

Retina CS Management Console

CENTRALIZED VULNERABILITY MANAGEMENT

Dramatically reduce security risks in physical, virtual, & mobile environments.

Retina CS is the only unified vulnerability and compliance management solution that integrates security risk discovery, prioritization, remediation, and reporting. With Retina CS, you close the gaps across the vulnerability management lifecycle to reduce risk for your organization.

Retina CS enables IT Security professionals to centrally manage organization-wide IT security from a single, web-based console. From this vantage point, the discovery, prioritization, and remediation of security risks is more efficient than ever. Having developed one of the first vulnerability scanners on the market, Retina, we've built on that foundation for more than a decade to provide end-to-end vulnerability lifecycle management for enterprises of any size.

RETINA INSIGHT (INCLUDED)

An advanced reporting engine, included at no additional cost with Retina CS. Retina Insight delivers analytics and trending across the vulnerability lifecycle for multi-dimensional reports on assets, vulnerabilities, attacks, and patches.

CONFIGURATION COMPLIANCE (ADD-ON MODULE)

Define and manage security policies to monitor compliance with industry and internally developed benchmarks such as Microsoft, NIST, USBCG, and DISA STIGs.

REGULATORY REPORTING (ADD-ON PACKS)

Automated solutions to help navigate complex corporate policies, government regulations, and industry standards such as SOX, PCI, FISMA, and ISO.

BENEFITS

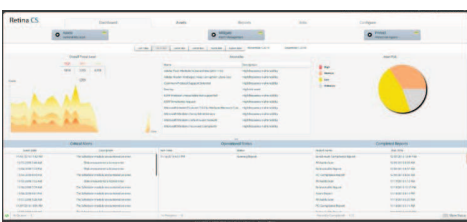
DISCOVER, PRIORITIZE, FIX, AND REPORT ON SECURITY RISKS MORE EFFICIENTLY.

CLOSE SECURITY GAPS WITH VULNERABILITY ASSESSMENT FOR MOBILE DEVICES AND VIRTUAL APPLICATIONS.

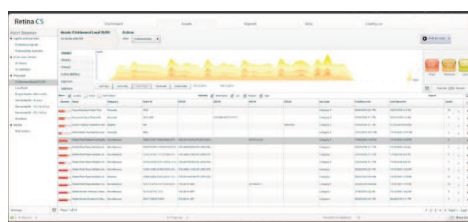
SIMPLIFY IT SECURITY WITH END-TO-END VULNERABILITY MANAGEMENT THAT INCLUDES BUILT-IN PATCH MANAGEMENT FOR MICROSOFT AND THIRD-PARTY APPLICATIONS.

BETTER ALLOCATE RESOURCES TO FIX VULNERABILITIES BASED ON THREAT LEVEL AND BUSINESS FUNCTION.

TIGHTEN SECURITY ACROSS ALL LOCATIONS AND ASSETS



Retina CS - Dashboard



Retina CS - Vulnerability by Asset



eEye Digital Security®

PATCH MANAGEMENT (ADD-ON MODULE)

Get integrated, agentless patch management for both Microsoft and third-party applications including Adobe (Distiller, Elements, Reader, Flash, Shockwave), Mozilla (Firefox), and many more, built on the Microsoft WSUS engine.

CENTRALIZED SECURITY MANAGEMENT

See a single view of security risk information within the IT environment – across all locations and assets.

FLEXIBLE RISK SCORING

Refine CVSS (Common Vulnerability Scoring System) based on business, assets, and risk appetite.

BROAD EXPLOIT INTELLIGENCE

Identify whether a vulnerability has an associated exploit from Core Impact, Metasploit, or Exploit-db.com to improve risk prioritization.

INTEGRATED ATTACK AND MALWARE INFORMATION

See malware and attack data – including attacks from third-party solutions – to improve asset risk prioritization.

EXECUTIVE AND TECHNICAL REPORTING

Generate enterprise-wide security reporting in easy-to-read layouts that include visual charts and graphs for quick assessment, mitigation, and protection.

ADVANCED ASSET CORRELATION

Filter events by date and time ranges, by severity, by assets, and by attack vectors and vulnerabilities.

SMART GROUPS

Dynamically populate asset groups based on any discovered attribute of a target including installed software and running process. Use predefined groups for common roles such as web servers and operating systems.

SMART RULES

Create business-intelligent rules on discovered asset traits such as operating system, open ports, and services running.

SMART TARGETING

Target assessment scans based on any discovered asset criteria including installed software or any other enumerated characteristic.

SYSTEM REQUIREMENTS

WINDOWS SERVER 2003 SP2 OR HIGHER (32-BIT)
 WINDOWS SERVER 2008 (32-BIT AND 64-BIT)
 WINDOWS SERVER 2008 R2 (64-BIT)
 MICROSOFT SQL SERVER 2005 SP1 OR HIGHER
 MICROSOFT SQL SERVER 2008 SP2 OR HIGHER
 INTEL DUAL CORE 2.0GHZ (OR COMPATIBLE)
 2GB MINIMUM, 4GB RECOMMENDED (REQUIRES X64 BIT OS)
 500MB FOR SOFTWARE INSTALL / 20GB FOR DATABASE
 NETWORK INTERFACE CARD (NIC) WITH TCP/IP ENABLED
 MICROSOFT .NET FRAMEWORK 3.5 (INCLUDED WITH INSTALLER)
 MICROSOFT IIS 6.0 OR HIGHER ASP.NET
 ADOBE FLASH PLAYER 10.0 OR HIGHER
 ORACLE SUN JAVA VERSION 6 UPDATE 21 OR HIGHER

About eEye Digital Security

Since 1998, eEye Digital Security has made vulnerability management simpler and more effective by providing the only unified vulnerability and compliance management solution that integrates security risk discovery, prioritization, remediation, and reporting into a complete offering. Consistently the first to uncover critical vulnerabilities and prevent their exploit, eEye leverages its world-renowned research and development to strategically secure customer assets. Thousands of mid-to-large size organizations, including some of the most complex IT environments in the world, rely on eEye solutions to protect against the latest known, unknown, and zero-day vulnerabilities. [See more at www.eeye.com](http://www.eeye.com)

CONTACT INFORMATION

UNITED STATES
1.866.282.8276

NORTH AMERICA SALES
sales@eeye.com

GERMANY
+49 (0) 8031 2227 432

INTERNATIONAL SALES
sales.eu@eeye.com

UNITED KINGDOM
+44 (0) 20 8432 3490

www.eEye.com

111 THEORY, SUITE 250 | IRVINE, CALIFORNIA 92617