered in many jurisdictions worldwide.

AIX, and z Systems are a registered trademark of International Business Machines Corp.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

This document is current as of the initial date of publication and may be changed by HCL at any time. Not all offerings are available in every country in which HCL operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

HCL products are warranted according to the terms and conditions of the agreements under which they are provided.

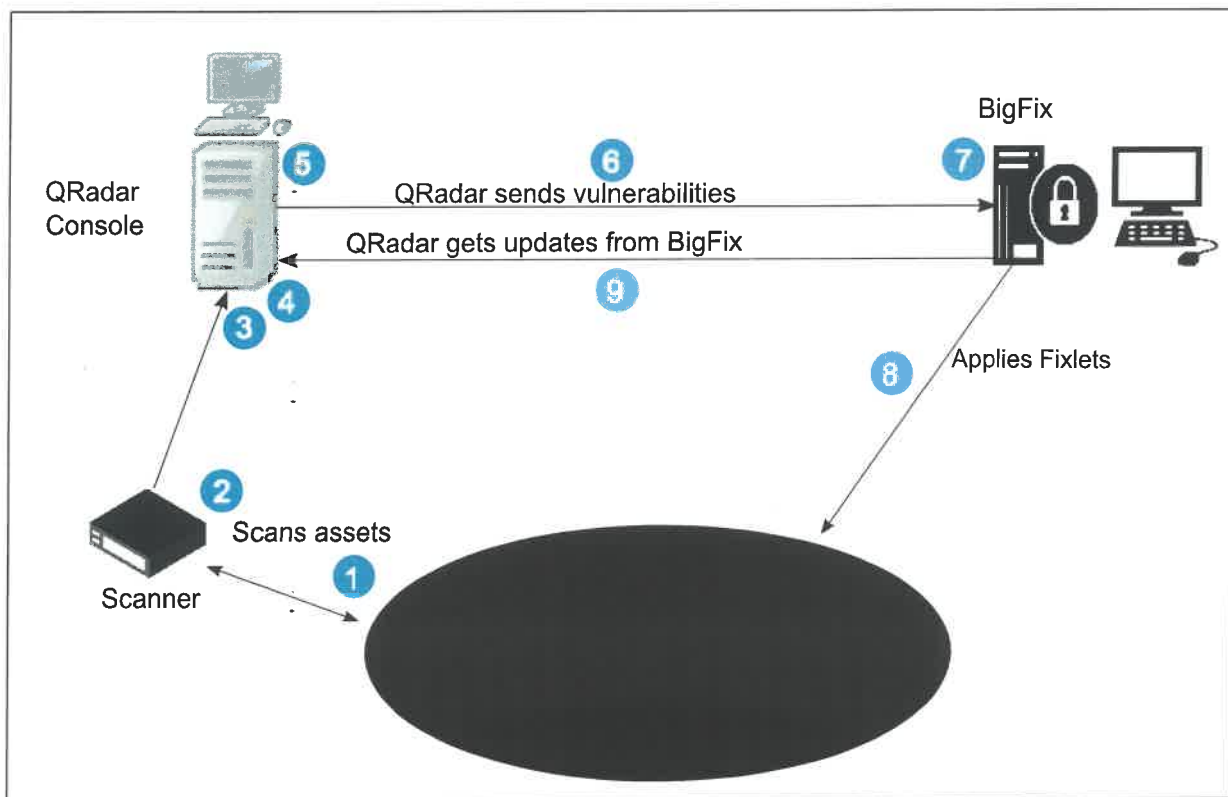
The client is responsible for ensuring compliance with laws and regulations applicable to it. HCL does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding HCL's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

Interactions between IBM QRadar and IBM BigFix

Before, you configure the integration between IBM® QRadar® and BigFix® it's important to understand how they interact with each other.

The following diagram shows a high-level overview of some interactions between QRadar and BigFix from the initial scan of assets, to remediation of vulnerabilities on the scanned assets.

Figure 1. QRadar Vulnerability Manager and BigFix interactions



The following list describes a broad outline of interactions between QRadar and BigFix from the initial scan for vulnerabilities to the remediation of those vulnerabilities:

1. QRadar Vulnerability Manager scanner completes an authenticated scan of assets to discover vulnerabilities. Only the vulnerabilities from assets that are configured in scan profiles that use Full, Patch, or PCI scan policies are eligible for processing by BigFix.

