Retina Network Security Scanner

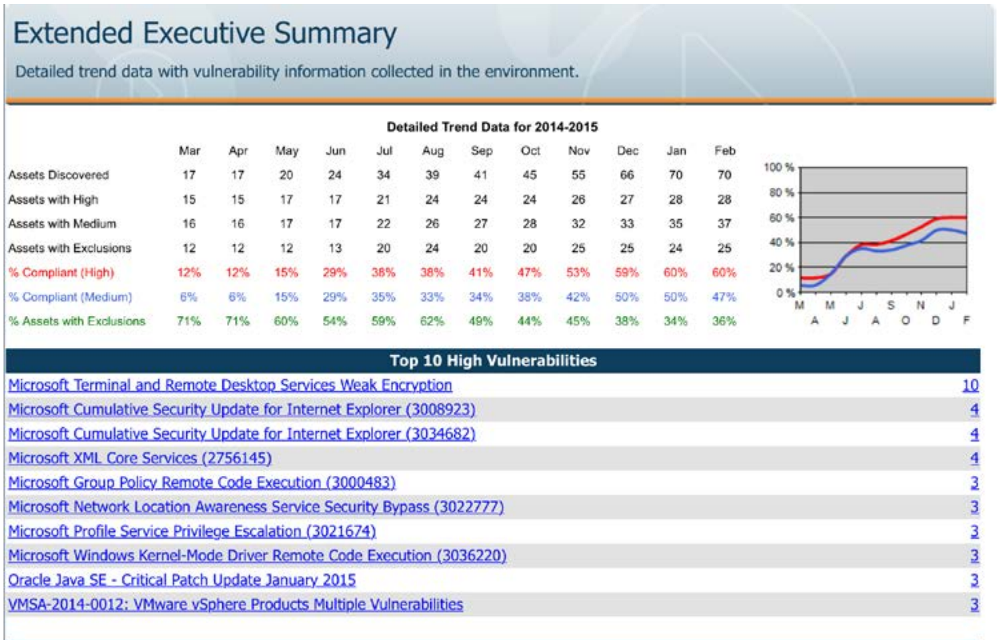
Integrated Network, Web, Database and Virtual Vulnerabilty Assessment

BeyondTrust™
VISIBILITY. KNOWLEDGE. ACTION.

With over 10,000 deployments since 1998, BeyondTrust® Retina® Network Security Scanner is the most sophisticated vulnerability assessment solution on the market. Available as a standalone application or as part of the Retina CS unified vulnerability management platform, Retina Network Security Scanner enables you to efficiently identify IT exposures and prioritize remediation enterprise-wide.

- Discover all network (local and remote), web, database and virtual assets in your environment
- Reveal at-risk personally identifiable information (PII) and other sensitive data
- Identify system, application, database, OS and web application vulnerabilities via agent-based and/or agentless scanning
- Assess risk and prioritize remediation based on exploitability (from Core Impact®, Metasploit®, Exploit-db), CVSS and other factors
- Confirm exploitability through penetration testing, with one click to the Metasploit Framework
- Report progress and results to management, compliance, audit, risk and other roles
- Analyze threats and gain security intelligence through the optional Retina CS vulnerability management console
- Share data with popular solutions for SIEM, GRC and other security management platforms

> "The Retina vulnerability management solution identified vulnerable computers, servers, printers, video encoders, and access control systems, while providing informative reports that made remediation possible. Retina significantly improves network security, facilitates security compliance, and continues to be an important tool in the enterprise."
>
> — Network Management Director California Dept of Transportation



Extended Executive Summary

Detailed trend data with vulnerability information collected in the environment.

Detailed Trend Data for 2014-2015

	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb
Assets Discovered	17	17	20	24	34	39	41	45	55	66	70	70
Assets with High	15	15	17	17	21	24	24	24	26	27	28	28
Assets with Medium	16	16	17	17	22	26	27	28	32	33	35	37
Assets with Exclusions	12	12	12	13	20	24	20	20	25	25	24	25
% Compliant (High)	12%	12%	15%	29%	38%	38%	41%	47%	53%	59%	60%	60%
% Compliant (Medium)	6%	6%	15%	29%	35%	33%	34%	38%	42%	50%	50%	47%
% Assets with Exclusions	71%	71%	60%	54%	59%	62%	49%	44%	45%	38%	34%	36%

Top 10 High Vulnerabilities

Microsoft Terminal and Remote Desktop Services Weak Encryption	10
Microsoft Cumulative Security Update for Internet Explorer (3008923)	4
Microsoft Cumulative Security Update for Internet Explorer (3034682)	4
Microsoft XML Core Services (2756145)	4
Microsoft Group Policy Remote Code Execution (3000483)	3
Microsoft Network Location Awareness Service Security Bypass (3022777)	3
Microsoft Profile Service Privilege Escalation (3021674)	3
Microsoft Windows Kernel-Mode Driver Remote Code Execution (3036220)	3
Oracle Java SE - Critical Patch Update January 2015	3
VMSA-2014-0012: VMware vSphere Products Multiple Vulnerabilities	3

The executive summary is one of several Retina reports that make it easy to identify, understand and act on critical vulnerabilities in your environment.

