



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

State of West Virginia
 Request for Quotation
 21 - Info Technology

Proc Folder: 401652

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

Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2018-01-22	2018-01-25 13:30:00	CRFQ 0210-ISC1800000007	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:

BB&T 304-348-7078
 300 Summers St.
 Charleston, WV 25301

FOR INFORMATION CONTACT THE BUYER

Stephanie L Gale
 (304) 558-8601
 stephanie.l.gale@wv.gov

Signature X *Michael H. Helms, SUP*

FEIN # 56-1074313

DATE 1/24/2018

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

ADDITIONAL INFORMATION

Addendum #1 issued to:

1. Provide responses to vendor questions

End of Addendum #1

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US	IS&C - CHIEF FINANCIAL OFFICER DEPARTMENT OF ADMINISTRATION BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Enterprise Vulnerability Management System (EVMS), License	1.00000	EA		

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

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US	IS&C - CHIEF FINANCIAL OFFICER DEPARTMENT OF ADMINISTRATION BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Central Management Appliance	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43210000			

Extended Description :

3.1.5-3.1.5.1.4 Central Management Appliance per specifications

INVOICE TO

DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US	IS&C - CHIEF FINANCIAL OFFICER DEPARTMENT OF ADMINISTRATION BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US
--	--

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	System Deployment	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81111500			

Extended Description :
3.1.6-3.1.6.3.1 System Deployment

INVOICE TO

DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US	IS&C - CHIEF FINANCIAL OFFICER DEPARTMENT OF ADMINISTRATION BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US
--	--

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	License Optional Renewal Year 2	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81112200			

Extended Description :
3.1.8 Optional Renewal Year 2

INVOICE TO

DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US	IS&C - CHIEF FINANCIAL OFFICER DEPARTMENT OF ADMINISTRATION BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US
--	--

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
5	License Optional Renewal Year 3	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81112200			

Extended Description :
3.1.8 Optional Renewal Year 3

INVOICE TO	BILL TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US	IS&C - CHIEF FINANCIAL OFFICER DEPARTMENT OF ADMINISTRATION BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
6	License Optional Renewal Year 4	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81112200			

Extended Description :
3.1.8 Optional Renewal Year 4

SCHEDULE OF EVENTS		
Line	Event	Event Date
1	Technical Questions Due	2018-01-18

REQUEST FOR QUOTATION
Enterprise Vulnerability Management System OT18048



BB&T/Trustwave

Proposal for Enterprise Vulnerability Management System

**State of WV, Department of Administration,
Office of Technology**

January 25, 2018

Presented by:

BB&T

Michael Holtsclaw

Senior Vice President

Business Deposits Officer

300 Summers Street

Charleston, West Virginia 25301

(304) 348-7078

MHoltsclaw@BBandT.com

In partnership as a subcontractor by:

Trustwave

Vincent Perry

Government Team Lead

70 W Madison Street

Suite 600

Chicago, IL 60602

(312) 995-5661

vperry@trustwave.com

REQUEST FOR QUOTATION
Enterprise Vulnerability Management System OT18048

January 25, 2018

Bid Clerk
State of WV Department of Administration
Purchasing Division
2019 Washington St E
Charleston WV 25305

CRFQ 0210 ISC 18*7
2018-01-25018:30:00

Purchasing:

Thank you for the opportunity to provide the Office of Technology the ("OT") with a response that meets your objectives to provide an Enterprise Vulnerability Management System (EVMS), utilizing our subcontractor Trustwave to provide the detailed services as requested in CRFQ 18*7.

BB&T, utilizing our partner for EVMS testing is well positioned to meet the requirements set forth by this RFP and we are committed to continuing to develop a strong relationship with the State by providing high quality, efficient testing services at very competitive prices. BB&T and Trustwave, have partnered using a reseller agreement to deliver the services and specifications as detailed in the response. All services provided under this response will be provided as direct services from the subcontractor Trustwave. BB&T has communicated to Trustwave and they have agreed to the terms of the services and to meet the standards and expectations of the State purchasing rules. Trustwave, as a subcontractor will be the lead contact to support the direct services provided by Trustwave as have been detailed in the attached response under the terms disclosed in the RFP and that of the reseller agreement with BB&T.

Trusted Advisor

For more than 145 years, BB&T has been a stable, safe and growing financial institution and is currently one of the largest financial holding companies in the United States. As a Fortune 500 company, we are consistently recognized for outstanding client satisfaction by the U.S. Small Business Administration, Greenwich Associates and others. We have also

BB&T was named by
Global Finance one of
**the World's Best
Treasury & Cash
Management
Providers** in 2016 for
the U.S. Regional
Middle Market
Providers – Southeast
region.



REQUEST FOR QUOTATION

Enterprise Vulnerability Management System OT18048

been named one of the World's Strongest Banks by Bloomberg Markets Magazine; one of the top three in the U.S. and in the top 15 globally. We currently have over \$13 billion in Public Fund deposits, with a long history of serving our clients and the communities we are in. We would be honored to have the City trust us with an important segment of your banking relationship.

Best in Class

BB&T strives to maintain its client-driven focus. We focus on our client relationships because our clients are our partners. Our clients are long-term partners and are treated accordingly. We are excellent at creating win/win relationships by delivering quality service and continuous improvement. BB&T trains its employees to deliver the perfect client experience every day.

Platform for Growth

In addition to execution and high quality service, BB&T also knows how important it is to make it easy for clients to do business with us. We put a lot of thought into how we can improve and design our organization and our products so that it is very easy for the City to execute payments, ask questions and find solutions to issues.

At BB&T, we take pride in managing and hosting the primary payment processing systems for our clients. We use technology partners where it makes sense, but our core processing of ACH, check processing, and return items is all managed and controlled in BB&T Operations with BB&T employees.

In summary, BB&T and Trustwave would be honored and privileged to provide the Office of Technology the services requested. Our pledge, along with our subcontractor, is to provide an unsurpassed level of expertise, service excellence, delivered by a highly personalized team of seasoned professionals, who will ensure a strong and successful relationship. We understand the importance of these processes to you and commit to working diligently and professionally to assist you wherever possible.

With kindest regards,



Michael Holtsclaw
Senior Vice President
Business Deposits Officer

REQUEST FOR QUOTATION
Enterprise Vulnerability Management System OT18048

Executive Summary: Why Choose BB&T?

BB&T wants to thank the City for giving us the opportunity to present our banking and treasury management solutions to you. BB&T is well positioned to continue to provide the City with financial services that meet your objectives while minimizing operating costs, safeguarding assets, and utilizing technology to help you effectively manage your business. We are committed to continuing to build a strong relationship with you and providing high quality, efficient collection and disbursement solution services at very competitive prices.

Treasury Management

BB&T offers a full portfolio of world-class, domestic Treasury Management solutions and can create customized solutions for the City. Through a collaborative, consultative approach to understanding your business strategies, BB&T delivers comprehensive solutions supported by a heritage of exceptional client service. As technology investment continues to be imperative for treasury management solution providers, BB&T has introduced new products and services that provide customers with faster, easier, and more efficient ways of doing business. Since 2004, BB&T has invested more than \$36 million in product development across its receipts, disbursements, information and electronic commerce solutions.

BB&T consistently receives Greenwich Excellence Awards in Treasury Management for Overall Treasury Management Satisfaction, Accuracy of Operations, Product Capabilities, Knowledge of Treasury Management, and Ease of Implementation. In The World's Best Treasury and Cash Management Providers from Global Finance (2016), BB&T was named best for US Regional Middle Market Providers - Southeast Region.

Client Service & Relationship Model

BB&T's size as a major U.S. financial institution, along with our unique service delivery model, provides clients with the most sophisticated products and services with locally-based primary points of contact who are best equipped to understand our clients' unique financial needs. BB&T provides the best of both worlds in banking. We have the size and scale to offer competitive, technologically-advanced services coupled with the community structure to address your banking needs and deliver on commitments in a local setting while steadfastly adhering to our core values and mission.

BB&T has financial experts available in many disciplines. We believe it is our job to understand the financial needs of our clients and bring the appropriate resources and financial solutions to the table. Our Integrated

REQUEST FOR QUOTATION

Enterprise Vulnerability Management System OT18048

Relationship Management approach ensures a relationship manager engages the appropriate BB&T resources on the client's behalf. This team approach ensures our clients benefit from the best solution possible among the wide array of financial services we offer.

BB&T has historically and consistently provided a high level of customer service which has contributed to the multiple Greenwich Associates awards we have won over the last 7 years. We are excited to share that BB&T won top national honors for overall customer satisfaction in serving businesses from Greenwich Associates. BB&T won more excellence citations than any other financial institution. BB&T was a National Award Winner in six categories, to include the following: Overall Customer Satisfaction, Cash Management Services Satisfaction, Business Bankers Satisfaction, Branch Services Satisfaction, Personal Banking Services for Business Owners Satisfaction and Call Center Satisfaction.

In addition to your Trustwave support, the local WV Support team will be available to assist in receiving the need answers to your questions. Trustwave has guaranteed technical phone support from 8 a.m. to 5 p.m. Monday-Friday.

Experience

BB&T has served the public sector for most of its 145-year history. We have a unique depth of experience in supporting organizations such as yours. BB&T has a wide array of resources dedicated to the public sector and prides itself on delivering quality customer service.

Our innovative partnerships provide solutions help improve visibility, optimize working capital and manage risk. BB&T also knows how important it is to make it easy for clients to do business with us. We put a lot of thought into how we can improve and design our organization and our products so that it is very easy for our clients needs to be met, we work hard to provide direct services, partners and subcontractors that find solutions to your issues.

Implementation

Trustwave will direct and lead all facets of the services provided. A representative will be assigned to support all aspects of implementation. BB&T will work closely with the OT and Trustwave each step of the way and ensure any new implementation will be seamless.

Pricing

BB&T understands the importance of market pricing and we believe you will find BB&T to be very competitive within the market. A copy of our pricing proformas outline the cost of services requested and the recommended account structure is attached for your review in the pricing section of this proposal.

REQUEST FOR QUOTATION

Enterprise Vulnerability Management System OT18048

Company Information

BB&T Corporation, headquartered in Winston-Salem, N.C., is considered *Well Capitalized* and is among the nation's top financial holding companies with \$221.2 billion in assets and market capitalization of \$36.7 billion as of June 30, 2017. We are rated as one of the country's safest and soundest financial institutions and have a reputation for integrity and service excellence.



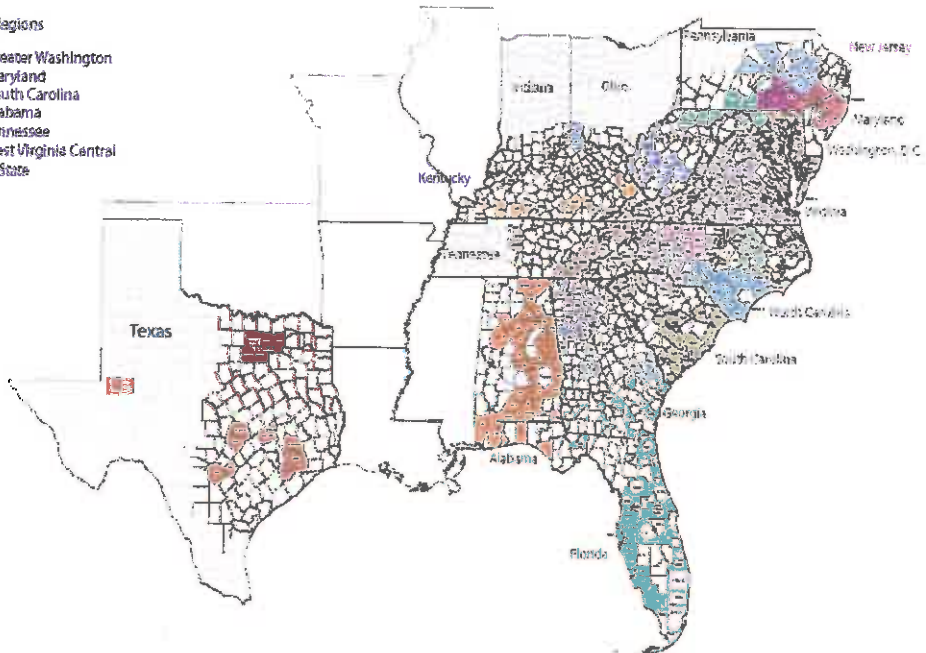
BB&T
named in the top 15
of the **World's
Strongest Banks** by
Bloomberg Markets
magazine.

A Fortune 500 company, BB&T is consistently recognized for outstanding client satisfaction by the U.S. Small Business Administration, Greenwich Associates and others. BB&T also has been named one of the World's Strongest Banks by Bloomberg Markets Magazine, one of the top three in the U.S. and in the top 15 globally. More information about BB&T and its full line of products and services is available at BBT.com.

Founded in 1872, its bank subsidiaries operate approximately 2,220 financial centers in 15 states and the District of Columbia. BB&T Corporation is one of the largest American banks, offering full-service commercial and retail banking services along with other financial services like insurance, investments, retail brokerage, mortgage, corporate finance, consumer finance, payment services, international banking, leasing and institutional trust services. BB&T has a strong presence nationally with branches and offices in the locations you need us most.

- Multi-Region States
- North Carolina
 - Metrolina
 - Triad
 - Triangle
 - Northeastern NC
 - Southeastern NC
- Virginia
 - Valley
 - James River
- Georgia
 - Northern GA
 - Southern GA
- Florida
 - North & Central Florida
 - West Florida
 - South Florida
- Texas
 - North Texas
 - Houston - Central
- Pennsylvania
 - Central PA
 - Northern PA
 - Greater Delaware Valley
- Kentucky
 - N Kentucky / Gr Cincinnati
 - Kentucky

- State Regions
- Greater Washington
- Maryland
- South Carolina
- Alabama
- Tennessee
- West Virginia Central
- TriState



REQUEST FOR QUOTATION

Enterprise Vulnerability Management System OT18048

BB&T's reputation has been built upon loyal, responsive customer service with a desire to exceed client expectations. At BB&T, we know the content of our business will, and should, experience constant change. Change is necessary for progress. However, the context, our vision, mission and values, are unchanging because these principles are based on basic truths. We provide full service capabilities with the products, services, resources and infrastructure to support relationships such as one with the City, and do so while steadfastly adhering to our following core values and mission.

Our goal is to make the world a better place to live by:

- Helping our CLIENTS achieve economic success and financial security;
- Creating a place where our EMPLOYEES can learn, grow and be fulfilled in their work;
- Making the COMMUNITIES in which we work better places to be; and thereby:
- Optimizing the long-term return to our SHAREHOLDERS, while providing a safe and sound investment

Dedicated to our Clients and the Local Community



We began the **BB&T Lighthouse Project** in 2009 and since then have completed 9,000 community service projects, provided more than 475,000 volunteer hours, and helped change the lives of more than 13 million people. During 2016, we completed more than 1,200 community service projects, provided more than 88,500 volunteer hours, and helped change the lives of more than 2.3 million people. At BB&T we are committed to our local community. We are committed to building more financially strong communities. At BB&T, we focus on financial education and literacy, including the **BB&T Financial Foundations** program that reaches high school students throughout our footprint. Since we began the program in 2011, we've reached over 78,000 students and provided them with basic concepts about banking, insurance, investments, budgeting, higher education, and more. BB&T is proud to be sharing knowledge for a brighter direction. In addition, we are committed to improving the financial confidence of those who bank with us. Through our **BB&T@Work program**, we offer financial education seminars to assist our customers in achieving economic success and financial security.

We differentiate ourselves with a highly consultative approach to client service. With multiple awards for client excellence in customer service from Greenwich Associates, we strive to be a trusted adviser for our clients; bringing them real solutions to problems as well as keeping them abreast of innovations coming into the marketplace that will help safeguard assets and streamline processes, saving both time and money. We will get to know your business through regular face-to-face account reviews and provide solutions that cater to your very specific needs. This proposal is simply a starting point. If you choose BB&T as your financial partner, we will continue to refine your processing structure and services to create the optimal scenario for the City.



REQUEST FOR QUOTATION
Enterprise Vulnerability Management System OT18048

We pride ourselves on tenured management, low associate turnover, and qualitative performance measures that consistently exceed Bank Administration Institute competitive benchmarks. Our treasury services are designed to meet client specifications and we provide fast, accurate and flexible solutions to enhance your payables and receivables process and improve productivity. Developing services that help assure you achieve economic success and financial security is the driving force behind our treasury services.

Headquarters

BB&T's Corporate Headquarters is located at 200 West Second St. in Winston-Salem, NC.

History

Providing banking services since 1872, BB&T has a long history of catering to the needs of our clients and the communities in which we work and live. Our bank and subsidiaries operate approximately 2,220 financial centers in 15 states and the District of Columbia. BB&T Corporation is one of the largest American banks, offering full-service commercial and retail banking services along with other financial services like insurance, investments, retail brokerage, mortgage, corporate finance, consumer finance, payment services, international banking, leasing and institutional trust services. In 2016, we were named by Global Finance as one of the World's Best Treasury & Cash Management Providers for the U.S. Regional Middle Market Providers – Southeast region.