2. If a BigFix agent is installed on an asset QRadar Vulnerability Manager retrieves the *BES agent ID* from the asset when it detects vulnerabilities on the asset. The *BES agent ID* is the unique identifier that is used by BigFix to identify the asset and to remediate vulnerabilities on that asset. BigFix refers to QRadar assets as computers.
3. The scan results are updated in the QRadar asset model, which includes the *BES agent ID* from any assets that have a BigFix agent. When the scan status in the scan profile displays a status of `progress=100%`, then the asset model is updated, and vulnerability data is sent to BigFix within 15 minutes by default.
4. When the asset model is updated with the scan data, the BigFix adapter that is installed on the QRadar Console receives the updated vulnerability data with risk scores from the asset model. The data contains the *BES agent ID*. The BigFix adapter processes only vulnerability information from assets when a *BES agent ID* is included.
5. The vulnerability data that is sent to BigFix is filtered on the risk-score parameters that are configured in the adapter properties file (`/opt/qvm/adaptor/config/adaptor.properties`) on the QRadar Console. The default risk score is 0.0, which means that all vulnerabilities are sent to BigFix.
6. The BigFix adapter uses the BigFix REST API to send the vulnerability information to BigFix and it correlates vulnerability CVEs with Fixlets. By default, data is sent to BigFix in 15-minute intervals.
7. The vulnerability information that is sent by the REST API is viewable on the BigFix **Manage Vulnerable Computers** dashboard. You can deploy Fixlets to the assets with high-risk vulnerabilities from the BigFix **Manage Vulnerable Computers** dashboard. BigFix uses the *BES agent ID* as the unique reference for the asset when it applies Fixlets directly to the asset.
8. BigFix applies Fixlets to the assets that have vulnerabilities.
9. The SOAP API (Web Reports) is used to get vulnerability patch status from BigFix. Use saved searches, and filters from the **Vulnerabilities** tab to view this updated vulnerability information. You must rescan the patched assets to update the asset model with the revised vulnerability status of your assets.

Solution Showcase

HCL BigFix

Seven Must-have Endpoint Management Capabilities

Date: September 2019 **Author:** Dave Gruber, Senior ESG Analyst

Abstract:

- When endpoint management systems are effectively integrated with security and IT operations tools, they play a major role in proving compliance, stopping threats, consolidating tools, and protecting brands.
- Since most cyber-attacks leverage known vulnerabilities, IT operations and security organizations need to collaborate to quickly address security risks that threaten the organization.
- Patch management, security configuration and compliance, software distribution, and inventory are core IT infrastructure capabilities that need to interoperate with the rest of the IT operations and security toolset. Organizations that want to tighten security should consider BigFix for its rich endpoint management capabilities and the ability to easily integrate with other IT and security tools, helping IT operations and security teams to collaborate more effectively.

Overview

Endpoints represent the operational engine that enables the modern knowledge worker to perform. Disruption to these systems impacts both individual productivity and the collaboration of teams, slowing overall business operations. A leading cause of systems disruption today comes from security-related attacks, which affect wholesale system function, and result in degradation in operational performance.

Modern attacks often leverage known vulnerabilities in software for which patches and remediation actions already exist. Misconfigured systems also provide a means of attack. Organizations can prevent cyber-attacks and costly data breaches by keeping current with operating system and application patches together with implementing configuration management to enforce compliance with standard security guidelines. IT teams therefore need a continuous, precise inventory of all endpoints, software, and configuration details across their environment. Using this inventory, IT teams can ensure these systems are: kept current with the latest OS and application patches; license- and regulatory-compliant; and securely configured.

Since security teams are typically responsible for the detection of vulnerabilities while IT operations teams are responsible for remediation, effective collaboration between these teams is imperative for business continuity. A properly implemented endpoint management system (EMS) can provide a collaborative platform for both IT operations and security

that enhances the overall security posture. To accomplish this, these solutions must be comprehensive, nimble, and integrated with IT and security infrastructure. They must enable rapid, consistent remediation of threats across all endpoints while continuously verifying that all endpoints are patched and compliant.

This paper will explore the challenges associated with endpoint management, the key capabilities needed, and a recommended solution.