Key Capabilities

- **Discover** all network (local and remote), web and virtual assets in your environment.
- **Reveal** at-risk personally identifiable information and other sensitive data.
- **Identify** system, application, database, OS and web application vulnerabilities via agent-based and/or agentless scanning.
- **Assess** risk and prioritize remediation based on exploitability (from Core Impact®, Metasploit®, Exploit-db), CVSS, & other factors.
- **Confirm** exploitability through penetration testing, with one click to the open-source Metasploit Framework
- **Audit** personally Identifiable Information (PII) on remote targets.
- **Report** progress and results to colleagues in management, compliance, audit, risk and other roles.
- **Analyze** threats and gain deeper security intelligence by upgrading to Retina CS Enterprise Vulnerability Management.
- **Share** data with popular solutions for SIEM, GRC and other security management platforms.

Why Retina?

VULNERABILITY SCANNING THAT IS FAST AND NON-INTRUSIVE

Retina Network Security Scanner optimizes network performance and scan network devices, operating systems, applications, and databases, without impacting availability or performance.

THE MOST COMPREHENSIVE VULNERABILITY DATABASE

The Retina vulnerability database is continually updated by the renowned BeyondTrust Research Team, allowing you to stay on top of the most current threats and vulnerabilities.

SCALABLE VULNERABILITY ASSESSMENT DEPLOYMENTS

Retina can be deployed as a standalone vulnerability scanner, distributed throughout an environment, and integrated with Retina CS for enterprise deployments.

FLEXIBLE LICENSING, UNLIMITED IPS FOR ONE LOW PRICE

Retina licensing is flexible to cost-effectively meet your specific vulnerability assessment needs. A full-featured, unlimited IP, unlimited user version is available for one low price.

CONTACT

North America
Tel: 800.234.9072 or 480.405.9131
info@beyondtrust.com

EMEA
Tel: +44 (0)1133 970445
emeainfo@beyondtrust.com

APAC
Tel: +65 6701 8267
apacinfo@beyondtrust.com

CONNECT

Twitter: @beyondtrust
Facebook.com/beyondtrust
Linkedin.com/company/beyondtrust
www.beyondtrust.com

Comprehensive Vulnerability Assessment Across Threat Vectors

NETWORK SYSTEMS

- Assess network devices, operating systems, applications, ports and services against a vast, constantly updated vulnerability database
- Accurately identify vulnerabilities with a false positive rate below 1%
- Perform Class C network scans in under 15 minutes on average
- Leverage ICMP, registry, NetBIOS, and the Nmap signature database, as well as proprietaryOS fingerprinting capabilities
- Audit Windows devices using local or domain credentials
- Perform local assessments of Cisco®, Linux, Unix® and other devices via SSH tunneling
- Adjust scans for custom machine configurations, ports and applications via automated input/output data reconciliation on each port
- Support SCAP-compliant, continuous vulnerability and configuration monitoring per DIACAP, FISMA, STIG, FDCC and USGCB guidelines
- Get PCI DSS scanning and reporting capabilities out of the box

WEB APPLICATIONS

- Conduct automated vulnerability assessment and web crawling with no scripting required
- Detect OWASP Top Ten vulnerabilities including SQL Injection, Cross-Site Scripting, Cross-Site Request Forgery, OS Command Injection and more
- Fully integrated into the Retina assessment engine Databases
- Scan Oracle®, Microsoft SQL Server® and MySQL databases for security exposures Virtual Environments
- Conduct VMware vCenter® scans with detailed risk intelligence for ESXi and virtual machines
- Scan online & offline virtual images, plus virtualized application templates (ThinApp® packages)
- Schedule scans to automatically update the vCenter console with centralized compliance and risk information
- Stay updated on new vulnerabilities that could impact the hyper-visor and virtual machines

DATABASES

- Scan Oracle®, Microsoft SQL Server® and MySQL databases for security exposures

VIRTUAL ENVIRONMENTS

- Conduct VMware vCenter® scans with detailed risk intelligence for ESXi and virtual machines
- Scan online & offline virtual images, plus virtualized application templates (ThinApp® packages)
- Schedule scans to automatically update the vCenter console with centralized compliance and risk information
- Stay updated on new vulnerabilities that could impact the hyper-visor and virtual machines

Since 1998, Retina vulnerability management solutions have provided customers with threat and risk information in real business context. Over 10,000 customers worldwide employ Retina to efficiently mitigate existing exposures and effectively secure against future threats.