Experience

We have a unique depth of experience in supporting organizations such as yours. Our innovative treasury banking solutions help improve visibility, optimize working capital and manage risk. In addition, B&T is organized as a group of community banks, each headed by a community bank president. Each of our presidents is responsible for ensuring that we are as responsive as possible to each client's needs.

Client-focused

With our focus on community, BB&T offers a unique blend: A Relationship Team who knows your business and has product expertise, stringent quality control, superior customer service, and on-call consultative specialists. These factors combine to provide added value for your banking dollar. This added value, coupled with our financial strength and stability, makes BB&T a solid solution to all your banking needs.

REQUEST FOR QUOTATION
Enterprise Vulnerability Management System OT18048

Commitment to Financial Stability

BB&T is rated one of the country's safest and most sound financial institutions. It has been named one of the World's Strongest Banks by Bloomberg Markets Magazine, one of the top three in the U.S. and in the top 15 globally. BB&T Corporation is considered Well Capitalized according to Federal Reserve Board, FDIC, and OCC guidelines, rules and regulations concerning capital requirement and financial stress testing under the Dodd-Frank Act.

As of June 30, 2017, BB&T is one of the largest financial services holding companies in the U.S. with \$221.2 billion in assets and market capitalization of \$36.7 billion. Based in Winston-Salem, N.C., the company operates 2,220 financial centers in 15 states and Washington, D.C., and offers a full range of consumer and commercial banking, securities brokerage, asset management, mortgage and insurance products and services. A Fortune 500 company, BB&T is consistently recognized for outstanding client satisfaction by the U.S. Small Business Administration, Greenwich Associates and others.

Direct links for our financial statements, including our annual reports, are available on our website:
<http://bbt.investorroom.com/overview>

Bank Comparison Credit Ratings as of July 11, 2017 are listed below.

	Company	S&P	Moody's	Outlook	Fitch
1	Bank of NY Mellon	AA-	Aa2	Stable	AA
2	Wells Fargo Bank	AA-	Aa2	Stable	AA
3	State Street Bank & Trust Co.	AA-	Aa3	Stable	AA
4	JPMorgan Chase	A+	Aa3	Stable	AA-
5	Bank of America	A+	A1	Positive	A+
6	Branch Banking & Trust Co.	A	A1	Stable	A+
7	U.S. Bank N.A.	AA-	A1	Stable	AA
8	Citibank	A+	A1	Stable	A+
9	Northern Trust Corporation	AA-	A2	Stable	AA-
10	PNC Bank	A	A2	Stable	A+
11	American Express Credit Co.	A-	A2	Stable	A
12	M&T Manuf & Trdrs Trust Co.	A	A3	Stable	A
13	Cullen Frost	A	A3	Stable	WD
14	Comerica Bank	A-	A3	Stable	A
15	Fifth Third Bank	A-	A3	Stable	A

REQUEST FOR QUOTATION
Enterprise Vulnerability Management System OT18048

About Trustwave

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit <https://www.trustwave.com>.

Founded **1995**

Employees **1,500+**

Headquarters **Chicago**

Smart Security on Demand

We deliver automated, sustainable and cost-effective data protection, risk management and threat intelligence to our customers—what we call SMART SECURITY ON DEMAND.

With more than three million enrollees, our TrustKeeper® platform is available in the cloud. We also offer industry-leading managed security services, award-winning technology products, as well as consulting, systems integration and other professional services. Many of our solutions are available across multiple delivery mechanisms, giving our customers flexibility as they design and implement their security infrastructure.

Must Have Data Protection

Financially-motivated hackers, corporate data breaches, compliance requirements, and the need for businesses to secure what many consider the lifeblood of their business—their confidential data—have put businesses on notice that security is a "must have." Our comprehensive suite of technologies and services help businesses secure critical information throughout its lifecycle and comply with sometimes daunting regulatory requirements.

Trusted Advisors

With automation, tools and intelligence, we find better ways for businesses to overcome their security challenges. Our qualified security assessors, ethical hackers and other experts are some of the industry's most trusted sources for risk assessments, threat research, forensic investigations, and security training. We performed hundreds of security breach investigations and thousands of ethical hacking projects last year. We're also selected by more enterprises for compliance than the next ten service providers

REQUEST FOR QUOTATION

Enterprise Vulnerability Management System OT18048

combined, and some of the world's largest financial institutions rely on our knowledge and technology to help their customers validate, achieve and maintain compliance.

Threat Intelligence Built-In

Our large, global client footprint gives us visibility into security threats—visibility enhanced by our SpiderLabs® teams' applied research and field testing.

Last year, we researched more than 9 million Web application attacks, more than 2 million network and vulnerability scans, more than 5 million malicious websites, more than 20 billion emails as well as zero-day threats, which—combined—fuels the threat intelligence we bake into our services and technologies to help customers prepare proactively for threats and reduce overall risk exposure.

Threat Intelligence Built-In

For years we've pioneered and led the PCI compliance space—helping enterprises, banks and their customers address risks and challenges of payment card fraud and compromise. But we excel at more than PCI. Our multi-compliance framework applies to other business-impacting regulations and standards including HIPAA, FISMA, GLBA, ISO, and SOX. We also offer enterprise risk assessment services related to big data, the cloud, and mobility.

Credentials

QSA - Qualified Security Assessor

ASV - Approved Scanning Vendor

PFI - PCI SSC Forensic Investigator

QPASC - Qualified Payment Application Security Company

REQUEST FOR QUOTATION

Enterprise Vulnerability Management System OT18048

Relationship Team



BB&T offers a unique blend: We provide you with a local market-based Relationship Team who understands your business and has product expertise, stringent quality control, and superior customer service and on-call consultative specialists. These factors combine to provide added value for your banking dollar. Our aim is to provide you the perfect client experience. This added value, coupled with our financial strength and stability, makes BB&T a solid solution to all your banking needs.

Your Relationship Team will arrange regular calls and meetings with key personnel to optimize efficiency, reduce unnecessary costs, mitigate fraud risk, and add overall value to the relationship. They will tackle each of these areas through a thorough review and discussion of the City's payment cycle. BB&T uses a consultative approach to all of our treasury and payments solutions and our goal is to be a trusted advisor.

There will be several individuals available to handle any issues with at any given time. Your Trustwave Relationship Manager, will work to ensure resolution to any issues, proactively service your account, and respond promptly to your needs.

Trustwave's support organization is a global "follow the sun" set up. Call center team leaders and directors are active participants in ongoing partner calls and engaged to ensure all user's needs are met and issues are solved quickly. Support includes 24X7X365 in English.

Trustwave's Vulnerability Management has an easy-to-use wizard that facilitates scan set up and management, and scan reports are easy to digest and address.

In addition, Trustwave support includes Vincent Perry, Government Team Lead and Derek Clark, Government Manager. Trustwave provides

Additional local support includes Mike Holtsclaw, Business Deposits Officer, will be available should you need support related to access or issues related to Trustwave's delivery of the services.

BECAUSE I CARE ABOUT MY CLIENTS:

- RELIABLE:** I am dependable and you can count on me.
- RESPONSIVE:** I act quickly to help you with your needs.
- EMPATHETIC:** I listen to you and am sensitive to your feelings.
- COMPETENT:** I am equipped with the skills and knowledge to help you.

REQUEST FOR QUOTATION
Enterprise Vulnerability Management System OT18048

Trustwave Service Description

Non Managed External Vulnerability Scanning

Service Description Overview

External Vulnerability Scanning (EVS) is a cloud based self-service vulnerability scanning service. The EVS service helps identify network vulnerabilities on the Client's external network segments. The EVS service consists of:

- Discovery, which is the information gathering and discovery process to understand the Client's System Target(s) and the scope of the required scanning of those targets.
- Scanning, helps to identify potential vulnerabilities or weak configurations of the Clients System Target(s).
- Reporting is the provision of results of the Client Target System(s) scans, as a completed report available through the TrustKeeper Client Portal.

Base Features

- Basic service features overview

The EVS service includes the following basic service features with TrustKeeper Client Portal access providing:

- Tracking of provisioning progress
- EVS portal account subscription
- Client Target System entry
- Change management and support requests creation and response
- Discovery-During this phase the Client information is collected and a port scan of the Client's network is completed.
- Scanning-Unlimited self-service scans during the EVS Scan Period, based on the predefined Scan Profile selected by the Client is performed on the Client's Target System(s).
- Reporting-Predefined reports are available through the TrustKeeper Client Portal, including PCI DSS reports for compliance.

Provisioning

- Provisioning and implementation
- The provisioning team is the Client's first point of interaction with Trustwave after the contract is executed. This team is responsible for working with Client to
- review and analyse the Client user information.
- provision and implement the Client in the TrustKeeper Client Portal.
- The EVS Service is deemed to be delivered and operational when Client has access to the TrustKeeper Client Portal.
- Service introductions and information gathering
- Trustwave provisioning, assurance and delivery teams are assigned to implement and facilitate the successful configuration of the Client's EVS Service, which includes the following actions:

REQUEST FOR QUOTATION

Enterprise Vulnerability Management System OT18048

- Send an introduction email to the Client providing guidance on how to provide the necessary Client information prior to a remote kick-off meeting.
- Notify the Client that they have access to the EVS service and the TrustKeeper Client Portal.
- Remotely create an account for, and establish the Client within, the TrustKeeper Client Portal.
- Client environment assessment
- Trustwave provisioning will work with the Client to verify that Client's environment can communicate with Trustwave Platform; and
- There is an active secure connection between the Trustwave Platform and the Client's environment.
- EVS portal account
- The Client accesses the TrustKeeper Client Portal to enable the service and Subscribe for the relevant EVS Package(s) through the TrustKeeper Client Portal.
- View the initial count of IP addresses available for scanning based on the number of EVS Packages purchased by the Client.
- The Client's IVS portal account will be updated each time the Client sets up a Client Target System IP address.

Trustwave Responsibilities

- Create a Client account in the TrustKeeper Client Portal.
- Provide applicable user guides, introduce and review the Client's usage and understanding of the TrustKeeper Client Portal and implement the applicable support process and procedures.
- Verify that the Client has access to the TrustKeeper Client Portal.

Client Responsibilities

- Respond to requests from the provisioning team when establishing contact and collecting the Client user information.
- Read and confirm the Client's understanding of all provided user guides and documentation.

Vulnerability assessment

- Client Target System setup
- The SOC works with the Client to help:
- Ensure completeness of the Client Setup Information for each scheduled scan.
- The Client's enter the Client's Target System(s).
- The selection of an appropriate EVS Scan Profile.
- The Client complete the scheduling of the EVS scans.

Trustwave Responsibilities

- Establish and maintain contact with the Client and navigate the Client through the setup process.
- Request and collect Client Setup Information.
- Provide and maintain a secure connection between the Client's Target System(s) and the Trustwave Platform.
- Provide and maintain the Trustwave vulnerability database and relevant software version upgrades and security policy updates, inclusive of changes to existing vulnerability and threat signatures and new vulnerability and threat signatures, to the Trustwave Platform.
- Maintain the accreditation of the Trustwave Platform, Trustwave engineers and the EVS service to ensure that the EVS scanning process remains validated and adheres to the PCI DSS requirements for performing vulnerability scans of Internet facing environments of merchants and service providers.
- Ensure that the EVS service and related reports are aligned to the PCI DSS ASV requirements.

REQUEST FOR QUOTATION

Enterprise Vulnerability Management System OT18048

- Provide remote support in response to any issues arising during scanning of the Client Target System(s).

Verify that Client's Target System(s) are visible to the Trustwave Platform; and

Client's Subscription is correctly updated based on the number of IP addresses scanned.

Client Responsibilities

- Enter the Client's Target System(s) and select the relevant EVS Scan Profile.
- Select the appropriate EVS Scan Profile.
- Schedule the purchased scans during the EVS Scan Period, through the TrustKeeper Client Portal.
- Make available an onsite resource during the time(s) scheduled for scanning of the Client's Target System(s).
- Provide appropriate credentialed access to Trustwave, to the Client's Target System(s).
- The Client acknowledges that the relevant IP address ranges relate directly to the EVS Package IP address block and identify the Client's Target System(s) on which an EVS scan is to be completed;
- the Client is responsible for Scheduling, configuring and conducting the scanning on the Client's Target System(s), through the TrustKeeper Client Portal; and
- Generating, reviewing, analyzing and interpreting the results of the relevant scans.
- Additional terms
- The Client represents and warrants that the Client has full right, power, and authority to consent to use the EVS service to perform scans against the IP address and/or URL and/or domain names provided to Trustwave by the Client, whether electronically or by any other means, whether during initial target entry or thereafter.
- Without limiting any other remedy that Trustwave may have, the Client agrees to indemnify and hold Trustwave and its affiliates harmless from and against all liabilities, losses, damages, costs and expenses, including without limitation reasonable attorney's fees and costs incurred by Trustwave resulting from the Client's breach of clause.
- If applicable, the Client shall obtain all consents and authorizations from any third parties necessary for Trustwave to perform the EVS services, including without limitation, third party datacenters, co-locations and hosts. Trustwave will not be required to execute agreements with any such third parties.
- The Client acknowledges and understands
- The Client may only use EVS scanning solution, reports and the TrusKeeper Client Portal:
- to scan IP addresses, URLs and domain names owned by and registered to Client;
- for Client's internal business purposes only, in accordance with all applicable laws (including any export control laws); and for the purposes stated in the Third Party Usage Terms.
- The Client shall limit access to TrustKeeper Client Portal to only those Client personnel or contractors who:
 1. have an obligation of confidentiality with Client; and
 2. have a requirement for such access on a "need to know" basis
- The Client is responsible for disabling TrustKeeper Client Portal credentials of those Client personnel and/or contractors who no longer require access
- agrees that the TrustKeeper Client Portal, including without limitation its functionality and contents, is confidential information, and the Client's use and/or access to the portal is subject to the terms of the mutual non-disclosure agreement executed by the parties.
- The Client acknowledges and understands that accessing and scanning IP addresses involves inherent risks, including, without limitation, risks related to system or network performance and availability, and data corruption or loss.

Reporting

REQUEST FOR QUOTATION

Enterprise Vulnerability Management System OT18048

- Report functions
- The EVS service includes the following available reporting features through the TrustKeeper Client Portal:
 - Online reporting and metrics: access to vulnerability assessment data (including risk, remediation status, and data compromised) and access to historical test results for trend analysis.
 - Pre-defined fields: generation of executive summary, summary recommendations, test methodology and findings.
 - Custom Reporting: Users selected fields, sorted by risk, finding status, project(s), selected fields or individual tests.
 - Common Vulnerability Scoring System (CVSSv2) Values: CVSS is a standard method for risk ranking and prioritizing security vulnerabilities.
 - Multi-format Reports: Export report data in PDF, Excel, XML, CSV and HTML
 - Report timelines targets
- Trustwave will use best efforts, but does not warrant availability of the relevant reports, within the following timelines from completion of the relevant scan:

Scanning—within 1 Business Day

- The timelines are dependent on and subject to the Client accurately completing the Client's Enrolment Information.

EVS Scan Profile

- The Client may select any of the following EVS Scan Profiles when setting up the Client System Target(s):
 - Vulnerability Scan;
 - PCI Scan;
 - HIPAA Scan
 - Live Host Discovery;
 - Port Service Fingerprint with additional advanced configurations.

Trustwave Internal Vulnerability Scanning Service

Service Description Overview

Internal Vulnerability Scanning (IVS) is a cloud based self-service vulnerability scanning services. The IVS service helps identify network vulnerabilities on the Client's internal network segments. The IVS service consists of:

- Discovery, which is the information gathering and discovery process to understand the Client's System Target(s) and the scope of the required scanning of those targets.
- Scanning, helps identify potential vulnerabilities or weak configurations of the Clients System Target(s).
- Reporting, is the provision of results of the Client Target System(s) scans, as a completed report available through the TrustKeeper Client Portal.

Base Features

- Basic Service Features Overview

REQUEST FOR QUOTATION

Enterprise Vulnerability Management System OT18048

The IVS service includes the following basic service features including TrustKeeper Client Portal access providing:

- Tracking of provisioning progress
- IVS portal account subscription
- Client Target System entry
- Change management and support requests creation and response
- Reporting
- Trustwave IVS Appliance
- Supply of a Trustwave IVS Appliance for use in the Client's Target System(s).
- Discovery-During this phase the Client information is collected and a port scan of the Client's network is completed.
- Scanning- Unlimited self-service scans during the IVS Scan Period, based on the predefined Scan Profile selected by the Client is performed on the Client's Target System(s).
- Reporting-Predefined reports are available through the TrustKeeper Client Portal.