Challenges

Perimeter defenses are no longer enough; endpoints themselves are now part of the attack surface. With a **continuously growing attack surface**—including new types of endpoints, servers, devices, and applications—**IT teams are struggling to keep up with configuration, patching, and compliance management**. This issue increases the risk of compromise due to exposed vulnerabilities in unpatched and misconfigured systems. Timely patching is critical to stay ahead of attackers. Without an effective endpoint management strategy and process, organizations will fail to secure their environment.

As security teams increase their use of threat detection and response tools, **the amount of work required to remediate identified threats overwhelms many IT organizations**. For example, when CVEs are released, security teams first need to assess the level of risk by identifying how many systems are impacted and prioritizing remediation actions based upon the severity of the vulnerability or threat. Threat remediation is “unplanned” work for most IT teams, often creating a growing backlog of unfinished IT expansion projects due to the distraction created by threat remediation. The question of “How do we fix what we find?” is all too common today.

Roaming endpoints and cloud-based endpoints are not seen by many endpoint management systems, creating a growing management challenge. While mobile device management solutions provide some needed capabilities, few have the scalability required to effectively manage endpoints, regardless of which operating system they are running, where they are located, or how they are connected.

Ensuring that security tools are installed, current, and active is critical to securing the infrastructure. However, continuous monitoring and automated remediation of rogue systems is challenging, especially with today’s highly mobile workforce.

Compliance management requires visibility into endpoint configuration and software inventory. With the growing diversity in endpoints, this level of consolidated visibility is challenging at best.

IT teams are struggling to keep up with configuration, patching, and compliance management.

Timely patching of security and configuration vulnerabilities can be the difference between a compromised system and an uncompromised one. When security tools identify issues, integration with EMS tools becomes critical to rapidly prioritize and remediate vulnerabilities. Yet few organizations have integrated these tools, leading to slower remediation times.

Supply chain vendors are progressively asking for **verification that systems and software are compliant with specific industry regulations**. Compliance is all too often thought of as an event. Organizations would be better served to verify compliance on an ongoing and continuous basis.

Reporting compliance verification to senior management and auditors can be challenging without continuous monitoring tools. Besides tracking, analyzing, and reporting on the current status of patching activities across all endpoints, IT organizations need to track compliance history as an overall percentage—a meaningful metric to gauge the progress of compliance efforts over time.

What's Needed

These **seven endpoint management capabilities** help operations and security teams to gain needed visibility, stop threats, and prove compliance, all while consolidating tools:

1. Comprehensive visibility.

- Rapid, continuous endpoint discovery and precise software and configuration inventory.
- Easy-to-visualize reporting with historical trending (compliance, inventory, and deviation).
- Drift detection and alerting.

2. Ease of management.

- Reliable, consistent software distribution.
- Fast, reliable patching, with high first-pass success rates.
- Configuration updates and verification.
- Automated software provisioning.

3. Continuous security hygiene.

- Continuous monitoring and patching.
- Configuration drift detection and remediation.
- Enforcement of security policies.

4. Continuous compliance.

- Continuous monitoring and verification of software and configuration against policy and regulations.
- Enforcement of regulatory policies.

5. Roaming endpoint management.

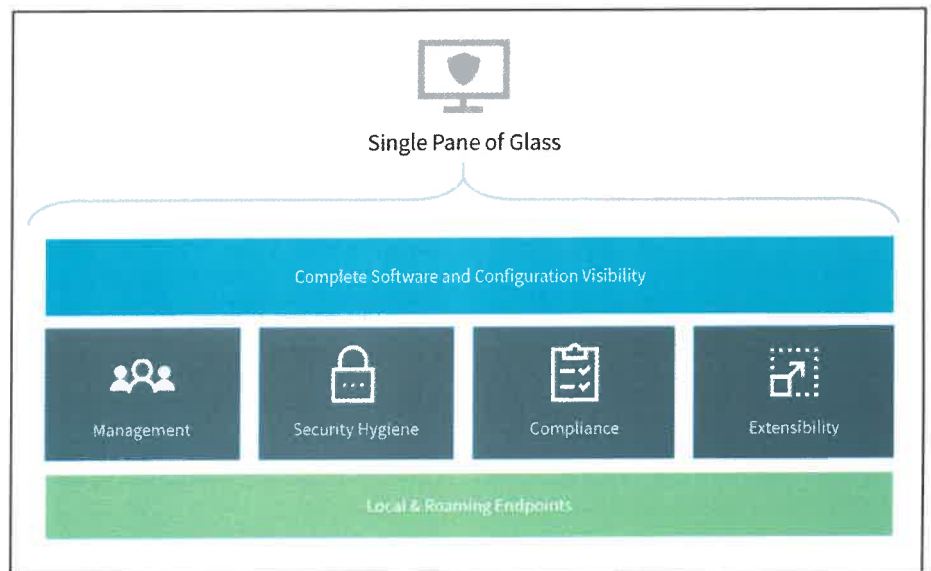
- Precise configuration control of remote endpoints.

