



VISIBILITY. KNOWLEDGE. ACTION.

# Retina CS Enterprise Vulnerability Management Manifesto

# Table of Contents

- Security Professionals Deserve More from Their Vulnerability Management Solutions..... 3
- Introducing Retina CS Enterprise Vulnerability Management: ..... 3
- Results-Driven Reporting and Analytics: The Secret to Relevant and Actionable Vulnerability Management ..... 4
  - Benefits ..... 4
  - Key Features ..... 4
- Unmatched Scalability, Flexibility and Performance for Large Enterprises..... 5
- Zero-Gap Vulnerability Management for Diverse IT Environments..... 6
  - Key Features ..... 6
  - Assessment Coverage ..... 7
- Retina CS and the BeyondInsight IT Risk Management Platform: Truly Unified Vulnerability Management ..... 8
  - The BeyondInsight Family of Vulnerability Management Solutions ..... 8
- Our Focus: Providing Customers with the Best Vulnerability Management Solutions and the Highest Level of Service ..... 9

# Security Professionals Deserve More from Their Vulnerability Management Solutions

Vulnerability management programs make up the front lines of risk reduction for security-conscious organizations worldwide. However, despite widespread deployment of vulnerability management technologies, many security professionals still struggle to decide how best to protect their organizations, achieve compliance, and communicate risk enterprise-wide.

The fact is, 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 data in the proper context:

- Results-driven reporting and analytics that provide relevant and actionable data to multiple stakeholders throughout the organization
- Enterprise-class scalability, flexibility and performance from software and appliances with the industry's simplest licensing model
- Zero-gap coverage of all devices enterprise-wide, including network, web, mobile, cloud and virtual infrastructure
- A unified solutions platform addressing all phases of vulnerability management – from assessment and remediation, to endpoint protection and privileged identity management
- A clear focus on providing customers with market-leading vulnerability management solutions that identify and mitigate threats to users and assets

## Introducing Retina CS Enterprise Vulnerability Management: A BeyondInsight™ IT Risk Management Platform Solution

Retina CS from BeyondTrust is the only vulnerability management solution designed from the ground up to provide IT security professionals 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 and virtual infrastructure.

Retina CS is part of the BeyondInsight IT Risk Management Platform, which unifies Retina's vulnerability management capabilities with BeyondTrust's PowerBroker® solutions for privileged account management. BeyondInsight fuses Retina's asset security intelligence with user security intelligence from a variety of PowerBroker solutions, providing Security and IT teams with a single, contextual lens through which to view and manage risk. Retina CS also benefits from BeyondInsight's centralized reporting and analytics platform, which provides IT and business leaders with visibility into

the real risks facing their organizations, while demonstrating the efficacy of risk reduction efforts enterprise-wide.

Built to scale and perform in large environments, Retina CS provides centralized command and control over assessments of disparate and heterogeneous infrastructure. Over 10,000 customers worldwide rely on Retina solutions to enable visible, measurable and actionable vulnerability management across their organizations.

## Results-Driven Reporting and Analytics: The Secret to Relevant and Actionable Vulnerability Management

Maintaining information security requires the involvement of several people across the organization, from security and IT operations professionals to end users and executives – each of whom consumes and understands data in different ways. Therefore, the relevancy and usefulness of vulnerability management data to different audiences can ultimately mean the difference between remaining secure and suffering a breach.

Retina CS leverages the BeyondInsight platform's results-driven reporting and analytics capabilities to bring risk into focus enterprise-wide. Using an intuitive dashboard interface, you simply indicate the type of information you need, such as an SLA report or a HIPAA compliance report, and define the business context of your assets. BeyondInsight then delivers customized, relevant and actionable data in a wide variety of report formats. This allows you to deliver the right information, in the proper context, to the people responsible for measuring and mitigating risk in your organization.

### Benefits

---

- **Determine** what to fix first, what to fix next – and why
- **Prioritize** the people, processes, and technology needed to address exposures
- **Predict** the return on remediation efforts prior to committing resources
- **Measure** the efficacy of vulnerability management processes over time
- **Share** results and data in terms and formats relevant to specific audiences

### Key Features

---

- **Results-Driven Architecture** – start by specifying what you want to accomplish, such as generating a PCI compliance report or analyzing vulnerability trends for the year
- **Intelligent Analytics** – drive decision-making by running what-if scenarios and analyzing security team capacity to achieve the greatest risk reduction benefits
- **Interactive Results** – fluidly interact with assessment results to hone in on data pertaining to a specific audience or business goal