Provisioning

Provisioning and implementation

The provisioning team is the Client's first point of interaction with Trustwave after the contract is executed. This team is responsible for working with Client to review and analyse the Client user information; and provision and implement the Client in the TrustKeeper Client Portal.

The IVS service is deemed to be delivered and operational when the Client has access to the TrustKeeper Client Portal to subscribe for the service, schedule scans and view reports.

- Service introductions and information gathering

Trustwave provisioning, assurance and delivery teams are assigned to implement and facilitate the successful configuration of the Client's IVS Service, which includes the following actions:

- Send an introduction email to the Client providing guidance on how to provide the necessary Client information prior to a remote kick-off meeting.
- Notify the Client that they have access to the IVS service and the TrustKeeper Client Portal.
- remotely create an account for, and establish the Client within, the TrustKeeper Client Portal.
- Client environment assessment

Trustwave provisioning will work with the Client to verify that:

- Client's environment can communicate with Trustwave Platform.
- there is an active secure connection between the Trustwave Platform and the Client's environment.
- IVS portal account

The Client accesses the the TrustKeeper Portal to enable the service and:

- Subscribe for the relevant IVS Package(s) through the TrustKeeper Client Portal.
- View the initial count of IP addresses available for scanning based on the number of IVS Packages purchased by the Client.
- The Client's IVS portal account will be updated each time the Client sets up a Client Target System IP address.

REQUEST FOR QUOTATION
Enterprise Vulnerability Management System OT18048

Trustwave Responsibilities

- Create a Client account in the TrustKeeper Client Portal.
- Provide applicable user guides, introduce and review the Client's usage and understanding of the TrustKeeper Client Portal and implement the applicable support process and procedures.
- Verify that the Client has access to the TrustKeeper Client Portal.

Client Responsibilities

- Respond to requests from the provisioning team when establishing contact and collecting the Client user information.
- Read and confirm the Client's understanding of all provided user guides and documentation.

Vulnerability assessment

- Client Target System setup

The SOC works with the Client to help:

- Ensure completeness of the Client Setup Information for each scheduled scan.
- With the correct installation and configuration of the Trustwave IVS Appliance in the Clients Target System(s) environment.
- The Client enter the Client's Target System(s).
- The selection of an appropriate IVS Scan Profile.
- The Client complete the scheduling of the IVS scans.
- SOC Welcome call

The Trustwave provisioning team will implement the SOC Welcome Call and complete the following actions:

- Schedule a welcome call with the Client.
- During that call introduce the Client to the TrustKeeper Client Portal ensuring that the Client understands how to access and use the services purchased.
- Review the Client's TrustKeeper Client Portal usage understanding including the following actions:
 - setup the Client's Target System(s)
 - configure the Client's Target System(s)
 - select an appropriate IVS Scan Profile
 - accessing and modifying support tickets
 - customizing and reviewing available reports
 - modifying permissions for other TrustKeeper Client Portal users as appropriate or available to the Client

Trustwave Responsibilities

Establish and maintain contact with the Client, implement the SOC welcome call and navigate the Client through the setup process.

- Request and collect Client Setup Information.
- Supply the Trustwave IVS Appliance for use in the Client's Target System(s).
- Establish and monitor a secure connection between the Client's Target System(s) and the Trustwave Platform.
- Provide and maintain a vulnerability signature database used by the Trustwave Platform.

REQUEST FOR QUOTATION

Enterprise Vulnerability Management System OT18048

- Provide Product Updates and Security Updates, to the Trustwave IVS Appliance and Trustwave Platform.
- Provide remote support to the Client to ensure the correct installation and configuration of the Trustwave IVS Appliance.

Provide remote support in response to any issues arising during scanning of the Client Target System(s).

Verify that:

- Client's Target System(s) are visible to the Trustwave Platform.
- Client's Subscription is correctly updated based on the number of IP addresses scanned.

Client Responsibilities

- Participate in the SOC welcome call.
- Enter the Client's Target System(s) and select the relevant IVS Scan Profile.
- Install the Trustwave IVS Appliance.
- Select the appropriate IVS Scan Profile.
- Schedule the purchased scans during the IVS Scan Period, through the TrustKeeper Client Portal.
- Make available an onsite resource during the time(s) scheduled for scanning of the Client's Target System(s).
- Provide appropriate credentialed access to Trustwave, to the Client's Target System(s).

The Client acknowledges that the relevant IP address ranges relate directly to the IVS Package IP address block and identify the Client's Target System(s) on which an IVS scan is to be completed.

The Client is responsible for scheduling, configuring and conducting the scanning on the Client's Target System(s), through the TrustKeeper Client Portal and generating, reviewing, analyzing and interpreting the results of the relevant scans.

Additional terms

The Client represents and warrants that the Client has full right, power, and authority to consent to use the IVS service to perform scans against the IP address and/or URL and/or domain names provided to Trustwave by the Client, whether electronically or by any other means, whether during initial target entry or thereafter.

If applicable, the Client shall obtain all consents and authorizations from any third parties necessary for Trustwave to perform the IVS services, including without limitation, third party datacenters, co-locations and hosts. Trustwave will not be required to execute agreements with any such third parties.

The Client agrees that the Trustwave Client Portal, including without limitation its functionality and contents, is confidential information, and the Client's use and/or access to the portal is subject to the terms of the mutual non-disclosure agreement executed by the parties.

The Client acknowledges and understands that accessing and scanning IP addresses involves inherent risks, including, without limitation, risks related to system or network performance and availability, and data corruption or loss.

REQUEST FOR QUOTATION
Enterprise Vulnerability Management System OT18048

Reporting

- Report functions

The IVS service includes the following available reporting features through the TrustKeeper Client Portal:

- Online reporting and metrics: access to vulnerability assessment data (including risk, remediation status, and data compromised) and access to historical test results for trend analysis.
- Pre-defined fields: generation of executive summary, summary recommendations, test methodology and findings.
- Custom Reporting: Users selected fields, sorted by risk, finding status, project(s), selected fields or individual tests.
- Common Vulnerability Scoring System (CVSSv2) Values: CVSS is a standard method for risk ranking and prioritizing security vulnerabilities.
- Multi-format Reports: Export report data in PDF, Excel, XML, CSV and HTML.
- Report timeline targets

Trustwave will use best efforts, but does not warrant availability of the relevant reports, within the following timelines from completion of the relevant scan:

- Scanning - within 1 Business Day

The timelines are dependent on and subject to the Client's the following:

- Accurately completing the Client's Enrolment Information; and
- Correct installation and configuration of the Trustwave IVS Appliance.

IVS Scan Profiles

The Client may select any of the following IVS Scan Profiles when setting up the Client System Target(s):

- Vulnerability Scan
- PCI Scan
- HIPAA Scan
- Live Host Discovery
- Port Service Fingerprint with additional advanced configurations

REQUEST FOR QUOTATION
Enterprise Vulnerability Management System OT18048

RFP Response

3 GENERAL REQUIREMENTS:

3.1 **Mandatory Contract Item Requirements:** Contract Item must meet or exceed the mandatory requirements listed below.

3.1.1 **Specification Validation:** Vendor must provide service/application capabilities and features documentation with the bid (operations manuals are preferred) for RFQ specification validation.

3.1.2 The Enterprise Vulnerability Management System (EVMS) must provide full-feature vulnerability management capabilities to include, but not limited to, the specifications outlined below.

3.1.3 The State will operationally utilize the EVMS application. The EVMS will not be provided as a managed service. The State will hold responsibility for leveraging the application to carry out vulnerability management activities. The back-end hosted by Trustwave. The client has full control over when and where the testing occurs. It is not managed.

3.1.4 **Enterprise Vulnerability Management System**

3.1.4.1 Enterprise Vulnerability Management System (EVMS) must adhere to the following architecture, performance, scalability and licensing functionality requirements:

3.1.4.1.1 The license must provide full functionality of the service for up to 25,000 individual hosts. The 25,000 does not apply to inactive IP addresses. Yes, the license will provide full functionality of the service up to 25,000 individual hosts. A discovery scan will be used to determine the number of internal IPs.

REQUEST FOR QUOTATION

Enterprise Vulnerability Management System OT18048

- 3.1.4.1.2 The license must provide capability to select which hosts are covered by the service, irrespective of network or subnet. All internal IPs are licensed for scans
- 3.1.4.1.3 The license must support discovery scanning (device enumeration) for an unlimited number of internal network IP addresses. The License will support a system discovery for an unlimited number of servers, appliances, and other devices on the network. The license will also provide a service discovery for open ports and services available on each discovered system, such as mail and web servers.
- 3.1.4.1.4 The license must include internal and external scanner device license(s)
The license is based on the number of IP addresses provided by the client. They are considered separate in testing, but capability is provided for both.
- 3.1.4.1.5 Minimum supported platforms for scanner hosts must include: Windows operating system, Linux operating system, virtual environments such as VMWare, Azure, Hyper-V, etc. Yes, all platforms are supported.
- 3.1.4.1.6 Must support internal network scanning in a distributed environment across multiple subnets.
- 3.1.4.1.7 Must support multiple deployment options to include: agent based, agentless, internal network scans and external network scan capabilities.
- 3.1.4.2 EVMS must adhere to the following risk and remediation management requirements:
 - 3.1.4.2.1 Must include an advanced risk scoring algorithm.
 - 3.1.4.2.2 Risk scoring must be based on CVSS scoring, asset exploitability and susceptibility to known malware kits.

Custom Reporting: Users selected fields, sorted by risk with CVSS scoring, finding status, project(s), selected fields or individual tests.
 - 3.1.4.2.3 Risk scoring must integrate organization determined variables, such as asset criticality (critical business assets).
We do not currently track "assets" beyond the IP.
 - 3.1.4.2.4 Capable of both quantitative and qualitative metrics.

Yes Trustkeeper is capable of both

REQUEST FOR QUOTATION

Enterprise Vulnerability Management System OT18048

3.1.4.2.5 Able to provide remediation information to include: engineer level instructions and cross linking to external database for patches, downloads, and references. Yes

3.1.4.2.6 Support identification and management of vulnerability exceptions, to include an approval workflow. Trustwave can support

3.1.4.3 EVMS must adhere to the following management requirements:

3.1.4.3.1 Include the following asset management functions: asset grouping, asset import, asset categorization, asset definition, and dynamic & static tagging.

3.1.4.3.2 Support data query based upon asset management functions.

3.1.4.3.3 Support role-based access control with both pre-defined and custom roles.

3.1.4.3.4 Support role-based access approval permissions to be assigned for vulnerability exclusions or exceptions.

3.1.4.3.5 Support credential management for authenticated scans.

3.1.4.3.6 Support automatic and manual update options for both the EVMS and for vulnerability and configuration updates.

3.1.4.3.7 Support workflow automation to include: scan scheduling, scan event and vulnerability alerts, and report generation and distribution.

3.1.4.4 EVMS must adhere to the following scanning requirements:

3.1.4.4.1 Capable of asset discovery/mapping scans, including operating system fingerprinting.

3.1.4.4.2 Capable of both unauthenticated and authenticated scans. Currently all scans are unauthenticated. Authenticated scans may be possible in the next few months.

3.1.4.4.3 Capable of configuration assessment scans in accordance with NIST Security Content Automation Protocol (SCAP). Trustwave as an approved scanning vendor all Trustwave configured assessment scans

are in accordance with SCAP as long as the standard does not require an authenticated scan.

- 3.1.4.4.4 Capable of database configuration scans. Yes
- 3.1.4.4.5 Support DAST system scan data through native or import capabilities. App Scanner is our DAST solution.
- 3.1.4.4.6 Identify exploits and malware kits associated with detected vulnerabilities. Yes
- 3.1.4.4.7 Include customizable, pre-configured scan templates. Customization would be available via Professional Services Engagements.
- 3.1.4.4.8 Include the ability to scan against a specific vulnerability. Customization would be available via Professional Services Engagements.
- 3.1.4.4.9 Include capability for scheduled scans, unsafe scan checks and scan blackout capabilities on a per-scan basis. Yes
- 3.1.4.4.10 Support a policy editor for custom configuration policy scans. Customization would be available via Professional Services Engagements.
- 3.1.4.4.11 Provide a log or feedback mechanism in the event scan failure.

3.1.4.5 EVMS must adhere to the following reporting requirements:

- 3.1.4.5.1 Capable of aggregated reporting, leveraging the data from multiple scan engines. Customization would be available via Professional Services Engagements.
- 3.1.4.5.2 Include pre-configured, customizable report templates to include compliance, risk prioritization and executive-level reports. Yes
- 3.1.4.5.3 Capable of scheduled reports and report distribution within the system and via email. Yes
- 3.1.4.5.4 Support vulnerability asset management variable report filtering. Yes
- 3.1.4.5.5 Supply reference IDs from vulnerability databases including WD and CVE.

3.1.4.5.6 Support the following report formats: HTML, PDF, CSV, or Multi-format Reports: Export report data in PDF, Excel, XML, CSV and HTML

3.1.4.6 EVMS must adhere to the following integration requirements:

3.1.4.6.1 Support integration with the patch management solutions, System Center Configuration Manager (SCCM) and Windows Server Update Services (WSUS). Solution does not currently support Patch Management. Customization would be available via Professional Services Engagements.

3.1.4.6.2 Support bi-directional API. API usage shall not require additional fees. Yes

3.1.4.6.3 Support integration with virtual environments, to include tracking virtual assets that may have a shared IP address and/or MAC address. Yes

3.1.4.7 The Vendor must provide EVMS support and maintenance for troubleshooting and errors as part of the licensed service.

3.1.4.7.1 Support and maintenance must be provided to include escalation, and multilevel support services. Support response time of four (4) hours or less is required. Yes

3.1.4.7.2 Support and maintenance must be available Monday — Friday, from 8AM - 5PM EST. Yes, in addition support is available 24x7x365

3.1.4.8 For any components of this system that use SaaS or cloud services, the vendor must adhere to the following requirements:

3.1.4.8.1 Meet or exceed all applicable controls of NIST Special Publication 800-53, Rev 4, for a moderate/moderate/moderate categorized information system. Trustwave meets all applicable controls of NIST special publications.

3.1.4.8.2 Provide strict data protection to all data transmitted, processed, and stored in the service, to include, at a minimum, data-in-transit and data-at-rest encryption. Yes

-
- 3.1.4.8.3 The cloud environment (primary and redundant sites) must reside in the continental United States. All cloud sites and data reside within the CONUS
 - 3.1.4.8.4 Agree to provide a cloud exit plan detailing the functionality, capability, and support to extract all stored data from the service in a non-proprietary format. The cloud lock-in protection cannot include additional fees or charges for data extraction. Yes
 - 3.1.4.8.5 Agree to include the method(s) of data destruction and how validation of data destruction will be provided to the State in the cloud exit plan. Yes
 - 3.1.4.8.6 Be willing to participate in a vendor assurance program, which can include, but not limited to, providing FedRAMP or Cloud Security Alliance documentation, for security and privacy protection validation. Yes

3.1.5 Central Management Appliance

- 3.1.5.1 The vendor will provide the central management appliance hardware to be physically installed by the State, but configured by the Vendor — in accordance with all State security procedures — with the following requirements: (Depending on number of internal IPs, Trustwave will provide an internal scanning appliance(s) to be installed by the State and configured by Trustwave. Trustwave will abide by all State Security procedures)
 - 3.1.5.1.1 The specifications of the appliance must be aligned with the size of an environment of 25,000+ assets. (Each appliance supports approximately 2,500 internal IP addresses. Depending on the number of internal IPs and subnets out of the total 25,000 assets determines how many appliances will be needed)
 - 3.1.5.1.2 The appliance must include all standard data connection and power cables. (Yes appliances include standard data connection and power cables)
 - 3.1.5.1.3 The appliance must include, at minimum, a 3-year warranty. (The appliances will be under warranty coverage for the duration of the service subscriptions, they cannot function without active subscriptions)

3.1.5.1.4 The vendor must provide a knowledge transfer concerning implementation, configuration, recommended maintenance actions, and troubleshooting guidance concerning the appliance.

3.1.6 System Deployment

3.1.6.1 Required Installation and Configuration support services will consist of a support engagement for conducting initial configuration and implementation support functions. The support engagement can be conducted in-person or remotely, leveraging voice, email and teleconference communication methods.

Trustwave's Vulnerability Management has an easy-to-use wizard that facilitates scan set up and management. Support is available 24x7365 to handle configuration and implantation support. Professional services hours are available for support and customization via voice, email and webex.

3.1.6.2 A Statement of Work (SOW) between the State and the Vendor will be drafted and agreed upon after the Contract is awarded. At a minimum, the SOW will address how the system will be initiated and configured for full operation, and support requirements that: (Upon being awarded the contract, a SOW can be provided including detailed service description and methodologies)

3.1.6.2.1 Provide the deliverable of a deployment project plan designed to ensure a sound architecture of the system.

3.1.6.2.2 Provide technical support during the deployment and initial configuration of the system. Technical Support is available during deployment to handle configuration of the system.