6. Extensibility and integration with existing infrastructure.

- Out-of-the-box integrations with security tools, including endpoint protection platform (EPP) and security information and event management (SIEM) tools.
- APIs that expose all aspects of endpoint management to drive automation.

7. A single pane of glass across the endpoint fleet.

- Common view of all system assets, regardless of operating system, location, or connection type.



HCL BigFix: A Collaborative Endpoint Management and Security Platform

HCL BigFix is a full-feature endpoint management and security system currently deployed on and managing over 100M endpoints worldwide. It provides a turnkey approach to asset discovery, software distribution, and OS provisioning, leading to secure and compliant systems, regardless of operating system, location, or connectivity.

Discover assets rapidly (hardware and software inventory, software license and usage, and compliance reporting).

- Rapidly inventory endpoints across multiple operating systems, identifying all endpoints while providing accurate and current information about the installed software, software usage, and configuration.
- Gain near-real time visibility into endpoint information from an individual device or from groups of endpoints using BigFix Query.
- Identify unmanaged endpoints including potentially rogue devices connected to the network.

Manage easily (software patching, distribution, and provisioning).

- Quickly deploy and patch operating systems and third-party software with high first-pass success rates.
- Reduce annual software spend by assessing application usage and licensing.
- Manage secure configuration across all endpoints, including roaming remote systems.
- Share a common view of all hardware and software assets with both IT and security teams.

“BigFix is like an aircraft carrier. It is central to our solution and is the platform that we have built upon to rapidly deliver value to our customers. We chose BigFix because of its flexibility and its ability to easily integrate with all aspects of our solution.”

John Livingston, CEO, Verve Industrial Protection

Secure continuously (continuous monitoring and patching, enforcement of security policies, and proper configuration).

- Continuously monitor, patch, and enforce security policies across all endpoints, regardless of operating system, location, or connection type.
- Keep cloud-based endpoints, remote servers, and roaming (internet-facing) endpoints updated, secure, and always properly configured.

Enforce compliance in real time.

- Improve compliance reporting by providing out-of-the-box support for security benchmarks published by CIS, DISA, STIG, USGCB, and PCI-DSS.
- Enable endpoint compliance across Windows, UNIX, Linux, and Macintosh operating systems.
- Continuously monitor and enforce endpoint security configurations to ensure compliance with regulatory or organizational security policies.

Manage remote endpoints.

- Get full visibility of your servers, desktops, and laptops, regardless of location, connection, type, or status.
- Manage and patch both on-prem and internet-facing endpoints.
- Discover unmanaged assets to quickly bring them under management.

Integrate seamlessly.

- Integrate with endpoint detection and response (EDR) tools to help security teams better identify threats and operations teams remediate endpoints at scale.

- Integrate with network access control software (VPN clients, firewalls, etc.) to quarantine endpoints and enforce compliance.
- Enable SOC teams to see endpoint data within their existing security information and event management (SIEM) and incident response tools. Accelerate and improve incident response through discovery, enrichment, and automated response.
- Use a rich set of APIs to customize and automate endpoint management activities.

“BigFix is an incredibly powerful and versatile tool and has huge power to be customized. The ease of integrating BigFix with other tools has proven to be one of its most powerful strengths.”

Stacy Lee, Information Security Systems Specialist, Stanford University

Provide common view of assets.

- With BigFix’s single console and single platform, IT operations and security organizations can collaborate more effectively to cut operational costs, compress endpoint management cycles, enforce compliance in real time, and improve productivity.

Using BigFix, security and infrastructure teams can see and act on the same endpoint data without switching between multiple applications, saving them time and accelerating decision making. IT operations and security teams can collaborate more effectively to cut operational costs, compress endpoint management cycles, and enforce compliance in real time while improving productivity.

