

Retina CS Enterprise Vulnerability Management

Intelligently Identify, Prioritize and Remediate System Vulnerabilities Across Diverse IT Environments

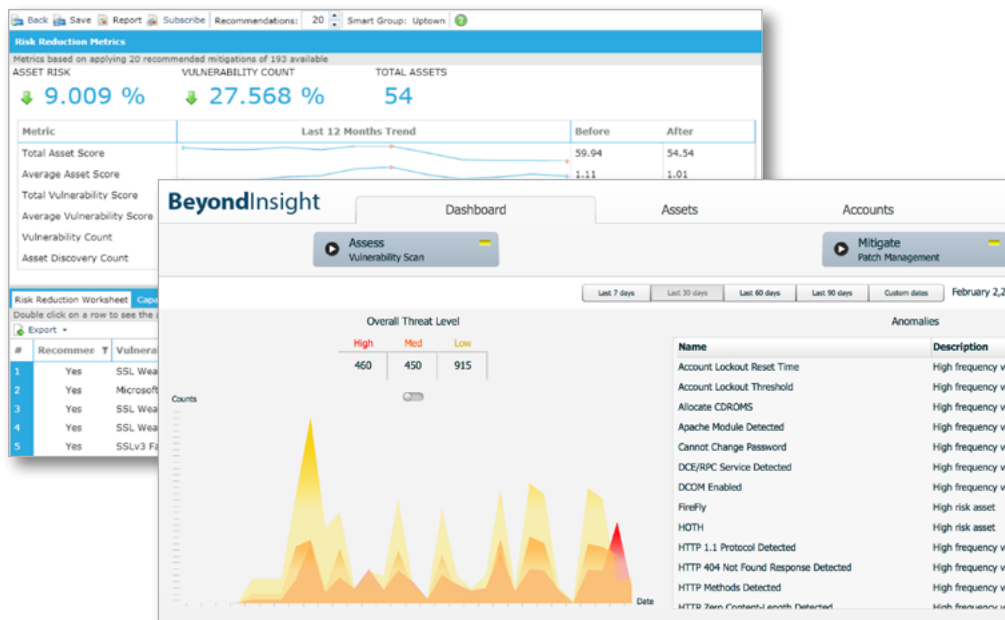


Most vulnerability management solutions do little to help security leaders put vulnerability and risk information in the context of business. Saddled with volumes of rigid data and static reports, the security team is left to manually discern real threats and determine how to act upon them. At BeyondTrust, we believe that security professionals deserve more from their vulnerability management solutions. That's why we deliver vulnerability data in the proper context.

Retina CS: The Context-Aware Vulnerability Management Solution

BeyondTrust® Retina CS is the only vulnerability management solution designed from the ground up to provide organizations with context-aware vulnerability assessment and risk analysis. Retina's results-driven architecture works with users to proactively identify security exposures, analyze business impact, and plan and conduct remediation across network, web, mobile, cloud, virtual, and IoT infrastructure.

- **Discover** network, web, mobile, cloud, virtual, and IoT infrastructure.
- **Profile** asset configuration and risk potential.
- **Pinpoint** vulnerabilities, malware and attacks.
- **Analyze** threat potential, return on remediation and more.
- **Isolate** high-risk assets through advanced threat analytics.
- **Remediate** vulnerabilities through integrated patch management.
- **Report** on vulnerabilities, compliance, benchmarks, etc.
- **Protect** endpoints against client-side attacks.



Retina CS enables you to understand and prioritize risk in the context of your business via the centralized BeyondInsight management, reporting and analytics console.

Key Capabilities

ZERO-GAP COVERAGE

Able to discover and assess any IT resource, Retina CS offers zero-gap coverage of the largest, most diverse IT environments. Agentless and agent-based scanning protects both online and offline assets.

UNMATCHED REPORTING

With the most powerful reporting capabilities in its class, Retina CS makes it easy to make smarter decisions, communicate risk, and report remediation progress to executives and compliance auditors.

ADVANCED THREAT ANALYTICS

With BeyondInsight Clarity, Retina CS discovers data breach threats typically missed by other vulnerability solutions. Clarity pinpoints specific, high-risk users and assets by correlating privilege, vulnerability and threat data from a variety of BeyondTrust and third-party solutions.

AUTOMATED CREDENTIALLED SCANS

Together with BeyondTrust PowerBroker Password Safe, Retina CS provides a secure and automated solution for performing authenticated scans with continuously rotating privileged credentials.

EXTENSIVE COMPLIANCE COVERAGE

Reporting for COBIT, GLBA, HIPAA, HITRUST, ISO, ITIL, NERC-FERC, NIST, PCI, SOX, and many more government & industry regulations.

