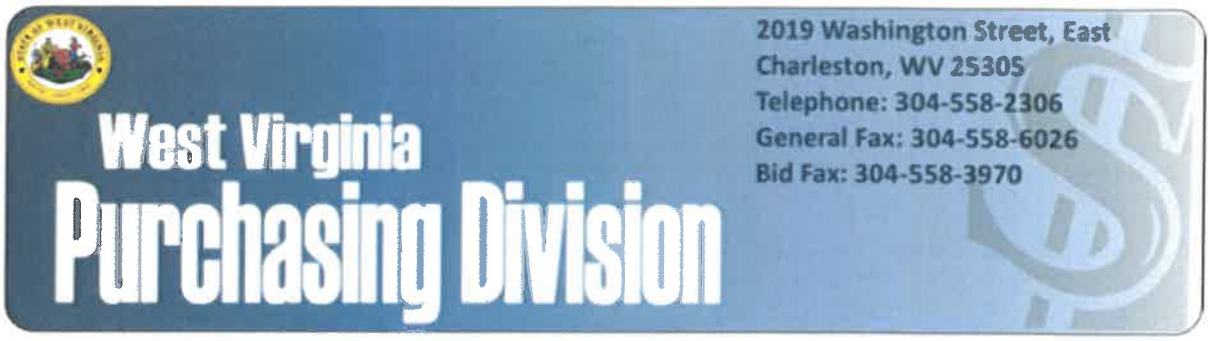
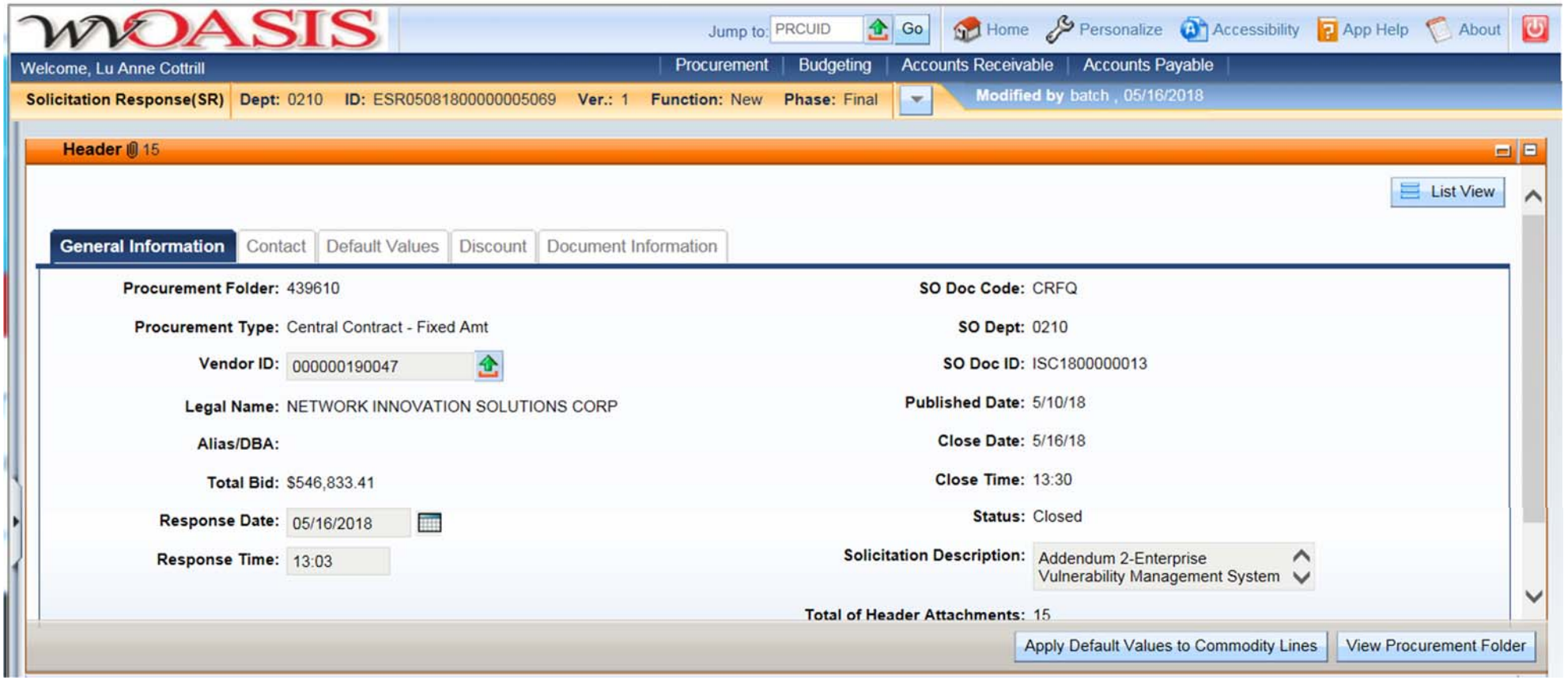


The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.


wvOASIS
Jump to: PRCUID Go
Home
Personalize
Accessibility
App Help
About
Welcome, Lu Anne Cottrill
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Solicitation Response(SR) Dept: 0210 ID: ESR05081800000005069 Ver.: 1 Function: New Phase: Final
Modified by batch , 05/16/2018
Header 15
List View
General Information
Contact
Default Values
Discount
Document Information
Procurement Folder: 439610
Procurement Type: Central Contract - Fixed Amt
Vendor ID: 000000190047
Legal Name: NETWORK INNOVATION SOLUTIONS CORP
Alias/DBA:
Total Bid: $546,833.41
Response Date: 05/16/2018
Response Time: 13:03
SO Doc Code: CRFQ
SO Dept: 0210
SO Doc ID: ISC1800000013
Published Date: 5/10/18
Close Date: 5/16/18
Close Time: 13:30
Status: Closed
Solicitation Description: Addendum 2-Enterprise Vulnerability Management System
Total of Header Attachments: 15
Apply Default Values to Commodity Lines
View Procurement Folder

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

State of West Virginia
Solicitation Response

Proc Folder : 439610

Solicitation Description : Addendum 2-Enterprise Vulnerability Management System (EVMS)

Proc Type : Central Contract - Fixed Amt

Date issued	Solicitation Closes	Solicitation Response	Version
	2018-05-16 13:30:00	SR 0210 ESR05081800000005069	1

VENDOR

000000190047

NETWORK INNOVATION SOLUTIONS CORP

Solicitation Number: CRFQ 0210 ISC1800000013

Total Bid : $546,833.41 **Response Date:** 2018-05-16 **Response Time:** 13:03:14

Comments:

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers

(304) 558-0246

jessica.s.chambers@wv.gov

Signature on File **FEIN #** **DATE**

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Enterprise Vulnerability Management System (EVMS), License	1.00000	EA	$124,908.970000	$124,908.97

Comm Code	Manufacturer	Specification	Model #
43233701			

Extended Description : 3.1.1-3.1.4.9 Enterprise Vulnerability Management System (EVMS), Annual License Service - 1 Year - 25,000 assets - Warranty Included

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Central Management Appliance	1.00000	EA	$22,500.000000	$22,500.00

Comm Code	Manufacturer	Specification	Model #
43210000			

Extended Description : 3.1.5-3.1.5.1.4 Central Management Appliance per specifications.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	System Deployment	1.00000	EA	$10,236.420000	$10,236.42

Comm Code	Manufacturer	Specification	Model #
81111500			

Extended Description : 3.1.6-3.1.6.3.1 System Deployment

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	License Optional Renewal Year 2	1.00000	EA	$129,729.340000	$129,729.34

Comm Code	Manufacturer	Specification	Model #
81112200			

Extended Description : 3.1.8 Optional Renewal Year 2

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
5	License Optional Renewal Year 3	1.00000	EA	$129,729.340000	$129,729.34

Comm Code	Manufacturer	Specification	Model #
81112200			

Extended Description : 3.1.8 Optional Renewal Year 3

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
6	License Optional Renewal Year 4	1.00000	EA	$129,729.340000	$129,729.34

Comm Code	Manufacturer	Specification	Model #
81112200			

Extended Description : 3.1.8 Optional Renewal Year 4

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: ISC 18000000 13

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)

[✓]	Addendum No. 1	[ ]	Addendum No. 6
[ ]	Addendum No. 2	[ ]	Addendum No. 7
[ ]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	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.

Network Innovation Solutions
Company

Authorized Signature

5-16-18
Date

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

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: ISC1800000013

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)

[ ]	Addendum No. 1	[ ]	Addendum No. 6
[✓]	Addendum No. 2	[ ]	Addendum No. 7
[ ]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	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.

Network Innovation Solutions
Company

Authorized Signature

5-16-18
Date

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

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

State of West Virginia
Request for Quotation
21 — Info Technology

Proc Folder: 439610

Doc Description: Addendum 1-Enterprise Vulnerability Management System (EVMS)

Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2018-05-10	2018-05-16 13:30:00	CRFQ 0210 ISC1800000013	2

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:

Network Innovation Solutions
821 4th Ave
Huntington, WV 25703
304-781-2282

FOR INFORMATION CONTACT THE BUYER

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

Signature X _____ **FEIN #** 46-1734617 **DATE** 5-16-18

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

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

State of West Virginia
Request for Quotation
21 — Info Technology

Proc Folder: 439610

Doc Description: Addendum 2-Enterprise Vulnerability Management System (EVMS)

Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2018-05-10	2018-05-16 13:30:00	CRFQ 0210 ISC1800000013	3

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:

Network Innovation Solutions
921 4th Ave
Huntington, WV 25703
304-781-2282

FOR INFORMATION CONTACT THE BUYER

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

Signature X [signature] **FEIN #** 46-1734617 **DATE** 5-16-18

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

NETWORK INNOVATION SOLUTIONS

Solicitation ISC1800000013

West Virginia OFFICE OF TECHNOLOGY

Delivered on:

05/08/2018

Submitted by:

Network Innovation Solutions

Enterprise Vulnerability Management System

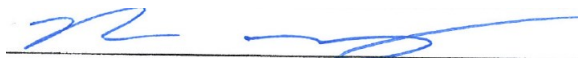
Solicitation ISC1800000013

Department of Administration
Office of Technology
1900 Kanawha BLVD E BLDG 5 10th Floor
Charleston, WV 25305

On behalf of Network Innovation Solutions, it is a privilege to submit the following response to the State of West Virginia Office of Technology for solicitation ISC1800000013. For more than five years Network Innovation Solutions has worked collaboratively across public and private sectors to ensure affordable IT products and services, creating a better business environment.

We have provided the WVOT with a price proposal for solicitation ISC1800000013 using Rapid 7 Insight Platform. This meets all specifications listed within the solicitation. We have attached all the documentation with the bid.

Please accept this response and commitment on the EVMS Project to WVOT. If you should have any questions, feel free to contact me by email rwhitley@gonis.us or by phone at 304-781-3410.



Sincerely,

Robert Whitley

Chief Executive Officer

Our Team Dedicated to WV Office of Technology

Robert Whitley - CEO

rwhitley@gonis.us

Jim Thomas - CTO

jthomas@gonis.us

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.

James Thomas CTO

(Name, Title)

(Printed Name and Title)

821 4th Ave Huntington, WV 25701

(Address)

304-781-3410

(Phone Number) / (Fax Number)

Jthomas@gonis.us

(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.

Network Innovation Solutions

(Company)

CEO

(Authorized Signature) (Representative Name, Title)

Robert Whitley CEO

(Printed Name and Title of Authorized Representative)

05/08/2018

(Date)

304-781-3410 304-781-6774

(Phone Number) (Fax Number)

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.

James Thomas CTO

(Name, Title)

(Printed Name and Title)

821 4th Ave Huntington, WV 25701

(Address)

304-781-3410

(Phone Number) / (Fax Number)

Jthomas@gonis.us

(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.

Network Innovation Solutions

(Company)

CEO

(Authorized Signature) (Representative Name, Title)

Robert Whitley CEO

(Printed Name and Title of Authorized Representative)

05/08/2018

(Date)

304-781-3410 304-781-6774

(Phone Number) (Fax Number)

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 exceed 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: Network Innovation Solutions

Authorized Signature: _____ Date: 05/08/2018

State of WV

County of Cabell, to-wit:

Taken, subscribed, and sworn to before me this 8 day of May, 2018.

My Commission expires 5-21, 2022

AFFIX SEAL HERE

REGINA REED
Notary Public Official Seal
State of West Virginia
My Comm. Expires May 21, 2022
Metro Community FCU
PO Box 5436 - 215 18th St. Huntington, WV 25703

NOTARY PUBLIC Regina Reed

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

State of West Virginia
Request for Quotation
21 — Info Technology

Proc Folder: 439610

Doc Description: Enterprise Vulnerability Management System (EVMS)

Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2018-04-17	2018-05-10 13:30:00	CRFQ 0210 ISC1800000013	1

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:

Network Innovation Solutions
821 4th Ave Huntington, WV 25703
Phone: 304-781-3410

FOR INFORMATION CONTACT THE BUYER

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

Signature X [signature] FEIN # 46-1734617 DATE 5-8-18

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

WV-10
Approved / Revised
09/15/17

State of West Virginia
VENDOR PREFERENCE CERTIFICATE

Certification and application is hereby made for Preference in accordance with ***West Virginia Code***, §5A-3-37. (Does not apply to construction contracts). ***West Virginia Code***, §5A-3-37, provides an opportunity for qualifying vendors to request (at the time of bid) preference for their residency status. Such preference is an evaluation method only and will be applied only to the cost bid in accordance with the ***West Virginia Code***. This certificate for application is to be used to request such preference. The Purchasing Division will make the determination of the Vendor Preference, if applicable.

1. [X] **Application is made for 2.5% vendor preference for the reason checked:**
Bidder is an individual resident vendor and has resided continuously in West Virginia, or bidder is a partnership, association or corporation resident vendor and has maintained its headquarters or principal place of business continuously in West Virginia, for four (4) years immediately preceding the date of this certification; **or,**

[ ] Bidder is a resident vendor partnership, association, or corporation with at least eighty percent of ownership interest of bidder held by another entity that meets the applicable four year residency requirement; **or,**

[ ] Bidder is a nonresident vendor which has an affiliate or subsidiary which employs a minimum of one hundred state residents and which has maintained its headquarters or principal place of business within West Virginia continuously for the four (4) years immediately preceding the date of this certification; **or,**

2. [ ] **Application is made for 2.5% vendor preference for the reason checked:**
Bidder is a resident vendor who certifies that, during the life of the contract, on average at least 75% of the employees working on the project being bid are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or,**

3. [ ] **Application is made for 2.5% vendor preference for the reason checked:**
Bidder is a nonresident vendor that employs a minimum of one hundred state residents, or a nonresident vendor which has an affiliate or subsidiary which maintains its headquarters or principal place of business within West Virginia and employs a minimum of one hundred state residents, and for purposes of producing or distributing the commodities or completing the project which is the subject of the bidder's bid and continuously over the entire term of the project, on average at least seventy-five percent of the bidder's employees or the bidder's affiliate's or subsidiary's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years and the vendor's bid; **or,**

4. [ ] **Application is made for 5% vendor preference for the reason checked:**
Bidder meets either the requirement of both subdivisions (1) and (2) or subdivision (1) and (3) as stated above; **or,**

5. [ ] **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**
Bidder is an individual resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard and has resided in West Virginia continuously for the four years immediately preceding the date on which the bid is submitted; **or,**

6. [ ] **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**
Bidder is a resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard, if, for purposes of producing or distributing the commodities or completing the project which is the subject of the vendor's bid and continuously over the entire term of the project, on average at least seventy-five percent of the vendor's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years.

7. [ ] **Application is made for preference as a non-resident small, women- and minority-owned business, in accordance with *West Virginia Code* §5A-3-59 and *West Virginia Code of State Rules*.**
Bidder has been or expects to be approved prior to contract award by the Purchasing Division as a certified small, women- and minority-owned business.

Bidder understands if the Secretary of Revenue determines that a Bidder receiving preference has failed to continue to meet the requirements for such preference, the Secretary may order the Director of Purchasing to: (a) rescind the contract or purchase order; or (b) assess a penalty against such Bidder in an amount not to exceed 5% of the bid amount and that such penalty will be paid to the contracting agency or deducted from any unpaid balance on the contract or purchase order.

By submission of this certificate, Bidder agrees to disclose any reasonably requested information to the Purchasing Division and authorizes the Department of Revenue to disclose to the Director of Purchasing appropriate information verifying that Bidder has paid the required business taxes, provided that such information does not contain the amounts of taxes paid nor any other information deemed by the Tax Commissioner to be confidential.

Bidder hereby certifies that this certificate is true and accurate in all respects; and that if a contract is issued to Bidder and if anything contained within this certificate changes during the term of the contract, Bidder will notify the Purchasing Division in writing immediately.

Bidder: Network Innovation Solutions **Signed:** _____

Date: 05/08/2018 **Title:** CEO

**Check any combination of preference consideration(s) indicated above, which you are entitled to receive.*

RAPID7

Cloud Security Overview

RAPID7 INSIGHT PLATFORM

Cloud Security Overview

RAPID7 INSIGHT PLATFORM

01 INTRODUCTION

Whether you're a Rapid7 customer today or tomorrow, it is important to us that you understand how Rapid7 secures the data you entrust to our Insight Platform. Just as within your own security-conscious organization, the initial proposal to develop software in the cloud was met with healthy opposition and a series of debates. Since our earliest days here at Rapid7 we have a sole focus on what our customers need, and thus we did not develop our cloud solutions to purely speed our time-to-market and simply apply security later. We carefully built the Insight Platform to equip security teams with modern data processing without the significant overhead of managing the infrastructure. We worked with our customers to methodically design the security controls necessary to ensure we are reducing the risk of compromise from the first day we started to provide these benefits.

> "Trust is the basis of relationships between individuals and companies"
>
> — Corey Thomas, Rapid7 CEO

Just as no two organizations' networks are the same, each cloud service is unique. Our well-read 2013 research into publically available data in Amazon Web Services (AWS) shed some light on the topic and it serves us well to reiterate what we wrote at the time:

"It should be emphasized that a public bucket is not a risk created by Amazon but rather a misconfiguration caused by the owner of the bucket."

It will be no surprise now that simultaneous to when this research was underway, our Products organization was evaluating multiple infrastructure-as-a-service (IaaS) providers and we determined the Insight Platform would best meet our customers' needs if built on AWS. Not only had we done our research, we had published it, critiqued it, and even shared it with the vendors. Based on this extensive work, it was clear that Amazon's continual release of innovative security controls gave us advantages we couldn't have realized were we building a traditional SaaS infrastructure in our own data centers.

In keeping with our usual Rapid7 approach, we mapped out the reasons someone would attempt to compromise our cloud, what data they would seek, and what methods they would use. We know attackers well because we help you defend against them every day, so it should be only natural for us to use this same mentality for our own solutions. This exercise is regularly run at Rapid7 and it steers all of the decisions we make to exceed the standards and expectations of our customers. As this was being discussed and tested, we focused on four key aspects of importance for securing our cloud:

1. How we collect your data
2. How we process your data
3. How we scale our infrastructure
4. How we automate our delivery

These are, not surprisingly, also the four primary benefits for which we designed the Insight Platform, and each has different security controls built directly into its core. In addition to all of these measures, we do exactly as we advise our own customers: we test their effectiveness against an attack. The Rapid7 team performs regular penetration tests and web application scans, but we also require penetration tests from parties not associated with Rapid7 to ensure unbiased results. Nothing is taken more seriously by the Rapid7 cloud development teams than potential risks discovered in these security assessments.

Let us now look at each of these four areas and how these controls were thought through.

02

SIMPLIFYING DATA COLLECTION FOR OUR CUSTOMERS

Rapid7's software, no matter the solution, is built to provide value to you, and this necessitates we make it easy for you to collect the relevant data for your security use cases. Whether the data provides an understanding of your organization's exposure to an attack or suspicious user behavior, our solutions must have access to various types of data, ranging from extremely sensitive to what may seem unimportant, in isolation. In considering the risks to our customers--and associated value to attackers—we designed all data collection and transmission to lower the possibilities of interception, impersonation, data mixing, and data poisoning.

Never Hold Onto the Attacker's Ultimate Prize

Much of the data collection for our solutions requires access to credentials with a high level of privilege on your networks. In our exercises to map out the motives and goals of an attack on the Insight Platform, these credentials were the ultimate prize – with them, an attacker can impersonate a legitimate user on a customers' network and move laterally into other systems. Considering this high risk and that the credentials only have value for the data collection taking place on your networks, we designed the Insight Platform to **never** have access to them in plain text. They are encrypted on the Collectors residing on your networks before transmission, and only ever decrypted on the Collector using a combination of the Collector's private key and the separate necessary parameters, which it must obtain from the cloud.

Only Trust the Right Source of Information

In considering how an attacker could attempt to impersonate a Rapid7 Collector or the Rapid7 Insight Platform, we established a single communication model that all data transmission must follow. Before any data can be transmitted from a customer's Collector to the Rapid7 Insight Platform, the Collector must first be registered with a dedicated customer's instance in the cloud via its unique activation key and fingerprint. Upon registration, all data from this collector will only ever be accepted by the corresponding customer instance with which it was registered. Any given activation key can be used for registration only once and the collector will only trust a recipient with its data upon verifying trust certificates with a signature chain meeting very specific criteria.

Every payload must be sent using this trust relationship, and the channel is never left open. All data transmitted to each customer's dedicated cloud instance is compressed and sent to the Insight Platform over the encrypted TLS channel. Each transmission must be initiated by the customer's registered Collector after mutual authentication has occurred. The cloud cannot initiate the communication with customer Collectors; it can only wait for requests from the Collector and respond with any necessary instructions for software updates or configuration changes. Communications to the cloud must be completely ignored if they are begun without the verification of an established trust relationship. There can be no exceptions to these rules.

03

PROVIDING ADVANCED ANALYTICS THROUGH MODERN DATA PROCESSING

After more than a decade packaging our software to run on-premise, the long internal debate over whether we would be adding enough value with cloud solutions finally ended when recent technologies opened new possibilities for processing massive amounts of data. With the advancement of IaaS providers, we could take advantage of cutting edge technology without the need to manage a new server every time we wanted to experiment with a new use case. After evaluating all of the market-leading providers, we chose the one we consider the most security-minded and innovative. Amazon runs one of the world's largest networks of web sites, and since early 2006, Amazon Web Services (AWS) has provided companies of all sizes with an infrastructure platform that powers business applications of tremendous scale.

With AWS, we have the ability to develop and run the advanced analytics you need with the right processing and storage technology for each. Our solutions that take advantage of the Insight Platform rely on various NoSQL and relational databases to store and process your data. Each Rapid7 customer is assigned their own relational database schema, which houses all asset names, other human-readable descriptions, and various public keys that support broader security processes related to your infrastructure. Much of the data processed and stored is encrypted at rest using various file or disk level encryption mechanisms.

Together, Rapid7 and AWS have a comprehensive approach to ensure security and reliability of the Rapid7 service. It starts with the physical datacenter, extends through the computer, network, and storage layers of the service, and is complemented by well-defined access policies and ongoing audit and certification by third parties.

Because "The Cloud" Is Still Made of Physical Servers

A secondary benefit of choosing Amazon as our IaaS provider was the mitigated risk of an attacker [or even our engineers] not having the ability to locate the physical servers running our software. AWS datacenters are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors and all physical access by employees is logged and audited routinely. When an employee no longer has a business need for these privileges, their access is immediately revoked, even if they continue to be an employee of Amazon.

Datacenter access and information is only provided to employees and contractors who have a legitimate business need for such privileges. All visitors and contractors are required to present identification and are signed in and continuously escorted by staff.

SAS 70 Type II

AWS has successfully completed a SAS70 Type II Audit, and is committed to continuously maintaining the appropriate security certifications and accreditations to demonstrate the security of their infrastructure.

AT-101 (SOC 2) Security Trust Service Principles

In addition to our own security policies, regular penetration tests, and application scans, we have a SOC II Type 2 in place for the foundation of our platform and are continuing to expand the specific compliance regimes for which we are audited.

Since Securing Your Own Cloud Is Enough Work

When considering other potential avenues of attack, we had to protect the Insight Platform against scenarios in which a different AWS customer gets compromised. By leveraging Amazon EC2 Security Groups in Virtual Private Clouds (VPCs), we logically isolate an extensive number of our services from both one another as well as the outside world. In addition to these controls, the AWS network provides protection against traditional network security issues including:

- *Distributed Denial of Service (DDoS) Attacks:* AWS network infrastructure leverages proprietary DDoS mitigation techniques developed as a result of running the world's largest online retailer. Additionally, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity.
- *Man in the Middle (MITM) Attacks:* Amazon EC2 VMs automatically generate new SSH host certificates on first boot and log them to the instance's console. Rapid7 leverages these secure APIs to access the host certificates before logging into an instance for the first time.
- *IP Spoofing:* Amazon EC2 VMs running the Rapid7 service cannot send spoofed network traffic. The AWS controlled, host-based firewall infrastructure does not permit an instance to send traffic with a source IP or MAC address other than its own.

04

AUTO-SCALING INFRASTRUCTURE TO MEET ANY SIZE CUSTOMER'S NEEDS

To truly offer you horizontally scalable solutions without any risk of one customer accessing another's data, we designed the Rapid7 Insight Platform around secure, multi-tenant services from its inception. Each data collector has its trust established with a specific instance in the cloud and any attempt to transmit data to a different instance would be completely ignored by the application to which the data is being sent. Similarly, each end user's account is tied only to the analytics and data to which its company owns, so the users experience each application as if it were built solely for their organizations.