The Bigger Truth

Endpoint management software plays a critical role in both security and compliance strategies. With an ever-changing attack surface in most organizations, securing endpoints is an almost impossible task without automating the inventory, patching, and configuration process.

EMS is a core component of IT infrastructure, and as such, must facilitate integration with the many other risk management systems that are operating in the security stack. This integration is paramount to enabling both IT and security teams to keep up with the rapidly expanding threat landscape.

While there are many patching solutions available today, organizations should closely evaluate options to ensure they offer robust capabilities supporting both security and compliance requirements, while offering the scalability, flexibility, and extensibility to support organizational growth and complexity.

HCL BigFix, widely recognized as a leading endpoint management software solution, meets or exceeds the seven endpoint management capabilities and should therefore be strongly considered when organizations are adding or upgrading their EMS.

All trademarks herein are property of their respective owners. All other trademarks in this publication have been obtained by sources: The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain sensitive or confidential information. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of ESG, may constitute a violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you need any assistance, please contact ESG at 1-866-427-0188.



Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

© 2019 by The Enterprise Strategy Group, Inc. All Rights Reserved.



IBM QRadar on Cloud

QRadar on Cloud provides IBM security professionals to manage the infrastructure, while your security analysts perform the threat detection and management tasks. You can protect your network, and meet compliance monitoring and reporting requirements, with reduced total cost of ownership.

QRadar product capabilities

Review the following table to compare the capabilities in each QRadar product.

Capability	QRadar SIEM	IBM QRadar on Cloud	IBM QRadar Log Manager
Full administrative capabilities	Yes	No	Yes
Supports hosted deployments	No	Yes	No
Customizable dashboards	Yes	Yes	Yes
Custom rules engine	Yes	Yes	Yes
Manage network and security events	Yes	Yes	Yes
Manage host and application logs	Yes	Yes	Yes
Threshold-based alerts	Yes	Yes	Yes
Compliance templates	Yes	Yes	Yes
Data archiving	Yes	Yes	Yes
IBM Security X-Force® Threat Intelligence IP reputation feed integration	Yes	Yes	Yes
WinCollect stand-alone deployments	Yes	Yes	Yes
WinCollect managed deployments	Yes	No	Yes
Network activity monitoring	Yes	Yes	No
Asset profiling	Yes	Yes	No ¹
Offenses management	Yes	Yes	No
Network flow capture and analysis	Yes	Yes	No
Historical correlation	Yes	Yes	No
QRadar Network Insights integration	Yes	Yes	No
QRadar Vulnerability Manager integration	Yes	Yes	Yes
QRadar Risk Manager integration	Yes	No	No
QRadar Incident Forensics integration	Yes	No	No

Capability	QRadar SIEM	IBM QRadar on Cloud	IBM QRadar Log Manager
Vulnerability assessment scanners	Yes	Yes	Yes

¹ QRadar Log Manager tracks asset data only if QRadar Vulnerability Manager is installed.

Table 1. Comparison of QRadar capabilities

Cyber resilience: Manage and mitigate the high cost of cyber threats with Zerto

Prepare for, respond to and recover from a cyber attack

The State of IT Resilience 2019 survey clearly shows the growing threat of facing a cyber-attack, such as ransomware, specifically the threat of data loss and significant business disruptions. Out of the 500 organizations surveyed, IDC found that:

- **84%** experienced a malicious attack in the past 12 months
- **89%** of which were successfully attacked
- **93%** of these attacks resulted in data corruption or loss

Cyber-attacks are here to stay, with new variants and technical methods expanding every day. The result is these attacks are growing in both severity and volume. Traditional cyber security strategies aren't evolving fast enough nor protecting us in a business world expecting 24/7 availability.

Therefore, organizations are shifting their cybersecurity strategies towards cyber resilience. Instead of focusing exclusively on securing network parameters, many are shifting towards mitigating risk across global, hybrid-cloud environments.

Cyber resilience is preparing for, responding and recovering from a cyber-attack. It's not just about prevention anymore. Rather, it's about consistently ensuring the integrity of your critical data. Cyber resilience spans your people, process and technology.

People & process: Building a strong process and culture focused on cyber resilience

Without the right framework, you are completely susceptible to any form of cyber-attack. Modern IT organizations adopt a specific framework, such as the NIST framework, to ensure they have the right processes for every step of their cyber security approach. This includes processes and methodologies for threat protection, detection, identification, and recovery.

