DATASHEET

beyondtrust
Beyond Traditional Security

Retina CS Vulnerability Management Console:

Patch Management, Configuration Compliance and Regulatory Reporting Modules

Complete the Retina CS Vulnerability Management Lifecycle

Unified vulnerability management is about much more than simply finding security weaknesses – it's about making smart decisions, taking the right actions to protect your organization, and clearly communicating with technical and non-technical stakeholders alike.

By adding Retina Patch Management, Configuration Compliance and Regulatory Reporting modules to Retina CS, you not only gain a more holistic view of your enterprise security posture, but also significantly improve the efficiency of your vulnerability management program. All Retina add-on modules offer:

- Integration with Retina CS for asset discovery, vulnerability assessment, threat scoring and security intelligence
- Data mapping to relevant patch, configuration and/or regulatory information
- Centralized dashboards for management, analysis and reporting
- Frequent vulnerability, patch, configuration and/or regulatory updates

Seamless, Risk-Based Patch Management

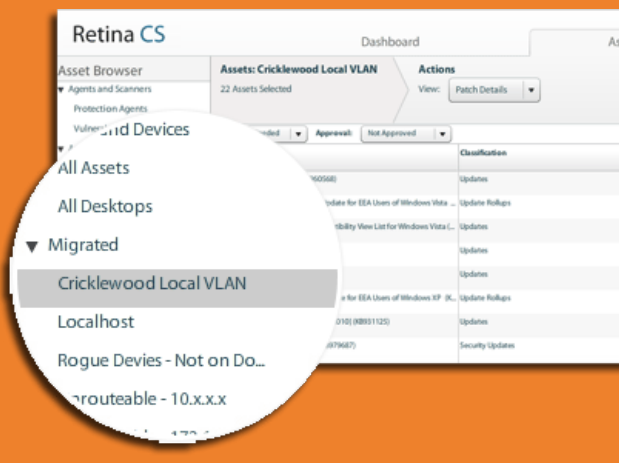
The Retina CS Patch Management Module empowers your existing team to deploy and manage patches as a natural extension of the Retina CS vulnerability management process. By integrating with Microsoft® System Configuration Manager (SCCM) and Windows® Server Update Service (WSUS), the module enables users to quickly assess risk and then deploy patches for Microsoft and third-party applications directly from the Retina CS console.

Key Features

- Mapping of identified vulnerabilities to available patches
- Automatic, on-demand and/or scheduled patch deployment
- Remediation verification via repeated vulnerability assessments
- Unmatched reporting of patching results, deltas and trends
- Role-based access for viewing and patching specific asset groups

Patch Management Module Benefits

- Quickly deploy patches for Microsoft and Adobe applications, web browsers and other third-party applications
- Prioritize patching based on asset scoring, exploitability, CVSS and more
- Address critical exposures with immediate patching, or deploy on a scheduled basis
- Simplify reporting to management, auditors and other stakeholders
- Measure and track patching progress, trends and deltas via an integrated data warehouse
- Complement your existing Microsoft WSUS implementation and support air-gapped WSUS environments



beyondtrust®
Beyond Traditional Security

Automated Configuration Auditing, Reporting and Alerting

In addition to patching and remediation, configuration management is widely accepted as one of the most effective ways to secure enterprise networks. The Retina Configuration Compliance Module makes it easy to audit configurations against internal policies or external best practices, while centralizing reporting for monitoring and regulatory purposes.

Key Features

- Out-of-the-box configuration auditing, reporting and alerting
- Templates for Windows operating systems, as well as for FDCC, NIST, STIGS, USGCB and Microsoft applications
- Assessments of audit and security settings, user rights, logging configuration and more
- Built-in reporting and integration with Retina CS for deltas, trends and other analytics
- An OVAL 5.6 SCAP-certified scan engine and interpreter

Regulatory Compliance Reporting and Analytics

The Retina Regulatory Reporting Module enables you to efficiently navigate through the complex regulatory compliance landscape. The module goes way beyond generic compliance reporting by mapping your network's specific vulnerabilities to relevant corporate policies, government regulations, and industry standards.

Key Features

- Seamless integration with Retina CS and the Retina Configuration Compliance Module
- Compliance reports for PCI, HIPAA, SOX, GLBA, NIST, FERC/NERC, MASS 201, ISO, COBiT, ITIL, HITRUST and other regulations
- Mapping of vulnerabilities and configuration issues to control objectives and mandates
- Compliance dashboards with drill-down capabilities that enable immediate and consistent responses to compliance violations
- Continual updates for newly discovered vulnerabilities and changes in regulatory controls

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.

CONTACT

BeyondTrust North America
Tel: 800.234.9072 or 818.575.4000
info@beyondtrust.com

BeyondTrust EMEA
Tel: + 44 (0) 8704 586224
emeainfo@beyondtrust.com

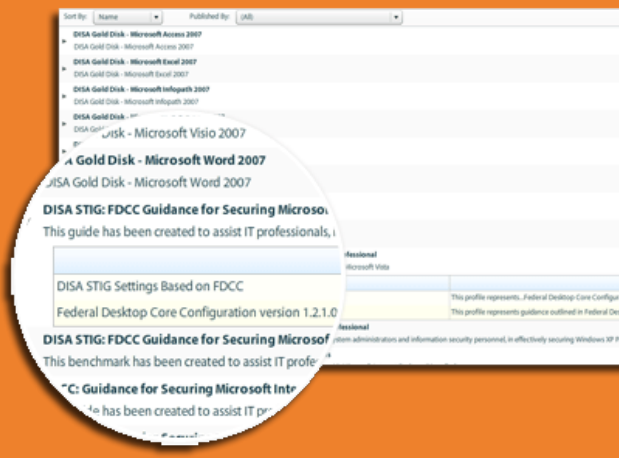
CONNECT

Twitter: @beyondtrust
Facebook.com/beyondtrust
Linkedin.com/company/beyondtrust

Learn more at www.beyondtrust.com

Configuration Compliance Module Benefits

- Ensure configuration compliance for all network, mobile, virtual & cloud infrastructure
- Save time with automated configuration audits delivered to a central Retina CS console
- Gain actionable data for making immediate improvements to system and device security
- Ease reporting with templates incorporating multiple best practice guidelines



Regulatory Reporting Module Benefits

- Quickly identify, assess and manage IT risks associated with regulation control objectives
- Efficiently demonstrate compliance via automated data mapping & report generation
- Consistently monitor and respond to compliance violations via a central dashboard
- Stay ahead of recent vulnerabilities and control changes with regular, automated updates from the BeyondTrust Research Team