- **260+ Actionable Reports** – quickly generate security, audit and compliance reports for technical and non-technical audiences alike
- **Compliance Reporting** – measure adherence to COBIT, GLBA, HIPAA, HITRUST, ISO-27002, ITIL, MASS 201, NERC-FERC, NIST, PCI, SOX, and more
- **Advanced Threat Intelligence** – gauge threat severity based on asset scoring, BeyondTrust malware and exploit research, exploit databases, exploitability indices, CVSS (base, temporal and environmental metrics), and more
- **Trending, Deltas, Threat Analyzers and Heat Maps** – share vulnerability management progress with executives, compliance auditors, and others
- **Configuration Benchmarking** – use an SCAP-certified engine to scan against benchmarks including DISA Gold Disk, SCAP, NIST, FDCC, USGCB, and Microsoft security compliance; customize standard images to match your in-house policies
- **SLA Reporting** – measure Service Level Agreement (SLA) compliance by threat severity level against dynamic asset groupings
- **Pivot Grid Ad-Hoc Reporting** – meet unique business requirements by creating customized reports using virtually any collected by Retina
- **Third- Party Integration** – share Retina data with leading SIEM, GRC, NMS and help desk solutions

## Unmatched Scalability, Flexibility and Performance for Large Enterprises

BeyondInsight's multi-tier architecture gives you optimal scalability and maximum control over Retina's enterprise vulnerability management capabilities. You can securely conduct scans across dispersed, heterogeneous environments with maximum performance and minimum service interruption. The product is architected for simple deployment and management of networks with multiple firewalls, IDS/IPS, VLANS and disparate locations.

- **Flexible Deployment Options** – deploy as software, appliances, virtual machines, or a combination of all three – without registering IP addresses
- **N-Tier, Multitenant Architecture** – ensure maximum scalability and gain centralized control over your vulnerability management environment
- **Role-Based Access** – provide individual users with permissioned access to view, assess and report on data associated with assigned asset groups
- **Centralized Dashboards** – consolidate, interact with, and report on data and analytics gathered from enterprise-wide vulnerability management activities
- **Scanner Pooling** – direct multiple scanner instances to collaboratively assess large environments with maximum performance
- **Integrated Data Warehouse** – view, sort and filter historical data to gain multiple perspectives for specific audiences or business goals

- **Modern User Interface** – interact seamlessly with massive amounts of data using a modern, web interface
- **Local and Remote Scanning** – ensure comprehensive coverage of segregated, firewalled, and otherwise disparate infrastructure, including support for air-gapped networks and non-network-based assets using agent and network scanning technologies
- **Effortless Updates and Upgrades** – expand capabilities through license key updates – no re-architecting, no re-installing, and no additional appliances required to add modules and capabilities
- **Patch Management** – remediate vulnerabilities with the only enterprise-class vulnerability assessment platform to offer on-board patch management for Microsoft and third-party applications

## Zero-Gap Vulnerability Management for Diverse IT Environments

Retina CS Enterprise Vulnerability Management offers zero-gap coverage of the largest, most diverse IT environments. The solution can discover and assess any IT resource in your organization, including network, web, mobile, cloud and virtual infrastructure.

### Key Features

---

- **Comprehensive Discovery** – locate known and previously unknown assets across network (local and remote), web, mobile, cloud and virtual environments
- **Asset Profiling** – gather information including IP, DNS, OS, Mac address, ports, services, software, processes, hardware, event logs, and more
- **Asset Smart Groups** – logically group, assess, and report on assets according to IP range, naming convention, operating system, domain, applications, business function, Active Directory, and more
- **Asset Context Awareness** – understand Smart Group value and risk based on collateral damage potential or target distribution, as well as confidentiality, integrity and availability requirements
- **Vulnerability Assessment** – flag vulnerabilities, attacks, and malware by asset for a complete view of a device's risk
- **Unmatched Reporting and Analytics** – tap into Retina's central data warehouse for targeted reports on vulnerabilities, regulatory compliance, benchmarks, threat analytics, what-if scenarios, SLA compliance, resource requirements, and more
- **User Risk Discovery** – map vulnerability management data to PowerBroker privileged account management data to reveal user-triggered risk and vulnerabilities within applications as users are actually executing them
- **Patch Management** – directly apply patches using extensive integration with Microsoft WSUS and SCCM for Microsoft and third-party applications
- **Scheduling and Alerts** – schedule assessments to run automatically and configure email alerts for a variety of scenarios, such as when reports are ready or when critical vulnerabilities have been found

- **Role-Based Access** – import from Active Directory or set custom permissions within Retina to allow users to see only the data and functions for which they are responsible
- **Third-Party Integration** – easily share data with help desks, GRC solutions, network management solutions, and a wide variety of SIEMs

## Assessment Coverage

---

Each of the following vectors includes integrated Retina vulnerability assessment, reporting, ticketing and real-time alerts – all managed through the BeyondInsight platform’s centralized console.

