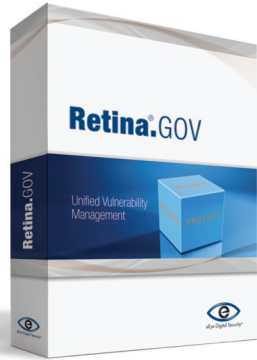


Retina®.GOV



Benefits

- Reduce the cost of security and compliance by automating configuration auditing and vulnerability management
- Ensure that you are protected from the latest known vulnerabilities with intelligently updated audits database that include a 48-hour SLA for critical vulnerabilities
- Prioritize resources and streamline remediation efforts through executive and task specific reporting offering risk scoring prescriptive and guidance on issues.
- Simplify assessments and lower cost with a single solution that provides non-intrusive, scalable remote scanning that will not impact business assets or operations.
- Distributed scanning and reporting of all discovered assets, compliance violations and vulnerabilities into a single management console.
- Perform local VA scanning on critical assets where credential or firewalls prevent accurate remote scanning or where more frequent scanning is desired.
- Retina can also offer continuous scanning monitoring as required by NIST 800-37*

Secure and Comply with eEye

Retina.GOV is a unified vulnerability management and compliance solution designed to help Government departments and agencies with vulnerability assessment and compliancy by defining and monitoring relevant IT controls.

- Implement policy-based security management including routine security assessments, demonstrated control, and use of timely reports as part of standard processes
- Capability to efficiently classify, respond to and resolve potentially high-volume threats
- Enable compliance for SCAP, FDCC, and DIACAP initiatives mandated by command authorities

Retina.GOV monitors both vulnerability and configuration of your IT assets, while correlating compliance requirements to pre-defined baselines and providing automated notification of violations. Your environment is assessed, capturing established security controls along with any vulnerabilities or configuration violations that impact the network. Detailed reports providing prescriptive guidance and recommendations are then forwarded and response is initiated to ensure that corrective action can be taken in a timely fashion.

Federal Government Regulations & Retina.GOV

SCAP and FDCC

Retina Network Security Scanner is now certified for the following SCAP requirements:

- Federal Desktop Core Configuration (FDCC v1.2) Scanner
- Authenticated Configuration Scanner
- Authenticated Vulnerability and Patch Scanner
- Unauthenticated Vulnerability Scanner

Retina's SCAP capabilities include the following standards: FDCC, XCCDF, OVAL, CCE, CPE, CVE and CVSS.

When utilizing Retina Network Security Scanner's SCAP engine, users are able to import SCAP content, such as FDCC benchmarks, for interpretation and assessment of network devices. Retina provides an easy-to-use wizard that guides the user through the steps of selecting desired content, providing information on the assets to be evaluated, and launching the assessment scan. Upon launch, the scan will run without user intervention, alerting you when complete. The assessment results are made available in both machine legible XML in OVAL and XCCDF formats as well as human readable reports. Both machine and human readable output contains associated CVE, CPE, CVE and CVSS references as applicable.

DIACAP:

Retina.GOV enables organizations to become DIACAP compliant:

- The DoD Information Assurance Certification and Accreditation Process (DIACAP) is the United States Department of Defense (DoD) process of ensuring that risk management is applied on information systems (IS).
- DIACAP defines a DoD-wide formal and standard set of activities, general tasks and management structure process for the certification and accreditation (C&A) of a DoD IS that will maintain the information assurance (IA) posture throughout the system's life cycle.

Assessment

Retina provides industry leading vulnerability management across network devices, operating systems, applications, databases and web applications. Retina safely scans both patch and configuration vulnerabilities against user-defined or pre-defined templates that include SCAP, FDCC, STIG and IAVA.

Mitigation

If computer controls or service levels are impacted by a network problem or intruder, alerts can be fired to notify appropriate administrators enabling the IT department to take immediate actions to re-establish operational and security control. Retina adheres to broadly accepted standards which include integration with SCAP, FDCC, and IAVM for assessment, risk scoring, and reporting purposes ensuring reports are easily comprehensible and suitable to our federal customers and their partners. The Retina management console is a fully integrated, complete web-based security and compliance solution available as software or appliance and is Common Criteria EAL2 Certified. Now you can simplify the management of distributed, complex infrastructures while protecting your mission critical assets from evolving threats with a single end-to-end management system.