ENTERPRISE SCALABILITY AND FLEXIBILITY

Retina's multi-tier architecture is designed for simple deployment and management of networks with multiple firewalls, IDS/IPS, VLANs and disparate locations.



BeyondInsight Threat and Vulnerability Intelligence

Retina CS is part of BeyondInsight Threat and Vulnerability Intelligence, which provides centralized management, policy, reporting, and analytics for BeyondTrust PowerBroker privileged access management and Retina vulnerability management solutions. Capabilities include:

- Centralized solution management and control via common dashboards
- Asset discovery, profiling and grouping
- Reporting and analytics
- Workflow and ticketing
- Data sharing between Retina and PowerBroker solutions

With BeyondInsight, IT and Security teams have a single console through which to view user and asset risk.

CONTACT

North America
info@beyondtrust.com

EMEA
emeainfo@beyondtrust.com

APAC
apacinfo@beyondtrust.com

LATAM
latam@beyondtrust.com

CONNECT

Twitter: [@beyondtrust](https://twitter.com/beyondtrust)
[Linkedin.com/company/beyondtrust](https://www.linkedin.com/company/beyondtrust)
[Facebook.com/beyondtrust](https://www.facebook.com/beyondtrust)
www.beyondtrust.com

© 2017 BeyondTrust Corporation. All rights reserved. BeyondTrust and PowerBroker are trademarks of BeyondTrust in the United States and other countries. Microsoft, Windows, and other marks are the trademarks of their respective owners. February 2017

UNMATCHED REPORTING & ANALYTICS

- **Results-Driven Architecture**
Tailor scans to specific reporting and compliance requirements.
- **Advanced Threat Analytics**
Detect critical threats thru volumes of data.
- **Resource Planning**
Run what-if scenarios and team capacity analyses to plan resource allocation.
- **270+ Actionable Reports**
Communicate with technical and non-technical audiences.
- **Compliance Reporting**
COBIT, GLBA, HIPAA, HITRUST, ISO-27002, ITIL, MASS 201, NERC-FERC, NIST, PCI, SOX and more.
- **Advanced Threat Intelligence**
Based on asset scoring, security research, exploit databases, exploitability, NSRL, CVSS v3, CWE, and more.
- **Trends, Deltas and Heat Maps**
Share progress with executives, compliance auditors and others.
- **Configuration Benchmarking**
DISA Gold Disk, SCAP, NIST, FDCC, USGCB, CIS, Microsoft®, and in-house policies; CIS Security Benchmark certified (optional).
- **SLA Compliance Reports**
Measure threat severity level against dynamic asset groupings.
- **Pivot Grid Ad-Hoc Reporting**
Create custom reports.
- **Third-Party Integration**
SIEM, GRC, NMS and help desk integration

MAXIMUM FLEXIBILITY

- **Flexible Deployment**
Deploy software, appliances and/or virtual machines.
- **Centralized Dashboards**
Consolidate enterprise-wide activities.
- **Integrated Data Warehouse**
Analyze historical data over time.
- **Role-Based Access**
Provide permissioned access to view, assess and report on data.
- **Effortless Updates and Upgrades**
Expand capabilities via license updates.

ZERO-GAP COVERAGE

- **Vulnerability Assessment**
Flag vulnerabilities, attacks, and malware by asset for a complete view of risk.
- **Comprehensive Discovery**
Locate network (local and remote), web, mobile, cloud, virtual and IoT assets.
- **Asset Profiling**
Gather information including IP, DNS, OS, MAC address, ports, services, software, processes, hardware, event logs and more.
- **Asset Smart Groups**
Group, assess, and report on assets by IP range, naming convention, OS, domain, applications, business function and more.
- **Asset Context Awareness**
Evaluate risk based on damage potential or target distribution, plus confidentiality, integrity and availability requirements.
- **Smart Credentials**
Automatically scan targets using the highest privilege level.
- **Asset Risk Analysis**
Compare asset risk levels with custom Threat Risk and Exposure Risk scoring.
- **Cloud Scanning**
Scan online & offline Amazon®, GoGrid®, Google®, IBM®, Rackspace® & VMware®.
- **VMware Verified**
Scan virtual environments requiring PCI and HIPAA compliance.
- **Patch Management**
Remediate with patch management for Microsoft WSUS and SCCM for Microsoft and third-party applications.
- **Scheduling and Alerts**
Schedule scans and configure email alerts.

ENTERPRISE SCALABILITY

- **N-Tier, Multitenant Architecture**
Gain maximum scalability and control.
- **Scan Engine Pooling**
Combine scan engines, each able to scan a Class-A network in under 15 minutes.
- **Retina Protection Agent**
Local scanning, zero-day monitoring, and intrusion prevention for offline devices.
- **Local and Remote Scanning**
Cover segregated, firewalled and disparate infrastructure.