- **Network Systems**
  - Assess network devices, operating systems, applications, ports and services against a constantly updated vulnerability database
  - Identify and manage user privileges (via BeyondTrust PowerBroker solutions)
  - Accurately identify vulnerabilities with a false positive rate below 1%
  - Perform Class C network scans in under 15 minutes on average
  - Get PCI DSS 2.0 scanning and reporting capabilities out of the box
  - Receive updates within 48 hours of new critical vulnerabilities
- **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 with no additional licensing needed
- **Private and Public Clouds**
  - Determine which instances are running, when they move, and how they behave when they interact with your environment – even when powered off
  - Track virtual machines by instance ID, rather than host name or IP, to properly determine state of the virtual machine.
  - Amazon AWS, IBM SmartCloud, GoGrid, Rackspace, and VMware vCenter connectors are available
- **Mobile Devices**
  - Identify mobile devices connecting to your network and mail system
  - Conduct agent-based and agentless vulnerability assessments
  - Ensure devices are in compliance with PCI, HIPAA and other regulations
  - Android, Blackberry Enterprise Server, and MS Exchange ActiveSync connectors are available
- **Virtual Environments**
  - Assess VMware ThinApp applications for vulnerabilities
  - Power-on and reconfigure VMware offline images for assessment
- **Data Discovery**
  - Identify personally identifiable information (PII) on assets

- Classify the results by data discovered, asset name, and type of data
- Verify data security for regulatory compliance initiatives

## Retina CS and the BeyondInsight IT Risk Management Platform: Truly Unified Vulnerability Management

At BeyondTrust, vulnerability management is about much more than simply finding security weaknesses – it’s about enabling you to make smart decisions and take the right actions to best secure your organization. Our solutions provide a holistic view of your enterprise-wide security posture and comprehensive control over your vulnerability management program.

- **Discover** network, web, mobile, cloud and virtual infrastructure
- **Profile** asset configuration and access risk potential
- **Detect** applications and OS functions that require administrator privileges
- **Manage** access to admin and root privileges across all infrastructure
- **Identify** vulnerabilities enterprise-wide
- **Analyze** threat potential, return on remediation, and more
- **Remediate** vulnerabilities through integrated patch management
- **Report** on vulnerabilities, compliance, benchmarks, and more
- **Protect** endpoints from client-side attacks

### The BeyondInsight Family of Vulnerability Management Solutions

---

All of the following BeyondTrust solutions are integrated under BeyondInsight IT Risk Management Platform, providing you with centralized management, analysis and reporting throughout the vulnerability management lifecycle:

#### **Retina CS Enterprise Vulnerability Management**

*A BeyondInsight Platform Solution*

The industry’s leading solution for the identification and reduction of real security risks in your dynamic IT infrastructure - including physical, virtual, mobile and cloud environments.

#### **Retina Network Security Scanner:**

*The Retina CS Scan Engine – Also available as a standalone solution*

The security industry’s most well respected network security scanner. Identifies vulnerabilities introduced via missing patches, misconfigurations and conflicts with industry standard best practices. The solution can operate as standalone application or in enterprise architecture as part of a BeyondInsight / Retina CS Enterprise Vulnerability Management deployment.

#### **Optional Vulnerability Management Add-Ons for the BeyondInsight Platform:**

- **Retina Patch Management Module**  
Closes the loop on vulnerabilities and provides seamless, agentless patching from the BeyondInsight console. Provides business intelligence and reporting on patch processes.



- **Retina Configuration Compliance Module**  
SCAP-certified security policy management module that monitors compliance with over 60 industry benchmarks, including Microsoft, NIST, USBCG, and DISA STIGs, as well as with internally developed organizational benchmarks.
- **Retina Regulatory Reporting Packs**  
Automates compliance management with reports that map vulnerability and configuration audits to specific mandates including PCI, HIPAA, SOX, GLBA, NIST, FERC/NERC, MASS 201, ISO, COBIT, ITIL, and HITRUST.
- **PowerBroker Endpoint Protection Platform**  
Stops 100% of client-side attacks on unpatched hosts. All-in-one firewall, virus and spyware protection, vulnerability assessment, intrusion prevention, buffer overflow protection, registry and execution protection, and optional web application firewall.

**PowerBroker Privileged Account Management Solutions:**

A comprehensive suite of server, desktop, cloud, and virtual privileged account management solutions. Current BeyondInsight-enabled PowerBroker solutions include:

- PowerBroker UNIX/Linux
- PowerBroker for Windows
- PowerBroker PasswordSafe

## Our Focus: Providing Customers with the Best Vulnerability Management Solutions and the Highest Level of Service

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

At BeyondTrust, we pledge to stay focused on providing the highest quality vulnerability management solutions available – now and into the future. We regularly share our product roadmap with customers, as they wield the greatest influence on its course. And because we remain focused on vulnerability management, we are able to provide constant innovation and upgrades to keep our customers ahead of evolving threats.

Customers are the common thread that drives everyone at BeyondTrust to build the best vulnerability management solutions on the market. From the first inquiry to our sales department, to interactions with our training and customer service staff, we are committed to providing dedicated, responsive and straightforward service to existing and prospective customers alike.

## About BeyondTrust

BeyondTrust® is a global security company that believes preventing data breaches requires the right visibility to enable control over internal and external risks.

We give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And because threats can come from anywhere, we built a [platform](#) that unifies the most effective technologies for addressing both internal and external risk: [Privileged Account Management](#) and [Vulnerability Management](#). Our solutions grow with your needs, making sure you maintain control no matter where your organization goes.

BeyondTrust's security solutions are trusted by over 4,000 customers worldwide, including over half of the Fortune 100. To learn more about BeyondTrust, please visit [www.beyondtrust.com](http://www.beyondtrust.com).