Retina Enterprise Vulnerability Management Solutions

New and Updated Features

BeyondTrust Retina enterprise vulnerability management solutions provide security professionals with vulnerability assessment and risk analysis in context. Retina enables teams to proactively identify security exposures, analyze business impact, and plan and conduct remediation across network, web, mobile, cloud and virtual infrastructures, and communicate that risk to operations and compliance teams to reduce risk. 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 5.7 and Retina Network Security Scanner version 5.23 add several features that further enhance scanning efficiency and visibility.

New Feature Highlights

Smart Credentials Improve Scanning Efficiency

As with the case in the majority of organizations, there is no one set of credentials that is used for the entire enterprise. Consider a common use case: An administrator needs to perform a vulnerability scan on an environment of Windows machines, and has a list of credentials for the environment. Those credentials have different rights on different machines, and so the admin needs to use the one with the most rights. This causes administrators to either manage more scan jobs than necessary as they have to create very targeted scans, or you run the risk of performing less than thorough scans. In either case this can become an administrative problem.

BeyondTrust has overcome this challenge in Retina CS version 5.7 and Retina Network Security Scanner 5.23 with a new feature called, Smart Credentials. This new capability is enabled by default and will cause Retina to select the credentials with the highest level of privileges on each scan target when multiple scan credentials are provided. This capability improves the efficiency of scanning, making scanning much more thorough than with other solutions available in the market.

Asset Risk Analysis Helps to Prioritize Remediation

Every organization categorizes IT asset risk differently based on their tolerance or the industry they are in. Regardless of *how* they measure it, organizations need the *flexibility* to measure it according to their needs.

Retina CS version 5.7 introduces new asset risk analysis, giving the end user the option to “weight” their asset score by what matters most – Threat Risks (i.e. vulnerabilities and attacks) or Exposure Risks (i.e. ports, shares, services, accounts). A new normalize function can be applied to redistribute the asset risks from the lowest risk to a maximum of 10. When enabled, there will always be a risk of 10, which would be the asset of most interest. For example, if assets were within a range of 1.23 to 5.67, normalization would redistribute the range from 1.23 – 10.00. This new capability provides additional visibility into the risks that matter most to organizations, helping them further prioritize remediation.

Analytics & Reporting Enhancements Improve Visibility

Retina CS version 5.7 and Retina Network Security Scanner version 5.23 introduce several new analytics and reporting enhancements meant to improve efficiency and visibility.

- New option to migrate subscriptions from one user account to another, for example in the case of users who change roles.

- New option to filter by Audit Group for all SLA breakdown reports.

- New Extended Vulnerability Export report enables users to filter by Audit Risk. This is a cloned report from the existing Extended Vulnerability Export report which is mapped to PCI risk.

- Enhanced Clarity Malware report. This report will now display the source of the malware detection (PBEPP, Network Based or Global Threat Detection).

- Import Summary Report can now be saved as a CSV, helpful when reviewing what was imported from BeyondSaaS, RTD, R7, Qualys and Tenable.

Certified and Expanded Benchmarks

In Retina CS version 5.7 and Retina Network Security Scanner version 5.23, BeyondTrust provides certified and expanded CIS benchmarks, including IE10, IE11, Win 7, Win 2008, Win 2008 R2, Win 8.1, and Win 2012 R2.

Other

Retina CS version 5.7 and Retina Network Security Scanner version 5.23 include several new general enhancements.

- Enumeration enhancements meant to improve discovery, including: Enumeration of Database Instances and Users, Certificate Enumeration on Windows, Enumeration of Accounts with SSH Key Authentication.

- New Port column option in the Assets grid. This column will display the port(s) associated with found vulnerabilities, when applicable.

- Added Audit Manager as an option in the Configure Tab. This significantly reduces the number of clicks needed to get to the Audit Manager section.

- Option to reboot remote Retina Network Security Scanners from BeyondInsight.

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.