To prevent any data sovereignty violations, every customer's instance of an application on the Rapid7 Insight Platform can only reside in that organization's global region of choice. While data replication is instrumented within each regional cloud, it will never be pooled across them. Given the extensive measures built into each cloud for redundancy and avoiding data loss during isolated service outages, Rapid7 has opted to use each region to host effectively independent clouds running the same version of each application. The flexibility to choose where you would like your data to reside is very important to us, especially given the variation in regulations affecting each customer.

To combat the possibility of Rapid7 employees getting their accounts compromised, because we have to recognize that it's possible for anyone, The Insight Platform's supporting infrastructure is designed to be fully automated to ensure security policies are consistently applied. These policies include two-factor authentication, bastion/jump hosting, service segregation, and by-service defined permissions ensuring least-privilege and access methodologies are applied.

05

CRAFTING AUTOMATED SOFTWARE DELIVERY TOOLS

Given the fast pace of the threat landscape and new exposure discoveries, the Rapid7 Platform Delivery team instruments the necessary tools to support the continuous deployment model we designed to respond to your needs in the fastest way possible. The combination of automated Amazon Machine Image (AMI) instance baking, least-privileges required, and AWS instance roles create a non-permissive environment that mitigates the ability of an attacker to easily move throughout the Rapid7 Insight Platform if they gained access to a specific system.

To remain secure while deploying software to production throughout the day, we use AWS Instance Roles to define the specific restricted-permission sets based on the server type. Instance roles dynamically receive AWS credentials used to authenticate with other AWS resources, eliminating the need to hard code or store credentials in a configuration service. Furthermore, the AWS Instance Role credentials are automatically changed by AWS frequently. The AWS SDK encapsulates the exact key rotation logic, but it is documented by AWS that the validity of these temporary credentials never exceeds a one-hour period.

Many SaaS vendors lose hours of productivity to manage an effective patch management program across the entirety of their data centers [unless they opt to rarely patch]. Cognizant of this challenge and the unacceptable risk of running our software on vulnerable servers, the Platform Delivery team built much of the Insight Platform software deployment process on AMI baking using Chef. As soon as a patch is released, we simply need to update the impacted base AMIs and restart them. By automating this within the deployment process, it ensures that each time new software is deployed or a solution is horizontally scaled, it is running on a fully-patched, properly configured virtual server.

To ensure our solutions are available when you need them without introducing risk through direct access, every EC2 instance (regardless of server type) is granted the necessary privileges to enable centralized, real-time monitoring of our servers and automated alarm notification email delivery.

One example of these mitigating controls and how they fit into the aforementioned exercise of thinking through how an attacker would attempt to compromise your data goes as follows:

- A data normalization server instance is granted permissions to read and poll the raw data upload buckets
- Every UI (web) server instance has no permissions whatsoever to access any S3 bucket
- If an attacker were to gain access to one of our AWS EC2 servers powering an application's web interface, they would not have permission to access raw data in S3

We have open sourced many components we've built to automate and secure our platform. If you'd like to take advantage of these components for your own software development, our public github repositories make them available for both use and contribution.

06
CONCLUSION

At Rapid7, we built the Insight Platform to meet our customers' evolving needs without demanding security professionals spend their time managing hardware, architecture, or scale. Unlike the many organizations which have attempted to add security later, every design decision and process proposal from the first day was evaluated for the risk it would introduce and security measures necessary to reduce it. We constantly strive to safeguard your data while incorporating cutting-edge technologies to more effectively address your needs.

We understand the inherent trust you are placing in us from the first byte of data you collect with our solutions and take this very seriously. Each aspect of our software, third-party technologies, infrastructure, and software development lifecycle involves deliberation and is opened to criticism from other parties. We have written this paper and deployed a Trust website in an attempt to be as transparent as possible with the public without revealing enough detail to put our customers at risk. If you would like to know more than is provided here or believe you can improve upon our approach, we welcome the conversation.

07
RECOMMENDED MATERIALS

If you'd like to learn more about Rapid7's approach to security, privacy, and trust, visit:
https://www.rapid7.com/trust/

If you would like to know more than is provided in this paper, our development team created a more in-depth Technical Primer we make available to our customers under NDA.

08

ABOUT RAPID7

With Rapid7 (NASDAQ: RPD), security and IT professionals gain the clarity and confidence they need to protect against risk and drive innovation. Rapid7 analytics transform data into answers, eliminating blind spots and giving customers the insight they need to securely develop and operate today's sophisticated IT infrastructures, networks, and applications. Rapid7 solutions include vulnerability management, penetration testing, application security, incident detection and response, SIEM and log management, and offers managed and consulting services across its portfolio. Rapid7 is trusted by more than 6,200 organizations across over 110 countries, including 38% of the Fortune 1000. To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.

RAPID7 PRODUCT CONSULTING

Vulnerability Management Deployment Services

Modern networks are no longer comprised simply of servers and desktops; remote workers, cloud and virtualization, and mobile devices mean your risk exposure is changing every minute. You need a vulnerability management solution as dynamic as your company; one that is quickly deployed and provides rapid time-to-value.

Rapid7's Product Consulting team is comprised of field experts with years of security experience, helping you extract the maximum value of our vulnerability management solutions. Our Deployment Services are tailored to operationalize your vulnerability management program, augmenting your deployment with product configurations, process automation, and reporting workflows. Working directly with your team and your current tools—onsite if you choose, we help you align InsightVM or Nexpose with industry best practices.* Rapid7 Deployment Services make the best use of valuable budget dollars and position you to maximize the success of your vulnerability management program.

Rapid7 Deployment Packages

Our model provides several deployment packages that have been carefully constructed based on the size of your environment, automated scanning needs, business-aligned configuration and reporting, and integrations with other solutions to enable end-to-end vulnerability management.

Environment Size (Live Endpoints)	Quick Start (InsightVM Only)	Basic	Standard	Enhanced	Premium	Premium+	Custom
0 – 5K	✓	✓	✓	✓	✓	✓	✓
5K – 50K			✓	✓	✓	✓	✓
50K – 100K				✓	✓	✓	✓
100K – 200K					✓	✓	✓
200K – 400K						✓	✓
400K +							✓

**All deployment packages can be delivered as an onsite service with the exception of Quick Start.*

DEPLOYMENT PHASES	Quick Start (InsightVM Only)	Basic	Standard	Enhanced	Premium	Premium+	Custom
Architecture							
Review deployment plan objectives	✓	✓	✓	✓	✓	✓	✓
Placement, specifications and connectivity for Console and Scan Engines	✓	✓	✓	✓	✓	✓	✓
Setup of AWS AMI Scan Engines				✓	✓	✓	✓
Configuration							
Scan Engine pairing	✓	✓	✓	✓	✓	✓	✓
Setup of Sites, Asset Groups, Tags, and Users tailored to your vulnerability management program	✓	✓	✓	✓	✓	✓	✓
Scan template optimization	✓	✓	✓	✓	✓	✓	✓
Scanning							
Strategizing and automating scanning in your enterprise environment				✓	✓	✓	✓
Authenticated/credentialed scanning best practices		✓	✓	✓	✓	✓	✓
Utilizing Automated Actions to scan dynamic environments			✓	✓	✓	✓	✓
Reporting							
Built-in reports walkthrough		✓	✓	✓	✓	✓	✓
Technical reporting workflows			✓	✓	✓	✓	✓
Executive reporting workflows				✓	✓	✓	✓
Data Analysis best practices				✓	✓	✓	✓
Insight Platform Features (InsightVM Only)							
Liveboards overview			✓	✓	✓	✓	✓
Customized cards tailored to your vulnerability management program				✓	✓	✓	✓
Track and prioritize remediation using Remediation Analytics					✓	✓	✓
Maintenance							
Automation of backup and maintenance tasks	✓	✓	✓	✓	✓	✓	✓
Disaster recovery best practices	✓	✓	✓	✓	✓	✓	✓

Integrations							
MS DHCP, Infoblox			✓	✓	✓	✓	✓
AWS, EPO, AD Mapping				✓	✓	✓	✓
Enterprise Work Flow Integrations • Splunk (up to version 6.3) • CyberArk • Thycotic • Lieberman • Cisco ISE • Palo Alto NGFW • ServiceNow Ticketing • BMC Remedy ITSM • Jira					Up to 1	Up to 2	Custom
Documentation							
As-Built Guide		✓	✓	✓			✓
Runbook					✓	✓	✓
Duration	2 days	3 Days	5 Days	10 Days	15 Days	20 Days	Custom

READY TO GET STARTED, FAST?

Contact us today:

+1-866-7RAPID7
+1-617-247-1717
sales@rapid7.com

Nexpose Certified Administrator: Introduction to Nexpose

What is it?

Are you a security professional that doesn't quite know where to begin getting an understanding of what kind of devices are in your environment, or how vulnerable some of them may be? Are you looking to deploy new vulnerability management software for your organization or just personal use? This two-day interactive class, led by a Rapid7 Security Consultant, will walk you through some basic to intermediate product features, best security practices, and techniques for vulnerability scanning various devices within a typical network environment.

The ***virtual*** class, which is hosted on a Rapid7 lab and delivered remotely, culminates in several exercises where users can apply learning in a fun, yet educational, simulation against multiple scenario driven target environments.

Customers who participate in Training ***on-site*** will experience hands-on opportunities to apply learned skills in a fun, yet educational, scenario in their own environment. The end result will be a strong understanding of Nexpose and how to use it to address your own network security goals.

All participants will have access to the **Nexpose Certified Administrator Exam** as part of their training program. Leverage the knowledge gained as part of the class to become a certified specialist and stand out from the crowd!

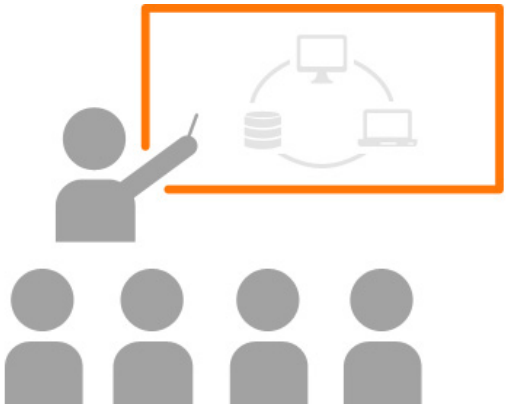
Who is the audience?

Geared toward security professionals who have little to no Nexpose experience, this hands-on training session is perfect for individuals within an organization who have been tasked with creating a security program from the ground up, or migrating from a different vulnerability management tool. Often over-taxed and under resourced, enabling security professionals the ability to learn how to use Nexpose will greatly enhance your understanding of your network. Those interested in automating your scanning and retrieving comprehensive reports for easy analysis will find this course a perfect fit.

What are the prerequisites?

Ideally, attendees should have experience with the following:

- Experience with Windows® and Linux Operating Systems
- Basic knowledge of network protocols
- Basic knowledge of IPv4 address spacing
- Vulnerability management system knowledge



What is the course content?

- Introduction to Nexpose
  - What is Nexpose and what are the main product components?
- Install
  - Requirements and recommendations
  - Performing a console backup
  - Installing and pairing a scan engine
- Operate
  - Getting Started with the console
  - Viewing results
  - Setting up sites
  - Running manual scans
  - Reporting on the environment

- Administer
  - Managing users, roles, and permissions
  - Managing scan credentials
  - Tuning scans
  - Creating custom report templates
  - Managing users
  - Creating custom scan and report templates

Course Agenda

Day 1

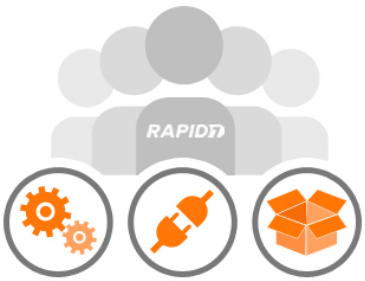
The first day will focus on vulnerability management methodology to give the attendee a refresher in the basic concepts and workflow of a standard vulnerability management program. During this session, we will complete a practical walkthrough of the Nexpose graphical user interface. Once and understanding of the Nexpose software is established attendees can progress to a number of activities to actually use the tool for scanning.

- Lecture – Introduction to Nexpose and the Architecture
- Activity – Restoring a backup
- Activity – Installing and pairing a scan engine
- Lecture – The Eight Scan Steps
- Activity – Creating a custom scan template and credentials
- Lecture – Slicing & Dicing – Organizing Your Data
- Activity – Running manual scans

Day 2

After working through the activities of day 1, the attendees will have a strong understand of Nexpose capabilities and can progress into more advanced labs. Day 2 will consist of lab and lecture and will conclude with outlying questions and delving into topics that may be specific to your particular environment.

- Lecture – Planning Your Deployment
- Lecture – Navigating the user interface
- Activity – Creating custom report templates and reporting
- Lecture – Vulnerability and Risk Scoring
- Lecture – Vulnerability Management
- Lecture – Administrative Overview
- Activity – Managing users



What is the cost?

- Open-enrollment class - $2,000 per student
- On-site class - $7,000 per course plus travel & expenses, up to 5 attendees
- Applicable CPEs: 16

Want to get started?

Call: 866.7.RAPID7 **Email:** sales@rapid7.com **Schedule:** http://www.rapid7.com/services

RAPID7 PRODUCT BRIEF

InsightVM

Live Vulnerability Assessment & Endpoint Analytics

As modern networks evolve, your risk exposure changes by the minute. Each year you see the amount of data grow exponentially, the threat of attacks become more sophisticated, and the challenges of minimizing risk and optimizing operations are becoming more challenging. It sometimes feels like a never-ending battle, but overcoming risk is possible by understanding it. How? Through shared visibility, analytics, and automation—principles core to the practice of SecOps.

Utilizing the power of Rapid7's Insight platform and the heritage of our award-winning Nexpose product, InsightVM provides a fully available, scalable, and efficient way to collect your vulnerability data, turn it into answers, and minimize risk. InsightVM leverages the latest analytics and endpoint technology to discover vulnerabilities in a real-time view, pinpoint their location, prioritize them for your business, facilitate collaboration with other teams, and confirm your exposure has been reduced.

"Rapid7 has already implemented what VRM will look like in the future."

— The Forrester Wave™: Vulnerability Risk Management, Q1 2018

SECURE YOUR MODERN NETWORK

Adapt to your modern network with complete ecosystem visibility, automated remediation, and SecOps agility. Pair that with unparalleled knowledge of the attacker mindset, and you'll be ready to act before impact.

Complete Ecosystem Visibility

- **Continuous Endpoint Monitoring Using the Insight Agent**
  The Rapid7 Insight Agent automatically collects data from all your endpoints, even those from remote workers and sensitive assets that cannot be actively scanned, or that rarely join the corporate network. Pair InsightVM with Rapid7 InsightIDR to get a complete picture of the risks posed by your endpoints and their users.
- **Liveboards, Not Static Dashboards**
  Drawing from fresh vulnerability data, InsightVM Liveboards are live and interactive by nature. You can easily create custom, tailored cards and full dashboards for anyone—from sysadmins to CISOs—and query each card with simple language to track progress of your security program. Visualize, prioritize, assign, and fix your exposures more easily than ever before.
- **Cloud, Virtual, and Container Assessment**
  InsightVM integrates with cloud services, virtual infrastructure, and container repositories like Amazon Web Services, Microsoft Azure, and VMware to make sure you don't miss any new instances and Docker containers that are brought online. You can also correlate deployed containers to assets, so you can secure both containers and container hosts—all at no additional cost.

Automated Remediation Workflows

- **Live Remediation Planning**
  Assign and track remediation duties in real time with Remediation Workflows. InsightVM integrates with IT ticketing solutions like Atlassian Jira and ServiceNow, making it easy for IT to take action. InsightVM also integrates with Rapid7 Komand, our security orchestration and automation platform, to expose your most critical vulnerabilities and bring automation to the patching process.
- **Attacker-Based Risk Analysis**
  Prioritize risk the way attackers would. InsightVM translates decades of attacker knowledge into proven analytics. The granular, 1-1000 Real Risk score takes into account CVSS scores, malware exposure, exploit exposure and ease of use, and vulnerability age. This makes it simpler—and more precise than CVSS alone—to prioritize vulnerabilities for remediation. Rapid7 Project Sonar data and threat feeds translate to dashboards within InsightVM, so you can understand which external network doors you're missing and which vulnerabilities attackers are actively exploiting.

SecOps Agility

To move faster and more securely, you need to go beyond scanning in silos. InsightVM is built to enable collaboration with IT operations and developers through shared visibility, analytics, and automation.

What does this look like in practice? InsightVM integrates with IT's existing workflows and ticketing systems to provide remediation instructions with context, thus accelerating remediation, and provides actionable reporting on program progress for every audience—from IT and compliance to the C-Suite. On the DevOps side of the house, InsightVM lets you assess containers to ensure services are secure before they go into production, and the Rapid7 Insight Agent helps infrastructure teams automatically assess new cloud infrastructure as soon as it goes live.

Compliance and Secure Configurations, Without the Headaches

Show auditors how your environment has changed over time, demonstrating how you're compliant against PCI DSS, NERC CIP, FISMA (USGCB/FDCC), HIPAA/ HITECH, Top 20 CSC, DISA STIGS, and CIS standards for risk, vulnerability, and configuration management. Take it one step further and harden your systems based on industry best practices like CIS and DISA STIG to get your network in shape.

"Thanks to the endpoint agent, these dashboards are the best view we have of our security posture across the whole organization, and remediation workflows make it easy for IT to incorporate remediation into the rest of their work."

- Sierra Vista Medical Center

READY TO GET STARTED?

Start your free 30-day trial of InsightVM today.

RAPID7 PRODUCT BRIEF

R7-5000X Appliance
For Rapid7 InsightVM or Nexpose

Overview

The Rapid7 R7-5000X Appliance is the hardware solution for simple deployment of the InsightVM or Nexpose product in your environment.

Simple Deployment

The R7-5000X Appliance is a pre-configured plug-and-play Appliance for simple deployment. With security in mind, Rapid7 has hardened the Appliance by ensuring that only required services are running on it.

Installation

The Rapid7 Appliance base OS is a minimal install of Ubuntu 14.04.
A minimal install provides the following benefits:

- Approximately 270 packages (a full server install typically consists of over 750 packages)
- Reduced attack surface (fewer packages to exploit)
- Faster patching (fewer packages to upgrade)

Security Consoles or Scan Engines

You can use a Rapid7 Appliance for an InsightVM or Nexpose Security Console, which provides an easy-to-use web interface to manage your vulnerability management program, or you can select a scan engine to increase your scanning performance.

3 Year Warranty

Rapid7 provides a three year warranty with the Appliance, coverage for all parts, and next business day on-site response or parts replacement to ensure dependable performance in your environment and a successful vulnerability management program.

KEY BENEFITS

- **Simple deployment** allows you to plug-and-play the Appliance for a successful vulnerability management program.
- **Reduced total cost of ownership**: Pricing includes Next Business Day Response warranty coverage as well as parts replacement.
- **Scalability** allows you to easily add new appliances as your environment grows.

082417

R7-5000 Specifications

Processor	(2) Intel® Xeon® E5-2609 v4 2 x 1.7 Ghz (8 cores)
Memory (GB)	256GB
Memory (Type)	Registered DIMMs, 2400 MHz
Storage (Total)	(16) 1TB drives — RAID 10 (1+0)
Storage (Available)	8TB
Operating System	Ubuntu Server 14.04 LTS (Hardened)
Delivery (Shipping ETA)	1-2 Weeks
Dimensions	Rack Units 2U 3.44 x 17.54 x 26.75 inches (8.73 x 44.55 x 67.94 cm) 51.5 lb (23.6 kg)
Network	HP Embedded 1Gb Ethernet 4-port 331i Adapter
Power (Supply)	(2) HP 500W Flex Slot Platinum Power Supply
Display	(1) VGA Rear
Ports	(1) USB 3.0 Front (2) USB 3.0 Rear (2) GbE Rear (1) Dedicated iLO connector
Storage Controller	HP Dynamic Smart Array B140i Controller HP Smart Array P440ar/2G FIO Controller
Other	Hazardous Material: None contained Serialized: Unique Serial Number per Appliance Country of Origin: USA/Mexico

About InsightVM

InsightVM is Rapid7's premier vulnerability management solution, providing a fully available, scalable, and efficient way to collect vulnerability data, turn it into answers, and minimize your risk. InsightVM is the evolution of our award-winning Nexpose product, and utilizes the power of the Rapid7 Insight Platform, our cloud-based security and data analytics solution.

The Rapid7 Insight Platform brings together Rapid7's library of vulnerability research, exploit knowledge, global attacker behavior, internet-wide scanning data, exposure analytics, and real-time reporting. InsightVM uses this platform to enable IT and security teams to collaborate and partner together through the use of continuous endpoint monitoring, dynamic dashboards, and end-to-end remediation workflows.

As a core component of Rapid7's security data and analytics platform, InsightVM promotes an active, analytics-driven approach to cybersecurity. Try it for free today at www.rapid7.com/insightvm.

About Nexpose

Rapid7 Nexpose is a threat exposure management solution that dynamically collects data and analyzes risk across vulnerabilities, configurations, and controls, from the endpoint to the cloud. Nexpose is engineered to enable IT security teams to identify, assess and respond to critical change as it happens with Adaptive Security. Users can more efficiently manage risk found in operating systems, third-party software, Web applications, browsers and databases all in one solution with over 68,000 vulnerabilities and 163,000 vulnerability checks. The unique integration with Rapid7's Metasploit, RealRisk score, and contextual business intelligence make Nexpose a threat exposure management solution that prioritizes remediation and helps reduce risk. Its user-interface, and smart analytics—such as the Top 25 Remediation report and custom reporting—allow security teams to communicate risk and remediation more effectively. Nexpose could be used to improve a company's overall risk posture to better comply with regulations, including security requirements for PCI, CIS, HIPAA, HITECH Act, FISMA (including SCAP Compliance), Sarbanes-Oxley (SOX), and NERC CIP. Nexpose, as a core component of Rapid7's Security Data and Analytics platform, promotes an active, analytics-driven approach to cybersecurity.

About Rapid7

With Rapid7, technology and security professionals gain the clarity, command, and confidence to safely drive innovation and protect against risk. We make it simple to collect operational data across systems, eliminating blind spots and unlocking the information required to securely develop, operate, and manage today's sophisticated applications and services. Our analytics and science transform your data into key insights so you can quickly predict, deter, detect, and remediate attacks and obstacles to productivity. Armed with Rapid7, technology professionals finally gain the insights needed to safely move their business forward. To learn more about Rapid7, visit www.rapid7.com.

LEARN MORE

About InsightVM and supporting services at:
www.rapid7.com/insightVM

About Nexpose and supporting services at:
www.rapid7.com/nexpose

White Paper

Leveraging Security Risk Intelligence

The strategic value of measuring Real Risk™

Introduction

Every battlefield commander understands the strategic necessity of reliable intelligence. Winning battles depends on accurate understanding of enemies, their tactics and goals, weighing risks against potential damage, and deploying resources to mitigate or neutralize threats. Gathering information is just a starting point; more importantly, is any of it relevant or meaningful? Within all the chatter and noise, effective commanders discern the one percent of useful intelligence and follow through with action.

Every IT security professional knows that the battle to protect IT resources and data is fully engaged. In its *2011 Data Breach Investigations Report*, Verizon studied 761 data compromise incidents that occurred in 2010, compared to just over 900 total breaches studied between 2004 and 2009. Verizon reported that of all breached records, 50 percent involved some form of hacking and 49 percent included use of malware.

The ongoing struggle to prevent hackers from breaching assets and malware from gaining a foothold requires a vulnerability management strategy that begins with a comprehensive measurement of security risk. Organizations must examine the entire IT stack, including the operating system, network, applications, and databases. The cycle of discovering assets, capturing and processing vulnerability data, identifying actual risks, testing and prioritizing mitigation tasks, and verifying effective controls grows more complex with every new technology that adds convenience but multiplies risk of a breach or incident. These new technologies include dynamic, virtualized environments and services outside traditional physical IT infrastructures, such as virtualized, cloud-based services and social networking.

Figure 1: The Security Risk Intelligence cycle – a holistic approach to minimizing risk

Rapid7 addresses the need for dynamic, in-depth risk management with Security Risk Intelligence, a holistic approach to minimizing risk (Figure 1). It is based on a unified solution set that includes vulnerability management, penetration testing, and best practices. Security Risk Intelligence helps organizations detect vulnerabilities, prioritize risks, and validate threats in a closed-loop system.

Beginning with an understanding of the need for effective risk management followed by a definition of the elements of risk, this discussion presents the advantages and strategic value of Rapid7 Security Risk Intelligence for your environment and illustrates its operation.

Situation report: State of the Battlefield

Attacks are smarter, sneakier, and easier to perpetrate than ever. The Verizon report found that "96 percent of breaches were avoidable through simple or intermediate controls," that 50 percent of records breached used some form of hacking, and 49 percent of records breached incorporated use of malware. Incidents investigated during 2010 presented "the largest caseload ever; it was also extremely diverse in the threat agents, threat actions, affected assets, and security attributes involved."

