Retina Protection Agent

Local Vulnerability Assessment for Complete Security and Visibility

BeyondTrust™
VISIBILITY. KNOWLEDGE. ACTION.

You have a complex IT environment. A one-size-fits-all approach to security won't keep everything completely safe. Remote vulnerability assessment will protect most systems, but what about those blocked by firewalls or segregated from the network? What about mobile and offline devices? These are potential gaps that could be exploited. For truly complete security, you need remote vulnerability assessment as well as local assessment. And, you need full visibility into the combined results of all scans to sustain a solid security posture.

Meet the Retina Protection Agent (RPA)

A lightweight agent that augments Retina CS Enterprise Vulnerability Management's remote vulnerability assessment with local vulnerability assessment capabilities. This simple tool eases the burden of meeting even the most stringent regulatory compliance, reduces security risks, and improves overall security across your environment.

AN ADDED LAYER OF PROTECTION

Zero-day vulnerabilities aren't slowing down and hackers have gotten smarter about how to enter your network via the desktop. With Retina Protection Agents, you get an additional layer of protection with continuous zero-day vulnerability monitoring and intrusion prevention.

ACCURATE ASSET DISCOVERY AND INVENTORY

Retina discovers all the assets on a given network, including operating systems, applications, services, databases and wireless devices. Retina's advanced OS discovery utilizes ICMP, registry, NetBIOS, and the Nmap signature database, as well as BeyondTrust's proprietary OS fingerprinting for more accurate and definitive OS identification.

WEB APPLICATION AND DATABASE SCANNING

Retina provides industry leading vulnerability assessment, unified configuration and vulnerability scanning across network devices, operating systems, applications, databases, and web applications using a scalable, non-intrusive approach.

> "Retina significantly improved network security, facilitates security compliance, and continues to be an important solution in the enterprise."
>
> — Network Management Director
> California Dept of Transportation

MITIGATION ASSESSMENT

Retina allows prioritized mitigation through its intuitive user interface, categorizing vulnerabilities according to risk level. Integration with third party help desk and ticketing systems is a simple process. Additionally, Retina's Fix-It function can be used to remotely correct security issues such as registry settings, file permissions, and more.

LOCALIZED SYSTEM AUDITS

Auditing of non-Windows devices includes SSH tunneling to perform local vulnerability assessment of Unix, Linux, Cisco, and other devices. This allows security professionals to identify vulnerabilities on non-Windows devices that need local file or setting checks.

Key Capabilities

LOCAL VULNERABILITY ASSESSMENT

Provides local vulnerability assessment capabilities to close the gap created by systems that can't be reached with a remote vulnerability assessment alone.

ZERO-DAY PROTECTION AND INTRUSION PREVENTION

Provides zero-day protection where a vendor has not yet created signatures or patches to protect against vulnerabilities in their operating system or application.

STORAGE PROTECTION

Prevents data leakage by regulating usage of USB and Firewire storage devices, helping demonstrate institutional control for highly-regulated organizations.

CENTRALIZED VISIBILITY

Provides full visibility into both remote and local vulnerabilities through the Retina CS Management Console and the integrated Retina Insight Threat Intelligence Module.

About Retina CS

The Retina Protection Agent is included with Retina CS Enterprise Vulnerability Management.

Retina CS is the only vulnerability management software solution designed from the ground up to provide organizations with context-aware vulnerability assessment and risk analysis. Retina's results-oriented architecture works with users to proactively identify security exposures, analyze business impact, and plan and conduct remediation across disparate and heterogeneous infrastructure.

Retina CS Enterprise Vulnerability Management software enables you to:

- Discover network, web, mobile, cloud and virtual infrastructure
- Profile asset configuration and risk potential
- Pinpoint vulnerabilities, malware and attacks
- Analyze threat potential and return on remediation
- Remediate vulnerabilities via integrated patch management (optional)
- Report on vulnerabilities, compliance, benchmarks, etc.
- Protect endpoints against client-side attacks

SMART PROTOCOL SCANNING

Retina reconciles the input/output data on each port to determine which protocols and services are running, including SSL. In this way, Retina makes adjustments for custom or unconventional machine setup.

ADVANCED SCHEDULING CAPABILITIES

Retina's scheduler function allows you to set the scanner to run on a regular basis to periodically check for vulnerabilities. Because Retina is non-intrusive, you can pre-schedule your scans without the risk of unplanned network downtime.

CONTACT

North America
Tel: 800.234.9072 or 818.575.4000
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