Retina CS v6.0

New and Updated Features

BeyondTrust Retina enterprise vulnerability management solutions provide security professionals with vulnerability assessment and risk analysis in context. Retina enables organizations to proactively identify security exposures, analyze business impact, communicate risk, and plan and conduct remediation across network, web, mobile, cloud and virtual infrastructures. Key capabilities include:

- 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 account management.

Retina CS version 6.0 adds several new features that further enhance an organization's ability to centralize vulnerability data from multiple scanners, eliminate security gaps caused by transient platforms and have greater risk visibility through sharing vulnerability intelligence with leading SIEM solutions.

New Feature Highlights

Centrally Manage Retina Host-based Scans with BeyondInsight

Can you guarantee that your virtual and cloud-based systems are online during a network-based scan? And what about the growing number of remote employee laptops that randomly pop on and off the network? You may also have a number of connected systems that have been hardened – limiting what you can see from the outside looking in. How can you cover these vulnerability gaps?

Retina CS 6.0 provides a next-generation host-based vulnerability scanner - Retina Host Security Scanner – to ensure you can reliably identify and scan these transient systems. This latest revision of our agent leverages Retina's award-winning scanning technology and builds on over 10 years of in-market host-based scanner experience across thousands of enterprise customers. This release allows organizations to now centrally manage host-based scans with the BeyondInsight platform to:

- Perform full authenticated vulnerability and configuration scans without the need to provide credentials
- Quickly scan systems within a matter of minutes
- Identify and scan remote user computers, transient virtual platforms, hardened systems and cloud environments where active scanning may be forbidden.
- Centrally report on and analyze all host-based scan data.

Additional and Enhanced Certified Cloud & Virtual Connectors to Close Gaps

Cloud and virtual infrastructures by nature are very elastic. As a result, their presence can be hard to predict making scanning them even more difficult. Unknown or undermanaged cloud and virtual environments pose a significant risk opening networks to security breaches, data loss, intellectual property theft, and regulatory compliance issues.

Having certified integrations for elastic and transient cloud and virtual environments enables organizations to reliably identify and scan them. Retina CS cloud connectors allow organizations to discover all cloud and virtual instances in an environment, group cloud assets for secure management, and scan for known and emerging vulnerabilities. New cloud and virtual connectors available in version 6.0 include:

- **Microsoft Azure** connector that interacts with Azure's Resource Manager Architecture, enabling asset identification and vulnerability scanning of Azure's cloud environment.
- **Microsoft Hyper-V** connector that allows for asset identification and vulnerability scanning of Hyper-V platforms.
- **Amazon AWS** enhanced connector that lets organizations select assets across regions and custom naming instances, and enumerate them by private IP address.

These connectors can perform an accurate inventory of all cloud and virtual instances regardless of runtime state. Once those instances are found, organizations can quickly arrange them into Smart Groups for easier management according to an organization's unique business needs – helping you eliminate security gaps created by these unpredictable systems.

Certified Security Information & Event Management (SIEM) Connectors

Having certified integrations for forwarding critical events to third party security solutions marks a critical step in escalating user and asset security in much the same way network management and automated help desk solutions perform these functions in a traditional IT infrastructure.

Adding real-time vulnerability intelligence to SIEM solutions, like FireEye TAP, HP ArcSight, IBM QRadar, LogRhythm, McAfee ESM, and Splunk arms organizations with superior targeted attack and breach detection, as well as broader compliance visibility. Retina CS 6.0 has the following new certified connectors, for sharing vulnerability data with leading SIEM solutions:

- **FireEye** connector forwards event data to a FireEye TAP server using on premise COM Broker. In addition, it allows for the extraction of data from FireEye AX to augment Clarity threat analytics.
- **HP ArcSight** connector forwards event data to HP ArcSight in Common Event Format (CEF).
- **IBM QRadar** connector forwards data to IBM QRadar in Log Extended Event Format (LEEF).
- **LogRhythm** connector forwards event data to LogRythm in Log Extended Event Format (LEEF).
- **McAfee ESM** connector forwards all data types to MacAfee ESM (Nitro) via Syslog.
- **Splunk** connector forwards event data via a Splunk HTTP Event Collector.
- **Universal Event Forwarding** connector forwards event data to configured listeners in a variety of customizable formats.

Tenable Security Center and Tripwire Scanner Integration

Adding to our list of supported 3rd party scanners [McAfee, Nessus (Tenable), Nexpose (Rapid7) and Qualys], BeyondTrust is pleased to announce connectors for both Security Center (Tenable) and Tripwire vulnerability scanners.

With Retina CS 6.0, Tenable and Tripwire customers can safely and easily export their existing vulnerability data (via CSV files) directly to Retina CS. In addition, Retina CS gives current Tenable and Tripwire users the ability to centralize all their scan data for prioritization and reporting as well as for Clarity advanced threat analytics. Lastly, Tenable and Tripwire customers will now have the unique opportunity to combine their vulnerability and privilege intelligence to achieve a level of security visibility and control not possible with their existing solutions.

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.