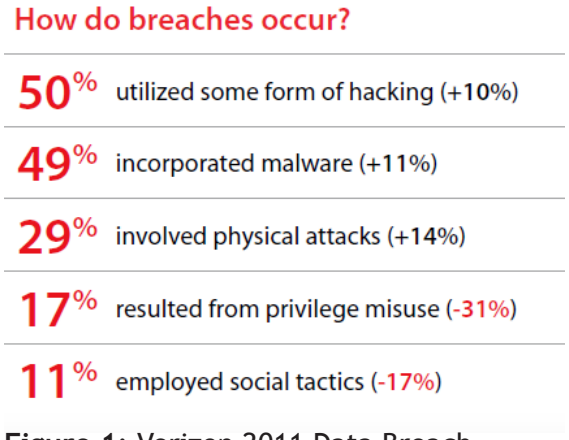


Figure 1: Verizon 2011 Data Breach Investigation Report (% change from 2010 report)

Security professionals struggle to reduce risk with limited staff and budget. To achieve effective risk management, they must abandon the limitations and expense of traditional, reactive approaches in favor of a proactive, data-driven investment model. They must overcome several challenges: interpreting massive amounts of data, monitoring dynamic assets, incorporating both compliance and security into best practices, moving beyond traditional "scan-and-patch" approaches to implement security best practice programs, and trusting conventional prioritization methods beyond their scope.

Data through a fire hose. Most security policies address some form of vulnerability management. Security professionals depend upon accurate assessments to determine whether intervention is necessary and implement proper steps for mitigation or remediation. There is no problem obtaining data: security devices and scanners generate terabytes of it. The challenge is interpreting data: identifying those specific vulnerabilities that truly represent a clear and present risk to security.

Security operators need solutions that help them distinguish the danger signals from the noise. For example, a mission-critical Web server may have ten known vulnerabilities, but which of those ten present genuine risk? Vulnerability management solutions should identify and dismiss seven of those attacks as "noise" and flag the other three as "signals" that require their attention.

Dynamic assets, static tools. Virtualization is re-defining how IT operations build and deliver services, but vulnerability scanners have not kept up. Traditional scanners provide a snapshot that goes obsolete within hours or minutes within a virtualized environment where VMs go online and offline or change hosts all day long. Virtualized environments—and the risks they present—are constantly changing, and scanners need a continuous discovery feature that tracks these changes as they occur.

Compliance does not equal security. Another challenge is the perception that attaining compliance (e.g., PCI, HIPAA, NERC, FDCC) reduces risk to acceptable levels. A breach of an asset unrelated to compliance can lead to the compromise of assets deemed compliant. Organizations spend billions of dollars on security solutions to address compliance, but most of them do not focus on deploying those solutions for maximum benefit beyond compliance.

Risk reduction encompasses more than "scan-and-patch." Many enterprises trust that "scan-and-patch" methods keep them secure. Patching inherently keeps hackers ahead, because vendors typically issue patches in response

to hacking incidents. While patching remains an important security step, security professionals need a variety of proactive solutions and best practices to put them ahead of hackers and malware.

Conventional risk prioritization doesn't tell you enough. For example, many enterprises rely solely on CVSS scores to define thresholds for mitigation. These base CVSS metrics measure only the potential risk (likelihood plus impact) of a given vulnerability, not requiring temporal or environmental metrics to calculate it's score. As such, base metrics CVSS scores do not consider the whole context of the identified vulnerability to the organization. Consider two vulnerabilities: one with a base metric CVSS score of 9 that is not exploitable, versus one with a CVSS score of 5 that is exploitable. A CVSS score of 9 may prompt a network operations manager to prioritize the fix of that vulnerability over the vulnerability with a score of 5. However, when the local environment is taken into consideration, and it becomes known that the higher CVSS scored vulnerability is not exploitable, while the lower vulnerability is, then it becomes obvious that the exploitable vulnerability should take priority.

For example: MS10-022: "Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution" has a CVSS score of 7.6. This score is deceptively low, because this particular vulnerability is exploitable by a malware kit. Rapid7 Metasploit software can exploit it. The actual risk associated with this particular vulnerability is greater than its CVSS score indicates and the Rapid7 Real Risk score of 867 (out of a total of 1000) more accurately reflects the severity of this particular vulnerability.

Elements of Risk

The battlefield commander relies upon useful intelligence to help determine the most effective way to deploy assets and forces. The commander needs to understand the advantages and limitations associated with terrain: desert or forest, mountains or plains; where the enemy is most likely to attack: by air, water, or land, across a field or bridge; what the enemy wants to accomplish: blow up the bridge or cross it and blow up a munitions depot; predict the consequences of a potential enemy incursion; and what to do to win the battle.

On the IT battlefield, security professionals need to measure the likelihood that a given vulnerability will be exploited and the potential impact such an exploit would cause. It is the security professional's mission to identify the critical vulnerabilities, quantify unacceptable risk levels, and then decide what, if anything, to do. It is impractical, and unnecessary, to attempt to remediate every vulnerability listed on a scan report. Most vulnerabilities present low risk for various reasons. Perhaps the asset is non-critical, or it is not exploitable by a malware kit, or compensating controls, such as a firewall, protect it.

Security professionals measure risks using four parameters: Exposure, Likelihood, Impact, and Mitigation (see Figure 2 below). A combination of automated and expert risk intelligence methods qualifies and quantifies actual risk. Automated risk intelligence is vulnerability scanning with a solution such as Rapid7 Nexpose. Expert risk intelligence is penetration testing with a solution such as Rapid7 Metasploit. The depth and breadth of these methods determines the success of the risk assessment and mitigation process. Following is a chart of questions associated with each parameter, followed by a list of capabilities that will support security professionals in their quest to answer those specific questions.

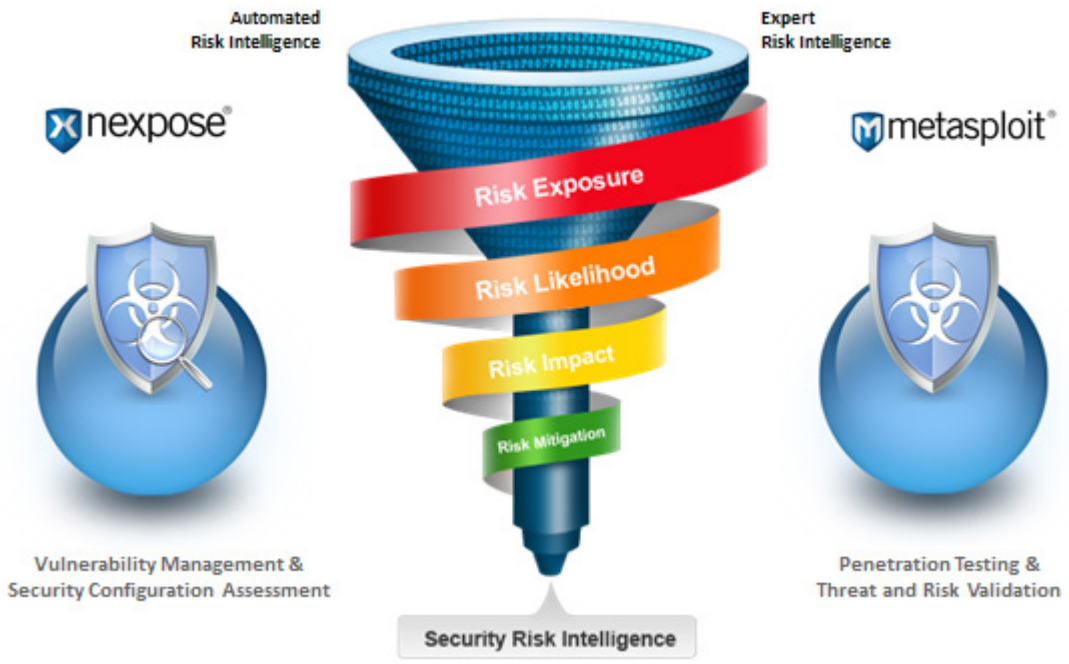


Figure 2: Accurate risk measurement requires both automated and expert risk intelligence.

Risk Exposure

Exposure determines where an attack might occur.

- Have I identified all potential risk exposure across my environment?

Automated Risk Intelligence	Expert Risk Intelligence
• Environment attack surface discovery and analysis • Network, OS, database, and application vulnerabilities • Web application scanning • Policy and configuration compliance • 0-day coverage • Vulnerability chaining • Support for virtualized environments	• Threat attack surface discovery and analysis • Social engineering • Network, OS, database, and application vulnerabilities • Advanced exploit research • Breach path analysis • Controls assessment and validation • Exploitations • Brute force password audits • Cross-site scripting

Risk Likelihood

Likelihood assesses whether an identified vulnerability presents an actual danger, accounting for the complexity of actually exploiting a given vulnerability (access complexity), the difficulty in reaching the specific vulnerability (access vector), and authentication requirements needed to exploit the vulnerability.

- Is there a clear path to the assets in question?
- Are the vulnerabilities exploitable?
- What is the level of authentication required in order to exploit a given vulnerability?

Automated Risk Intelligence	Expert Risk Intelligence
• Consistent, single point of view • Risk scoring determination based on vulnerability age, existence of known exploits and malware kits integrated with CVSS metrics	• Determination of access complexity • Confirm exploitability of identified vulnerabilities • Assess the level of authentication required to successfully exploit this vulnerability

Risk Impact

Impact measures the consequences of a security incident resulting from exploitation of a vulnerability. It considers asset or data confidentiality, integrity, and availability.

- How business-critical are the assets at risk?
- What data or information does an attacker gain access to when a vulnerability is exploited?
- What are the consequences if an incident occurs?

Automated Risk Intelligence	Expert Risk Intelligence
• Asset criticality: weighting the importance of this asset • Vulnerability chaining: assessing the “ripple-affect” of an exploited vulnerability	• Post-exploitation analysis and VPN pivoting • Automated reporting for all stakeholders

Risk Mitigation

After determining what Real Risks are present in your environment, you will want to determine what mitigation and remediation efforts you want to take.

Risk mitigation takes steps to prevent or allay security incidents.

- What actions should I take? Should I remediate, mitigate, defer, transfer, or accept this risk?
- When do I need to take this action?
- What is my acceptable level of risk? And, am I adding in any new risk with my proposed solution?

Automated Risk Intelligence	Expert Risk Intelligence
• Remediation reporting • Integration with best-of-breed penetration testing and mitigation systems	• Root cause analysis • Mitigation verification

Assessing the Battlefield: Security Risk Intelligence

Combining vulnerability management, penetration testing, and best practices, Rapid7 Security Risk Intelligence re-defines and improves risk management. Security Risk Intelligence delivers the combination of qualitative and quantitative risk analysis that security professionals need to tackle the multi-faceted challenges of achieving useful information about risk. It measures contextual risk, provides step-by-step mitigation instructions, and enables rapid, trustworthy verification.

Security Risk Intelligence generates a Real Risk score. A Real Risk score adjusts a CVSS value based on contextual elements that analyze each risk element separately, for the first time incorporating both temporal and governance parameters. This provides greater insight into overall risk posture and drives more efficient risk reduction practices.

$$\text{Rapid7 Real Risk} = \frac{\text{CVSS Impact Metrics}}{\text{CVSS Likelihood Metrics}} \times \text{Exposure}\left(\begin{matrix}\text{Malware Kits} \\ \text{Exploit Rank}\end{matrix}, \text{time}\right)$$

Figure 3: Calculating Real Risk utilizes both standard and environmental metrics for contextual insight

Temporal parameters weigh the age of a vulnerability against the likelihood that a hacker tool or malware exists to exploit it. The temporal score increases over time, bringing vulnerabilities to the attention of security managers before an incident occurs.

For example, the Troj/Protux-Gen attack in 2009 exploited MS06-028, a seemingly innocuous vulnerability in Microsoft PowerPoint patched in June 2006. The rising temporal score would have flagged that vulnerability, enabling remediation before the attack commenced.

Governance parameters follow internal policies that qualify the criticality of assets, raising or lowering risk scores accordingly and establishing where compensating controls should be put in place.

For example, a company has a proprietary software application that runs on a 2003 version of Microsoft Windows NT. Patching the server would cause the application to crash. The company is unwilling to invest millions of dollars in an application upgrade with minimal business value. The security team implements compensating controls such as an intrusion protection system and a dedicated firewall, tests the

effectiveness of these measures, and if successful, files an exclusion for this specific vulnerability. This governance process reduces the Real Risk score by including the vulnerability exception put in place in response to the old OS version.

Tactical: Components of Rapid7 Security Risk Intelligence

Rapid7 Security Risk Intelligence is a combination of award-winning solutions and expertise that enable closed-loop risk verification and risk validation (see Figure 4 below):

Rapid7 Nexpose—Provides automated risk intelligence. It presents reports that prioritize critical and non-critical vulnerabilities using a contextual Real Risk score, provides step-by-step instructions for mitigation or remediation, and directly integrates with Metasploit. Its comprehensive vulnerability scanner uses one of the world's largest databases of known vulnerabilities. The Nexpose database lists more than 75,000 vulnerability checks for more than 22,000 vulnerabilities. A large or mid-sized business easily generates a vulnerability report with 5,000 identified vulnerabilities, but only a fraction of them are exploitable and present a current and concrete risk. Rapid7 worked with VMware to build the first vulnerability-scanning solution that offers continuous discovery of dynamic assets in virtualized environments. It is the first vulnerability management solution included in the VMware security reference architecture.

Rapid7 Metasploit—Provides expert risk intelligence. Its powerful penetration-testing capabilities think like a hacker, using the world's largest database of known exploits. It allows security operators to validate critical vulnerabilities, verify successful mitigation, and automatically update Nexpose to reduce false positives.

Self-serve expertise—Enhance your own skills with Rapid7 training in best practices, world-class customer support, and straightforward user interface in Rapid7 solutions. The Rapid7 Community (https://community.rapid7.com/index.jspa) empowers security professionals with a forum for sharing content, collaborating on best security practices, and providing feedback.

Rapid7 Professional Services—Provide expertise for periodic assessments, testing, mitigation, and application of security best practices.

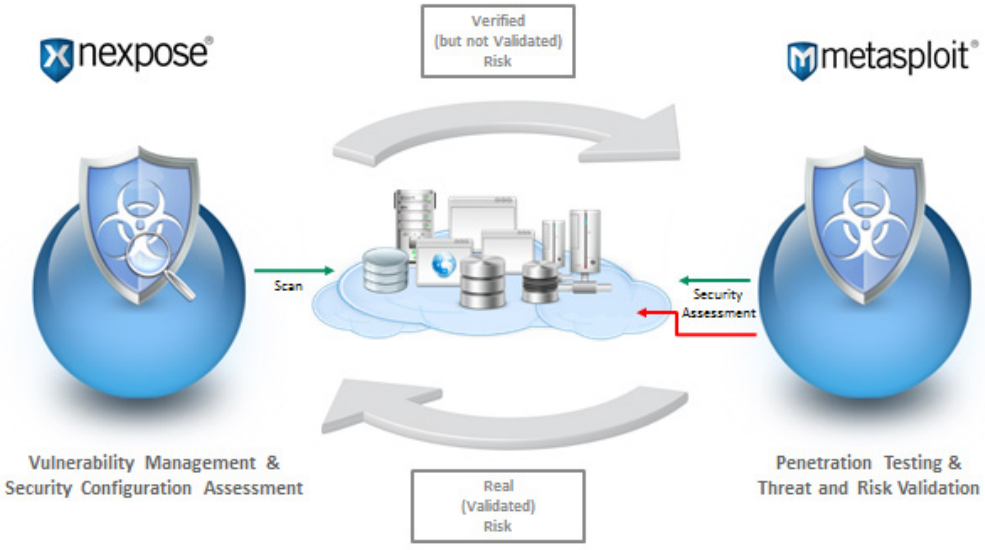


Figure 4: Closed-loop Security Risk Intelligence from Rapid7

Benefits of Security Risk Intelligence

The benefits of implementing a Security Risk Intelligence strategy include:

Improve business decision-making through better insight. High-quality risk intelligence helps security professionals improve operational practices and technology investment. For example, server managers can work with the security manager to test and harden servers and virtual machines before they go online. Business intelligence; security information and event management; and governance, risk-management and compliance tools can use security risk information to determine the success of risk-management and compliance-management practices and whether a risk requires further mitigation.

Create operational efficiencies with repeatable best practices. Nexpose reports help security managers deliver clear, correct, prescriptive advice to server and network administrators tasked with mitigation and remediation. Metasploit helps security professionals validate vulnerabilities and verify that mitigation steps provide protection. This closed-loop system is more effective than the endless "scan-and-patch" cycle that often plagues network administrators using other vulnerability scanning solutions, allowing them to meet the needs of the security team along with their other IT infrastructure responsibilities.

Incorporates compliance requirements. Security Risk Intelligence helps security managers view compliance as one aspect of a security practice, not the end goal. Enlarging the perspective of what needs securing also leads to compliance.

Measurably reduce risk level over time. When Security Risk Intelligence is the basis of regular vulnerability management operations, organizations can substantially reduce their overall risk posture over time. Using an iterative approach to continuously identify the highest risks alongside risk trending for critical assets, organizations can establish best practices for risk reduction.

Reduce signal-to-noise ratio. With Real Risk scoring, Nexpose and Metasploit provide reliable intelligence that quantifies the criticality of a given risk and supports threshold-based management decisions to cost-effectively reduce risk and strengthen security postures.

Improve existing investments in third party security solutions. Both Nexpose and Metasploit are essential intelligence systems that feed data into third-party systems such as Governance, Risk Management & Compliance solutions (GRC), security information and event management (SIEM) and intrusion prevention system (IPS) solutions, such as Sourcefire, making those tools more effective. For example, Rapid7 vulnerability data can be imported into the Sourcefire Defense Center® (http://www.sourcefire.com/security-technologies/cyber-security-products/3d-system/centralized-management). The vulnerability data adds to visibility gathered by Sourcefire RNA (http://www.sourcefire.com/products/3D/rna). At the same time, administrators can use Metasploit to verify correct configuration of third-party systems, such as testing the effectiveness of a given mitigating control.

Security Risk Intelligence in Action

Two use cases illustrate the value of Rapid7 Security Risk Intelligence.

Use Case: Cloud Services

A sales representative in Paris selects an applet in the corporate cloud that copies a virtual machine (VM) image from a server in New York onto her hard drive. The VM spins up on her laptop in Paris. Back at the IT operations center in New York, the Nexpose continuous discovery feature finds the new image and reports it to the security console, triggering an alert.

The alert is used to trigger a suspension of the new VM until the security manager can verify its security posture. Using Nexpose, the operator scans the VM and determines that the image is five patches behind. A critical vulnerability, MS06-071, with a Real Risk score of 918 and a CVSS value of 7.6 is present that a hacker could exploit and allow remote code execution within the private cloud. The higher Real Risk score is a result of its consideration of the environmental metrics associated with MS06-071: the age of the vulnerability (5 years since it was identified) and the fact that known exploits exists for this specific vulnerability.

Nexpose recommends remediation steps for patching the VM. The security manager forwards this information to the server administrator, flagging it for immediate attention. The server administrator patches the original VM in New York and reports task completion to the security manager. Using Metasploit Pro, the security manager verifies that the patches are effective for stopping an attack. He sends an email to the representative in Paris indicating that she can use the updated applet.

Use Case: Malware Exploit

An email with an Excel attachment is delivered to the corporate server. Employees know not to open files from untrusted sources, but this email looks like it came from the recipient's college buddy.

The Excel attachment contains a macro that contains malware that exploits a known vulnerability in Windows to propagate itself and set up a bot network. The vulnerability exploited in this attack, MS06-014, has a Real Risk score of 760, because any kid with a computer can "weaponize" an Excel file using a malware kit. The base metric CVSS score of 5.1 for this specific vulnerability would not flag the danger within this environment, but the Rapid7 Real Risk score identifies the malware kits that have been known to exploit this vulnerability, combines it with other known exploits for this vulnerability, and increments the score appropriately.

Just last week, the security manager used Metasploit to send a malicious email and verify that antivirus software on the email server detects this macro and deletes it before delivering the message to the user. Knowing that compensating controls are in place, the security manager used Metasploit to mark the Windows vulnerability as "acceptable" within Nexpose.

Why Choose Rapid 7 Security Risk Intelligence

Rapid7 offers all the solutions and best practices that support comprehensive Security Risk Intelligence. Built upon award-winning Rapid7 Nexpose and Metasploit solutions, Security Risk Intelligence helps organizations make better business decisions related to IT security with specific guidance to answer: "What do we fix first? How do we fix it? What level of risk are we willing to accept?"

Central to Security Risk Intelligence is the Rapid7 Real Risk™ score, a contextual risk metric that accurately prioritizes mitigation tasks to reduce overall risk as quickly as possible. More informative than conventional risk prioritization schemas such as the Common Vulnerability Scoring System (CVSS), Real Risk incorporates criteria specific to each IT environment and its security policies.

Rapid7 Security Risk Intelligence delivers strategic advantages in the battle for control of your IT environment. In an industry crowded with vendors claiming to deliver proactive vulnerability management, only Rapid7 has everything you need for continuous security improvement. Only Rapid7 offers unified vulnerability-scanning and penetration-testing solutions, customer training in best practices, and professional expertise that organizations need to implement Security Risk Intelligence. Security Risk

Intelligence helps organizations implement operational best practices in closed-loop vulnerability management, build productive relationships with IT operations, and achieve measurable drops in risk exposure over the shortest period of time.

IDC agrees: "Rapid7's leadership and strong growth indicate that it is on solid ground, and it can meet the requirements to succeed in its markets. Rapid7 has critical awareness of market forces and vendor competitive positioning and is focused on leveraging its strengths to increase its share. The overarching strategy that centers around converged vulnerability management and penetration testing, context-rich security intelligence, and testing of security controls outside of patch distribution creates a compelling strategy that has the potential to redefine Rapid7's segment."[1]

For More Information

To learn more about Security Risk Intelligence and Real Risk scoring, contact Rapid7 sales at 866.772.7437 or online at sales@rapid7.com.

About Rapid7

Rapid7 is a leading provider of IT security risk management software. Its integrated vulnerability management and penetration testing products, Nexpose and Metasploit, and mobile risk management solution, Mobilisafe, enable defenders to gain contextual visibility and manage the risk associated with the IT environment, users and threats relevant to their organization. Rapid7's simple and innovative solutions are used by more than 2,000 enterprises and government agencies in more than 65 countries, while the Company's free products are downloaded more than one million times per year and enhanced by more than 175,000 members of its open source security community. Rapid7 has been recognized as one of the fastest growing security companies by Inc. Magazine and as a "Top Place to Work" by the Boston Globe. Its products are top rated by Gartner®, Forrester® and SC Magazine. The Company is backed by Bain Capital and Technology Crossover Ventures. For more information about Rapid7, please visit http://www.rapid7.com.

1 IDC: Charles Liebert, Charles J. Kolodgy, and Christian A. Christiansen, "Rapid7 Private Vendor Watchlist Profile: Security Risk Intelligence," July 2011

RAPID7

InsightVM

Installation and Quick-start Guide

Table of contents

About this guide

Use this guide to help you to perform the following tasks:

- install the Windows or Linux version of InsightVM software
- enable FIPS mode (if necessary)
- start InsightVM
- log onto the Security Console Web interface
- get started using InsightVM

Other documents and Help

Click the **Help** link on any page of the Security Console Web interface to find information quickly. You can download any of the following documents from the *Support* page in Help.

User's guide

The user's guide helps you to gather and distribute information about your network assets and vulnerabilities using the application. It covers the following activities:

- logging onto the Security Console and familiarizing yourself with the interface
- managing dynamic discovery
- setting up sites and scans
- running scans manually
- viewing asset and vulnerability data
- creating remediation tickets
- using preset and custom report templates
- using report formats
- reading and interpreting report data
- configuring scan templates
- configuring other settings that affect scans and report

Administrator's guide

The administrator's guide helps you to ensure that InsightVM works effectively and consistently in support of your organization's security objectives. It provides instruction for doing key administrative tasks:

- configuring host systems for maximum performance
- planning a deployment, including determining how to distribute scan engines
- managing users and roles
- maintenance and troubleshooting

API guide

The API guide helps you to automate some InsightVM features and to integrate its functionality with your internal systems.

Installing the application

This section provides the following information about installing InsightVM:

Installation requirements

Make sure that your host hardware and network support InsightVM operations.

Hardware requirements

See the Rapid7 Web site for hardware requirements:

http://www.rapid7.com/products/insightvm/system-requirements/.

It is recommended that you install InsightVM on a computer that does not have an Intrusion Detection System (IDS), an Intrusion Prevention System (IPS), or a firewall enabled. These devices block critical operations that are dependent on network communication.

The 64-bit configuration is recommended for enterprise-scale deployments.

Network activities and requirements

The Security Console communicates over the network to perform four major activities:

Activity	Type of communication
manage scan activity on Scan Engines and pull scan data from them	outbound; Scan Engines listen on 40814
download vulnerability checks and feature updates from a server at updates.rapid7.com	outbound; server listens on port 80
upload PGP-encrypted diagnostic information to a server at support.rapid7.com	outbound; server listens on port 443
provide Web interface access to users	inbound; Security Console accepts HTTPS requests over port 3780

Scan Engines contact target assets using TCP, UDP, and ICMP to perform scans. They do not initiate outbound communication with the Security Console.