An excellent report from Gartner summarizes this: *How to prepare for and respond to business disruptions after aggressive cyberattacks*

[Click here to access the report.](#)

Having the right preparation is crucial, but equally important is deploying the right data recovery technology, such as the Zerto IT Resilience Platform™ that employs Continuous Data Protection (CDP).

KEY HIGHLIGHTS

Recovery in seconds

Recover entire sites, applications, VMs and files with granularity and within seconds

Application consistency

Restore entire multi-VM applications quickly from the same checkpoint for a consistent recovery

Short & long-term retention

Use Zerto's journaling technology across short- and long-term retention periods

Continuous non-disruptive testing

Perform recovery testing with no impact to production in an isolated environment with additional reporting capabilities

Data forensics

Isolate your data in a separate network and ensure its integrity before restoring back to production

Continuous Data Protection in an era of cyber threats

The IDC State of IT Resilience 2019 survey also found that 82 percent of respondents undergoing digital transformation believe that evolving their data protection is critically important to their digital transformation success. Why? Because traditional recovery solutions haven't evolved. The nature of snapshot backup technology leads to time gaps, data loss and lengthy recovery times that are a disruption to your entire organization.

The Zerto difference: Continuous Data Protection

Continuous stream of recovery points: The Elastic Journal combines the granular journal technology with long-term repositories, providing a continuous stream of recovery points from any point in time going back just seconds, to hours, months, or even years.

Application consistency: Protect and recover entire application stacks with guaranteed consistency through Virtual Protection Groups. Consistency is maintained across multiple virtual machines (VMs) no matter where they are running in your infrastructure.

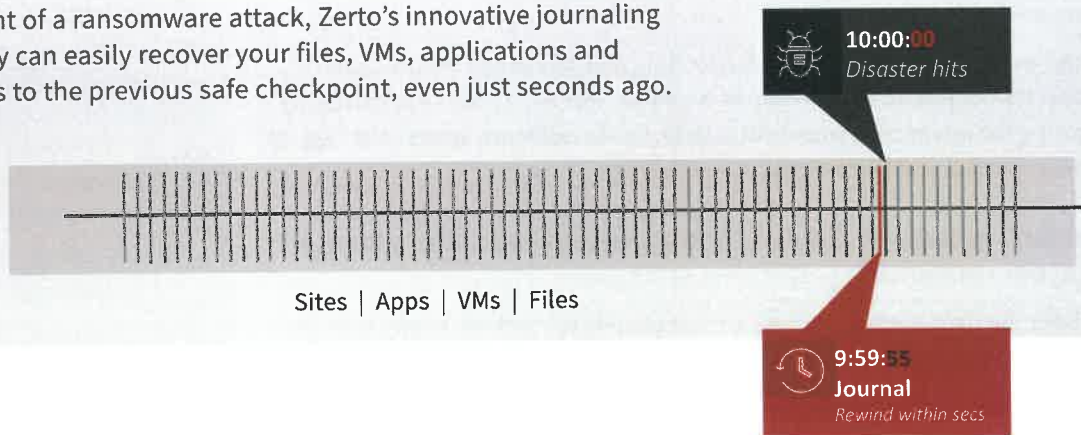
Continuous non-disruptive testing: Zerto's IT Resilience Platform™ enables orchestrated and automated disaster recovery testing, carried out any time, with just four simple clicks.

During our last ransomware attack, we were able to stop it within 15 minutes and be back up and running within 3 hours! Without Zerto, we would have had to pay the ransom and we still don't know if we'd be able to get our data back.

RUBYANNE O'BRYAN
Systems Administrator
ClearPath Mutual

Ransomware recovery in seconds

In the event of a ransomware attack, Zerto's innovative journaling technology can easily recover your files, VMs, applications and entire sites to the previous safe checkpoint, even just seconds ago.



SCHEDULE A DEMO

About Zerto

Zerto helps customers accelerate IT transformation by eliminating the risk and complexity of modernization and cloud adoption. By replacing multiple legacy solutions with a single IT Resilience Platform, Zerto is changing the way disaster recovery, data protection and cloud are managed. With enterprise scale, Zerto's software platform delivers continuous availability for an always-on customer experience while simplifying workload mobility to protect, recover and move applications freely across hybrid and multi-clouds. www.zerto.com

Copyright 2020 Zerto. All information may be subject to change.