Depth and Safety of Unified Scan Engines

- Unified scanning across network devices, operating systems, applications, databases, web applications, virtualized environments and much more
- Innovative, non-intrusive and safe scanning technology with extensive network throttling capabilities
- Complete asset inventory with accurate OS detection using multiple engines for verification
- Wireless asset detection from the network or wireless using a dedicated WiFi scanner

Standards Based

- The most comprehensive vulnerability database with PCI and CVSS scoring
- Independently tested and reviewed by NSS Labs for use with PCI Compliance
- Integrated STIG, IAVA, and SCAP support
- Customizable audits using wizards - no programming experience required

Flexible Deployment

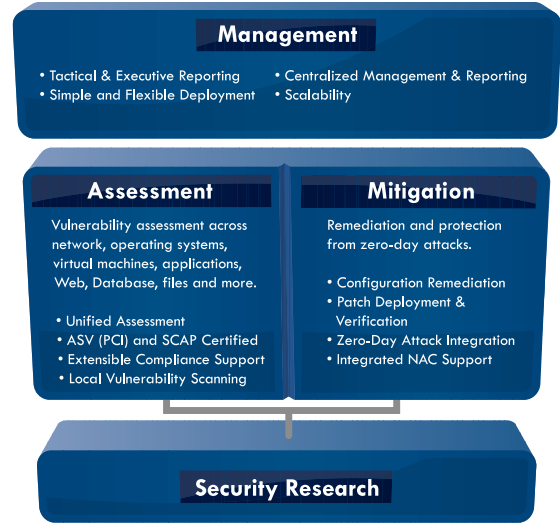
- Runs on Windows 2000, XP, 2003, Vista, Windows 7, and 2008
- Software or appliance
- Role based security delegation for managing tasks and reporting
- Open architecture for third party integration and compatibility

Unparalleled Audit Support

- Backed by an unrivalled vulnerability research team
- Identifies known and published zero-day vulnerabilities
- Automated updates for latest vulnerability checks and information (SLA – 48 hours)

* footnote: Guide for applying the Risk management framework to Federal Information Systems published February 2010.

Unified Vulnerability Management Security and Compliance



Reporting

- Team members from CIOs to Security Engineers, can execute a wide variety of reports including vulnerability details, assets and hardware inventory, delta reports, patch reports, trending graphs, and can even customize reports to include sections unique to their business needs
- Reports can be executed ad-hoc, scheduled, or emailed

Interoperability

- Retina adheres to broadly accepted standards which include integration with IAVA and CVE for risk scoring and reporting purposes to ensure reports are easily understood and suitable to our government customers
- Retina is standard based and supports IAVA, CVE, CVSS, CCE, OVAL and XCCDF
- Retina is EAL2 (common criteria) certified
- Retina employs an open architecture and readily integrates with industry leading SIM, NAC and GRC.

Support / Maintenance

- 24/7 Support
- 48 hour SLA for Critical Vulnerabilities
- Technical Training and Certification Workshops

Optional Protection Modules

eEye offers optional threat protection modules which are available through our Retina solutions. Please contact an eEye representative to discuss additional solutions available for your installation.

Read more about eEye for Government: www.eeye.com/GOV

About eEye Digital Security

Founded in 1998, eEye Digital Security is a leader in vulnerability management and compliance, providing the only unified solution that integrates assessment, mitigation and protection into a complete offering. eEye enables secure and compliant computing through world-renowned research and is consistently the first to identify and protect systems from zero-day threats. The company's flagship product, Retina, meets security and compliance requirements for SMBs and enterprise-class organizations across all verticals worldwide. eEye is a trusted advisor providing network security education, product deployment services and enterprise-wide integration.

U.S. Toll Free: 1.866.282.8276
Main Office: 1.949.333.1900

Federal Sales: federal@eeye.com
State & Local: sled@eeye.com