Ideally there should be no firewalls or similar devices between a Scan Engine and its target assets. Also, scanning may also require some flexibility in security policies. For more information, see the *administrator's guide*.

Supported platforms

See the Rapid7 Web site for supported platforms:

http://www.rapid7.com/products/insightvm/system-requirements/.

Making sure you have necessary items

Make sure you have all of the following items before you begin the installation process:

- installers for all supported environments (.bin files for Linux and .exe files for Windows)
- the md5sum, which helps to ensure that installers are not corrupted during download
- documentation, including this guide
- a product key, which you need to activate your license when you log on

If you do not have any of these items, contact your account representative. If you purchased InsightVM or registered for an evaluation, Rapid7 sent you an e-mail that includes links for downloading these items and the product key. It is recommended that you add InsightVM to your e-mail client white list communication to ensure you receive future e-mails about InsightVM.

During the installation, the installer runs a system check and identifies any system components or settings that meet the minimum requirements but not the recommended requirements. If any items are identified, you can continue the installation, but you should consider modifying your system after the installation to ensure optimal performance. For example, if your system does not have the recommended the amount of RAM, you may encounter performance issues with RAM-intensive operations, such as running scans or reports. To prevent this, you should consider adding RAM to your system.

Uninstalling a previously installed copy

Installing and using multiple copies of the software on the same server is not supported. If you install multiple copies on the same server, the application will not function properly.

Each copy of the software must be installed from scratch. This means that if you already have a copy installed, you must uninstall it before you install the new copy you downloaded.

Use the procedure in the section *Running the Windows uninstaller* on page 11 or *Running the Linux uninstaller* on page 15 to uninstall any previously installed copies.

Creating an account during installation

When you install the application, you create a default Global Administrator account. You will use the account to log onto the application after you complete the installation.

Recovery of credentials is not supported. If you forget your user name or password, you will have to reinstall the program. Credentials are case-sensitive.

As you enter credentials, the complexity requirements are displayed to ensure that you create strong (secure) credentials. Even if your password meets the requirements, it is recommended that you make your password as strong as possible for better security. A “heat bar” is displayed that gradually changes color from red to green as you make your password stronger.

A Global Administrator can create and modify accounts after installation. See *Managing users and authentication* in Help or the administrator’s guide.

Installation choices

During the installation, you will make several choices, including the following:

- Select the component(s) you want to install and where to install them.
- Enable the application to initialize during the installation and start automatically after installation.
- If you install only the Scan Engine, you must select a communication direction between an existing Security Console and the new Scan Engine.

Selection of components

You can either install a Security Console with a local Scan Engine or you can install a distributed Scan Engine. If you install the latter, you must have a Security Console running in your environment before you can use the Scan Engine. The Security Console controls all Scan Engine activity.

Application initialization and automatic start option

You can choose to have the application initialize during installation and automatically start once you finish the installation. By default, this option is enabled. If you do not want initialization to

occur during installation, you must disable it.

You can only leave this option enabled if you install both components (the Scan Engine and Security Console). If you choose to install only the Scan Engine, this option is not available.

The benefit to leaving the option enabled is that you can start using the application immediately after the installation is complete. This is because the initialization process prepares the application for use by updating the database of vulnerability checks and performing the initial configuration.

Because the time required for the initialization process ranges from 10 to 30 minutes, leaving the option enabled increases the total installation time by 10 to 30 minutes. Although disabling the option shortens the installation time, it takes longer to start the application because it has to initialize before you can begin using it.

Communication direction between Console and Engine

Which direction is preferred depends on your network configuration:

- Engine to Console: The Scan Engine will actively inform the Security Console that it is available for communication. This configuration allows a console that is behind a firewall and is configured to allow inbound connections to establish a communication channel.
- Console to Engine: The Scan Engine will listen for communication from the Security Console. This configuration is most effective when the engine and console are on the same area of the network.

Tips for using the installation wizard

The pages of the wizard are listed in the left page of the wizard, and the current page is highlighted. You can use the list to check your progress.

Each page of the wizard has a **Previous** button and a **Cancel** button. Use the **Previous** button to go to a previous page if you need to review or change an installation setting. Use the **Cancel** button only if you need to cancel the installation. If you cancel at any point in during the installation process, no files are installed and you need to go back to the beginning of the installation process.

Installing in Windows environments

This section describes how to install InsightVM on a Windows host. It also describes options that are available to you during the installation.

Before you begin

Confirm the following items:

- You are logged onto Windows as an administrator.
- Your system meets the minimum installation requirements. See *Installation requirements* on page 6 for details.
- You have all of the items you need to complete the installation. See *Making sure you have necessary items* on page 7 for details.
- You have uninstalled any previously installed copies of the application. See *Running the Windows uninstaller* on page 11 for details.

Running the Windows installer

To install the application in Windows, take the following steps:

1. Double-click the **installer icon**.

   The installer displays a message that it is preparing the wizard to guide you through the installation. Then the *Welcome* page of the wizard is displayed.

   Command-line windows open once you begin the installation. Although you do not need to interact with them, do not close them.

   Note: The installation will stop if you close the command line interface windows.

   Click **Next**. The *Type and destination* page is displayed.

2. Follow the instructions in the installer. If you want to enable FIPS mode, do not select the option to initialize the application after installation. FIPS mode must be enabled before the application runs for the first time.

   If you are installing just the Scan Engine, you may need to specify the Shared Secret to pair it with a Security Console. Global Administrators can generate a Shared Secret in the Administration section of the Security Console. Select **manage** next to *Engines*, click **Generate** next to *Shared Secret*, and copy and paste the Shared Secret into the Installation Wizard.

3. See *Getting Started* on page 20 for information on getting started using the application.

Running the Windows uninstaller

Each copy of InsightVM must be installed from scratch. This means that if you already have it installed on your system, you must uninstall it before intalling the new copy you downloaded.

Warning: To prevent a loss of sites, configurations, reports, and other data, make sure you back up all of your data before you begin the procedure.

Uninstalling completely removes all components. It also deletes sites, configurations, reports, and any scan data on discovered assets, nodes, and vulnerabilities.

To uninstall the application:

1. Start the program to uninstall by doing one of the following:
   - Click the Windows **Start** button and select the **Control Panel**.
   - Select the **uninstall** option or the **remove a program** option (depends on the version of Windows you are running).
   - (If you have a shortcut folder.) Click the Windows **Start** button, go to the InsightVM folder, and select the **Uninstaller**.
2. Double-click InsightVM in the list of programs.
3. Run the uninstaller program.

   The uninstaller displays a *Welcome* page. Read the warning about backing up data.
4. Click **Next**.

   The uninstaller displays a status bar with a message that uninstallation is in progress followed by a message that the uninstallation is complete.

   Do not close the command line window.
5. Click **Finish**.

Installing in Linux environments

See the instructions for your specific supported Linux distribution.

Do I need to disable SELinux?

SELinux is a security-related feature that must be disabled before you can install the application.

Tip: Later versions of Ubuntu do not include SELinux, or it is automatically set to `permissive`. It is recommended that you check the status before you start the installation.

To disable SELinux, take these steps:

1. Open the SELinux configuration file in your preferred text editor.

   Example: `$ vi /etc/selinux/config`

2. Go the line that begins with `SELINUX=`.

   If the setting is `enforcing`, change it to `disabled: SELINUX=disabled`

3. Save and close the file.
4. Restart the server for the change to take effect: `$ shutdown -r now`

At this point you can check the installer file to make sure it is not corrupted or begin the installation. It is recommended that you check the installer file before you begin the installation.

Ensuring that the installer file is not corrupted

This procedure shows you how to check the installer file you downloaded to make sure it is not corrupted. This helps to prevent installation problems.

Make sure that you downloaded the installation file and the md5sum file. See *Installing the application* on page 6 for details.

To check the installer file, take these steps:

1. Go to the directory that contains the installer and the md5sum file. If you have not changed any settings, this will be `Downloads`.
2. Run the md5sum program with the -c option to check the MD5 checksum:

```
$ md5sum -c [installer_file_name].md5sum
```

   - If this command returns an `OK` message, the file is valid.
   - If it returns a "FAILED" message, download the installer and md5sum file again, and repeat this procedure.

Installing in Ubuntu

Make sure that:

- You have downloaded all items necessary for installation. See *Installing the application* on page 6 for details.
- You have root-level access.
- (Recommended) You check the installer file to make sure it was not corrupted during the download. See *Ensuring that the installer file is not corrupted* on page 12.

Manually installing necessary packages in Ubuntu

If sudo is active in your environment, and if your account is listed in the sudoers file, you can use sudo -i to run the commands.

Tip: Rapid7 recommends using apt-get to install packages on Ubuntu.

To install the necessary packages:

1. To verify that you have apt-get, run:

```
$ apt-get -v
```

2. To determine if you have a required package and install it if necessary, run:

```
$ apt-get install [package_name]
```

The following package should be installed:

- screen

Next Steps

Run the Linux installer. See "Running the Linux installer" below.

Installing in Red Hat

You must have root-level access to run the installation. If sudo is active in your environment, and if your account is listed in the sudoers file, you can use sudo -i to run the commands.

Make sure that:

- You have downloaded all items necessary for installation. See *Installing the application* on page 6 for details.
- You have yum and RPM, which you need to install packages on Red Hat.
- You have a Red Hat Enterprise Linux license.
- (Recommended) You check the installer file to make sure it was not corrupted during the download. See *Ensuring that the installer file is not corrupted* on page 12.

Manually installing necessary packages in Red Hat

You need yum and RPM to install packages on Red Hat.

1. To verify that you have yum and RPM, run: `$ yum --version`
2. To determine if you have a required package and install it as necessary, run:

   ```
   $ yum install [package_name]
   ```

The following package should be installed: `screen`.

Running the Linux installer

This procedure shows you how to install the application in a Linux environment.

If you are using a graphical user interface

If you are using an interface such as KDE or Gnome, omit the `-c flag` in step 3 of the procedure. The installer opens a wizard to guide you through the installation (similar to the Windows installation wizard (see *Installing in Windows environments* on page 10). The rest of the steps in this procedure reflect installation using the command line interface.

Before you begin

Make sure that:

- Your system meets the minimum installation requirements.
- You have all of the items you need to complete the installation. See *Installing in Linux environments* on page 1.
- You have disabled SELinux (if necessary). See *Do I need to disable SELinux?* on page 1.
- (Recommended) You check the installer file to make sure it was not corrupted during the download. See *Ensuring that the installer file is not corrupted* on page 12.
- You have installed the required packages for your Linux platform.
- You have uninstalled any previously installed copies. See *Running the Linux uninstaller* on page 15.

Warning: The installation will fail if you do not install all necessary packages.

To install the application, take these steps:

1. Go to the directory that contains the installer.
2. Change the permissions for the installation file to make it executable:

   ```
   $ chmod +x [installation_file_name]
   ```

3. Start the installer:

   ```
   $ ./[installation_file_name] -c
   ```

   The installer displays information about the application.

4. Follow the instructions in the installer. If you want to enable FIPS mode, do not select the option to initialize the application after installation. FIPS mode must be enabled before the application runs for the first time.

   If you are installing just the Scan Engine, you may need to specify the Shared Secret to pair it with a Security Console. Global Administrators can generate a Shared Secret in the Administration section of the Security Console. Select **manage** next to *Engines*, click **Generate** next to *Shared Secret*, and copy and paste the Shared Secret into the Installation Wizard.

5. See *Getting Started* on page 20 for information on getting started using the application.

Running the Linux uninstaller

Each copy of InsightVM must be installed from scratch. This means that if you already have it installed on your system, you must uninstall it before you install the new copy you downloaded.

Warning: To prevent a loss of sites, configurations, reports, and other data, make sure you back up all of your data before you begin the procedure.

Uninstalling completely removes all components. It also deletes sites, configurations, reports, and any scan data on discovered assets, nodes, and vulnerabilities.

To uninstall the application, take these steps:

1. Run: `$ cd [installation directory]/.install4j`

   `install4j` is a hidden directory. To list hidden directories, run: **`ls -a`**

2. Run: `$./uninstall`

Enabling FIPS mode

If you are operating the application in an environment where the use of FIPS-enabled products is mandatory, or if you want the security of using a FIPS-certified encryption module, you should enable FIPS mode. The application supports the use of Federal Information Processing Standard (FIPS) 140-2 encryption, which is required by government agencies and companies that have adopted FIPS guidelines.

What is FIPS?

The FIPS publications are a set of standards for best practices in computer security products. FIPS certification is applicable to any part of a product that employs cryptography. A FIPS-certified product has been reviewed by a lab and shown to comply with FIPS 140-2 (Standard for Security Requirements for Cryptographic Modules), and to support at least one FIPS-certified algorithm.

Government agencies in several countries and some private companies are required to use FIPS-certified products.

What is FIPS mode?

FIPS mode is a configuration that uses FIPS-approved algorithms only. When the application is configured to operate in FIPS mode, it implements a FIPS-certified cryptographic library to encrypt communication between the Security Console and Scan Engines, and between the Security Console and the user for both the browser and API interfaces.

FIPS mode considerations

It is important to note that due to encryption key generation considerations, the decision to run in FIPS mode or non-FIPS mode is irrevocable. The application must be configured to run in FIPS mode immediately after installation and before it is started for the first time, or else left to run in the default non-FIPS mode. Once the application has started with the chosen configuration, you will need to reinstall it to change between modes.

Activating FIPS mode

When InsightVM is installed, it is configured to run in non-FIPS mode by default. The application must be configured to run in FIPS mode before being started for the first time. See *Activating FIPS mode in Linux* on page 18.

When FIPS mode is enabled, communication between the application and non-FIPS enabled applications such as Web browsers or API clients cannot be guaranteed to function correctly.

Activating FIPS mode in Linux

You must follow these steps after installation, and BEFORE starting the application for the first time.

To enable FIPS mode:

1. Install rng-utils.

   The encryption algorithm requires that the system have a large entropy pool in order to generate random numbers. To ensure that the entropy pool remains full, the rngd daemon must be running while the application is running. The rngd daemon is part of the rng-utils Linux package.

2. Download and install the rng-utils package using the system's package manager.

Tip: Add the rngd command to the system startup files so that it runs each time the server is restarted.

3. Run the command `rngd -b -r /dev/urandom`.
4. Create a properties file for activating FIPS mode.
5. Create a new file using a text editor.
6. Enter the following line in this file:

   ```
   fipsMode=1
   ```

7. Save the file in the [install_directory]/nsc directory with the following name:

   CustomEnvironment.properties

8. Start the Security Console.

Activating FIPS mode in Windows

You must follow these steps after installation, and before starting the application for the first time.

To enable FIPS mode:

1. Create a properties file for activating FIPS mode.
2. Create a new file using a text editor.
3. Enter the following line in this file:

   ```
   fipsMode=1
   ```

Note: You can disable database consistency checks on startup using the CustomEnvironment.properties file. Do this only if instructed by Technical Support.

4. Save the file in the [install_directory]\nsc directory with the following name:

   CustomEnvironment.properties

5. Start the Security Console.

Verifying that FIPS mode is enabled

To ensure that FIPS mode has been successfully enabled, check the Security Console log files for the following messages:

```
FIPS 140-2 mode is enabled. Initializing crypto provider

Executing FIPS self tests...
```

Getting Started

If you haven't used the application before, this section helps you to become familiar with the Web interface, which you will need for running scans, creating reports, and performing other important operations.

- *Running the application* on page 21: By default, the application is configured to run automatically in the background. If you need to stop and start it automatically, or manage the application service or daemon, this section shows you how.
- *Using the Web interface* on page 24: This section guides you through logging on, navigating the Web interface, using configuration panels, and running searches.

Running the application

This section includes the following topics to help you get started with the application:

Manually starting or stopping in Windows

InsightVM is configured to start automatically when the host system starts. If you disabled the initialize/start option as part of the installation, or if you have configured your system to not start automatically as a service when the host system starts, you will need to start it manually.

Starting the Security Console for the first time will take 10 to 30 minutes because the database of vulnerabilities has to be initialized. You may log on to the Security Console Web interface immediately after the startup process has completed.

If you have disabled automatic startup, use the following procedure to start the application manually:

1. Click the **Windows Start** button
2. Go to the application folder.
3. Select **Start Services**.

Use the following procedure to stop the application manually:

1. Click the **Windows Start** button.
2. Open the application folder.
3. Click the **Stop Services** icon.

Changing the configuration for starting automatically as a service

By default the application starts automatically as a service when Windows starts. You can disable this feature and control when the application starts and stops.

1. Click the **Windows Start** button, and select **Run...**
2. Type services.msc in the *Run* dialog box.
3. Click **OK**.
4. Double-click the icon for the Security Console service in the *Services* pane.
5. Select *Manual* from the drop-down list for **Startup type:**
6. Click **OK**.
7. Close *Services*.

Manually starting or stopping in Linux

If you disabled the initialize/start option as part of the installation, you need to start the application manually.

Starting the Security Console for the first time will take 10 to 30 minutes because the database of vulnerabilities is initializing. You can log on to the Security Console Web interface immediately after startup has completed.

To start the application from graphical user interface, double-click the InsightVMin the *Internet* folder of the *Applications* menu.

To start the application from the command line, take the following steps:

1. Go to the directory that contains the script that starts the application:

   ```
   $ cd [installation_directory]/nsc
   ```
2. Run the script: `./nsc.sh`

Working with the daemon

The installation creates a daemon named *nexposeconsole.rc* in the /etc/init.d/ directory.

WARNING: Do not use <**CTRL+C**>, it will stop the application.

To detach from a screen session, press <**CTRL +A + D**>.

Manually starting orstopping the daemon

To manually start or stop the application as a daemon, run the following commands:

```
service nexposeconsole start/stop

systemctl nexpose start/stop
```

Preventing the daemon from automatically starting with the host system

To prevent the application daemon from automatically starting when the host system starts, run the following command:

```
$ update-rc.d [daemon_name] remove
```

Using the Web interface

This section includes the following topics to help you access and navigate the Security Console Web interface:

Activating and updating on private networks

If your Security Console is not connected to the Internet, you can find directions on updating and activating on private networks. See the topic *Managing versions, updates, and licenses* in the administrator's guide.

Logging on

The Security Console Web interface supports the following browsers:

- Google Chrome (latest) (RECOMMENDED)
- Mozilla Firefox (latest)
- Mozilla Firefox ESR (latest)
- Microsoft Internet Explorer 11

If you received a product key, via e-mail use the following steps to log on. You will enter the product key during this procedure. You can copy the key from the e-mail and paste it into the text box; or you can enter it with or without hyphens. Whether you choose to include or omit hyphens, do so consistently for all four sets of numerals.

If you do not have a product key, click the link to request one. Doing so will open a page on the Rapid7 Web site, where you can register to receive a key by e-mail. After you receive the product key, log on to the Security Console interface again and follow this procedure.

If you are a first-time user and have not yet activated your license, you will need the product key that was sent to you to activate your license after you log on.

To log on to the Security Console take the following steps:

1. Start a Web browser.

   If you are running the browser on the same computer as the console, go to the following URL: `https://localhost:3780`

   Indicate HTTPS protocol and to specify port 3780.

   If you are running the browser on a separate computer, substitute `localhost` with the correct host name or IP address.

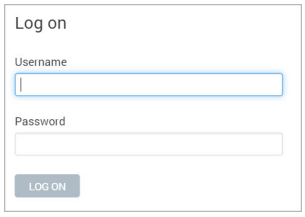
   Your browser displays the *Logon* window.

Tip: If there is a usage conflict for port 3780, you can specify another available port in the *httpd.xml* file, located in [installation_directory]\nsc\conf. You also can switch the port after you log on. See the topic *Changing the Security Console Web server default settings* in the administrator's guide.

Note: If the logon window indicates that the Security Console is in maintenance mode, then either an error has occurred in the startup process, or a maintenance task is running. See *Running in maintenance mode* in the administrator's guide.

2. Enter your user name and password that you specified during installation.

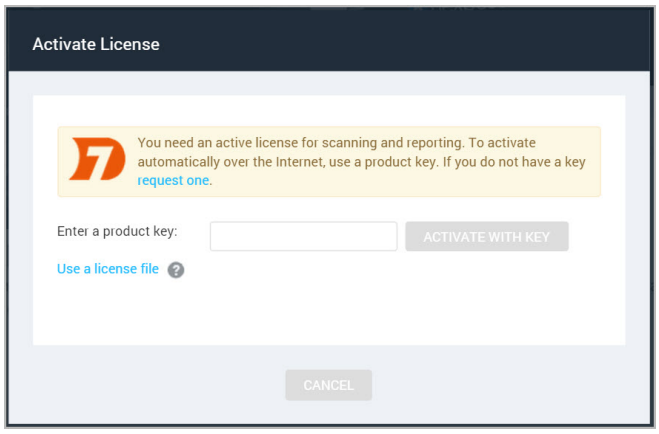
   User names and passwords are case-sensitive and non-recoverable.



Logon window

3. Click the **Logon** icon.

If you are a first-time user and have not yet activated your license, the Security Console displays an activation dialog box. Follow the instructions to enter your product key.



Activate License window

4. Click **Activate** to complete this step.
5. Click the **Home**icon to view the Security Console *Home* page.
6. Click the **Help** icon on any page of the Web interface for information on how to use the application.

The first time you log on, you will see the *News* page, which lists all updates and improvements in the installed system, including new vulnerability checks. If you do not wish to see this page every time you log on after an update, clear the check box for automatically displaying this page after every login. You can view the *News* page by clicking the **News** link that appears under the **Help** icon dropdown. The **Help** icon can be found near the top right corner of every page of the console interface.

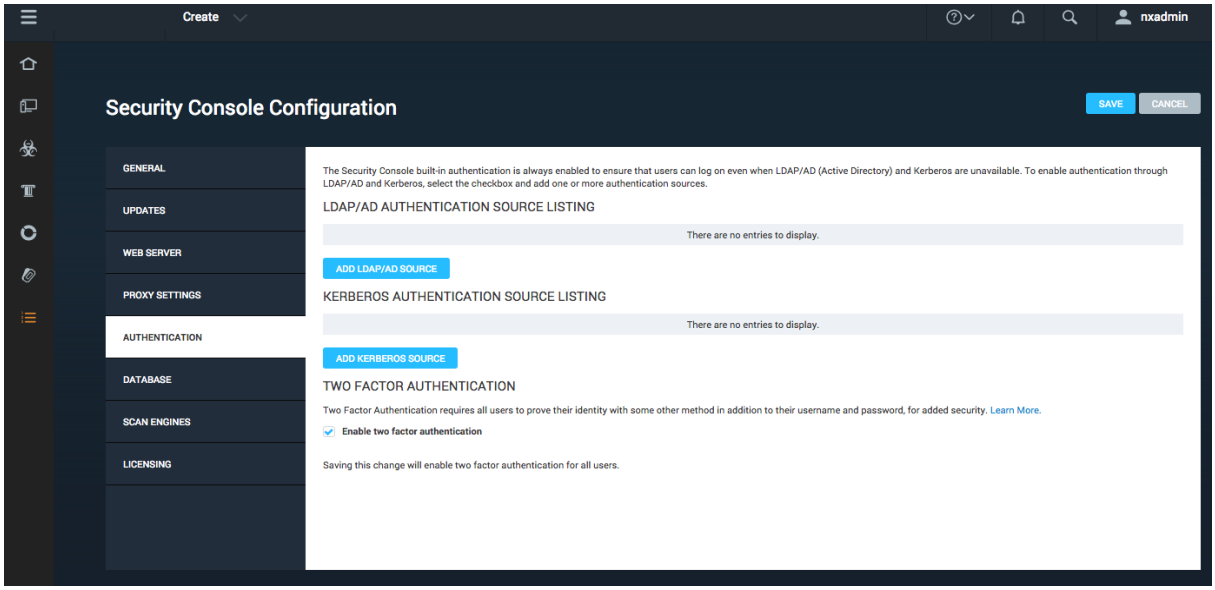
Enabling Two Factor Authentication

For organizations that want additional security upon login, the product supports Two Factor Authentication. Two Factor Authentication requires the use of a time-based one-time password application such as Google Authenticator.

Two Factor Authentication can only be enabled by a Global Administrator on the *Security Console*.

To enable Two Factor Authentication:

1. As a Global Administrator, go to the **Administration** tab.
2. Click the **Administer** link in the *Global and Console Settings* section.
3. Select **Enable two factor authentication**.