3.1.6.2.3 Provide the deliverables of all documentation pertaining to the service to include installation, operation, maintenance, troubleshooting and support manuals.

3.1.6.3 Training Services.

3.1.6.3.1 Provide two (2) training seats for application administration, configuration, & operations training. The training can be a single course or multiple courses, but must encompass both basic and advanced functionality of the application. The training must be a live training environment, but can be web-delivered and each training seat can be scheduled independently. (Trustwave will provide access to training

resources on TrustKeeper usage. In addition, Trustwave has included 1 day of onsite Training for App Scanner up to 10 students/training seats)

Pricing

Exhibit A - Pricing Page - EVMS - OT18048

Note to Vendors: The Pricing Page is locked. Only the column for Alternate Part Manufacturer/Model and for Unit Cost is unlocked.

CRFQ #: 0210 ISC 180000007

DATE: 1/25/2018

VENDOR: BB&T/Trustwave (subcontractor)

RETURN BY: 1/25/2018

Contract Item	Product/Service	Quantity	UOM	Price	Max Price
3.1.1 - 3.1.4.9	Enterprise Vulnerability Management System (EVMS), Annual License Subscription, Maintenance, and Support - 1 Year - 25,000 assets	25,000	\$6 per IP per year	\$150,000.00	\$150,000.00
3.1.5 - 3.1.5.1.4	Central Management Appliance - Warranty Included (Each appliance supports approximately 2,500 Internal IP addresses - Price may vary depending upon IP count breakdown)	1 (up to 10)	\$2,000 per Appliance	\$2,000.00	\$20,000.00
3.1.4.4.5	DAST App Scanner	Unlimited Applications and Scans		\$22,100	\$22,100
	App Scanner Training	1 Day (up to 10 Students)	1 onsite	\$4,000.00	\$4,000.00
3.1.6 - 3.1.6.3.1	System Deployment - (Price can vary need additional time/ information to scope, but additional hours cost \$225 per hour)	10	\$225 per Hour	\$2,250.00	\$2,250
3.1.8	Year 2 Subscription License Renewal, Support and Maintenance	1	Each	\$178,000.00	
3.1.8	Year 3 Subscription License Renewal, Support and Maintenance	1	Each	\$178,000.00	
3.1.8	Year 4 Subscription License Renewal, Support and Maintenance	1	Each	\$178,000.00	
			Total:	\$714,350.00	
			1st Year Total:	180,350	\$198,350.00

Contract will be evaluated on all lines but only awarded on first year. Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the West Virginia Office of Technology as Change Orders for subsequent years.

Vendor Signature: Michael Hottel

Date: 1/25/2018

PRICE

Disclosures

Please note that the quoted terms, conditions and pricing are valid for 90 days from the proposal due date, unless expressly reaffirmed in writing.

BB&T continually evaluates, adapts and modifies our financial center network, operations centers and platforms to fit the evolving needs of our customers and our business. Therefore the financial center, vault and/or processing center hours of operation, location and platforms, while current as of this proposal, are subject to change in the future. Any changes will be communicated in a timely and comprehensive manner.

BB&T offers a wide array of services to its clients. Each service has many features and options. In the course of providing these services we may employ agents, employees or subcontractors (vendors) to service all of our clients utilizing a service to a particular client. In general, we will disclose in a proposal response any agents, employees or subcontractors (vendors) retained by us exclusively for and are dedicated solely to, the provision of services to a specific client and/or contract.

Our response to this RFP does not constitute the acceptance of any binding terms or contract. BB&T's response includes services that are offered in accordance with the attached banking agreements, applicable banking Agreement(s) and/or Attachment(s).

Appendix

1. Treasury Management Agreement
2. State required documents
3. Addenda acknowledgement



TMA

Tax ID #:

BB&T
TREASURY MANAGEMENT AGREEMENT

THIS AGREEMENT, as dated below, is made by and between Branch Banking and Trust Company ("Bank") and
("Customer")

1. Service

Subject to the terms and conditions contained in this Agreement, the applicable Banking Agreement and any Attachment which describe specific Treasury Management ("Services") (whether attached hereto or relating to any Service requested subsequent to the date of this Agreement), each of which are incorporated herein by reference, Bank will furnish Customer with those Services that it may request. Customer agrees to pay for all said Services in accordance with this Agreement and the Bank's current fee schedule for such Services. Initiation by Customer of any Services constitutes acceptance of the terms and conditions of this Agreement, the applicable Banking Agreement and any applicable Attachment.

2. Customer's Duties. Customer shall:

- a) Perform and observe all conditions, covenants and restrictions as set forth in this Agreement and any Attachments, and if required by a particular Service, maintain, at a minimum, a Deposit Account at Bank subject to the applicable Banking Agreement.
- b) Pay any bill rendered by Bank within 30 days after the billing date and grant to the Bank a right of set-off in all of Customer's deposit accounts for any bills, costs or expenses owed to Bank under this Agreement or any Attachment.
- c) Warrant that Customer is fully authorized to effect transaction concerning any account, whether or not in Customer's name, that at Customer's request is the subject of, or is affected by, any Service.
- d) Carefully examine any statement, notification or confirmation of a transaction and notify the Bank within 30 days of the statement date of any errors, discrepancies or fraudulent transactions. Customer agrees that the Bank will not be liable for any erroneous, unauthorized or fraudulent transaction resulting from the Customer's failure to safeguard any security or access device used in connection with any Services or its failure to reasonably supervise its employees or agents entrusted with the security or access device. Customer agrees to conduct a detailed background check of all employees or agents having authority to implement any cash management transaction and to periodically check such others' work. The Customer further agrees that the Bank will not be liable for any erroneous, fraudulent or unauthorized transaction which was not otherwise caused by the Bank's gross negligence or willful misconduct.
- e) Indemnify and hold Bank, its affiliates, subsidiaries, officers, directors and employees harmless against any claim, loss, damage, deficiency, penalty, cost or expense resulting from: (a) any breach or default by the Customer in the performance or observance of this or any other Agreement; (b) any negligence or willful misconduct of the Customer; (c) incorrect, incomplete, or inaccurate data or information furnished by Customer to Bank; (d) any action taken by Bank (i) at the direction of Customer or its agent, (ii) at any direction authenticated by any device, symbol, or code assigned to or chosen by Customer in connection with a Service (unless Bank has actual knowledge that such direction is unauthorized), or (iii) in accordance with the procedures set forth in any Attachment.

3. Bank's Duties. Bank shall:

- a) Instruct Customer and its personnel in the proper use and operation of the Service(s) furnished herewith.
- b) Exercise ordinary care in the performance of Bank's obligations under this Agreement and any Attachment, including the maintenance of the confidentiality of Customer's account and of any identification device, symbol, or code utilized by Customer in obtaining a Service.
- c) Not be responsible for any liability, loss or damage resulting from any delay in its performance of, or from any failure to perform, its responsibilities under this Agreement or any Attachment, or for any error in transmission which: (i) was not caused by the Bank's gross negligence or willful misconduct; (ii) results from any malfunction, including data related processing, that may occur in Customer's computer software or computer system; or (iii) from an act of God; a natural catastrophe or event, whether or not abetted or aggravated by human or unnatural agencies; the unavailability, interruption, or malfunction of communications facilities or utilities; acts of, delays, or failures to act by other banks or financial institutions, intermediaries or their personnel; and criminal acts by persons other than Bank personnel; or any other circumstances beyond the Bank's control.
- d) Consistent with any security procedures agreed upon between Bank and Customer, confirm the identity of any person executing a transaction pursuant to this Agreement or any Attachment. The Bank, otherwise, may rely upon any written or verbal instruction by any person if the bank reasonably believes such authority is genuine and shall not be liable or responsible for any action taken or not taken in accordance thereof.
- e) Indemnify and hold Customer harmless against any loss, damage, deficiency, penalty, cost or expense claims brought against Customer to the extent that such claims arise out of the Bank's gross negligence or willful misconduct. Any liability of Bank to Customer shall be limited to direct losses suffered by Customer, not to exceed the sum of the fees and charges then imposed for Services purchased by Customer hereunder for a period of one year.

EXCEPT AS PROVIDED IN THIS AGREEMENT, THE BANK MAKES NO REPRESENTATION OR WARRANTY, WHETHER STATUTORY, EXPRESS, OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT AND UNDER ANY CIRCUMSTANCES SHALL BANK BE LIABLE FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR INDIRECT DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS OF PROFITS, EVEN IF THE BANK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

4. Term.

- a) This Agreement shall remain in full force and effect on the same terms and conditions as expressed herein, or as may be amended, until such time as it is terminated by either party as provided herein. Subject to section 4(b) and 4(c), either party may terminate this Agreement or any Service by giving thirty (30) days prior written notice to the other party. The liabilities of the parties shall cease on the effective date of termination, except as to events that shall have previously occurred.
- b) All Services are provided subject to applicable laws and rules. In the event Bank reasonably determines it is no longer able to provide a Service due to a change in laws or rules, this Agreement or a specific Service may be terminated immediately upon written notice by Bank to Customer.
- c) In the event of Customer's failure to perform or observe any of the conditions, covenants, and restrictions herein set forth, or if in the good faith opinion of Bank the Customer is involved in illegal or unethical business practices or is financially unstable and/or the prospect of payment or performance has been impaired, then in addition to any other available remedies, Bank may terminate this Agreement or any Service immediately by giving written notice to Customer.

5. Miscellaneous.

Bank may amend this Agreement and any Attachment, including any provision as to fees, by giving Customer prior written notice of the amendment, but this Agreement may not otherwise be amended or assigned except in writing signed by both parties.

- a) Any notice under this Agreement shall be deemed given: (i) to Bank when such notice is received at its Payment Solutions Division, Attn: Payments Client Support, 5130 Parkway Plaza Boulevard, 500-96-01-

05, Charlotte, NC 28217-1964, or at such other location as Bank may hereafter provide to Customer in writing; (ii) to Customer when mailed, postage prepaid, or delivered to Customer's current address, as shown on Bank's records.

- b) All information, whether printed, written or oral, furnished by either party shall be held in confidence and used only for the purpose of furnishing or utilizing Services rendered herewith and in compliance with the applicable Banking Agreement.
- c) This Agreement, together with the applicable Banking Agreement and any applicable Attachments contain the entire understanding of the parties and supersedes any previous discussions, proposals, or agreement, whether oral or written. In the event of any conflict between a provision set forth in this Agreement and a provision contained in an Attachment, the latter provision shall prevail. This Agreement shall not supersede or govern any other banking or lending relationship between the parties.
- d) The invalidity of any provision of this Agreement, either in its entirety or in any particular circumstance, shall not impair the validity of the remaining provisions or the validity of such provision in any other circumstance. This Agreement shall be governed, as to both interpretation and performance by the laws of the State in which Bank's main office is located, without regard to its conflict of laws provisions.
- e) Either party has the option of requiring that all disputes that may arise between the Customer and Bank, or any affiliate of the Bank, related to this Agreement, any Attachment or Services, or any products or investments provided to Customer shall be decided by arbitration held in the city where the Bank's main office is located. The parties are also advised that: (i) Arbitration is final and binding on the parties; (ii) The parties are waiving their rights to seek remedies in court, including the right to jury trial; (iii) Pre-arbitration discovery is generally more limited than and different from that in court proceedings; (iv) The arbitrators' award is not required to include factual findings or legal reasoning and any party's right to appeal or seek modification of rulings by the arbitrator is strictly limited; and (v) The panel of arbitrators may include arbitrators who were or are affiliated with the banking or securities industry. Any arbitration shall be conducted under the Rules of the American Arbitration Association ("AAA"), except that arbitration of disputes involving a Broker-Dealer affiliate of the Bank may be conducted under the Rules of the National Association of Securities Dealers ("NASD") or an Exchange or self-regulatory organization of which the Broker is a member. In matters involving the Broker as a party, the Customer may elect in the first instance whether arbitration shall be by the AAA, NASD, an Exchange or other self-regulatory organization of which the Broker is a member, but if the Customer fails to make such election, by registered letter to the Broker at the Broker's main office, before the expiration of ten days after receipt of a written request from the Broker to make such election, then the Broker may make such election.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized officers and to be effective as of the day and year first above written. Customer hereby acknowledges receipt of copies of this Agreement and any applicable Attachments and consents to the terms and conditions contained therein. *Customer further acknowledges and consents to the pre-dispute arbitration clause contained in the paragraph 5(e) above.*

CUSTOMER *

Signed: _____
By: _____
Title: _____
Date: _____

* Individual signing as "Customer" above must be an authorized individual appearing on the ***BB&T Resolution and Agreement for Deposit Account.***

FORWARD COMPLETED DOCUMENT TO YOUR PAYMENT SOLUTIONS SALES REPRESENTATIVE:

Name: _____ Fax # / Email Addr: _____

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: _____

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

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

Addendum Numbers Received:

(Check the box next to each addendum received)

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

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

BB&T

Company

Michael Holtz SVP

Authorized Signature

1/24/2018

Date

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

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: BB&T

Authorized Signature: Michael J. Heltsclaw, SVP Date: 1/25/2018

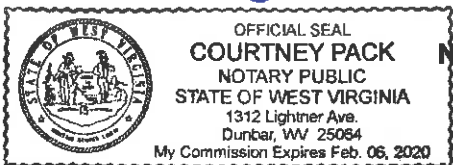
State of West Virginia

County of Kanawha, to-wit:

Taken, subscribed, and sworn to before me this 25 day of January, 2018.

My Commission expires February 16, 2020

AFFIX SEAL HERE



NOTARY PUBLIC

Courtney Pack

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.

Michael Holtsclaw, SVP
(Name, Title)
MICHAEL HOLTSCRAW, SENIOR VICE PRESIDENT
(Printed Name and Title)
300 SUMMERS ST., CHARLESTON WV 25301
(Address)
304-348-7078 / 304-348-1185
(Phone Number) / (Fax Number)
mholtscraw@bbandt.com
(email address)

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

BB&T
(Company)

Michael Holtscraw, SVP
(Authorized Signature) (Representative Name, Title)

MICHAEL HOLTSCRAW, SENIOR VICE PRESIDENT
(Printed Name and Title of Authorized Representative)

01/25/2018
(Date)

304-348-7078 / 304-348-1185
(Phone Number) (Fax Number)

West Virginia Ethics Commission
Disclosure of Interested Parties to Contracts

(Required by W. Va. Code § 6D-1-2)

Contracting Business Entity: BB&T Address: 300 Summers St.

Charleston WV 25301

Authorized Agent: MICHAEL HOLTSCLAW Address: (Same)

Contract Number: CRFO 0210 ISL 18*7 Contract Description: EVMS LICENSE

Governmental agency awarding contract: DEPT OF Administration, 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 neces sary):

1. Subcontractors or other entities performing work or service under the Contract

Check here if none, otherwise list entity/individual names below.

TRUSTWARE HOLDINGS INC.

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.

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.

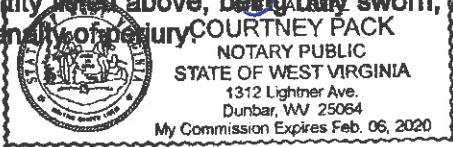
Signature: Michael H. Hetsclaw, SVF

Date Signed: 1/25/2018

Notary Verification

State of West Virginia, County of Kanawha:

I, Courtney Pack, 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.



this 25 day of January 2018

Courtney Pack

Notary Public's Signature

To be completed by State Agency:

Date Received by State Agency: _____

Date submitted to Ethics Commission: _____

Governmental agency submitting Disclosure: _____

TRUSTWAVE VULNERABILITY MANAGEMENT USER GUIDE

Table of Contents

Introducing Trustwave Vulnerability Management	3
1 Logging In and Accessing Scans	4
1.1 Portal Navigation and Utility Functions	5
1.1.1 Navigation	5
1.1.2 Notifications	5
1.1.3 Support and Help	5
1.1.4 Change Customer	5
1.1.5 Utility Functions	6
1.1.6 Column and Export Options	7
1.1.7 Data refresh	8
1.1.8 Action Bar	8
2 Scan Configuration	9
3 Creating and Editing Scans	11
3.1 Scan Settings	11
3.1.1 Advanced Configurations	12
3.2 Scan Targets	13
3.2.1 Exclusions	14
3.3 Schedule	14
3.3.1 Blackouts	15
3.4 Editing a Scan Series and Disabling Individual Scans	16
3.5 Deleting a Scan Series	16
4 Viewing Reports	17
4.1 TVM Reports	17
4.2 Reports Results	18
4.2.1 Vulnerabilities	19
4.2.2 Excepted Vulnerabilities	21
4.2.3 Asset inventory	23
4.2.4 Targets	23
4.2.5 Live Host Discovery	23
4.3 Report Files	23
4.4 Disputes	24
4.5 Bulk Disputes	25
4.6 Disputes Screen	25
4.7 Exceptions	26

4.7.1 Exceptions Screen	28
4.8 PDF Reports	29
4.9 Notifications	30
5 Reviewing Account Information	31
6 Managing Scans for the Enterprise	32
Hierarchy Rules	32
About Trustwave	34

Introducing Trustwave Vulnerability Management


Trustwave Vulnerability Management (TVM) is a network vulnerability scanning product.

