Retina Network Security Scanner

Integrated Network, Database and Virtual Vulnerability Assessment

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 enterprise vulnerability management solution, Retina Network Security Scanner enables you to efficiently identify IT exposures and prioritize remediation enterprise-wide.

- **Key Capabilities**
  - Discover all network (local and remote), database, virtual and IoT assets in your environment.
  - Scan network assets as well as web applications, providing a complete picture of vulnerabilities in a single console.
  - 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 (Core Impact®, Metasploit®, Exploit-db, CANVAS), CVSS v3, CWE and other factors.
  - Automatically selects the credentials with the highest level of privileges on each scan target when multiple scan credentials are provided.
  - 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 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

---

**Top 5 Vulnerable Hosts**

**Num. of Vulnerabilities by Risk**

**% of Vulnerabilities by Risk**

**Avg. of Vulnerabilities by Risk**

The Executive Report is one of many Retina reports that make it easy to get an overview of your network and its vulnerabilities.
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.

Comprehensive Vulnerability Assessment Across Threat Vectors

NETWORK SYSTEMS

- Assess network devices, operating systems, applications, ports and services against a vast, constantly updated vulnerability database
- Identify vulnerable IoT devices, and safely check them for default and hard-coded credentials used with Telnet, SSH, or Basic HTTP Authentication
- 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 proprietary OS 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 3.0 scanning and reporting capabilities out of the box
- Achieve complete vulnerability and configuration scanning across IPv4 and IPv6 networks
- Simplify ad-hoc scanning with single use target types entered as IP address, IP ranges, CIDR, named host or a combination of any of those types

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
- Retina provides the user interface for launching web scans and displaying a Web Assessment Report that contains findings from those scans

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.