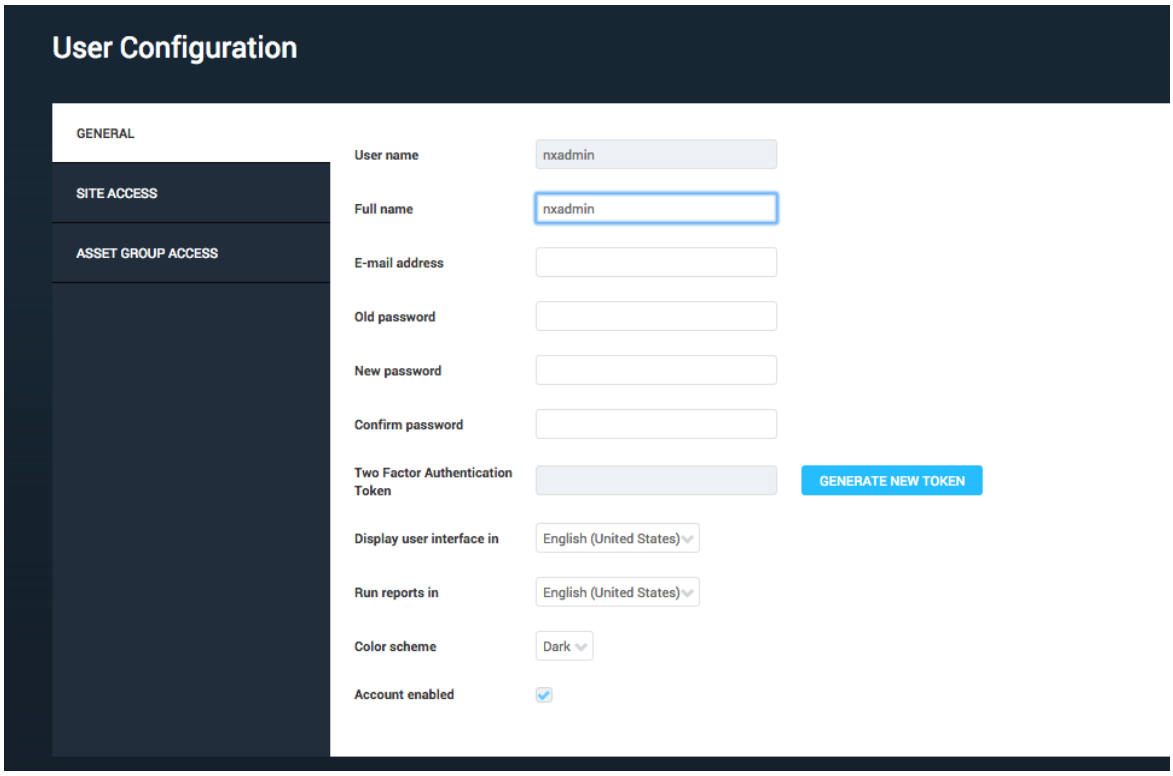


The next step is to generate a token for each user. The users can generate their own tokens, or you can generate tokens for them that they then change. In either case, you should communicate with them about the upcoming changes.

Method 1: Tokens created by users

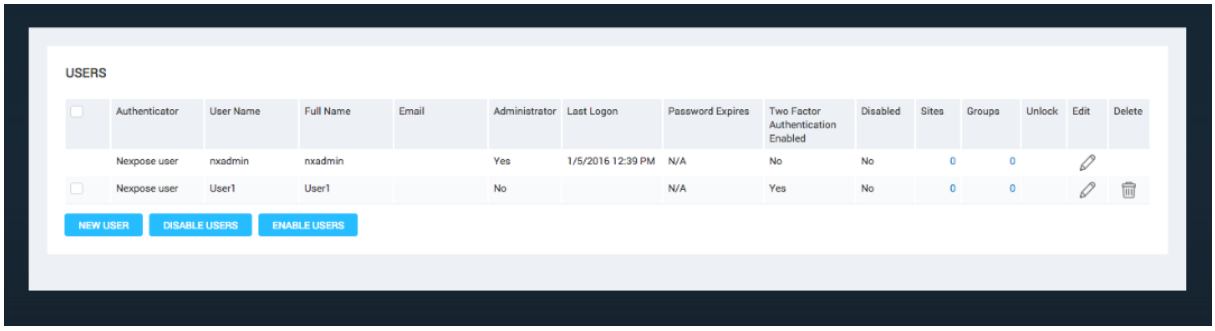
Once Two Factor Authentication is enabled, when a user logs on, they will see a field where they can enter an access code. For the first time, they should log in without specifying an access code.

Once the user logs in, they can generate a token in the *User Preferences* page.



The user should then open their time-based one-time password application such as Google Authenticator. They should enter the token as the key in the password application. The password application will then generate a new code that should be used as the user's access code when logging in.

A Global Administrator can check whether users have completed the Two Factor Authentication on the *Manage Users* page. The *Manage Users* page can be reached by going to the *Administration* tab and clicking the **Manage** link in the *Users* section. A new field, **Two Factor Authentication Enabled**, will appear in the table and let the administrator know which users have enabled this feature.



If the user doesn't create a token, they will still be able to log in without an access code. In this case, you may need to take steps to enforce enablement.

Method 2: Generating tokens for users

You can enforce that all users log in with a token by disabling the accounts of any users who have not completed the process, or by creating tokens for them and emailing them their tokens.

To disable users:

1. Go to the *Manage users* page by going to the **Administration** tab and clicking the **Manage** link in the Users section.
2. Select the checkbox next to each user for whom the Two Factor Authentication Enabled column shows No.
3. Select **Disable users**.

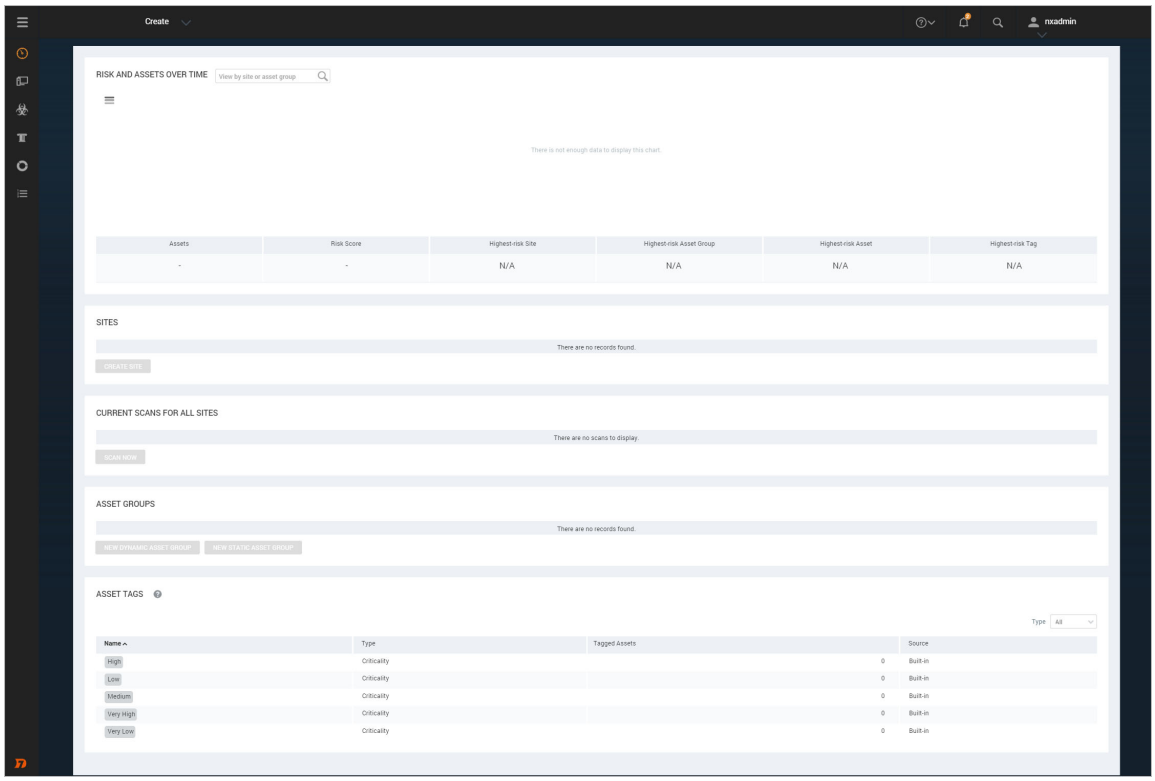
To generate a token for a user:

1. Go to the *Manage users* page by going to the **Administration** tab and clicking the **Manage** link in the *Users* section.
2. Select **Edit** for that user.
3. Generate a token for that user.
4. Provide the user with the token.
5. Once the user logs in with their access code, they can change their token if they would like in the *User preferences* page.

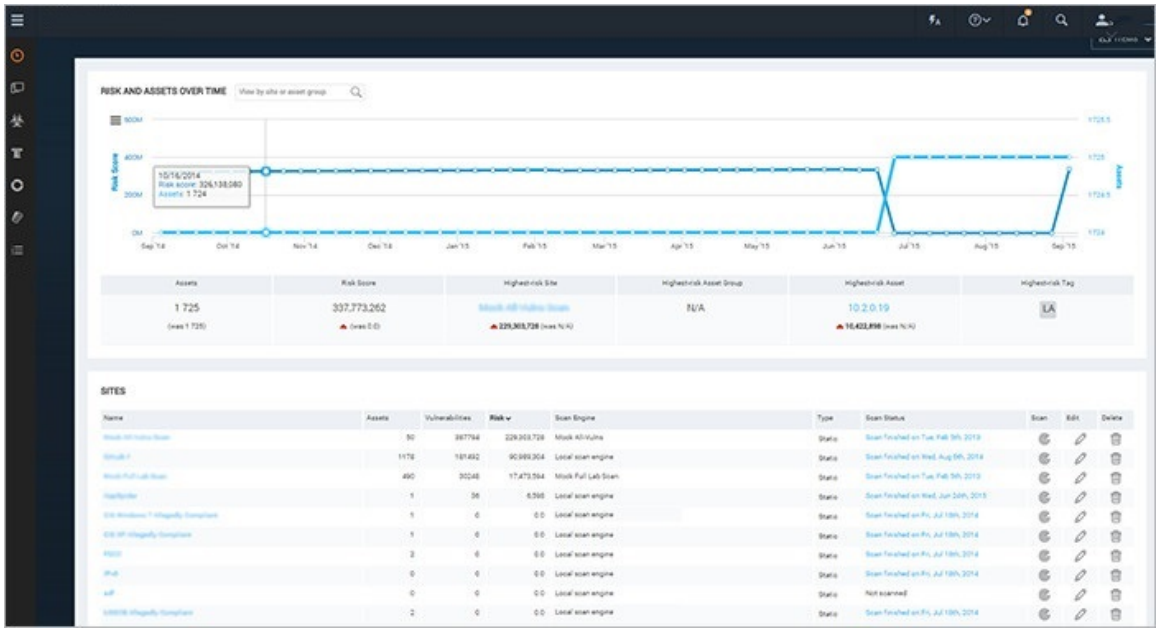
Navigating the Security Console Web interface

The Security Console includes a Web-based user interface for configuring and operating the application. Familiarizing yourself with the interface will help you to find and use its features quickly.

When you log on to the to the *Home* page for the first time, you see place holders for information, but no information in them. After installation, the only information in the database is the account of the default Global Administrator and the product license.



The Home page as it appears in a new installation



The Home page as it appears with scan data

The *Home* page shows sites, asset groups, tickets, and statistics about your network that are based on scan data. If you are a Global Administrator, you can view and edit site and asset group information, and run scans for your entire network on this page.

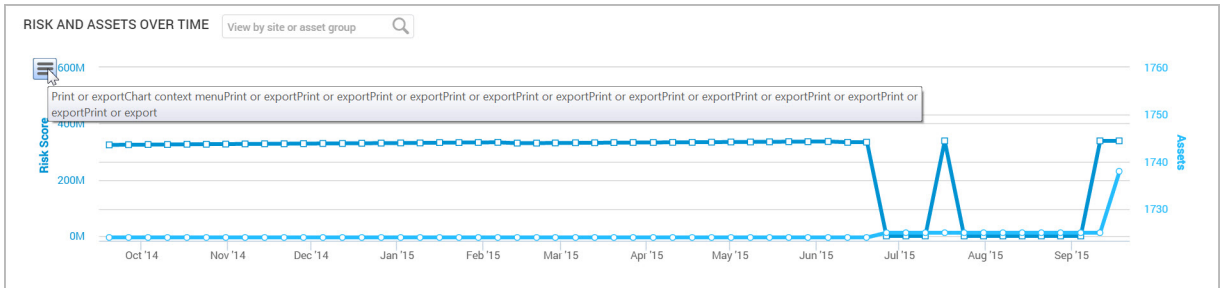
The *Home* page also displays a chart that shows trends of risk score and number of assets over time. The growth in assets over time is an increase in your surface area (total number of assets). As you add assets to your environment your level of risk can increase because the more assets you have, the more potential there is for vulnerabilities.

Each point of data on the chart represents a week. The darker blue line and measurements on the left show how much your risk score has increased or decreased over time. The lighter blue line displays the number of assets.

Note: This interactive chart shows a default of a year's worth of data when available; if you have been using the application for a shorter historical period, the chart will adjust to show only the months applicable.

The following are some additional ways to interact with charts:

- In the search filter at the top left of the chart, you can enter a name of a site or asset group to narrow the results that appear in the chart pane to only show data for that specific site or group.
- Click and drag to select a smaller, specific timeframe and view specific details. Select the **Reset/Zoom** button to reset the view to the previous settings.
- Hover your mouse over a point of data to show the date, the risk score, and the number of assets for the data point.
- Select the sidebar menu icon on the top left of the chart window to export and print a chart image.



Print or export the chart from the sidebar menu

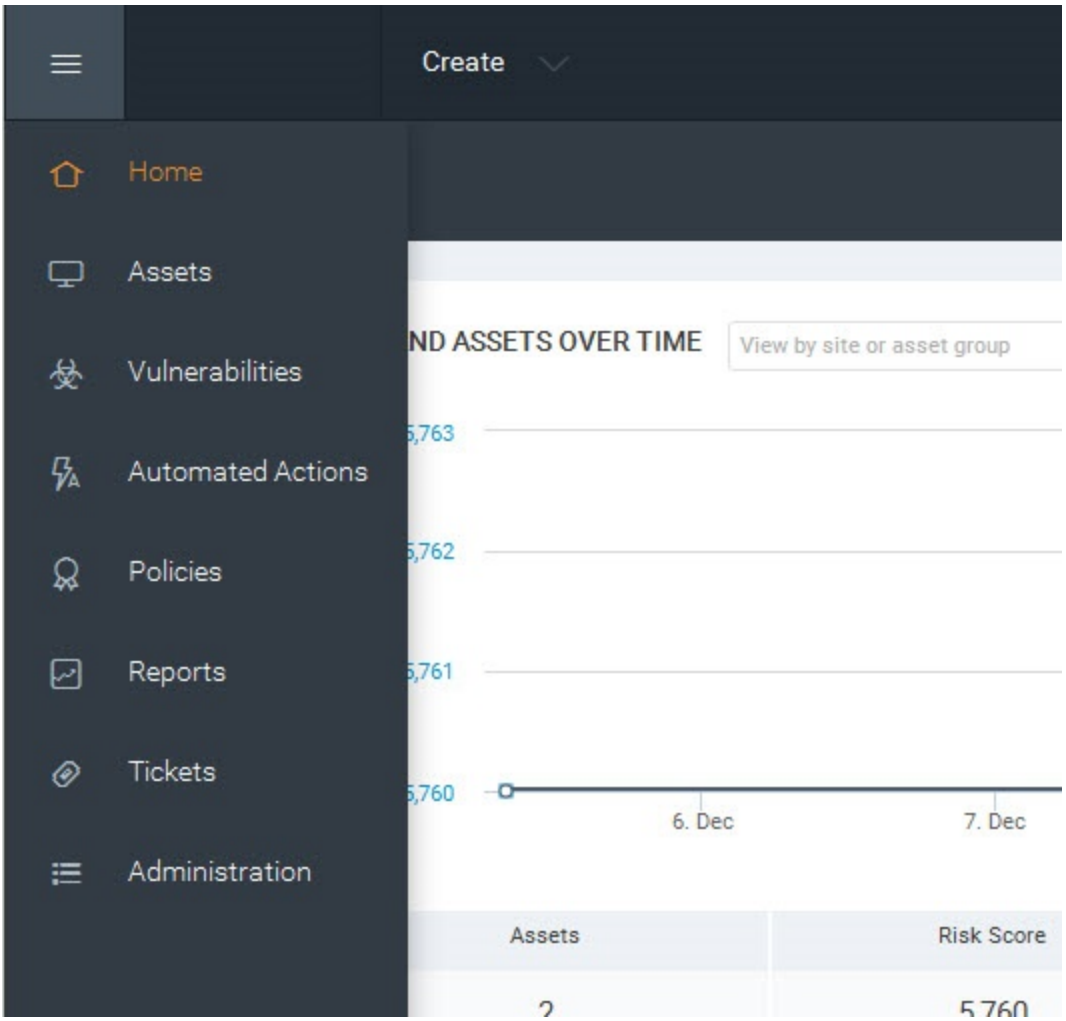
On the *Site Listing* pane, you can click controls to view and edit site information, run scans, and start to create a new site, depending on your role and permissions.

Information for any currently running scan appears in the pane labeled *Current Scan Listings for All Sites*.

On the *Ticket Listing* pane, you can click controls to view information about tickets and assets for which those tickets are assigned.

On the *Asset Group Listing* pane, you can click controls to view and edit information about asset groups, and start to create a new asset group.

A menu appears on the left side of the *Home* page, as well as every page of the Security Console. Mouse over the icons to see their labels, and use these icons to navigate to the main pages for each area.



Icon menu

The *Home* page links to the initial page you land on in the Security Console.

The *Assets* page links to pages for viewing assets organized by different groupings, such as the sites they belong to or the operating systems running on them.

The *Vulnerabilities* page lists all discovered vulnerabilities.

The *Policies* page lists policy compliance results for all assets that have been tested for compliance.

The *Reports* page lists all generated reports and provides controls for editing and creating report templates.

The *Tickets* page lists remediation tickets and their status.

The *Administration* page is the starting point for all management activities, such as creating and editing user accounts, asset groups, and scan and report templates. Only Global Administrators see this icon.

Selecting your language

Some features of the application are supported in multiple languages. You have the option to set your user preferences to view Help in the language of your choosing. You can also run Reports in multiple languages, giving you the ability to share your security data across multi-lingual teams.

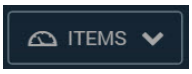
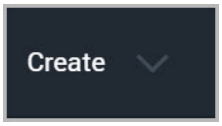
To select your language, click your user name in the upper-right corner and select **User Preferences**. This will take you to the *User Configuration* panel. Here you can select your language for Help and Reports from the corresponding drop down lists.

When selecting a language for Help, be sure to clear your cache and refresh your browser after setting the language to view Help in your selection.

Setting your report language from the *User Configuration* panel will determine the default language of any new reports generated through the *Create Report Configuration* panel. Report configurations that you have created prior to changing the language in the user preferences will remain in their original language. When creating a new report, you can also change the selected language by going to the **Advanced Settings** section of the *Create a report* page. See the topic *Creating a basic report* in the user's guide.

Using icons and other controls

Throughout the Web interface, you can use various controls for navigation and administration.

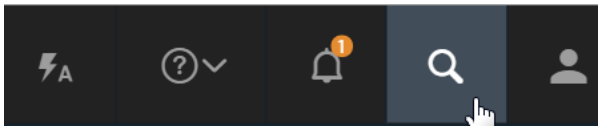
Control	Description	Control	Description
▼	Minimize any pane so that only its title bar appears.		Add items to your dashboard.
▲	Expand a minimized pane.		Copy a built-in report template to create a customized version.
x	Close a pane.		Edit properties for a site, report, or a user account.
	Click to display a list of closed panes and open any of the listed panes.		View a preview of a report template.
	Export data to a comma-separated value (CSV) file.		Delete a site, report, or user account.
	Start a manual scan.		Exclude a vulnerability from a report.
	Pause a scan.	?	View Help. View the Support page to search FAQ pages and contact Technical Support. View the *News* page which lists all updates.
	Resume a scan.	Product logo	Click the product logo in the upper-left area to return to the *Home* page.
	Stop a scan.	**User: <user name>** link	This link is the logged-on user name. Click it to open the User Configuration panel where you can edit account information such as the password and view site and asset group access. Only Global Administrators can change roles and permissions.
	Initiate a filtered search for assets to create a dynamic asset group.	**Log Out** link	Log out of the Security Console interface. The *Logon* box appears. For security reasons, the Security Console automatically logs out a user who has been inactive for 10 minutes.
	Expand a drop-down list of options to create sites, asset groups, tags, or reports.		

Using the search feature

With the powerful full-text search feature, you can search the database using a variety of criteria, such as the following:

- full or partial IP addresses
- asset names
- site names
- asset group names
- vulnerability titles
- vulnerability CVE IDs
- internal vulnerability IDs user-added tags
- criticality tags
- Common Configuration Enumerator (CCE) IDs
- operating system names

Access the **Search** box on any a page of the Security Console interface by clicking the magnifying glass icon near the top right of the page.



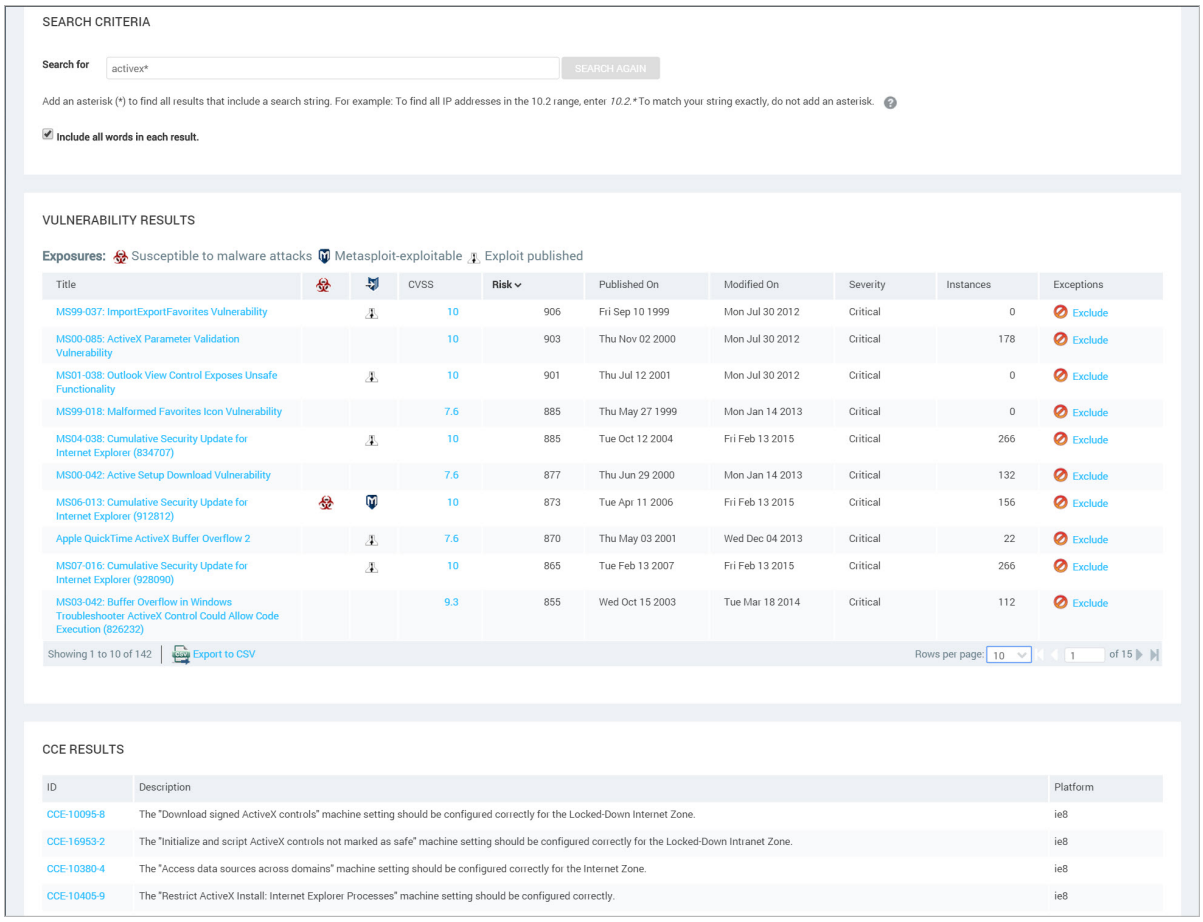
Clicking the Search icon

Enter your search criteria into the **Search** box and then click the magnifying glass icon again. For example, if you want to search for discovered instances of the vulnerabilities that affect assets running ActiveX, enter *ActiveX* or *activex* in the **Search** text box. The search is not case-sensitive.

Starting a search

The application displays search results on the *Search* page, which includes panes for different groupings of results. With the current example,

ActiveX, results appear in the *Vulnerability Results* table. At the bottom of each category pane, you can view the total number of results and change settings for how results are displayed.