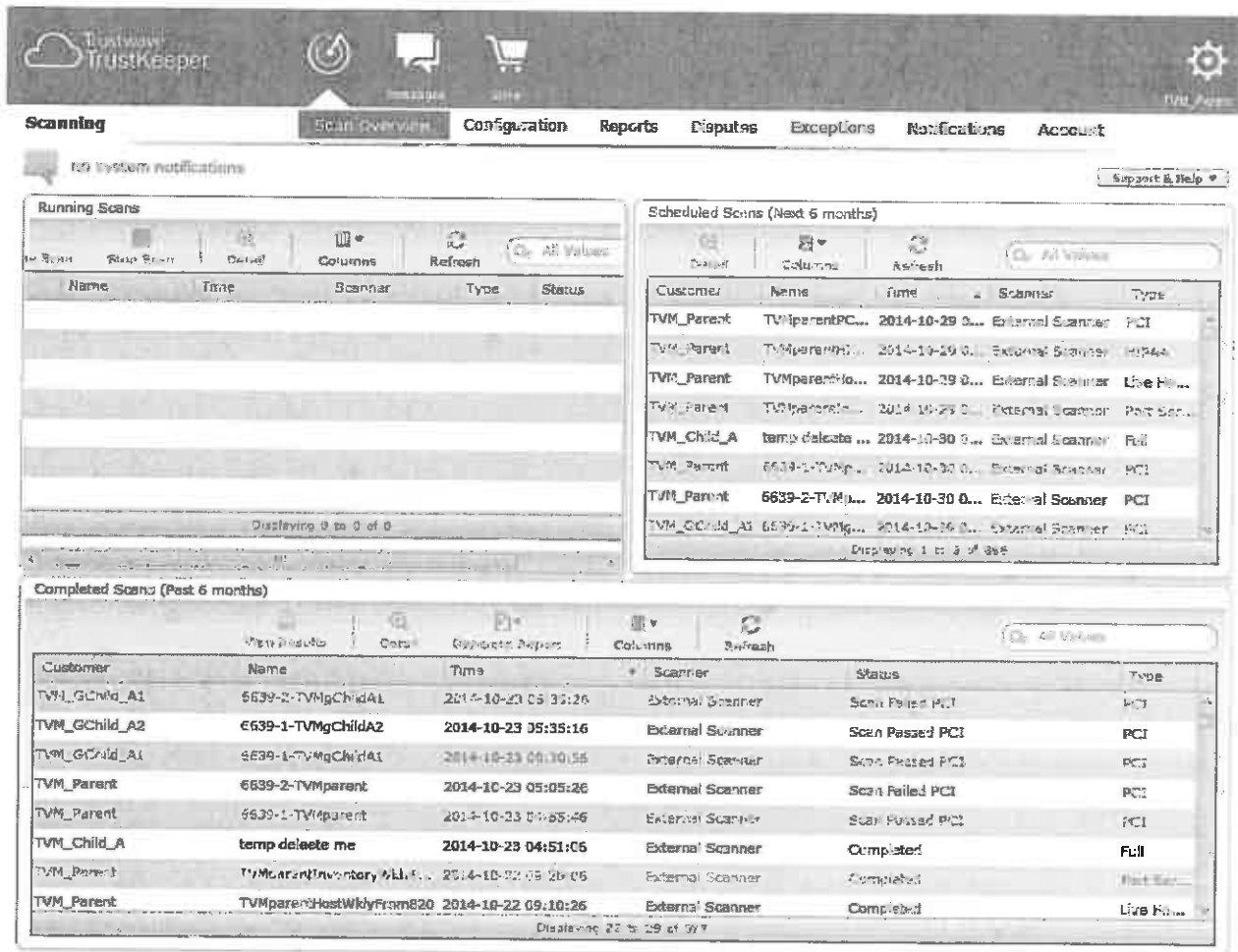
You can use TVM to

- Schedule a variety of network scans (including Live Host Discovery, Port Service Fingerprinting, PCI, or Full scans)
- Perform internal or external vulnerability scans
- Choose “blackout” dates and times when scanning will not be performed
- Review the scan results
- Dispute scan findings for external PCI scans
 - Renew disputes with every recurring scan
 - Extend dispute expiration dates
- Set Exceptions for future instances of specific findings in scans that are not external PCI scans
- Manage Notifications for Scans and Disputes
- Maintain an asset list
- Compare scan results from month to month
- Create reports of scans and findings
- Manage scans and findings for an enterprise with parent and child companies (choose to manage items for the entire enterprise or a sub-group). *(This function is in Beta test and is not available unless enabled for a customer by Trustwave.)*

1 Logging In and Accessing Scans

To access the TVM interface, log in at <https://login.trustwave.com>

Select the scans icon  to see the **Scan Overview** as shown below. This is the default view of TVM. The screen shows lists of running scans, scheduled scans (all instances within the next 6 months), and completed scans run within the past 6 months.



The screenshot displays the TVM interface with a navigation bar at the top containing 'Scanning', 'Scan Overview', 'Configuration', 'Reports', 'Disputes', 'Exceptions', 'Notifications', and 'Account'. Below the navigation bar, there are three main panels:


- Running Scans:** A table with columns: Name, Time, Scanner, Type, Status. It shows 0 scans.
- Scheduled Scans (Next 6 months):** A table with columns: Customer, Name, Time, Scanner, Type. It lists several scheduled scans.
- Completed Scans (Past 6 months):** A table with columns: Customer, Name, Time, Scanner, Status, Type. It lists 22 completed scans.





Tip: In the Running Scans pane, hover over the Status to see the progress of the scan. Refresh the pane to update the status.

For each list on this screen, you can:

- See additional items (if any) using the scrollbar at the right.
- Click a column heading to sort by that column.

- Filter the list by text in any column, using the search box at the top of the pane. Click the  icon to filter on text in a single column.
- Select a row in the list and use the buttons at the top of the list to take action:
 - View details of the scan
 - Stop or pause/resume a running scan
 - View detailed results of a completed scan
 - Generate a report of a completed scan (for scan types that support generation of reports)



Tip: You can expand any of the lists to a full screen view. To expand a list, hover over the pane that contains the list. A “Maximize” icon  displays at the top right of the pane. Click this icon to expand the list pane. To return to the default view, click the “Restore” icon  on the maximized pane.


1.1 Portal Navigation and Utility Functions

1.1.1 Navigation

To access the functions included in TVM, use the breadcrumb menu below the icons.



Tip: Click the arrow at the right of the list (if it is present) to access additional items.

When you are viewing a specific item such as a report, the menu shows a sub-item with an arrow: 

1.1.2 Notifications

Messages from the Portal system display at the top left (immediately below the menu). To see a list of notifications, click .

1.1.3 Support and Help

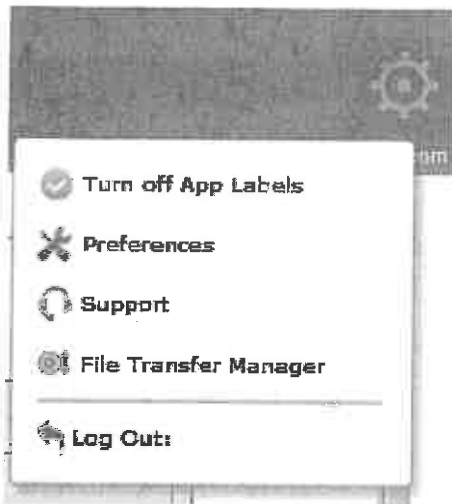
To find links to the latest version of this Guide and other documents, use the menu at the top right of each screen as shown in the image above.

1.1.4 Change Customer

If your login is defined as a Manager or Enterprise Manager (see Section 6), you can view information for each company by using the menu at the top right of each screen as shown in the image above. This selection affects the TVM section of the Portal.

1.1.5 Utility Functions

The gear icon at the top right of the page gives access to utility functions. Click this icon to log out, change your password or contact information, or get support information about your session.



1.1.5.1 Preferences

Use this option to:

- Add **contact information**. This information will be visible to other users if they have permission.
- Add or change **security information** (change your password and set security questions).

1.1.5.2 Support

Use this option to see support contact information, and to find customer and session details that can be useful for Portal support calls.

1.1.5.3 File Transfer Manager

Use this option to view the status of file downloads from the Portal (and uploads to the Portal Files section where supported). Transfers in progress are also indicated by an icon at the top right near the gear icon, and completed transfers are reported in the notifications.





Note: The Portal uses its own secure download feature, and does not use the download feature built in to web browsers.

1.1.5.4 Log Out

Use this option to end your Portal session. **Trustwave recommends** you *always log out* when you are finished with the Portal (do not just close your browser window or navigate away from the page).

1.1.6 Column and Export Options


Some screens include a "gear" menu. This menu may be available above the list  or at the left of the list header row . You can use this menu to choose columns in a list, to copy data to the clipboard, or to export data in file formats.

Shortcuts to these functions may also be available as "action bar" icons above the list.

1.1.6.1 Column Chooser

Click the gear and then select **Choose Columns** (or see the Columns section of the context menu).

On the Choose Columns window:

- Check the columns you want to show.
- If a choice **Show All** is available, check it to display all available columns.
- If required, click **OK** to apply your selection.
- Alternatively, use the column chooser menu above a list  to select from available columns. Check or uncheck boxes to change the displayed columns.

1.1.6.2 Clipboard Tool

Click the gear and then select **Copy Page to Clipboard**. Or, use the clipboard menu .

Choose CSV or HTML format (or select **Export > Copy as CSV** or **Export > Copy as HTML** from the context menu).

- **CSV** (Comma Separated Value) exports data in a format suitable for pasting to a spreadsheet or other table.
- **HTML** exports data in a format suitable for pasting to a word processing document or web page.

1.1.6.3 Data Export

Click the gear and then click **Export** (or see the Export section of the context menu).

On the Export Grid Data window:


- Choose a format. Available formats include:
 - Excel
 - CSV (For use with a spreadsheet or database).
 - PDF (Best for immediate presentation, but consumes more resources to generate).
 - HTML (For use with web pages or word processing).
 - XML (For import to other tools that understand this format).
- Choose the columns you want to export.
- Choose whether to include a header row that gives the column names (does not apply to XML output).

- Click **Export** to select a download location and begin generation.

1.1.7 Data refresh

Use the refresh button  or  to check for new data on any screen or list.

1.1.8 Action Bar

From the  context menu of a list, you can choose to display links to list options above the list. By default the action bar shows icons (*Compact*). You can choose to hide it (*Hidden*), or to include text with the icons (*Visual*).

2 Scan Configuration

Click **Configuration** in the main navigation to see all the existing scan profiles as shown below.

The screenshot shows the 'Scan Configuration' page in the Trustwave Vulnerability Management interface. At the top, there is a navigation bar with 'Scan Overview', 'Configuration', 'Reports', 'Disputes', 'Exceptions', 'Notifications', and 'Account'. Below the navigation bar, there is a header area with 'External Targets: 15/250', 'Score: 98/1000', and 'License Expires: 2016-03-03'. The main content area is divided into two panes. The left pane contains a table of scan profiles, and the right pane shows the 'Configuration Details' for the selected scan profile.

Configuration Name	Status	Scan Type	Schedule	Next Scan
Multi Test	Disabled	Vulnerability Scan	Weekly	2015-05-29 02:57
6639EntView-TVMparent-2	Enabled	PCI Scan	Monthly	2015-05-30 07:40
bu1tescan	Disabled	vulnerability Scan	Monthly	2015-05-21 07:12
TVMparentInventoryMonthly...	Enabled	Port Service Fingerprint	Monthly	2015-06-01 05:15
TVMparentHostMonthlyWk...	Enabled	Live Host Discovery	Weekly	2015-05-24 08:18
TVMparentPCIdentMonthlyLa...	Enabled	PCI Scan	Monthly	2015-06-01 05:15
TVMparentHIPAAWeeklyFrom...	Enabled	HIPAA Scan	Weekly	2015-06-01 05:15
TVMparentHostDiscovery...	Enabled	Live Host Discovery	Weekly	2015-06-01 05:15
TVMparentPCIIdentMonthlyFrom...	Enabled	PCI Scan	Weekly	2015-06-01 05:09
TVMparentHIPAAWeeklyFrom...	Enabled	HIPAA Scan	Weekly	2015-06-03 05:05
TVMparentHostDiscovery...	Enabled	Live Host Discovery	Weekly	2015-06-01 05:15
TVMparentInventoryWeeklyPro...	Enabled	Port Service Fingerprint	Weekly	2015-05-09 02:20
Ent-2-TVMparent	Enabled	PCI Scan	Weekly	2015-01-01 04:00
TVMparentInventoryMonthly	Enabled	Port Service Fingerprint	Monthly	2015-06-21 09:00
TVMparentHIPAAWeeklyFrom...	Enabled	HIPAA Scan	Weekly	2015-05-21 04:00
TVMparentHostIdentMonthly	Enabled	PCI Scan	Monthly	2015-06-21 04:00
TVMparentFullMonthly	Enabled	Vulnerability Scan	Monthly	2015-06-21 04:00

The 'Configuration Details' pane for the selected scan shows the following information:

- Configuration Name: TVMparentFullMonthlyLastWeekEndDay
- Scanner: External Scanner
- Scan Type: Vulnerability Scan
- Schedule: Monthly on the last weekend day at 07:15 ...
- Checkouts: [None]
- Targets: 10.70.244.5 10.70.244.5
- Global Exclusions: [None]
- Last Completed Scan: 2015-05-31 15:58



This screen provides a list of configured scans. For each scan profile, the next scan time displays. The screen also shows licensing information at the top.

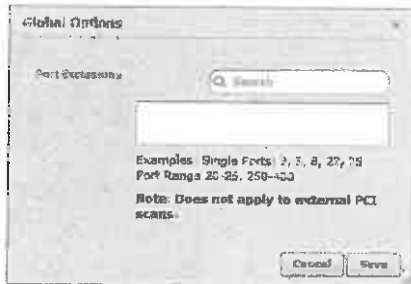
- Select a row in the list to see more information about the scan in the right pane.



Note: If global port exclusions are applied to a configuration, the Configuration Details listing shows the line **Global Port Exclusions** present.

- Use the icons above the list to take action on the selected scan:
 - **Scan Now** to start the scan immediately, even if it is disabled.
 - **Delete** the scan.
 - **Edit** the scan properties. See Section 3 for a description of available options.
 - **Clone** the scan (create a new scan with the same properties). The cloned scan will be created disabled. You can edit the clone, make any required changes, and enable it.
 - **Disable** or **Enable** the scan (depending on the scan status). A disabled scan remains in the list, but it will never be started automatically even if it is scheduled.

- Click **New**  to create a new scan.
- You can scroll through the list, or use the filter control above the list, to find specific scans. You can sort the list on the values in any column by clicking the column header.
- As a user with Enterprise Manager permission, click **Global**  to create or edit port exclusions that will apply to all scans except external PCI scans.



On the Global Options window, enter or edit a comma-separated list of ports that should not be scanned, and then click **Save**.

- You cannot make duplicate port entries.
- When you save, any series of ports are saved as ranges.
- You can search the list using the search box.
- You can enlarge the window using the handle at the bottom right.

3 Creating and Editing Scans

To create a new scan (one-time or series), on the Configuration page, click **New +** at the top left. Review or complete information on the next three panes. The system provides default values where possible.



Tip: To return to the Configuration page, click **Cancel** at the bottom of the pane. You cannot exit the configuration editor by clicking items in the main site menu.

3.1 Scan Settings

On the **Settings** pane, complete the name, scanner, and scan type.

The screenshot shows the 'Configuration' page for a scan. At the top, there are navigation tabs: Scanning, Scan Overview, Configuration (selected), Reports, Disputes, Exceptions, Notifications, and Account. Below these are system notifications and customer information (Customer: TVM_Parent). The main content area is divided into 'Basic Configurations' and 'Advanced Configurations'. In 'Basic Configurations', the 'Configuration Name' is 'Test Scan', the 'Scanner' is 'External', and the 'Scan Type' is 'Vulnerability Scan'. In 'Advanced Configurations', 'Live Host Discovery' is set to 'Light TCP/UDP scan: common ports (default)' and 'Port Service Fingerprinting' is set to 'Comprehensive: 65K TCP ports and more (default)'. At the bottom, there are 'Cancel', 'Next', 'Save & Exit', and 'Save' buttons. A note at the bottom left states: 'Note that the TrustKeeper external scan will exclude from IP addresses in these ranges: 194.13.203.0/24 (194.13.203.1 through 194.13.203.254) and 94.37.231.0/24 (94.37.231.1 through 94.37.231.254)'.