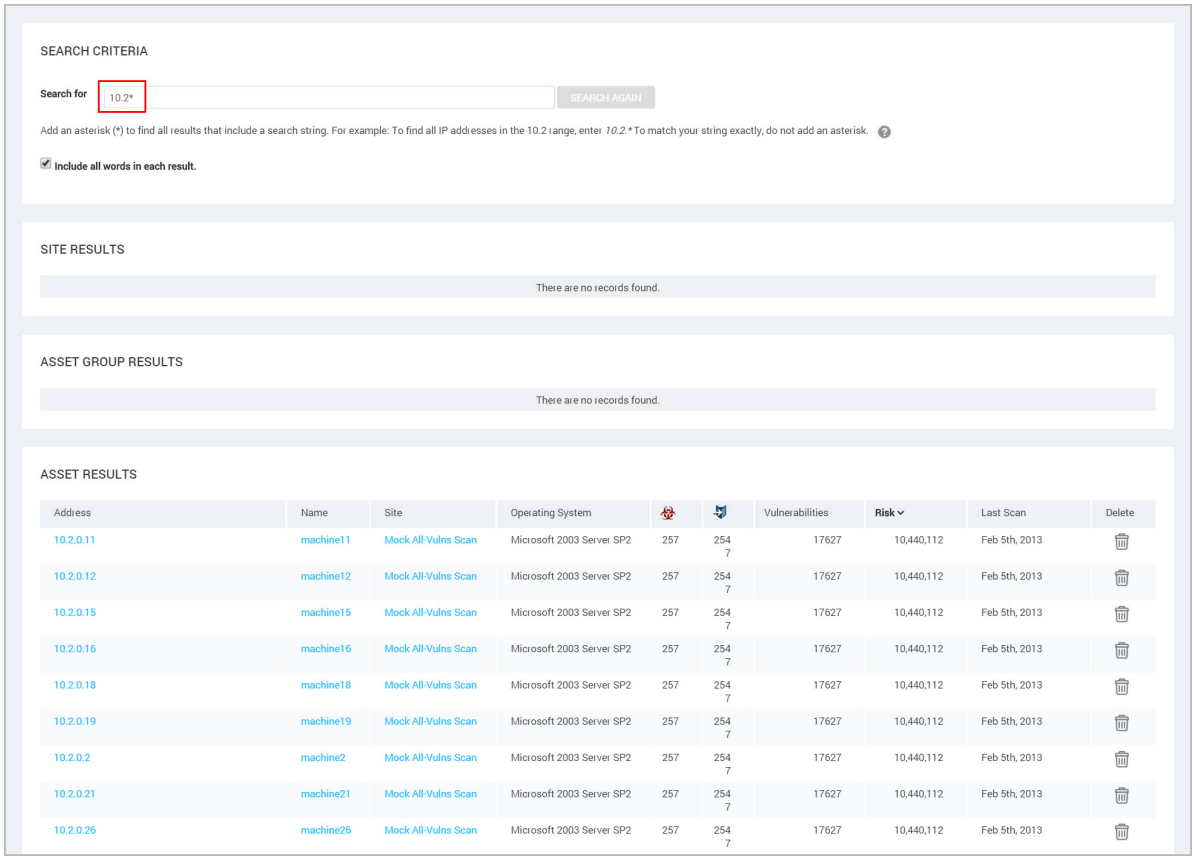
Search results

In the *Search Criteria* pane, you can refine and repeat the search. You can change the search phrase and choose whether to allow partial word matches and to specify that all words in the phrase appear in each result. After refining the criteria, click the **Search Again** button.

Using asterisks and avoiding *stop words*

When you run initial searches with partial strings in the *Search* box that appears in the upper-right corner of most pages in the Web interface, results include all terms that even partially match those strings. It is not necessary to use an asterisk (*) on the initial search. For example, you can enter *Win* to return results that include the word Windows, such as any Windows operating system. Or if you want to find all IP addresses in the 10.20 range, you can enter 10.20 in the Search text box.

If you want to modify the search after viewing the results, an asterisk is appended to the string in the *Search Criteria* pane that appears with the results. If you leave the asterisk in, the modified search will still return partial matches. You can remove the asterisk if you want the next set of results to match the string exactly.



Searching with a partial string

If you precede a string with an asterisk, the search ignores the asterisk and returns results that match the string itself.

Certain words and individual characters, collectively known as *stop words* return no results, even if you enter them with asterisks. For better performance, search mechanisms do not recognize stop words. Some stop words are single letters, such as *a*, *i, s*, and *t*. If you want to include one of these letters in a search string, add one or more letters to the string. Following is a list of stop words:

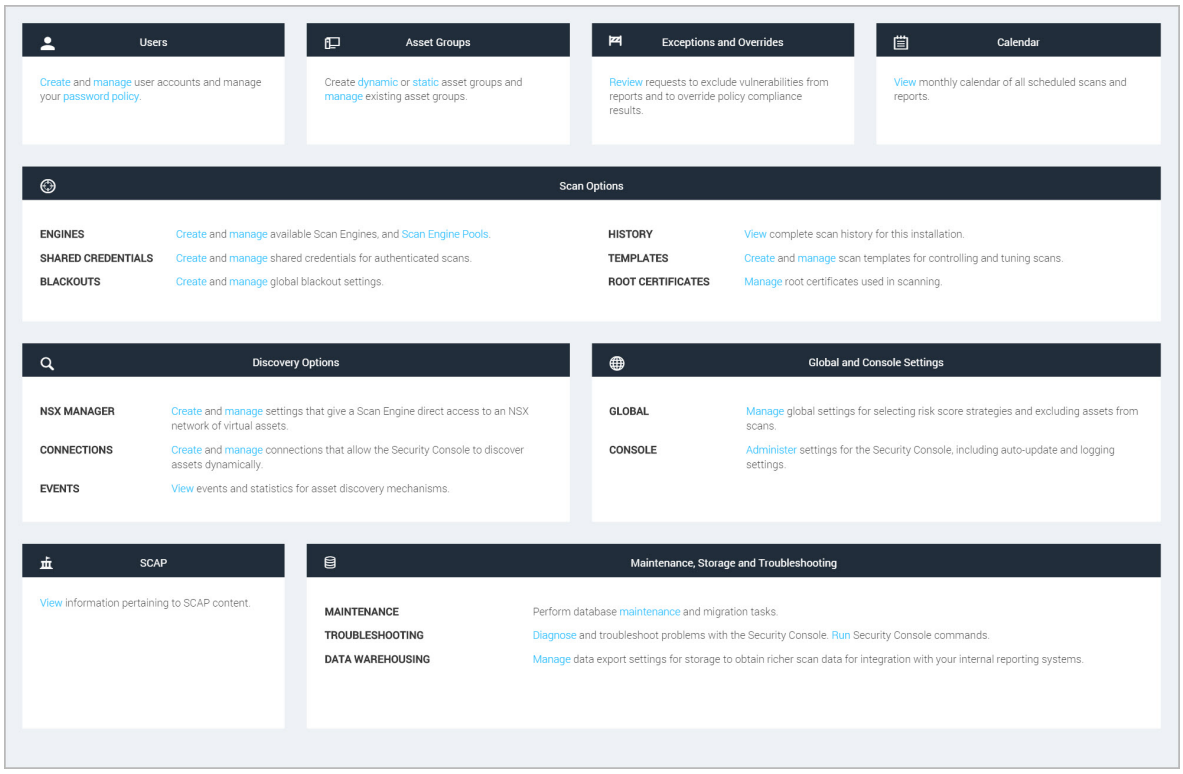
a	about	above	after	again	against	all	am	an	and
any	are	as	at	be	because	been	being	below	before
between	both	but	by	can	did	do	doing	don	does
down	during	each	few	for	from	further	had	has	have
having	he	her	here	hers	herself	him	himself	his	how
i	if	in	into	it	is	its	itself	just	me
more	most	my	myself	no	nor	not	now	of	off
on	once	only	or	other	our	ours	ourselves	out	over
own	s	same	she	should	so	some	such	t	than
that	the	their	theirs	them	themselves	then	there	these	they
this	those	through	to	too	under	until	up	very	was
we	were	what	when	where	which	while	who	whom	why
will	with	you	your	yours	yourself	yourselves			

Accessing operations faster with the Administration page

You can access a number of key Security Console operations quickly from the *Administration* page. To go there, click the **Administration** icon. The page displays a panel of tiles that contain links to pages where you can perform any of the following operations to which you have access:

- managing user accounts
- managing asset groups
- reviewing requests for vulnerability exceptions and policy result overrides
- creating and managing Scan Engines
- managing shared scan credentials, which can be applied in multiple sites
- viewing the scan history for your installation
- managing scan templates
- managing different models, or strategies, for calculating risk scores
- managing various activities and settings controlled by the Security Console, such as license, updates, and communication with Scan Engines
- managing settings and events related to discovery of virtual assets, which allows you to create dynamic sites
- viewing information related to Security Content Automation Protocol (SCAP) content
- maintaining and migrating the database
- troubleshooting the application
- using the command console to type commands
- managing data export settings for integration with third-party reporting systems

Tiles that contain operations that you do not have access to because of your role or license display a label that indicates this restriction.



Administration page

After viewing the options, select an operation by clicking the link for that operation.

Using configuration panels

The Security Console provides panels for configuration and administration tasks:

- creating and editing sites
- creating and editing user accounts
- creating and editing asset groups
- creating and editing scan templates
- creating and editing reports and report templates
- configuring Security Console settings
- troubleshooting and maintenance

Note: Parameters labeled in red denote required parameters on all panel pages.

Extending Web interface sessions

Note: You can change the length of the Web interface session. See *Changing Security Console Web server default settings* in the administrator's guide.

By default, an idle Web interface session times out after 10 minutes. When an idle session expires, the Security Console displays a logon window. To continue the session, simply log on again. You will not lose any unsaved work, such as configuration changes. However, if you choose to log out, you will lose unsaved work.

If a communication issue between your browser and the Security Console Web server prevents the session from refreshing, you will see an error message. If you have unsaved work, do not leave the page, refresh the page, or close the browser. Contact your Global Administrator.

Troubleshooting your activation

Your product key is your access to all the features you need to start using the application. Before you can being using the application you must activate your license using the product key you received. Your license must be active so that you can perform operations like running scans and creating reports. If you received an error message when you tried to activate your license you can try the troubleshooting techniques identified below before contacting Technical Support.

Product keys are good for one use; if you are performing the installation for a second time or if you receive errors during product activation and these techniques have not worked for you, contact Technical Support.

Try the following techniques to troubleshoot your activation:

Did I enter the product key correctly?

- Verify that you entered the product key correctly.

Is there an issue with my browser?

- Confirm the browser you are using is supported. See *Using the Web interface* on page 24 for a list of supported browsers.
- Clear the browser cache.

Are my proxy settings correct?

- If you are using a proxy server, verify that your proxy settings are correct because inaccurate settings can cause your license activation to fail.
  - Go to the *Administration* page and click **Manage** *settings for the Security Console* to open the Security Console Configuration panel. Select Update Proxy to display the Proxy Settings section ensure that the address, port, domain, User ID, and password are entered correctly.
  - If you are not using a proxy, ensure the **Name or address field** is specified as *updates.rapid7.com*. Changing this setting to another server address may cause your activation to fail. Contact Technical Support if you require a different server address and you receive errors during activation.

Are there issues with my network or operating system?

- By running diagnostics, you can find operating system and network issues that could be preventing license activation.
  - Go to the *Administration* page and click **Diagnose** *and troubleshoot problems with the Security Console*.
  - Select the OS Diagnostics and Network Diagnostics checkboxes.
  - Click **Perform diagnostics** to see the current status of your installation. The results column will provide valuable information such as, if DNS name resolution is successful, if firewalls are enabled, and if the Gateway ping returns a 'DEAD' response.
- Confirm that all traffic is allowed out over port 80 to updates.rapid7.com.
  - If you are using Linux, open a terminal and enter `telnet updates.rapid7.com 80`. You will see `Connected` if traffic is allowed.
  - If you are using Windows, open a browser and enter http://updates.rapid7.com. You should see a blank page.
  - White-list the IP address of the application server on your firewall so that it can send traffic outbound to http://updates.rapid7.com.
  - Make the same rule changes on your proxy server.
  - If you see an error message after adding the IP address to a white-list you will need to determine what is blocking the application.

Are there issues with firewalls in my network?

- Confirm that host-based firewall and antivirus detection are disabled on the system you are installing the application on. See *Using anti-virus software on the server* in the *administrator's guide* for more information.
- Ensure the IP address of the application server is white-listed through firewalls and content filters. This will allow you to reach the update server and pull down any necessary .jar files for activation and updates.

Have I tried everything?

- Restart the application, in some cases a browser anomaly can cause an error message that your activation failed. Restarting may be successful in those rare cases.

Scanning, viewing results, and reporting

Use this section to get started quickly by taking a three-step approach to vulnerability management:

1. ***Discover* on page 44:** To know what your security priorities are, you need to discover what devices are running in your environment and how these assets are vulnerable to attack. You discover this information by running scans.
2. ***Assess* on page 46:** After you discover all the assets and vulnerabilities in your environment, it is important to parse this information to determine what the major security threats are, such as high-risk assets, vulnerabilities, potential malware exposures, or policy violations.
3. ***Act* on page 51:** After you discover what is running in your environment and assess your security threats, you can initiate actions to remediate these threats.

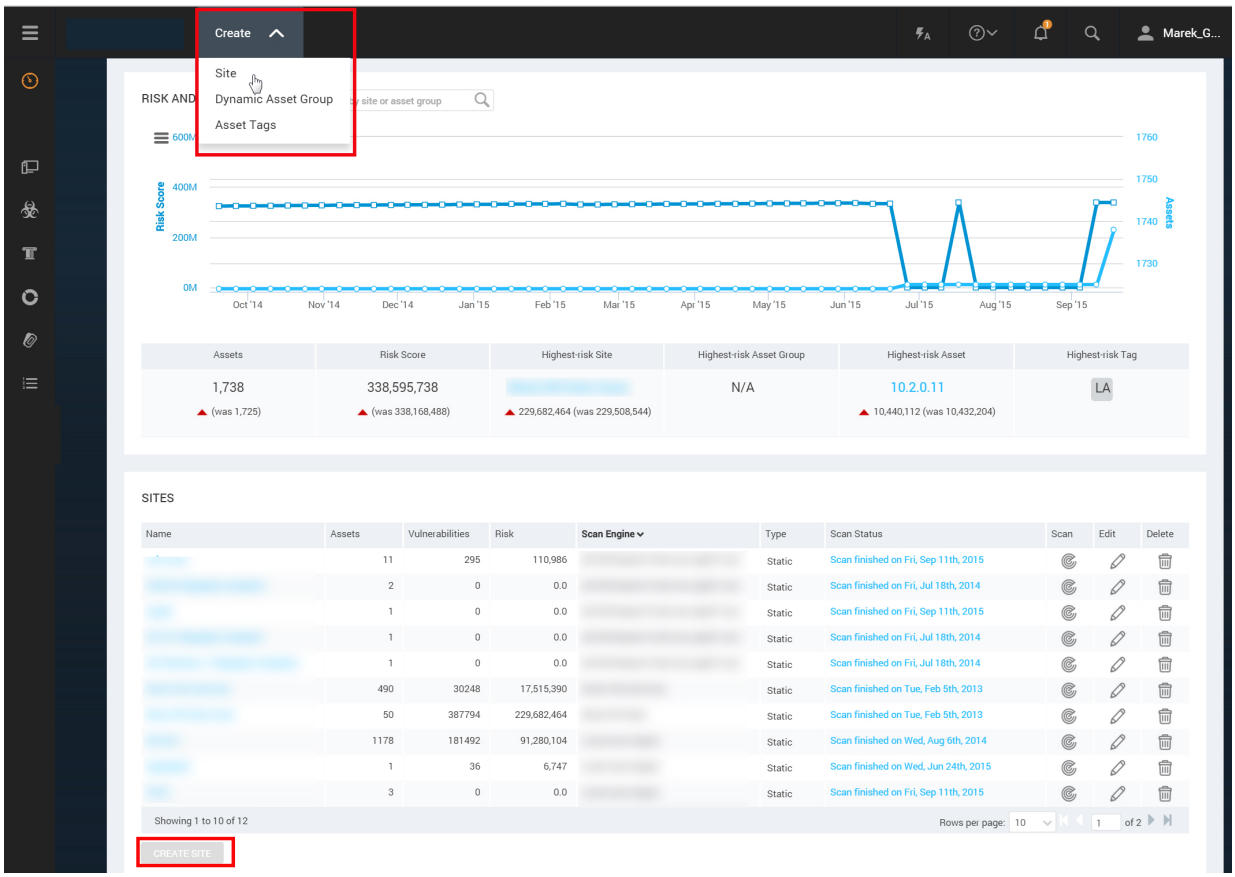
Discover

Find vulnerabilities in your environment.

Create a site

A site is a collection of assets to scan. You must have a site created before you run a scan.

1. On the *Home* page, click the **Create** tab at the top and then select *Site* from the drop-down list.
   OR
   Click the **Create Site** button at the bottom of the *Sites* table.



New static site button

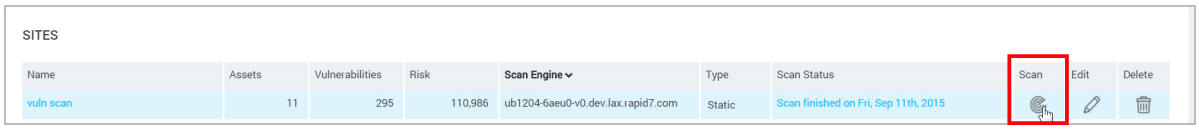
2. On the **Info & Security** tab of the *Site Configuration* panel, enter a unique name for the site.
3. Click the **Assets** tab.
4. In the Include text box, enter host names, single IP addresses, or a range.
5. Click **Save**. The new site appears on in the *Site Listing* table of the *Home* page.

A site configuration also includes a scan template, which defines the settings for the scan. The default Full Audit without Web Spider template is good for first-time scans because it covers a large number of vulnerability checks. Click the **Templates** tab in the *Site Configuration* panel to see a list of scan templates.

Run a scan

Run a scan to discover assets and vulnerabilities.

1. Click **Scan** for the site you created.

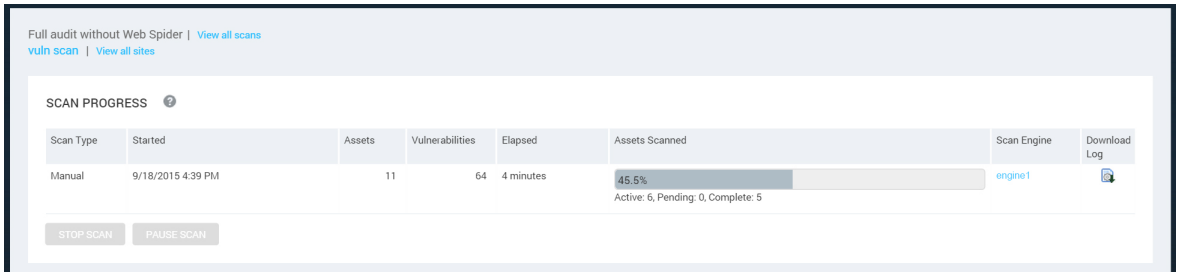


Site listing panel

2. In the *Start New Scan* window, click **Start now**.

Start New Scan dialog

3. The Security Console displays the page for your scan, so you can watch its progress as it discovers assets and vulnerabilities.



Scan progress

4. You can confirm that the scan has completed by looking at the *Site Listing* table on the *Home* page.

Scan status

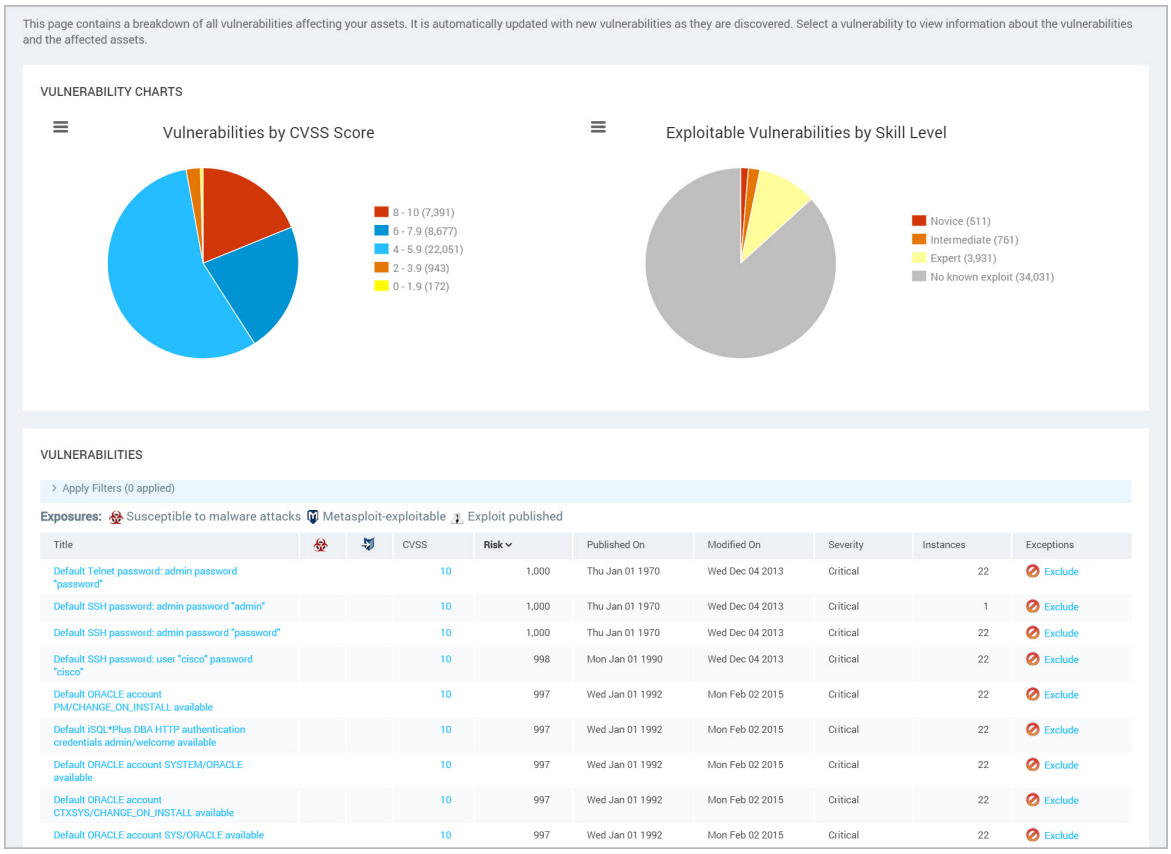
Assess

View and sort scan results to find out your security posture and remediation priorities.

You can drill down through scan data two different ways:

Option A

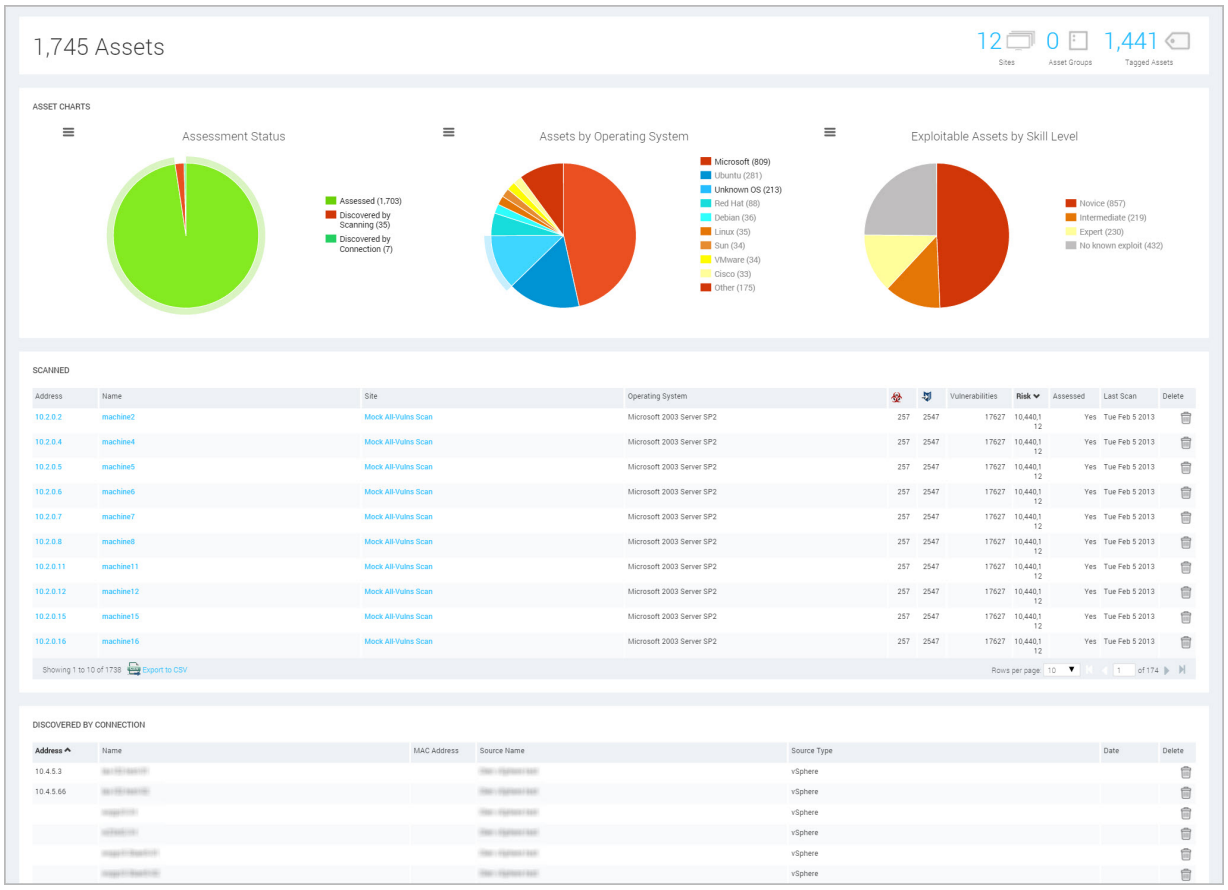
Click the **Vulnerabilities** icon to view and compare discovered vulnerabilities and then find out which assets are affected by each vulnerability. This approach is useful if you are concerned about specific vulnerabilities.