- If you have one or more internal scanners you can select them; otherwise you can only use the External Scanner option.

Choose from the following scan types:

- **Vulnerability Scan:** This scan executes all tools and tests against the target network. This type of scan cannot be used as the PCI Compliance Affecting scan. It could be used in to show fixed or updated findings within a PCI Report on Compliance (RoC).

- *Optional:* Choose **Advanced Configurations** to change the default port scanning options (see Table 1 for details of the options). Select the arrow or text to expand this section.
- **PCI Scan:** This scan type is used to confirm PCI compliance. With this type of scan, you cannot change the settings for Live Host Discovery or Port Service Fingerprinting, as these are specified by the PCI SSC. If you also use Trustwave's PCI Manager, you can choose whether the scan is a PCI compliance affecting scan.
 - Specify whether you have a load balancer and whether all the servers behind the load balancer are identically configured or not.
- **Live Host Discovery:** A lightweight scan designed to identify live hosts on the network through a number of different enumeration techniques. This scan is useful to assist in understanding the number of hosts on a network before running a PCI or Full scan.
 - *Optional:* Choose **Advanced Configurations** to change the default port scanning options (see Table 1 for details of the options). Select the arrow or text to expand this section.
- **Port Service Fingerprint:** A proprietary advanced port fingerprinting scan to identify which protocols and services are running on live hosts. This scan examines the specified TCP and UDP ports for each host, and attempts to identify the services if any that are responding. It can be used to understand what services are present on the network (such as web servers, mail servers or database servers).
 - *Optional:* Choose **Advanced Configurations** to change the default port scanning options (see Table 1 for details of the options). Select the arrow or text to expand this section.
- **HIPAA Scan:** A full scan that generates a report suited to the requirements of HIPAA.

After selecting configurations, click **Next** to continue.

3.1.1 Advanced Configurations

Some scan types allow you to choose network scanning configurations. These configurations are defined as follows:

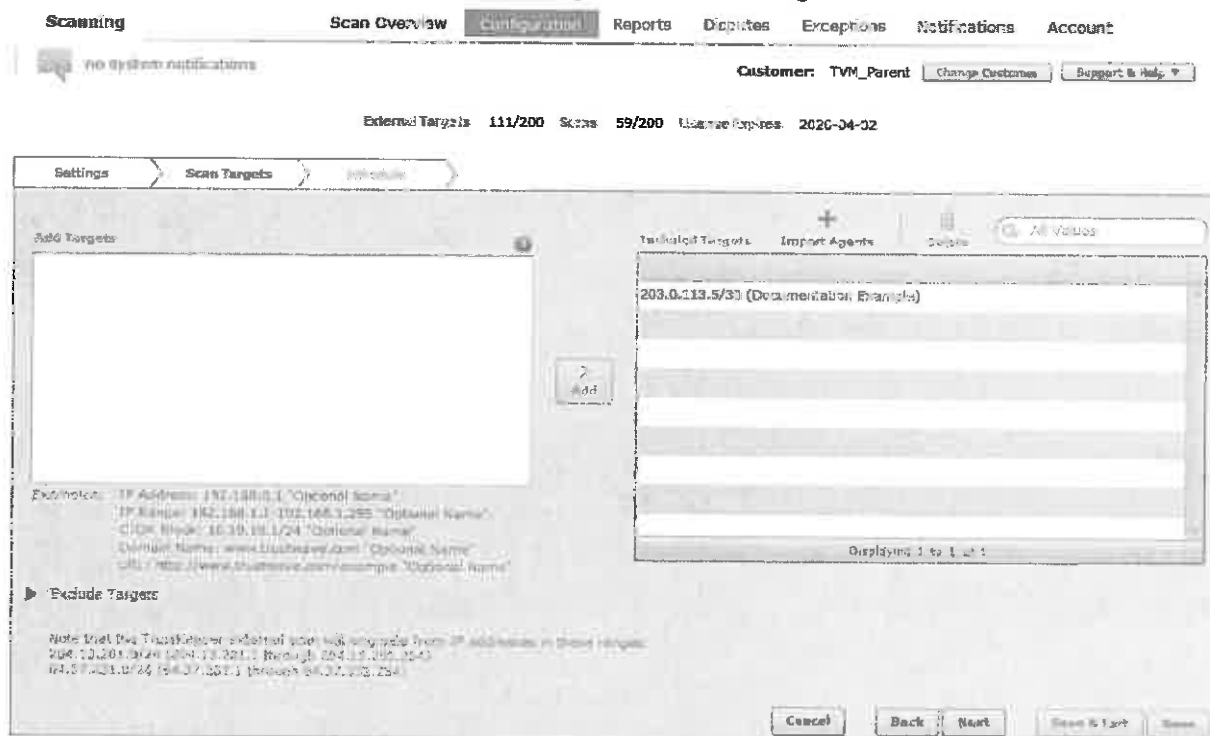
Table 1: Advanced Configuration Options

Configuration Type	Description
ICMP Ping	For host discovery, uses only a network ping to determine accessible host addresses
Light TCP/UDP scan: common ports	In addition to ICMP, scans on TCP commonly used ports (21, 22, 23, 25, 53, 80, 110, 111, 135, 139, 143, 389, 443, 445, 993, 995, 1433, 1521, 1723, 3306, 3389, 5432, 5631, 5900, 8080) and UDP commonly used ports (53, 67, 68, 69, 123, 137, 138, 161, 500). <ul style="list-style-type: none"> • This is the default configuration for live host discovery.
Medium TCP/LDP scan	In addition to ICMP, scans on TCP ports 0 – 1023, as well as TCP ports 1433, 1521, 1723, 3306, 3389, 5432, 5631, 5900, 8080 and commonly used UDP ports (53, 67, 68, 69, 123, 137, 138, 161, 500).

Configuration Type	Description
Comprehensive scan (65000 TCP ports and more)	In addition to ICMP, scans on all TCP ports and commonly used UDP ports (53, 67, 68, 69, 123, 137, 138, 161, 500). Also checks all other available methods. <ul style="list-style-type: none"> This is the default configuration for port service fingerprinting.

3.2 Scan Targets

On the **Scan Targets** pane, click in the **Add Targets** box to add targets.




Targets can be entered as an IP address, range of IP addresses, CIDR network block, domain name, or URL. You can give each target a friendly name (entered in quotes after the target information).

Note the examples shown below the target field, and hover over  for more suggestions.




Note: A URL must start `http://` or `https://` and can include subdirectories. A domain entry cannot include subdirectories.

- Once you have entered the text, click **Add** to populate the Included Targets list.
- You can also select Agents – to provide the IP address of internet facing devices to be scanned – by clicking **Import Agents**  (found above the Included Targets list).



Note: Agents can only be used with External Vulnerability Scans [EVS]. They cannot be used to configure Internal Vulnerability Scans [IVS] run from a Trustwave appliance.

- To delete a target, select it and then click **Delete** .
- Click **Next** to continue.

3.2.1 Exclusions

You may want to exclude some devices within the target ranges. To exclude devices, click the **Excluded Targets** arrow at bottom left to expand the exceptions/exclusions section. Click in the **Add Exclusions** box to enter targets that will not be scanned. Use the same techniques as for the Scan Targets pane.

After configuring targets, click **Next** to continue or **Back** to return to the Settings pane.

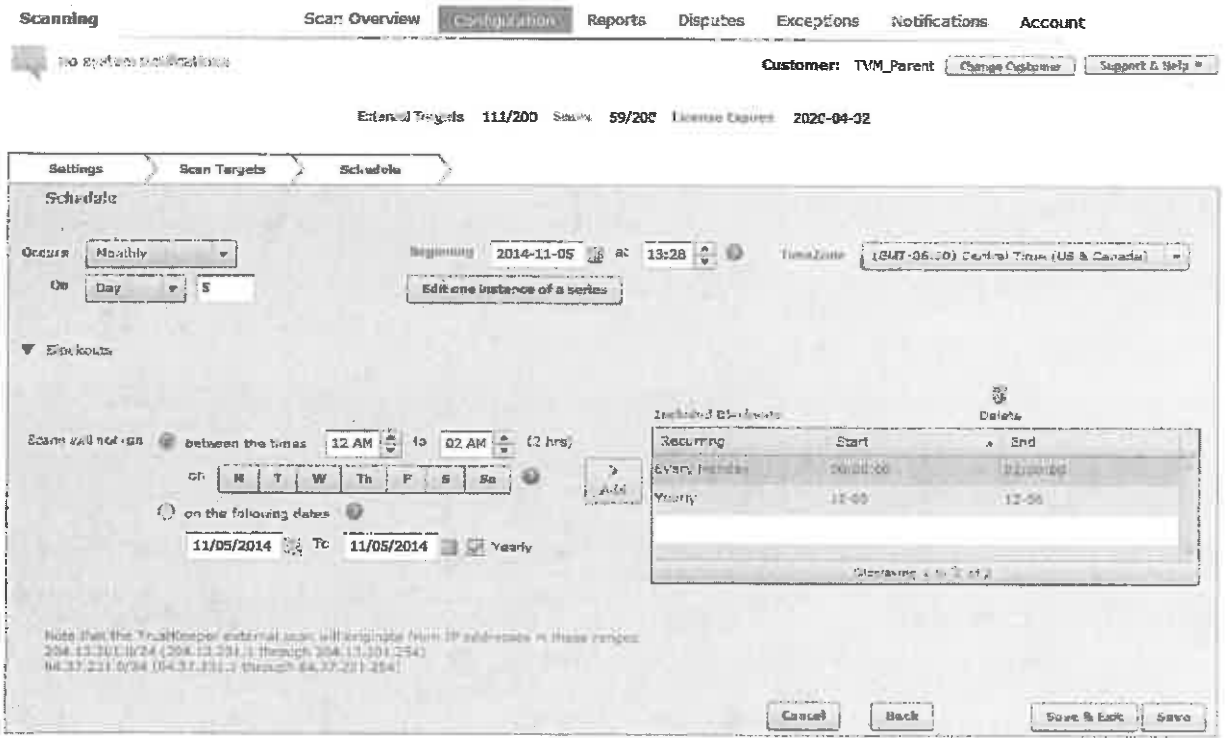


Tip: As an Enterprise Manager you can globally exclude ports from scanning. Global exclusions do not apply to External PCI Scans. For details, see Section 2.

3.3 Schedule

On the Schedule pane, choose when the scan should run. You can choose an immediate one-time scan, or schedule a scan to run once, weekly, monthly, or quarterly. For monthly scans you can choose the date of the scan or the recurring day of the week each month.

Enter a date and time for the first scan. Select the time zone. The default time zone matches the time zone of your browser.



3.3.1 Blackouts


You may want to prevent scanning on particular dates or at certain times of day. To set up these options, click the **Blackouts** arrow to expand the blackouts section.

In the blackouts section, optionally enter dates or times when scanning should be suspended.

- You can choose to black out specific times on certain days of the week.
- You can choose to black out specific dates.
- You can add more than one set of blackout dates or times to build complex rules.


Be aware that blackouts can cause the scan to take a long time.

To add a blackout period:

- Select times and days, or select a starting and ending date and optionally select Yearly to repeat every year.
- Click **Add** to add the blackout period to Included Blackouts.
- To remove a blackout period, select it in the list and then click **Delete** .

Click **Save & Exit** to save and enable the scan or scan series. The scan or series is added to the list viewable from the schedule pane. The scan will run as scheduled, unless you disable it.

3.4 Editing a Scan Series and Disabling Individual Scans

After you save a scan or series, you can edit it. To edit, select the scan in the list on the Configuration page, and then click **Edit** . Alter scheduling or targets as required. Some settings such as the basic scan type are disabled and cannot be changed.

To disable an individual scan in a series:

- On the Schedule pane click **Enable/Disable one instance of a series**.
- The pop-up window shows all instances of the series for the next year. To disable an instance, clear the associated checkbox. To re-enable an instance, check the box.
- When you have made all selections, click **Close** to close the pop-up, and then click **Save & Exit** on the Schedule pane (or click **Cancel** to ignore any changes).

3.5 Deleting a Scan Series

To delete a scan series, select it from the list and then click **Delete** .



Note: If you want to cancel a single instance of a scan in a series, see Section 3.4.

4 Viewing Reports


Select the scans icon  and click **Reports** in the main navigation to see the Reports Summary screen.

This screen includes two lists:

TVM Reports provides a summary of completed scans and identified vulnerabilities. You can export the summary data in several formats. You can view detailed results of each scan online. Depending on the type of scan you can generate Executive Summary, Full Vulnerability, Vulnerabilities by IP, Vulnerabilities by Severity, or PCI reports in PDF format. You can also generate reports from the Completed Scans pane on the Scan Overview tab, and from the Vulnerabilities tab when viewing scan results.

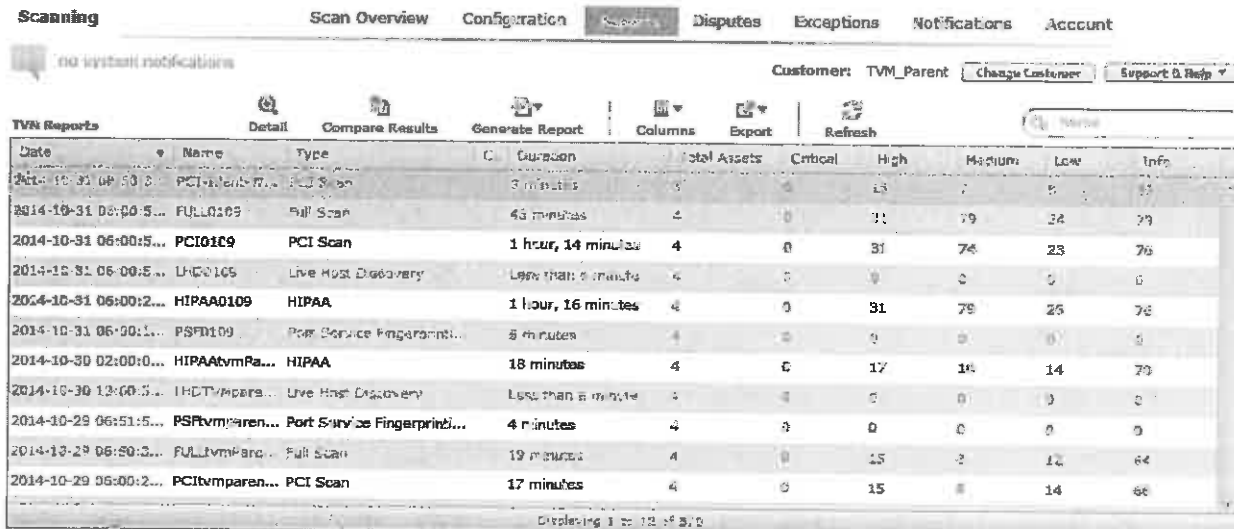
Report Files allows you to generate importable data files (in CSV format) that list detailed scan results, disputes, or targets for a range of dates. The list shows files that have been requested or completed.



Tip: You you can adjust the size of the lists by dragging the handle  between the panes.

4.1 TVM Reports

The TVM Reports list shows all successfully completed scans along with scan summary information. This listing provides a quick view across all scans and can be used to track assets or aggregate finding counts by risk. You can sort and filter scan results, and export summary results into several formats.



The screenshot shows the TVM Reports interface. At the top, there are navigation tabs: Scanning, Scan Overview, Configuration, **Reports**, Disputes, Exceptions, Notifications, and Account. Below the tabs, there is a notification area that says "no instant notifications" and a customer selection area for "TVM_Parent".

The main content area is titled "TVM Reports" and contains a table with the following columns: Date, Name, Type, C, Duration, Total Assets, Critical, High, Medium, Low, and Info. The table lists several scans, including PCI scans, Full Scans, Live Host Discovery, and HIPAA scans. Each row provides details such as the scan name, type, duration, total assets, and counts for different risk levels (Critical, High, Medium, Low).


Date	Name	Type	C	Duration	Total Assets	Critical	High	Medium	Low	Info
2014-10-31 04:50:0...	PCIvmparen... Full Scan	Full Scan	0	3 minutes	3	0	13	7	5	52
2014-10-31 06:00:5...	FULL109	Full Scan	0	43 minutes	4	0	31	79	24	79
2014-10-31 06:00:5...	PCI0109	PCI Scan	0	1 hour, 14 minutes	4	0	31	74	23	74
2014-10-31 06:00:5...	LH00109	Live Host Discovery	0	Less than 5 minutes	4	0	0	0	0	0
2014-10-31 06:00:2...	HIPAA0109	HIPAA	0	1 hour, 16 minutes	4	0	31	79	25	74
2014-10-31 06:00:1...	PSFD109	Port Service Fingerprin...	0	5 minutes	4	0	0	0	0	0
2014-10-30 02:00:0...	HIPAAvmpa...	HIPAA	0	18 minutes	4	0	17	14	14	79
2014-10-30 13:00:5...	LHDTvmpars...	Live Host Discovery	0	Less than 5 minutes	4	0	0	0	0	0
2014-10-29 06:51:5...	PSFvmparen...	Port Service Fingerprin...	0	4 minutes	4	0	0	0	0	0
2014-10-29 06:50:2...	FULLvmpare...	Full Scan	0	19 minutes	4	0	15	2	12	44
2014-10-29 06:00:2...	PCIvmparen...	PCI Scan	0	17 minutes	4	0	15	8	14	44


At the bottom of the table, it says "Displaying 1 to 12 of 3,0" and "11 items".