Vulnerabilities page

Option B

Click the **Assets**icon to see specific assets and then find out which vulnerabilities affect them. This approach is useful if you are concerned about certain sensitive assets. This guide shows the asset-based approach.

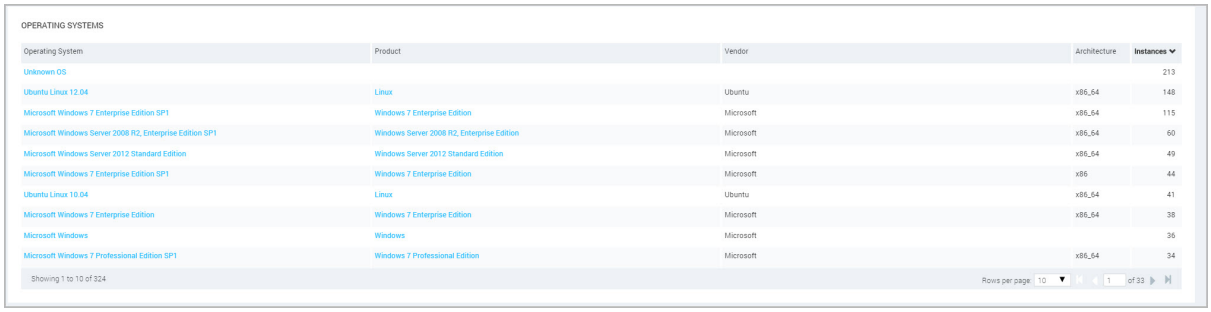


Assets panel

Using an asset-based approach

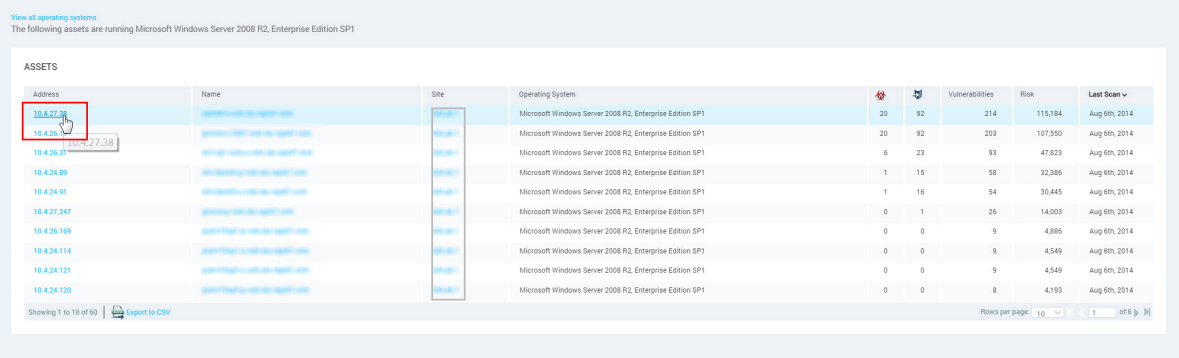
To see specific assets and find out which vulnerabilities affect them:

1. After a scan completes, click the **Assets** icon and drill down to the subset of assets that you want to see.



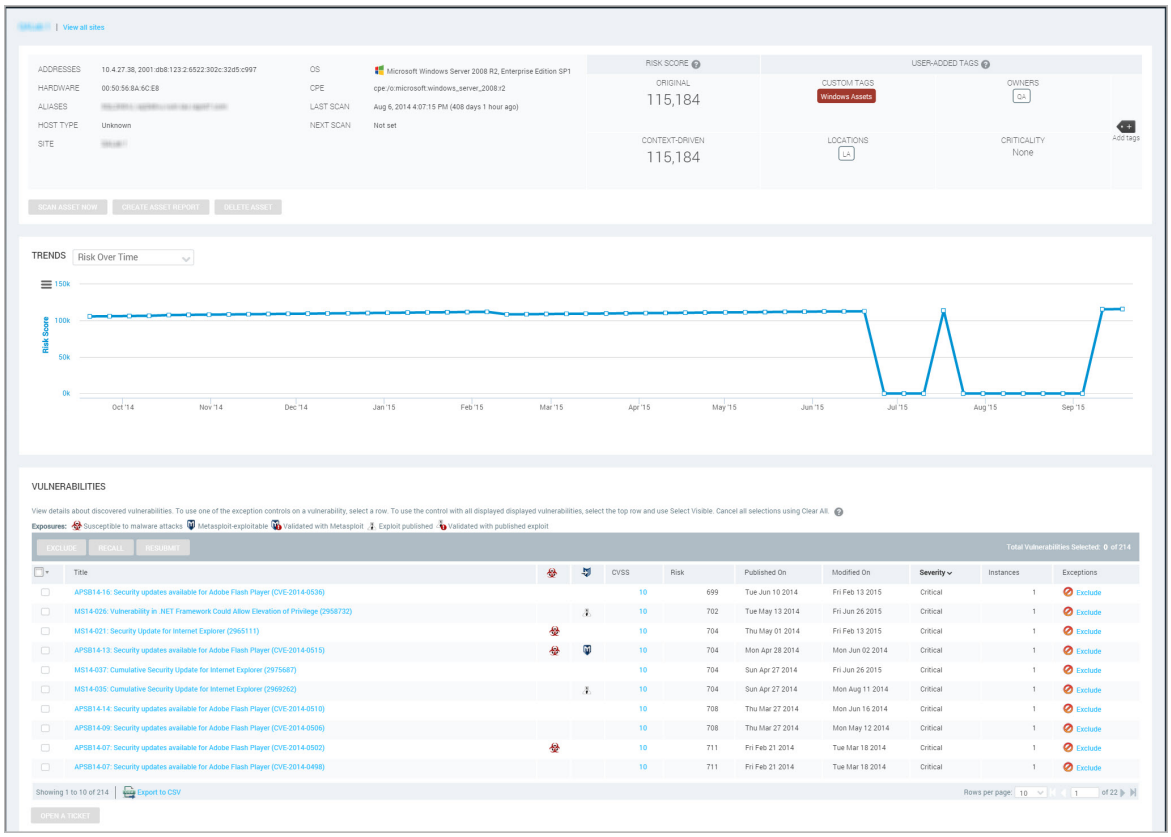
Assets panel-Operating System Listing

2. Compare assets by different security metrics: Click column headings to sort assets by malware or exploit exposures, total vulnerabilities or risk scores.
3. Click an asset's IP address or host name to view details about it.



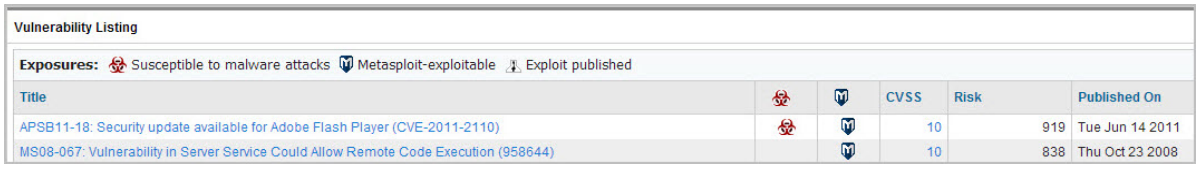
Assets panel-Asset Listing table

4. View details about the asset, including all discovered vulnerabilities.
   - To sort vulnerabilities by name, click the **Title** heading in the *Vulnerability Listing* table.
   - To compare and prioritize vulnerabilities, click other column headings and sort them by different security metrics.



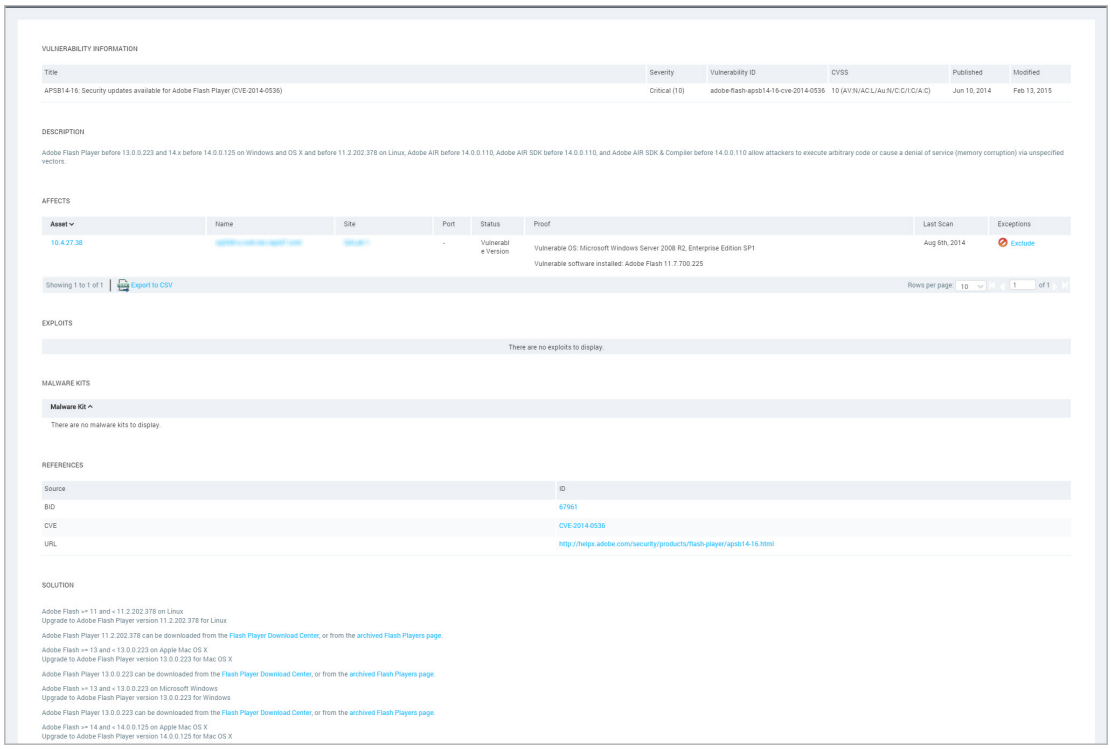
Asset properties page

5. Click the name of a listed vulnerability to view details about it.



Vulnerabilities Listing panel

6. The Security Console displays a page with details about the vulnerability, including its security metrics, affected assets, and remediation solutions.



Vulnerabilities overview

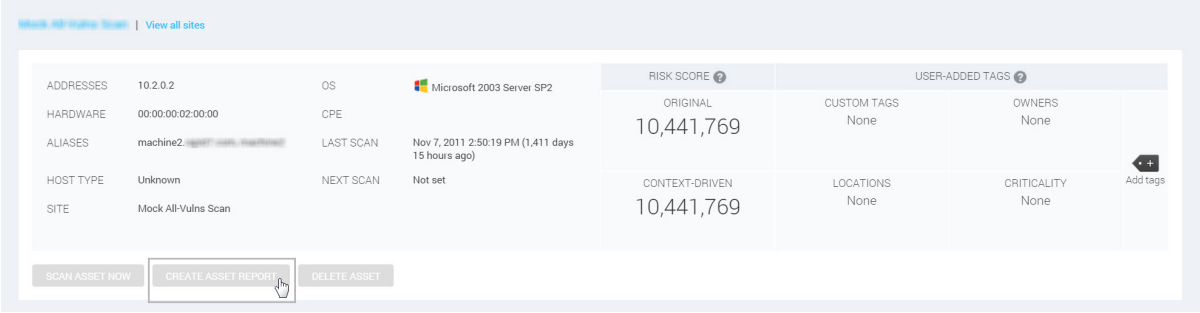
7. Click the **Back** arrow on your browser to return to the asset details page.

Act

Create a report so that your organization can view its security posture and start to prioritize and remediate vulnerabilities.

Option A

If you want to share urgent information about a sensitive asset, click the **Create asset report** button on the page for that asset.



Create asset report

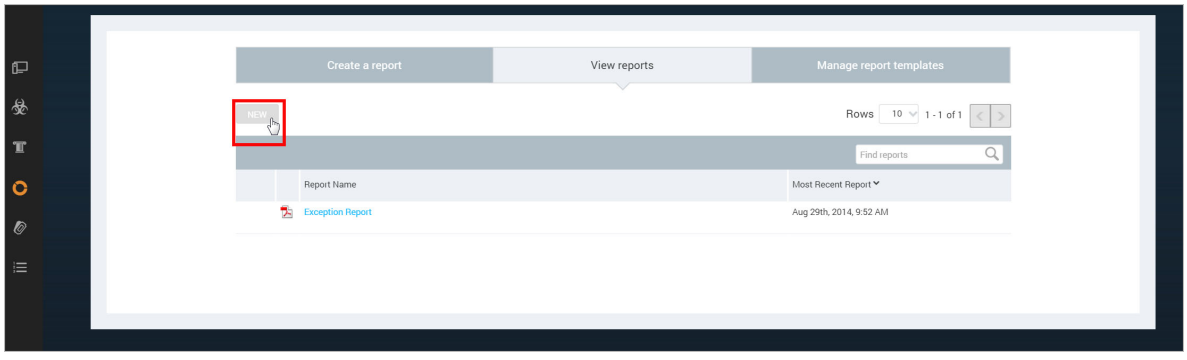
Option B

If you want to report on multiple assets, click the **Reports** icon. This guide shows the multiple-asset approach for creating an audit report in PDF format.

Using a multiple-asset based approach

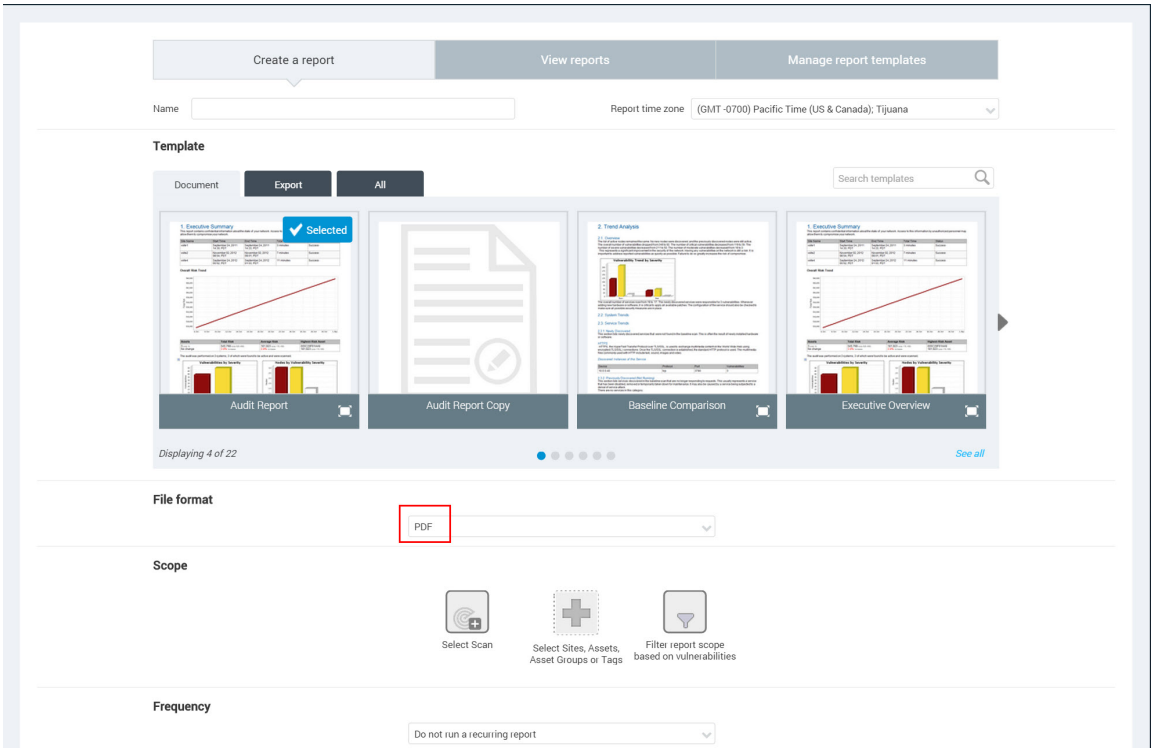
For creating audit report in PDF format:

1. Click the **Reports** icon. The *Reports* page lists any reports that have been created.
   OR
   Click the **Create** tab at the top and then select *Site* from the drop-down list.
2. Click **New**.



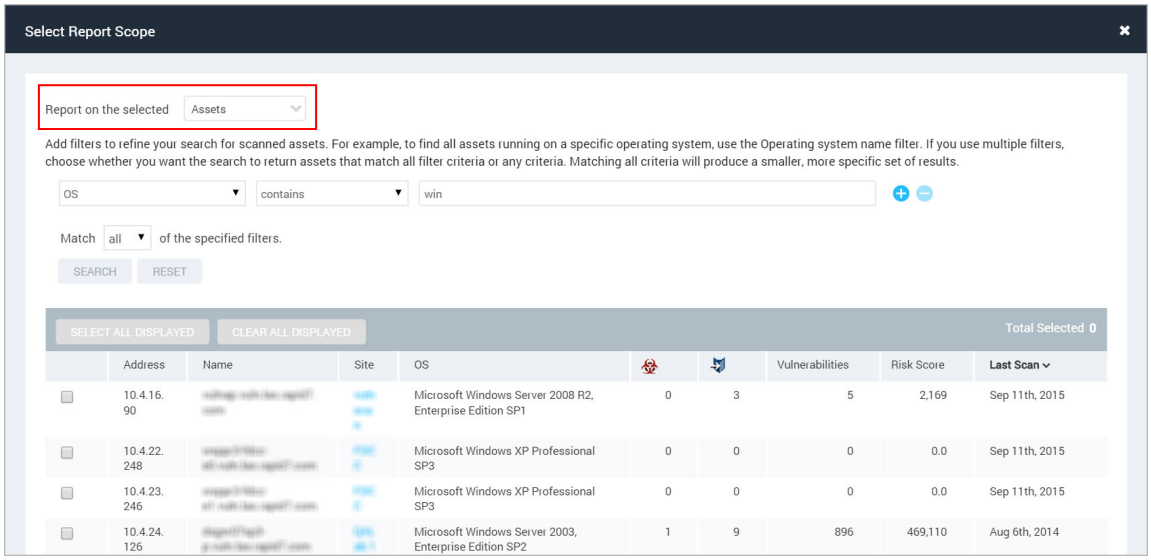
Report panel–View Reports tab

3. Select the *Audit Report* template. Each template controls what specific information is included in the report.
4. Select the PDF format on the *Create a report* panel.



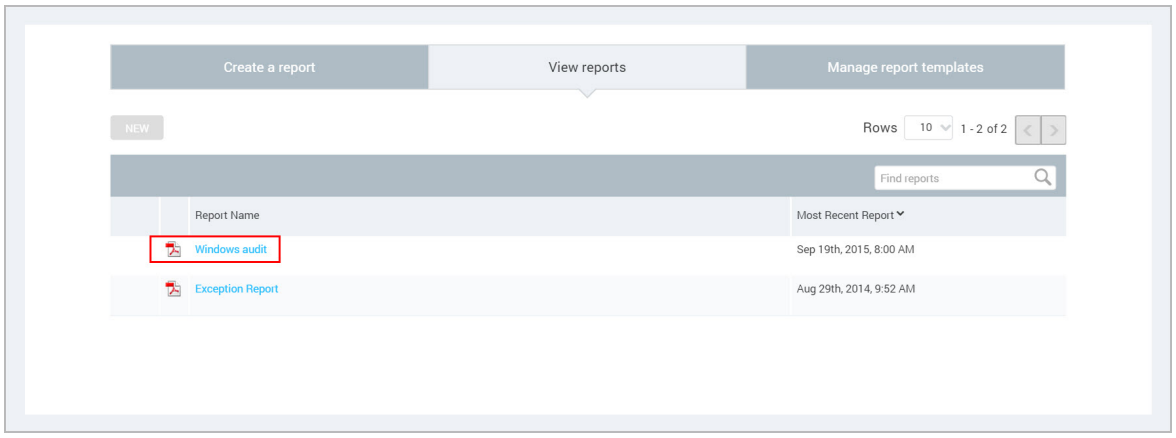
Selecting the PDF report format

5. Click **Select Sites, Assets, or Asset Groups** to view the *Select Report Scope* page.
6. Select **Assets** from the drop-down list.



Select Report Scope panel

7. Enter or select search criteria, and click **Search**. A list of assets is displayed.
8. Click check boxes for assets that you want to include in the reports, and click **Done**.
9. Click **Run the report** to generate the report. The Security Console displays the status of the report generation. When the report is complete, the creation date and time appear in the *View reports* page.
10. Click the report name to view the report.



Selecting a report

The report shows remediation steps for each vulnerability on each asset.

3.3.1. ICMP timestamp response (generic-icmp-timestamp)

Description:

The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services.

In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.

Affected Nodes:

Affected Nodes:	Additional Information:
10.4.16.90	Able to determine remote system time.

References:

Source	Reference
CVE	CVE-1999-0524
OSVDB	95
XF	306

Source	Reference
XF	322

Vulnerability Solution:

•HP-UX

Disable ICMP timestamp responses on HP/UX

Execute the following command:

ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Cisco IOS

Disable ICMP timestamp responses on Cisco IOS

Use ACLs to block ICMP types 13 and 14. For example:

deny icmp any any 13

deny icmp any any 14

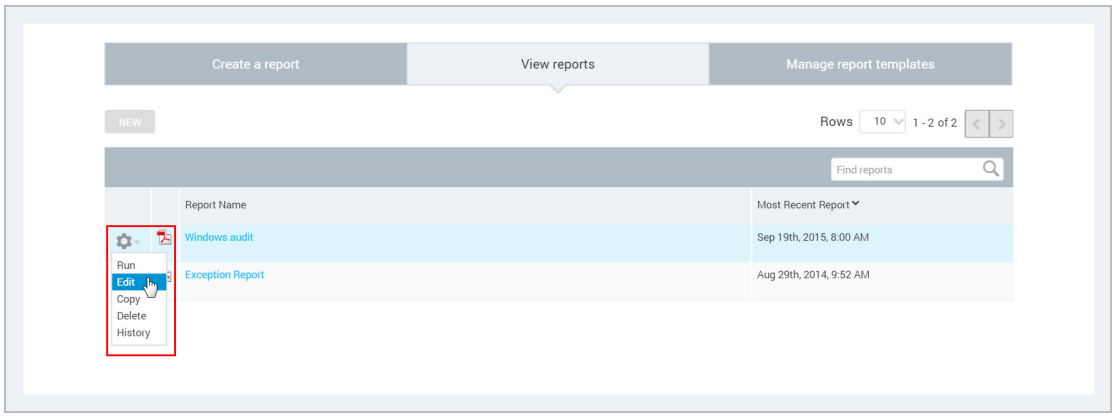
Note that it is generally preferable to use ACLs that block everything by default and then selectively allow certain types of traffic in. For example, block everything and then only allow ICMP unreachable, ICMP echo reply, ICMP time exceeded, and ICMP source quench:

permit icmp any any unreachable

Audit report-remediation steps

11. Click the *View Reports* tab to access the report again, if you want to **Edit** it **or Generate** a new instance.

Tip: You can schedule reports to run automatically. This is useful if you create multiple sites and run scans on a regular basis. You can schedule reports to run after these scans are complete. To see scheduling options, select the **Run a reoccuring report** on a schedule option on the *Frequency* dropdown menu in the *Report Configuration* panel.



View reports tab-tools drop-down menu

Glossary

API (application programming interface)

An API is a function that a developer can integrate with another software application by using program calls. The term *API* also refers to one of two sets of XML APIs, each with its own included operations: API v1.1 and Extended API v1.2. To learn about each API, see the API documentation, which you can download from the *Support* page in Help.

Appliance

An Appliance is a set of InsightVM components shipped as a dedicated hardware/software unit. Appliance configurations include a Security Console/Scan Engine combination and an Scan Engine-only version.

Asset

An asset is a single device on a network that the application discovers during a scan. In the Web interface and API, an asset may also be referred to as a *device*. See *Managed asset* on page 63 and *Unmanaged asset* on page 70. An asset's data has been integrated into the scan database, so it can be listed in sites and asset groups. In this regard, it differs from a *node*. See *Node* on page 64.

Asset group

An asset group is a logical collection of managed assets to which specific members have access for creating or viewing reports or tracking remediation tickets. An asset group may contain assets that belong to multiple sites or other asset groups. An asset group is either static or dynamic. An asset group is not a site. See *Site* on page 69, *Dynamic asset group* on page 61, and *Static asset group* on page 69.

Asset Owner

Asset Owner is one of the preset roles. A user with this role can view data about discovered assets, run manual scans, and create and run reports in accessible sites and asset groups.

Asset Report Format (ARF)

The Asset Report Format is an XML-based report template that provides asset information based on connection type, host name, and IP address. This template is required for submitting reports of policy scan results to the U.S. government for SCAP certification.

Asset search filter

An asset search filter is a set of criteria with which a user can refine a search for assets to include in a dynamic asset group. An asset search filter is different from a *Dynamic Discovery filter* on page 61.

Authentication

Authentication is the process of a security application verifying the logon credentials of a client or user that is attempting to gain access. By default the application authenticates users with an internal process, but you can configure it to authenticate users with an external LDAP or Kerberos source.

Average risk

Average risk is a setting in risk trend report configuration. It is based on a calculation of your risk scores on assets over a report date range. For example, average risk gives you an overview of how vulnerable your assets might be to exploits whether it's high or low or unchanged. Some assets have higher risk scores than others. Calculating the average score provides a high-level view of how vulnerable your assets might be to exploits.

Benchmark

In the context of scanning for FDCC policy compliance, a benchmark is a combination of policies that share the same source data. Each policy in the Policy Manager contains some or all of the rules that are contained within its respective benchmark. See *Federal Desktop Core Configuration (FDCC)* on page 62 and *United States Government Configuration Baseline (USGCB)* on page 70.

Breadth

Breadth refers to the total number of assets within the scope of a scan.

Category

In the context of scanning for FDCC policy compliance, a category is a grouping of policies in the Policy Manager configuration for a scan template. A policy's category is based on its source, purpose, and other criteria. See*Policy Manager* on page 65, *Federal Desktop Core Configuration (FDCC)* on page 62, and *United States Government Configuration Baseline (USGCB)* on page 70.

Check type

A check type is a specific kind of check to be run during a scan. Examples: The Unsafe check type includes aggressive vulnerability testing methods that could result in Denial of Service on target

assets; the Policy check type is used for verifying compliance with policies. The check type setting is used in scan template configurations to refine the scope of a scan.

Center for Internet Security (CIS)

Center for Internet Security (CIS) is a not-for-profit organization that improves global security posture by providing a valued and trusted environment for bridging the public and private sectors. CIS serves a leadership role in the shaping of key security policies and decisions at the national and international levels. The Policy Manager provides checks for compliance with CIS benchmarks including technical control rules and values for hardening network devices, operating systems, and middleware and software applications. Performing these checks requires a license that enables the Policy Manager feature and CIS scanning. See *Policy Manager* on page 65.

Command console

The command console is a page in the Security Console Web interface for entering commands to run certain operations. When you use this tool, you can see real-time diagnostics and a behind-the-scenes view of Security Console activity. To access the command console page, click the **Run Security Console commands** link next to the *Troubleshooting* item on the *Administration* page.

Common Configuration Enumeration (CCE)

Common Configuration Enumeration (CCE) is a standard for assigning unique identifiers known as CCEs to configuration controls to allow consistent identification of these controls in different environments. CCE is implemented as part of its compliance with SCAP criteria for an Unauthenticated Scanner product.

Common Platform Enumeration (CPE)

Common Platform Enumeration (CPE) is a method for identifying operating systems and software applications. Its naming scheme is based on the generic syntax for Uniform Resource Identifiers (URI). CCE is implemented as part of its compliance with SCAP criteria for an Unauthenticated Scanner product.

Common Vulnerabilities and Exposures (CVE)

The Common Vulnerabilities and Exposures (CVE) standard prescribes how the application should identify vulnerabilities, making it easier for security products to exchange vulnerability data. CVE is implemented as part of its compliance with SCAP criteria for an Unauthenticated Scanner product.

Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS) is an open framework for calculating vulnerability risk scores. CVSS is implemented as part of its compliance with SCAP criteria for an Unauthenticated Scanner product.

Compliance

Compliance is the condition of meeting standards specified by a government or respected industry entity. The application tests assets for compliance with a number of different security standards, such as those mandated by the Payment Card Industry (PCI) and those defined by the National Institute of Standards and Technology (NIST) for Federal Desktop Core Configuration (FDCC).

Continuous scan

A continuous scan starts over from the beginning if it completes its coverage of site assets within its scheduled window. This is a site configuration setting.

Coverage

Coverage indicates the scope of vulnerability checks. A coverage improvement listed on the News page for a release indicates that vulnerability checks have been added or existing checks have been improved for accuracy or other criteria.

Criticality

Criticality is a value that you can apply to an asset with a RealContext tag to indicate its importance to your business. Criticality levels range from *Very Low* to *Very High*. You can use applied criticality levels to alter asset risk scores. See *Criticality-adjusted risk*.

Criticality-adjusted risk

or

Context-driven risk

Criticality-adjusted risk is a process for assigning numbers to criticality levels and using those numbers to multiply risk scores.

Custom tag

With a custom tag you can identify assets by according to any criteria that might be meaningful to your business.

Depth

Depth indicates how thorough or comprehensive a scan will be. Depth refers to level to which the application will probe an individual asset for system information and vulnerabilities.

Discovery (scan phase)

Discovery is the first phase of a scan, in which the application finds potential scan targets on a network. Discovery as a scan phase is different from *Dynamic Discovery* on page 61.

Document report template

Document templates are designed for human-readable reports that contain asset and vulnerability information. Some of the formats available for this template type—Text, PDF, RTF, and HTML—are convenient for sharing information to be read by stakeholders in your organization, such as executives or security team members tasked with performing remediation.

Dynamic asset group

A dynamic asset group contains scanned assets that meet a specific set of search criteria. You define these criteria with asset search filters, such as IP address range or operating systems. The list of assets in a dynamic group is subject to change with every scan or when vulnerability exceptions are created. In this regard, a dynamic asset group differs from a static asset group. See *Asset group* on page 57 and *Static asset group* on page 69.

Dynamic Discovery

Dynamic Discovery is a process by which the application automatically discovers assets through a connection with a server that manages these assets. You can refine or limit asset discovery with criteria filters. Dynamic discovery is different from *Discovery (scan phase)* on page 61.

Dynamic Discovery filter

A Dynamic Discovery filter is a set of criteria refining or limiting Dynamic Discovery results. This type of filter is different from an *Asset search filter* on page 58.

Dynamic Scan Pool

The Dynamic Scan Pool feature allows you to use Scan Engine pools to enhance the consistency of your scan coverage. A Scan Engine pool is a group of shared Scan Engines that can be bound to a site so that the load is distributed evenly across the shared Scan Engines. You can configure scan pools using the Extended API v1.2.

Dynamic site

A dynamic site is a collection of assets that are targeted for scanning and that have been discovered through vAsset discovery. Asset membership in a dynamic site is subject to change if the discovery connection changes or if filter criteria for asset discovery change. See *Static site* on page 70, *Site* on page 69, and *Dynamic Discovery* on page 61.

Exploit

An exploit is an attempt to penetrate a network or gain access to a computer through a security flaw, or vulnerability. Malicious exploits can result in system disruptions or theft of data. Penetration testers use benign exploits only to verify that vulnerabilities exist. The Metasploit product is a tool for performing benign exploits. See *Metasploit* on page 64 and *Published exploit* on page 66.

Export report template

Export templates are designed for integrating scan information into external systems. The formats available for this type include various XML formats, Database Export, and CSV.

Exposure

An exposure is a vulnerability, especially one that makes an asset susceptible to attack via malware or a known exploit.

Extensible Configuration Checklist Description Format (XCCDF)

As defined by the National Institute of Standards and Technology (NIST), Extensible Configuration Checklist Description Format (XCCDF) “is a specification language for writing security checklists, benchmarks, and related documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring.” Policy Manager checks for FDCC policy compliance are written in this format.

False positive

A false positive is an instance in which the application flags a vulnerability that doesn’t exist. A false negative is an instance in which the application fails to flag a vulnerability that does exist.

Federal Desktop Core Configuration (FDCC)

The Federal Desktop Core Configuration (FDCC) is a grouping of configuration security settings recommended by the National Institute of Standards and Technology (NIST) for computers that are connected directly to the network of a United States government agency. The Policy

Manager provides checks for compliance with these policies in scan templates. Performing these checks requires a license that enables the Policy Manager feature and FDCC scanning.

Fingerprinting

Fingerprinting is a method of identifying the operating system of a scan target or detecting a specific version of an application.

Global Administrator

Global Administrator is one of the preset roles. A user with this role can perform all operations that are available in the application and they have access to all sites and asset groups.

Host

A host is a physical or virtual server that provides computing resources to a guest virtual machine. In a high-availability virtual environment, a host may also be referred to as a node. The term *node* has a different context in the application. See *Node* on page 64.

Latency

Latency is the delay interval between the time when a computer sends data over a network and another computer receives it. Low latency means short delays.

Locations tag

With a *Locations* tag you can identify assets by their physical or geographic locations.

Malware

Malware is software designed to disrupt or deny a target systems's operation, steal or compromise data, gain unauthorized access to resources, or perform other similar types of abuse. The application can determine if a vulnerability renders an asset susceptible to malware attacks.

Malware kit

Also known as an exploit kit, a malware kit is a software bundle that makes it easy for malicious parties to write and deploy code for attacking target systems through vulnerabilities.

Managed asset

A managed asset is a network device that has been discovered during a scan and added to a site's target list, either automatically or manually. Only managed assets can be checked for vulnerabilities and tracked over time. Once an asset becomes a managed asset, it counts against the maximum number of assets that can be scanned, according to your license.

Manual scan

A manual scan is one that you start at any time, even if it is scheduled to run automatically at other times. Synonyms include *ad-hoc scan* and *unscheduled scan*.

Metasploit

Metasploit is a product that performs benign exploits to verify vulnerabilities. See *Exploit* on page 62.

MITRE

The MITRE Corporation is a body that defines standards for enumerating security-related concepts and languages for security development initiatives. Examples of MITRE-defined enumerations include Common Configuration Enumeration (CCE) and Common Vulnerability Enumeration (CVE). Examples of MITRE-defined languages include Open Vulnerability and Assessment Language (OVAL). A number of MITRE standards are implemented, especially in verification of FDCC compliance.

National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. The agency mandates and manages a number of security initiatives, including Security Content Automation Protocol (SCAP). See *Security Content Automation Protocol (SCAP)* on page 68.

Node

A node is a device on a network that the application discovers during a scan. After the application integrates its data into the scan database, the device is regarded as an *asset* that can be listed in sites and asset groups. See *Asset* on page 57.

Open Vulnerability and Assessment Language (OVAL)

Open Vulnerability and Assessment Language (OVAL) is a development standard for gathering and sharing security-related data, such as FDCC policy checks. In compliance with an FDCC requirement, each OVAL file that the application imports during configuration policy checks is available for download from the *SCAP* page in the Security Console Web interface.

Override

An override is a change made by a user to the result of a check for compliance with a configuration policy rule. For example, a user may override a Fail result with a Pass result.

Payment Card Industry (PCI)

The Payment Card Industry (PCI) is a council that manages and enforces the PCI Data Security Standard for all merchants who perform credit card transactions. The application includes a scan template and report templates that are used by Approved Scanning Vendors (ASVs) in official merchant audits for PCI compliance.

Permission

A permission is the ability to perform one or more specific operations. Some permissions only apply to sites or asset groups to which an assigned user has access. Others are not subject to this kind of access.

Policy

A policy is a set of primarily security-related configuration guidelines for a computer, operating system, software application, or database. Two general types of polices are identified in the application for scanning purposes: *Policy Manager* policies and *standard* policies. The application's Policy Manager (a license-enabled feature) scans assets to verify compliance with policies encompassed in the United States Government Configuration Baseline (USGCB), the Federal Desktop Core Configuration (FDCC), Center for Internet Security (CIS), and Defense Information Systems Agency (DISA) standards and benchmarks, as well as user-configured custom policies based on these policies. See *Policy Manager* on page 65, *Federal Desktop Core Configuration (FDCC)* on page 62, *United States Government Configuration Baseline (USGCB)* on page 70, and *Scan* on page 67. The application also scans assets to verify compliance with standard policies. See *Scan* on page 67 and *Standard policy* on page 69.

Policy Manager

Policy Manager is a license-enabled scanning feature that performs checks for compliance with Federal Desktop Core Configuration (FDCC), United States Government Configuration Baseline (USGCB), and other configuration policies. Policy Manager results appear on the *Policies* page, which you can access by clicking the **Policies** icon in the Web interface. They also appear in the *Policy Listing* table for any asset that was scanned with Policy Manager checks. Policy Manager policies are different from standard policies, which can be scanned with a basic license. See *Policy* on page 65 and *Standard policy* on page 69.

Policy Result

In the context of FDCC policy scanning, a result is a state of compliance or non-compliance with a rule or policy. Possible results include *Pass*, *Fail*, or *Not Applicable*.

Policy Rule

A rule is one of a set of specific guidelines that make up an FDCC configuration policy. See *Federal Desktop Core Configuration (FDCC)* on page 62, *United States Government Configuration Baseline (USGCB)* on page 70, and *Policy* on page 65.

Potential vulnerability

A potential vulnerability is one of three positive vulnerability check result types. The application reports a potential vulnerability during a scan under two conditions: First, potential vulnerability checks are enabled in the template for the scan. Second, the application determines that a target is running a vulnerable software version but it is unable to verify that a patch or other type of remediation has been applied. For example, an asset is running version 1.1.1 of a database. The vendor publishes a security advisory indicating that version 1.1.1 is vulnerable. Although a patch is installed on the asset, the version remains 1.1.1. In this case, if the application is running checks for potential vulnerabilities, it can only flag the host asset as being potentially vulnerable. The code for a potential vulnerability in XML and CSV reports is *vp* (vulnerable, potential). For other positive result types, see *Vulnerability check* on page 72.

Published exploit

In the context of the application, a published exploit is one that has been developed in Metasploit or listed in the Exploit Database. See *Exploit* on page 62.

RealContext

RealContext is a feature that enables you to tag assets according to how they affect your business. You can use tags to specify the criticality, location, or ownership. You can also use custom tags to identify assets according any criteria that is meaningful to your organization.

Real Risk strategy

Real Risk is one of the built-in strategies for assessing and analyzing risk. It is also the recommended strategy because it applies unique exploit and malware exposure metrics for each vulnerability to Common Vulnerability Scoring System (CVSS) base metrics for likelihood (access vector, access complexity, and authentication requirements) and impact to affected assets (confidentiality, integrity, and availability). See *Risk strategy* on page 67.

Report template

Each report is based on a template, whether it is one of the templates that is included with the product or a customized template created for your organization. See *Document report template* on page 61 and *Export report template* on page 62.

Risk

In the context of vulnerability assessment, risk reflects the likelihood that a network or computer environment will be compromised, and it characterizes the anticipated consequences of the compromise, including theft or corruption of data and disruption to service. Implicitly, risk also reflects the potential damage to a compromised entity's financial well-being and reputation.

Risk score

A risk score is a rating that the application calculates for every asset and vulnerability. The score indicates the potential danger posed to network and business security in the event of a malicious exploit. You can configure the application to rate risk according to one of several built-in risk strategies, or you can create custom risk strategies.

Risk strategy

A risk strategy is a method for calculating vulnerability risk scores. Each strategy emphasizes certain risk factors and perspectives. Four built-in strategies are available: *Real Risk strategy* on page 66, *TemporalPlus risk strategy* on page 70, *Temporal risk strategy* on page 70, and *Weighted risk strategy* on page 72. You can also create custom risk strategies.

Risk trend

A risk trend graph illustrates a long-term view of your assets' probability and potential impact of compromise that may change over time. Risk trends can be based on average or total risk scores. The highest-risk graphs in your report demonstrate the biggest contributors to your risk on the site, group, or asset level. Tracking risk trends helps you assess threats to your organization's standings in these areas and determine if your vulnerability management efforts are satisfactorily maintaining risk at acceptable levels or reducing risk over time. See *Average risk* on page 58 and *Total risk* on page 70.

Role

A role is a set of permissions. Five preset roles are available. You also can create custom roles by manually selecting permissions. See *Asset Owner* on page 57, *Security Manager* on page 69, *Global Administrator* on page 63, *Site Owner* on page 69, and *User* on page 71.

Scan

A scan is a process by which the application discovers network assets and checks them for vulnerabilities. See *Exploit* on page 62 and *Vulnerability check* on page 72.

Scan credentials

Scan credentials are the user name and password that the application submits to target assets for authentication to gain access and perform deep checks. Many different authentication mechanisms are supported for a wide variety of platforms. See *Shared scan credentials* on page 69 and *Site-specific scan credentials* on page 69.

Scan Engine

The Scan Engine is one of two major application components. It performs asset discovery and vulnerability detection operations. Scan engines can be *distributed* within or outside a firewall for varied coverage. Each installation of the Security Console also includes a local engine, which can be used for scans within the console's network perimeter.

Scan template

A scan template is a set of parameters for defining how assets are scanned. Various preset scan templates are available for different scanning scenarios. You also can create custom scan templates. Parameters of scan templates include the following:

- methods for discovering assets and services
- types of vulnerability checks, including safe and unsafe
- Web application scanning properties
- verification of compliance with policies and standards for various platforms

Scheduled scan

A scheduled scan starts automatically at predetermined points in time. The scheduling of a scan is an optional setting in site configuration. It is also possible to start any scan manually at any time.

Security Console

The Security Console is one of two major application components. It controls Scan Engines and retrieves scan data from them. It also controls all operations and provides a Web-based user interface.

Security Content Automation Protocol (SCAP)

Security Content Automation Protocol (SCAP) is a collection of standards for expressing and manipulating security data. It is mandated by the U.S. government and maintained by the National Institute of Standards and Technology (NIST). The application complies with SCAP criteria for an Unauthenticated Scanner product.

Security Manager

Security Manager is one of the preset roles. A user with this role can configure and run scans, create reports, and view asset data in accessible sites and asset groups.

Shared scan credentials

One of two types of credentials that can be used for authenticating scans, shared scan credentials are created by Global Administrators or users with the Manage Site permission. Shared credentials can be applied to multiple assets in any number of sites. See *Site-specific scan credentials* on page 69.

Site

A site is a collection of assets that are targeted for a scan. Each site is associated with a list of target assets, a scan template, one or more Scan Engines, and other scan-related settings. See *Dynamic site* on page 62 and *Static site* on page 70. A site is not an asset group. See *Asset group* on page 57.

Site-specific scan credentials

One of two types of credentials that can be used for authenticating scans, a set of single-instance credentials is created for an individual site configuration and can only be used in that site. See *Scan credentials* on page 68 and *Shared scan credentials* on page 69.

Site Owner

Site Owner is one of the preset roles. A user with this role can configure and run scans, create reports, and view asset data in accessible sites.

Standard policy

A standard policy is one of several that the application can scan with a basic license, unlike with a Policy Manager policy. Standard policy scanning is available to verify certain configuration settings on Oracle, Lotus Domino, AS/400, Unix, and Windows systems. Standard policies are displayed in scan templates when you include policies in the scope of a scan. Standard policy scan results appear in the *Advanced Policy Listing* table for any asset that was scanned for compliance with these policies. See *Policy* on page 65.

Static asset group

A static asset group contains assets that meet a set of criteria that you define according to your organization's needs. Unlike with a dynamic asset group, the list of assets in a static group does not change unless you alter it manually. See *Dynamic asset group* on page 61.

Static site

A static site is a collection of assets that are targeted for scanning and that have been manually selected. Asset membership in a static site does not change unless a user changes the asset list in the site configuration. For more information, see *Dynamic site* on page 62 and *Site* on page 69.

Temporal risk strategy

One of the built-in risk strategies, Temporal indicates how time continuously increases likelihood of compromise. The calculation applies the age of each vulnerability, based on its date of public disclosure, as a multiplier of CVSS base metrics for likelihood (access vector, access complexity, and authentication requirements) and asset impact (confidentiality, integrity, and availability). Temporal risk scores will be lower than TemporalPlus scores because Temporal limits the risk contribution of partial impact vectors. See *Risk strategy* on page 67.

TemporalPlus risk strategy

One of the built-in risk strategies, TemporalPlus provides a more granular analysis of vulnerability impact, while indicating how time continuously increases likelihood of compromise. It applies a vulnerability's age as a multiplier of CVSS base metrics for likelihood (access vector, access complexity, and authentication requirements) and asset impact (confidentiality, integrity, and availability). TemporalPlus risk scores will be higher than Temporal scores because TemporalPlus expands the risk contribution of partial impact vectors. See *Risk strategy* on page 67.

Total risk

Total risk is a setting in risk trend report configuration. It is an aggregated score of vulnerabilities on assets over a specified period.

United States Government Configuration Baseline (USGCB)

The United States Government Configuration Baseline (USGCB) is an initiative to create security configuration baselines for information technology products deployed across U.S. government agencies. USGCB evolved from FDCC, which it replaces as the configuration security mandate in the U.S. government. The Policy Manager provides checks for Microsoft Windows 7, Windows 7 Firewall, and Internet Explorer for compliance with USGCB baselines. Performing these checks requires a license that enables the Policy Manager feature and USGCB scanning. See *Policy Manager* on page 65 and *Federal Desktop Core Configuration (FDCC)* on page 62.

Unmanaged asset

An unmanaged asset is a device that has been discovered during a scan but not correlated against a managed asset or added to a site's target list. The application is designed to provide

sufficient information about unmanaged assets so that you can decide whether to manage them. An unmanaged asset does not count against the maximum number of assets that can be scanned according to your license.

Unsafe check

An unsafe check is a test for a vulnerability that can cause a denial of service on a target system. Be aware that the check itself can cause a denial of service, as well. It is recommended that you only perform unsafe checks on test systems that are not in production.

Update

An update is a released set of changes to the application. By default, two types of updates are automatically downloaded and applied:

Content updates include new checks for vulnerabilities, patch verification, and security policy compliance. Content updates always occur automatically when they are available.

Product updates include performance improvements, bug fixes, and new product features. Unlike content updates, it is possible to disable automatic product updates and update the product manually.

User

User is one of the preset roles. An individual with this role can view asset data and run reports in accessible sites and asset groups.

Validated vulnerability

A validated vulnerability is a vulnerability that has had its existence proven by an integrated Metasploit exploit. See *Exploit* on page 62.

Vulnerable version

Vulnerable version is one of three positive vulnerability check result types. The application reports a vulnerable version during a scan if it determines that a target is running a vulnerable software version and it can verify that a patch or other type of remediation has not been applied. The code for a vulnerable version in XML and CSV reports is *vv* (vulnerable, version check). For other positive result types, see *Vulnerability check* on page 72.

Vulnerability

A vulnerability is a security flaw in a network or computer.

Vulnerability category

A vulnerability category is a set of vulnerability checks with shared criteria. For example, the Adobe category includes checks for vulnerabilities that affect Adobe applications. There are also categories for specific Adobe products, such as *Air*, *Flash*, and *Acrobat/Reader*. Vulnerability check categories are used to refine scope in scan templates. Vulnerability check results can also be filtered according category for refining the scope of reports. Categories that are named for manufacturers, such as *Microsoft*, can serve as supersets of categories that are named for their products. For example, if you filter by the *Microsoft* category, you inherently include all Microsoft product categories, such as *Microsoft Path* and *Microsoft Windows*. This applies to other "company" categories, such as *Adobe*, *Apple*, and *Mozilla*.

Vulnerability check

A vulnerability check is a series of operations that are performed to determine whether a security flaw exists on a target asset. Check results are either negative (no vulnerability found) or positive. A positive result is qualified one of three ways: See *Vulnerability found* on page 72, *Vulnerable version* on page 71, and *Potential vulnerability* on page 66. You can see positive check result types in XML or CSV export reports. Also, in a site configuration, you can set up alerts for when a scan reports different positive results types.

Vulnerability exception

A vulnerability exception is the removal of a vulnerability from a report and from any asset listing table. Excluded vulnerabilities also are not considered in the computation of risk scores.

Vulnerability found

Vulnerability found is one of three positive vulnerability check result types. The application reports a vulnerability found during a scan if it verified the flaw with asset-specific vulnerability tests, such as an exploit. The code for a vulnerability found in XML and CSV reports is ve (vulnerable, exploited). For other positive result types, see *Vulnerability check* on page 72.

Weighted risk strategy

One of the built-in risk strategies, Weighted is based primarily on asset data and vulnerability types, and it takes into account the level of importance, or weight, that you assign to a site when you configure it. See *Risk strategy* on page 67.

West Virginia Ethics Commission

Disclosure of Interested Parties to Contracts

(Required by *W. Va. Code* § 6D-1-2)

Contracting Business Entity: Network Innovation Solutions **Address:** 821 4th Ave

Huntington, WV 25703

Authorized Agent: Robert Whitley **Address:** _____

Contract Number: ISC1800000013 **Contract Description:** EVMS

Governmental agency awarding contract: WV Office of Technology

☐ **Check here if this is a Supplemental Disclosure**

List the Names of Interested Parties to the contract which are known or reasonably anticipated by the contracting business entity for each category below *(attach additional pages if necessary)*:

1. **Subcontractors or other entities performing work or service under the Contract**
   ☐ Check here if none, otherwise list entity/individual names below.
   Rapid 7

2. **Any person or entity who owns 25% or more of contracting entity (not applicable to publicly traded entities)**
   ☐ Check here if none, otherwise list entity/individual names below.
   Robert Whitly, Bryan Johnson, James Thomas

3. **Any person or entity that facilitated, or negotiated the terms of, the applicable contract (excluding legal services related to the negotiation or drafting of the applicable contract)**
   ☒ Check here if none, otherwise list entity/individual names below.

Signature: _____ Date Signed: 5-8-18

Notary Verification

State of WV, County of Cabell:

I, Robert Whitley, the authorized agent of the contracting business entity listed above, being duly sworn, acknowledge that the Disclosure herein is being made under oath and under the penalty of perjury.

Taken, sworn to and subscribed before me this 8 day of May, 18.

Regina Reed
Notary Public's Signature

To be completed by State Agency:

Date Received by State Agency: _____

Date submitted to Ethics Commission: _____

Governmental agency submitting Disclosure: _____

REGINA REED
Notary Public Official Seal
State of West Virginia
My Comm. Expires May 21, 2022
Metro Community FCU
PO Box 5438 - 215 18th St, Huntington, WV 25703