Use the filter field at top right to limit the list results by name or scan type (click  to select the limit).

If the list includes many results, use the scrollbar at right to move through the list.


Use the icons above the list to choose specific columns, to copy data to the clipboard, or to export data in a variety of formats. For details of the available options, see Section 1.1.5 above.

To see detailed scan results and asset information, select a specific row in the list and click **Detail** , or double-click the row. For details of this information see Section 4.2.

To generate a report in PDF format, click **Generate Report**  and then select the type of report. Reports are generated and downloaded using the browser functionality. The generated report will be available in the Reports > Report Files list at the bottom of the page.



Note: Report Status will first display as "In Progress". When the report is ready the status changes to "Completed." You can refresh the grid to update the status display, or simply return to the page later.

To compare results of two scans (in the same series), select a row and click **Compare Results** . On the pop-up list, choose two scans to compare, and then click **Compare**. The result shows changes in vulnerability status between the scans.

Scanning Scan Overview Configuration Reports > Compare Results: CVE-2014-0397 CVE-2009-3555

no system notifications Support & Help

Comparing Scan Results: 2015-04-06 18:31:52 and 2015-03-03 07:04:56

Site	Scan Date	IP	Domain	Vulnerability Name	Proto	Port No.	Severity	CVE
Addr	2015-04-06 1	10.70.33.1		Oracle Solaris Buffer Errors vulnerability in libdsol	-	0	CRITICAL	CVE-2014-0397
Addr	2015-04-06 1	10.70.33.1		Unencrypted Communication Channels/Accessibility	tcp	22	LOW	
Addr	2015-04-06 1	10.70.33.1		SSL / TLS Renegotiation Handshakes MITM Plaintext Data Injection	tcp	32803	MEDIUM	CVE-2009-3555
Addr	2015-04-06 1	10.70.33.1		SSL / TLS Renegotiation Handshakes MITM Plaintext Data Injection	tcp	6785	MEDIUM	CVE-2009-3555
Addr	2015-04-06 1	10.70.33.1		TCP Timestamp Options Enabled	tcp	80	LOW	

Displaying 1 to 5 of 5 Page 1 of 1

4.2 Reports Results

The Results screen shows details of vulnerability findings and asset inventory for a specific scan. The screen includes the following tabs: Summary, Vulnerabilities, Asset Inventory, Targets, and Live Host Discovery.

You can return to the Reports listing by clicking Reports in the main navigation.

From any tab, you can move between scan series and scans using the two menus at the top of the listing.

4.2.1 Vulnerabilities

This screen shows vulnerability findings for a specific scan. Navigate the available information using the tabs.

The Summary tab provides basic information about the scan.



Note: For scans other than external PCI scans, if ports are globally excluded this information displays in the right column as **Port Exclusions**.

The screenshot shows the 'Scanning' interface with the 'Summary' tab selected. The scan series name is 'TVMparentPCIdentMonthlyLastWkEndDay' and the scan status is 'Completed, Scan Failed PCI'. The scan started on 2014-06-01 05:15:15 AM and ended on 2014-06-01 05:32:13 AM. The duration was 17 minutes and the scanner used was an 'External Scanner'. The 'Vulnerability Count' table shows 15 PCI Affecting, 0 Critical, 11 High, 6 Medium, and 12 Low vulnerabilities. The 'Hosts Scanned' table shows 2 Attempted, 2 Scanned, and 0 Not Found.

Hosts Scanned:	Attempted	Scanned	Not Found
	2	2	0

Vulnerability Count:	PCI Affecting	Critical	High	Medium	Low
	15	0	11	6	12



Note: For scans other than external PCI scans, if ports are globally excluded this information displays in the right column as **Port Exclusions**.

Scanning Scan Overview Configuration **Reports > Results** Disputes Exceptions

notifications history available

bluTestScan 2015-05-29 15:43:37

Summary Vulnerabilities Asset Inventory Targets Live Host Discov...

Scan Series Name bluTestScan (Hosts Scanned)

Scan Status Completed ✓

Start 2015-05-29 15:43:37

End 2015-05-29 15:59:35

Duration 9 minutes

Type Full Scan

Scanner External Scanner

Vulnerability Count			
Attempted	Scanned	Not Found	
2	1	1	
Critical	High	Medium	Low
0	7	8	6

Port Exclusions 47, 9876, 43633

The Vulnerabilities tab shows more information about vulnerabilities identified by the scan.

Scanning Scan Overview Configuration **Reports > Results** Disputes Exceptions Notifications

no system notifications

Customer: TVM_Parent Change Customer Support & Help

TVMparentPCIDemMonthlyLastWeekEndDay 2014-06-01 09:15:16 AM

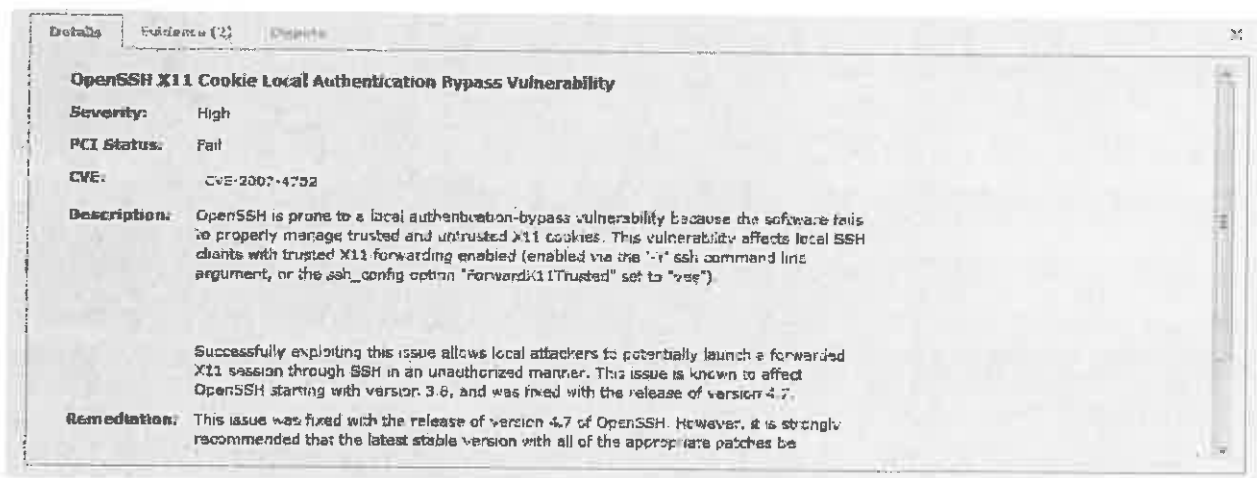
Summary Vulnerabilities Asset Inventory Targets Live Host Discovery

Dispute Rescan Compare Report Type: Generate Report

Status	IP	Domain	Vulnerability Name	Protocol	Port	Severity	PCI	CVE
<input type="checkbox"/>	10.70.244.6		OpenSSH Duplicate Block Denial of Service Vulnerability	tcp	22	Medium		CVE-2005-4024
<input type="checkbox"/>	10.70.244.6		OpenSSH v. 4.4 Multiple Vulnerabilities	tcp	22	Medium		CVE-2006-50...
<input type="checkbox"/>	10.70.244.6		OpenSSH Privilege Separation Monitor Weakness	tcp	22	Medium		CVE-2006-5794
<input type="checkbox"/>	10.70.244.6		OpenSSH XLI Cookie Local Authentication Bypass Vulnerability	tcp	22	Medium		CVE-2007-4050
<input type="checkbox"/>	10.70.244.5		OpenSSH Duplicate Block Denial of Service Vulnerability	tcp	22	Medium		CVE-2005-4024
<input type="checkbox"/>	10.70.244.5		OpenSSH v. 4.4 Multiple Vulnerabilities	tcp	22	Medium		CVE-2006-50...
<input type="checkbox"/>	10.70.244.5		OpenSSH Privilege Separation Monitor Weakness	tcp	22	Medium		CVE-2006-5794
<input type="checkbox"/>	10.70.244.5		OpenSSH XLI Cookie Local Authentication Bypass Vulnerability	tcp	22	Medium		CVE-2007-4050

Displaying 1 to 82 of 82 Page 1 of 1

Select a row to view more details in a pane below the list. On this pane, the Details tab includes a description of the issue, and remediation steps. The Evidence tab includes any available evidence of the vulnerability that was gathered during the scan. For vulnerabilities that have been disputed (as described in Sections 4.3 through 4.5), dispute history will be shown in the Disputes tab.



- **Rescan:** Click this button to re-run the last scan. A rescan does not count against your total scan count.



Note: This option re-runs an entire scan. It is not limited to items that are selected.

- **Compare:** Click this button to compare the results of two scans in a series.

4.2.2 Excepted Vulnerabilities

For all non-PCI ASV scans (non-External PCI scans), you can choose to make an Exception to a vulnerability. Exceptions allow you to avoid reporting on vulnerabilities that are incorrect or are not valid security risks because they are mitigated through technical or non-technical controls or processes.



Tip: For more information about Exceptions, see Section 4.7.

If a vulnerability matches a previously entered Exception, the status column displays **Excepted**. You can review the exception information on the Exceptions tab of the detail pane.

Scanning Scan Overview Configuration **Reports** Disputes Exceptions Notifications Account

Parent_Full 2013-04-10 09:41:05

Summary Vulnerabilities Asset Inventory Targets Live Host Discov...

Subscription Rescan Compare Generate Report Columns Export Refresh

Status	IP	Domain	Vulnerability Name	Port	Part	Sev.	CVE
Excepted	10.70.24...		OpenSSH Duplicate Block Denial of Service vulnerability	22	top	CRITICAL	CVE-200...
Excepted	10.70.24...		OpenSSH 4.4 Multiple Vulnerabilities	top	22	CRITICAL	CVE-200...
Excepted	10.70.24...		OpenSSH Privilege Separation Monitor Weakness	top	22	CRITICAL	CVE-200...
	10.70.24...		OpenSSH X11 Cookie Local Authentication Bypass Vulnerability	top	22	CRITICAL	CVE-200...
	10.70.24...		AJP (Apache JServ Protocol) Service Detected	top	8009	CRITICAL	
	10.70.24...		OpenSSH X11 Session Hijacking Vulnerability	top	22	CRITICAL	CVE-200...
	10.70.24...		Apache Tomcat Denial of Service via Slow HTTP Requests	top	8080	CRITICAL	CVE-201...

Page 1 of 1

Details Evidence (1) Exception (1)

Exception Name	Vulnerability Name	Scan Name	IP	Port	Domain	Created Date	Expires
I am using updated/backports...	OpenSSH Duplicate Block Deni...	Parent_Full	10.70.244.46	22	scantest-centos6-	2015-02-24	2015-05-0

To see details of all vulnerabilities that have been excepted by the same exception, double-click the entry on the Exception tab to open the Exceptions screen as a child view. (For details of the Exceptions screen, see Section 4.7.1.) You can further click a detail item on this screen to review another scan. You can return to parent items using the breadcrumb navigation.

Scanning Scan Overview Configuration **Reports** Disputes Exceptions Notifications Account

Notifications History Available Support & Help

Delete Edit Detail Disable Clone Columns Export Refresh Show Deleted Exceptions

Status	Exception Name	Vulnerability Name	Scan Name	IP	Port	Domain	Created	Expires
Enabled	Test-0309	Remote Access Service Detected	Any	10.70.244.46	Any	Any	2015-03-10	2015-03-20
Enabled	This Field Cannot Hold More than ...	Cisco SSH Denial of Service Vuln...	CVE-2014-0422	Any	Any	Any	2015-03-10	2015-03-10
Enabled	All Instances of this vulnerability i...	Cisco IOS IPv4 Denial of Service ...	IVS-MixTargetTypeRegressionTest	Any	Any	Any	2015-03-10	2015-03-10
Enabled	All Instances of this vulnerability i...	Cisco IOS Secure Shell Service V...	Any	Any	Any	Any	2015-03-10	2015-03-10
Enabled	test-0310	Cisco SSH Denial of Service Vuln...	Any	10.70.33.12	Any	Any	2015-03-11	2015-04-05
Enabled	This is the test for Exception Name...	Cisco SSH Denial of Service Vuln...	Any	10.70.33.12	Any	Any	2015-03-11	2015-03-11
Enabled	This is the test for Exception Name...	CISCO IOS H.323 Protocol Impl...	Any	10.71.33.12	Any	Any	2015-03-11	2015-03-11

Page 1 of 1

Details Summary

Scan Name	IP	Port	Domain	Scan Date
IVS-MixTargetTypeRegressionTest	10.70.33.12	0		2015-03-06
IVS-MixTargetTypeRegressionTest	10.70.33.12	0		2015-03-06
IVS-MixTargetTypeRegressionTest	10.70.33.12	0		2015-03-06

Displaying 1 to 3 of 3

4.2.3 Asset Inventory

The Asset Inventory tab contains a list of all discovered hosts with host information such as open ports and service banners. The list can be sorted or filtered on IP, Domain, OS, or Ping Status, and exported in a variety of formats.

4.2.4 Targets

The Targets tab shows a list of the included and excluded targets for the scan.

4.2.5 Live Host Discovery

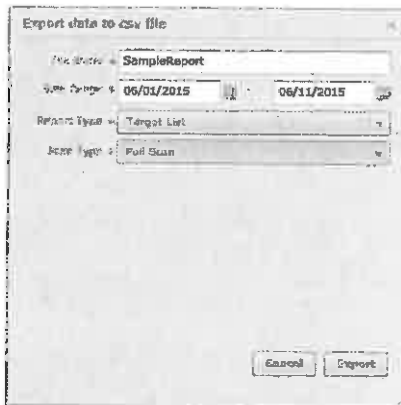
The Live Host Detection Discovery tab shows a list of targets that were detected, or not detected, during the scan. The full contents of this list can be exported to a CSV file. Limit the content of the export by performing a search prior to the export.

4.3 Report Files

This section of the main reports screen allows you to generate CSV data files containing details of scan results, disputes, or scan targets. The list shows files that have been requested.

To create a report file, click **New** . On the pop-up window:

1. Enter a name.
2. Select dates to report on.
3. Select a report type (Scan Results, Disputes, Target List, or Exceptions).
4. For reports on scan results or targets, enter a scan type. The Disputes and Exceptions types report on data from all relevant scan types.




5. Click **Export** to start generation of the file. You can check the status of the report in the list.

The result file includes a line for each scan that matches the criteria selected.



Note: If your role is Manager or Enterprise Manager (see Section 6), you can create reports that include data from one or more companies in the hierarchy. Before creating the report file, select a customer using the menu at the top right. The report will include results for the selected customer and all customers in the hierarchy beneath that customer. Each result line will show the customer name.

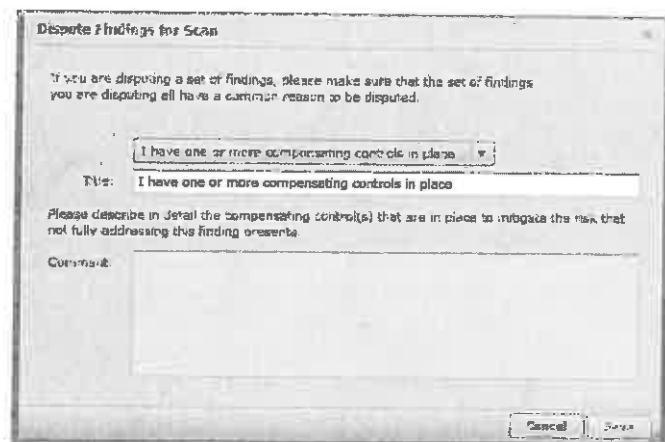
To **download a file** (if the status is COMPLETED), select the row and then click **Download** . The file downloads using File Transfer Manager as described in Section 1.1.4.

To **remove a file** from the list, select the row and then click **Delete** .

4.4 Disputes

Disputes apply to External PCI scans only. For other types of scans see Section 4.7, Exceptions.

Due to the nature of external vulnerability scanning and certain compliance requirements, there may be times when scan results report vulnerabilities that are incorrect or are not valid security risks because they are mitigated through technical or non-technical controls or processes. When these cases occur, you can dispute the finding using the **Dispute** button on the vulnerabilities list. Use the checkboxes to select one or more vulnerabilities to dispute, and then click the button. On the form that displays, enter a reason and comments. A support representative will review the information provided and help resolve the issue.



4.5 Bulk Disputes

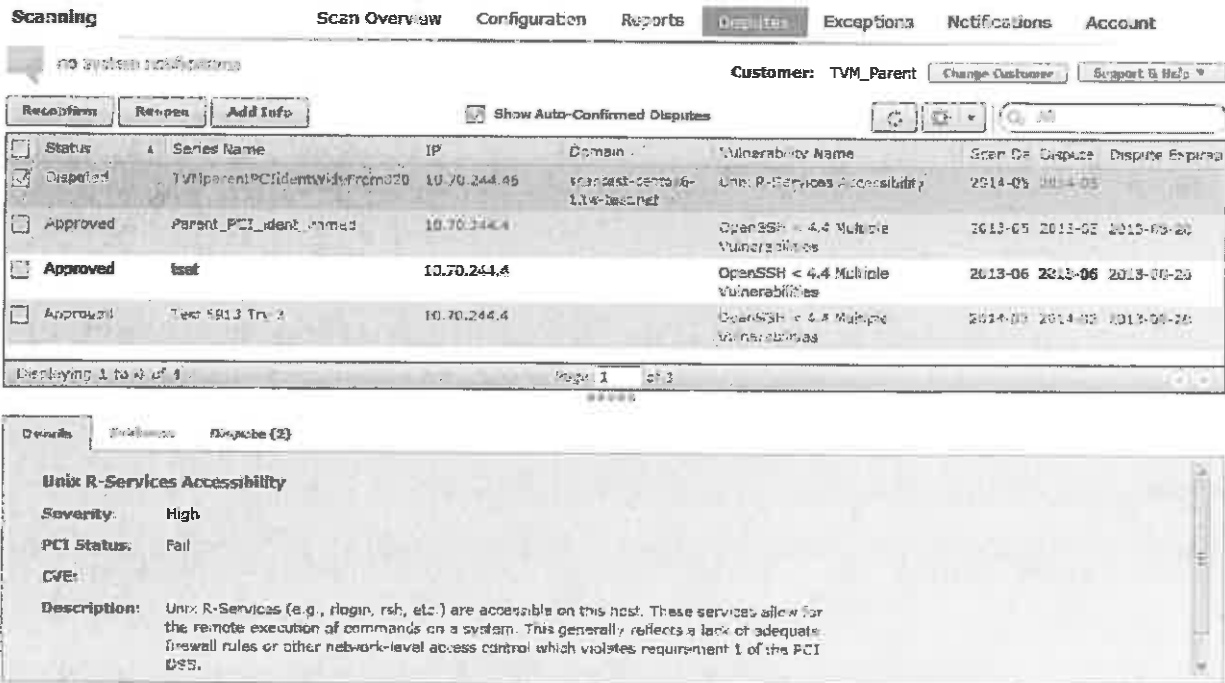
In addition to disputing a single finding, multiple vulnerability findings in a single scan can be selected and then disputed at the same time if they have the same dispute reason. For example, certain Linux operating systems patch software packages using a process called “backporting”. When software is “backported”, bugs, including security vulnerabilities, are fixed but the software banner version is not always updated. This frequently causes issues when detecting vulnerabilities remotely through vulnerability scanning. During scanning, if this occurs it generally results in a vulnerability finding being reported for all hosts that run that version of software when the test relies on the banner version. To ease the process of disputing these findings, multiple findings can be selected and disputed at once.

You can also apply a filter to the findings table to provide a list of specific vulnerabilities, such as “Apache 2.2 prior to 2.2.15 Multiple Vulnerabilities”, which can then be bulk disputed. To set a filter, enter the search terms in the filter box in the top right section of the vulnerability findings table.

4.6 Disputes Screen

The dispute management screen provides a view of all disputes and provides a way to reconfirm expiring disputes, reopen closed disputes, or add information for the Trustwave support team. For PCI scans, vulnerability disputes must be expired after 3 months. For non-PCI scans, disputes are automatically accepted.

Select a dispute to see details in a new section below the list.



The status of disputes can be one of the following:

- **Disputed:** The dispute request has been submitted but not yet reviewed by Trustwave
- **Need info:** The dispute has been reviewed and is currently denied. However, with additional information it will be reconsidered and is likely to be accepted.
- **Denied:** The dispute has been reviewed and rejected. The original vulnerability finding stands.
- **Approved:** The dispute has been reviewed and accepted.

Available actions on the Disputes screen include:

- **Reconfirm:** Request an extension of time for an approved dispute for the remote execution of commands on a system. This generally reflects a lack of adequate firewall rules or other network-level access control which violates requirement 1 of the PCI DSS.
- **Reopen:** Request reconsideration of a denied dispute
- **Add Info:** Provide additional information for a dispute that is currently in the Disputed or Need Info status.

4.7 Exceptions

Scan results may report vulnerabilities that are incorrect or are not valid security risks because they are mitigated through technical or non-technical controls or processes. When these cases occur in a non-PCI ASV scan, you can choose to make an Exception to the finding from the list on the Vulnerabilities tab of the scan results.

This functionality is available for the most recent scan in a series.

Scanning Scan Overview Configuration **Reports & Results** Disputes Exceptions Notifications Account

00 Results Notifications Customer: TVM_Parent Change Customer Support & Help

Parent_Full 2013-04-10 02:41:05

Summary Vulnerabilities **Asset Inventory** Targets Live Host Discov...

Status	IP	Domain	Vulnerability Name	Req...	Port	Sev...	CVE
<input type="checkbox"/> Excepted	10.70.24...		OpenSSH Duplicate Block Denial of Service Vulnerability	top	22	UNKNOW	CVE-200...
<input type="checkbox"/> Excepted	10.70.24...		OpenSSH - 4.4 Multiple Vulnerabilities	top	22	UNKNOW	CVE-200...
<input type="checkbox"/> Excepted	10.73.24...		OpenSSH Privilege Separation Monitor Weakness	top	22	UNKNOW	CVE-200...
<input type="checkbox"/>	10.70.24...		OpenSSH X11 Denial of Service via Authentication Process Vulnerability	top	22	UNKNOW	CVE-200...
<input type="checkbox"/>	10.70.24...		AJP (Apache JServ Protocol) Service Detected	top	8009	UNKNOW	
<input type="checkbox"/>	10.70.24...		OpenSSH X11 Session Hijacking Vulnerability	top	22	UNKNOW	CVE-200...
<input type="checkbox"/>	10.70.24...		Apache Tomcat Denial of Service via Slow HTTP Requests	top	8080	UNKNOW	CVE-201...

Use the checkboxes to select one or more vulnerabilities to be affected, and then click **Exception**. On the form that displays, enter the required information.

Vulnerability Exception

Exception Name:

Description:

Duration: Expiration Date Forever

Apply to: This one instance of this vulnerability for this one target (IP, Domain, URL) All instances of this vulnerability in THIS scan configuration All instances of this vulnerability in ALL subsequent scans (does not include currently running scans)

- **Exception Name:** A name that will enable you to recognize this exception in a listing.
- **Description:** Detailed information about the reason for the exception.
- **Duration:** Choose to maintain this exception for a limited time, or forever.



Tip: As security best practice, Trustwave recommends that you set a limited time and regularly review the need for each exception.

- **Apply to:** Choose to apply the exception to
 - A specific target (such as an IP address, domain, or URL depending on the vulnerability type)
 - All instances of the named vulnerability in this specific scan configuration
 - All instances of this vulnerability in this scan and all future scans in all configurations

Click **Save** to create the exception. The status * displays in the row(s) of the vulnerability listing, indicating that the exception will be applied.

Tips:



- All exceptions are applied to the current scan where you set the exception.
- Exceptions are applied to matching scans started after the exception was created. In many cases exceptions are applied to scans that are running when the exception is created, depending on the completion status of the running scans.
- Once the exception has been processed, the status of the vulnerability for this scan changes to **Excepted**.

You can manage exceptions on the Exceptions screen.



Note: If you selected more than one item, a separate exception will be created for EACH item. The names and other properties of all the exceptions created will be identical.

4.7.1 Exceptions Screen

The exception management screen shows a view of all exceptions and provides a way to enable or disable an exception, and change the name, description, and expiration of the exception.

Select an exception to see details in a new section below the list.

The status of exceptions can be one of the following:

- **Enabled:** The exception is applied to matching scans that start while the exception is enabled (and the date is within the duration specified).
- **Disabled:** The exception is not applied to any scans that start while the exception is disabled, regardless of the duration specified.

- **Deleted:** The exception will not be applied to any future scans and will not appear in the list of exceptions, unless the **Show Deleted Exceptions** box is checked. Deletion cannot be reversed.

Available actions on the Exceptions screen include:

- **Delete:** Delete one or more exceptions. Select the exceptions for this action using the checkboxes.



Note: Deleting an exception does not remove the exception from past scan findings.

- **Edit:** Change the name, description, or expiration of a specific exception. (You cannot change the Apply to section. Use "Clone" to apply an exception to a different set of scans.)
- **Disable:** Disable one or more enabled exceptions. Select the exceptions for this action using the checkboxes.
- **Enable:** Enable one or more disabled exceptions. Select the exceptions for this action using the checkboxes.
- **Clone:** Create a new exception using the settings of the selected exception as a base. You can use this feature to effectively change the "Apply to" section of an existing exception (create a clone and then delete or disable the original item).
- **Show Deleted Exceptions:** If this box is checked, the list includes deleted exceptions. Checking or unchecking the box refreshes the list.

The details section includes two tabs:

- **Details:** Shows a list of scan names, target details, and dates where the exception was applied.
- **Summary:** Shows the vulnerability name, exception name, and exception description.

4.8 PDF Reports

When a scan has completed, several different PDF reports can be generated from the Vulnerabilities tab.

Currently the following report types are supported, depending on the scan type:

- **Executive Summary:** A one-page summary of the scan, scan findings, trends, and top vulnerabilities.
- **PCI Report:** A report suitable for submitting for PCI compliance detailing all PCI violations.
- **Vulnerabilities by IP:** all vulnerabilities found for each IP address. A simple list with severity, CVSS, vulnerability name, CVEs, ports and services.
- **Vulnerabilities by Severity:** all vulnerabilities found, each listed once. A simple list with severity, CVSS, vulnerability name, IP addresses and port.
- **Full Vulnerability Report:** A complete vulnerability report containing an executive summary, scan inventory, Vulnerabilities & Policy Violations, Web Servers and Part 4 SSL Certificate Information, and any Disputed Vulnerabilities and Policy Violations.



Note: Report Status will first display as “In Progress”. When the report is ready the status changes to “Completed.” You can refresh the grid to update the status display, or simply return to the page later.

To generate a report, select the appropriate report type from the dropdown on the top left area of the vulnerability findings table, then select “Generate Report”.

4.9 Notifications

E-mail alert notifications can be sent instantly when certain scan events occur by selecting the notification checkboxes. When these are selected, email alerts will be sent for all scans.

Email notifications can be sent for one or more of the following actions:

- Scan Scheduled and Completed
- Status change for Disputes (information needed, accepted, declined)
- Dispute Expiration
- Scan Notification 1 hour prior to scan starting
- Scan Notification 24 hour prior to scan starting
- Scan Notification 48 hour prior to scan starting
- Scan Notification 72 hour prior to scan starting

By default, scan notifications are enabled for scan changes, 1 and 24 hours before the scan starts.

5 Reviewing Account Information

Click **Account** in the sub-menu to see information about your account.

The screenshot displays the 'Account' page in the Trustwave Vulnerability Management interface. At the top, there are navigation tabs: Scanning, Scan Overview, Configuration, Reports, Disputes, Exceptions, Notifications, and Account. A 'no system notifications' message is visible on the left. The main content area shows account details for 'TVM_Parent'.

Customer: TVM_Parent [Change Customer](#) [Support & Help](#)

Package: Basic PCI exp: 2016-03-02 Scans: Unlimited 250 (58 consumed)

Scanning Type: PCI Targets: 0 (0 consumed) 250 (18 consumed)

Internal External

System Users [Copy All Values](#)

Username	First Name	Last Name	Email	Company	Last Login	Disabled	Locked	Roles
Child_A	Child_A	int-b	Child_A@blah-b.cc	TVM_Child_A	2013-03-09 11:13			BASIC_USER
Child_B	Child_B	intb	Child_B@blah.com	TVM_Child_B	2013-03-09 11:13			BASIC_USER
GChild_A1	GChild_A1	intb	GChild_A1@blah.c	TVM_GChild_A1	2013-03-09 11:13			BASIC_USER
GChild_A2	GChild_A2	intb	GChild_A2@blah.c	TVM_GChild_A2	2013-03-09 11:13			BASIC_USER
GChild_B1	GChild_B1	intb	GChild_B1@blah.c	TVM_GChild_B1	2013-03-31 02:10			BASIC_USER
GChild_B2	GChild_B2	intb	GChild_B2@blah	TVM_GChild_B2	2013-03-09 11:28			BASIC_USER
Parent	Parent	int-b	Parent@blah-b.cor	TVM_Parent	2013-03-09 11:14			ENTERPRISE_MANAGE
TVM_Child_A	TVM_Child_A	intb	TVM_Child_A@intb	TVM_Child_A	2013-12-08 00:41			MANAGER_USER
TVM_Child_B	TVM_Child_B	int-b	TVM_Child_B@intb	TVM_Child_B	2013-08-15 03:14			MANAGER_USER
TVM_GChild_A1	TVM_GChild_A1	int-b	TVM_GChild_A1@intb	TVM_GChild_A1	2013-08-23 08:47			BASIC_USER
TVM_GChild_A2	TVM_GChild_A2	intb	TVM_GChild_A2@intb	TVM_GChild_A2	2013-08-22 06:18			BASIC_USER
TVM_GChild_B1	TVM_GChild_B1	intb	TVM_GChild_B1@intb	TVM_GChild_B1	2014-03-24 10:30			MANAGER_USER

The box at the top of this screen shows the customer information, including details of the package and expiration, and the scans available and consumed.

The **System Users** box includes details of users in the enterprise hierarchy, and their roles. This feature allows users from the higher levels of the organization to have an overview of the users and roles for all entities set up under them. Users at lower levels do not see information about the entities above them. For more details of the enterprise features, see the next section.

6 Managing Scans for the Enterprise

A customer using TVM can request Trustwave to set up a hierarchy of views for child companies. The hierarchy can have up to four levels.

Logins can be created with any one of three roles, known as Enterprise Manager, Manager, and User. This feature allows users from the higher levels of the organization to have an overview of the scans for all entities set up under them, while allowing the other entities to set up and review only their own scans.

In addition to the three roles, TVM provides for each role to have either read only or read/write access.

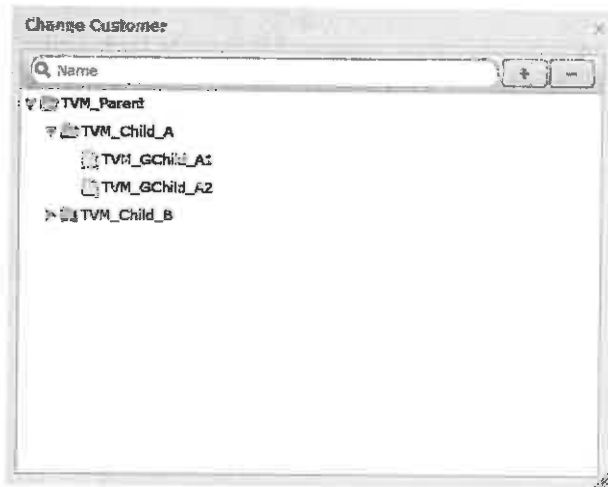
Hierarchy Rules

- A person can be assigned to only one company.
- A login with the Enterprise Manager role can see ALL companies in the hierarchy, regardless of what company their user account is in.
- A login with the Enterprise Manager role can manage global port exclusions for scans (exclusions do not apply to External PCI scans). Exclusions apply to a specific customer company and not to the entire hierarchy.
- A login with the Manager role can have access to more than one company, defined by the company hierarchy structure. Any company 'below' the one in which they are a user is accessible. For example, in the list shown below, a Manager in TVM_Child_A would also see scans created for TVM_GChild_A1 and TVM_GChild_A2.
- A login with the User role would *never* have access to a company other than the one in which they are a user. For example, in the list shown below, a User in TVM_Parent would have access only to scans created for TVM_Parent.
- For each role there are two access levels available: read/write [full] or read only.
- The company hierarchy can be up to 4 layers deep, after which it becomes too difficult to manage.

If your login is set up as an Enterprise Manager or Manager, at the top right of the screen you will see the name of the Customer currently shown, and a Change Customer button:

Customer: TVM_Parent

Click **Change Customer** to view the list of customer names available to you:



You can filter entries by name. You can expand or collapse the entire hierarchy using the + and – buttons. You can expand or collapse a branch using the arrow for that branch. To select a customer, click that name.

About Trustwave

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations—ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide. For more information, visit <https://www.trustwave.com>.