

Retina.GOV

DESIGNED FOR GOVERNMENT DEPARTMENTS AND AGENCIES

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

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.

- 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
- 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

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

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.

FAST FACTS

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

DISTRIBUTED SCANNING AND reporting of all discovered assets, compliance violations and vulnerabilities into a single management console



eEye Digital Security®

Federal Regulations & Retina.GOV

SCAP

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.

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

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

Retina’s SCAP capabilities include the following standards:

- XCCDF, OVAL, CCE, CPE, CVE, and CVSS

FDCC

Retina Network Security Scanner, the flagship solution component of Retina.GOV is compliant with FDCC 1.2.

The Federal Desktop Core Configuration (FDCC) is an OMB-mandated security configuration which exists for Microsoft Windows Vista and XP operating systems. The Windows Vista FDCC is based on DoD customization of the Microsoft Security Guides for both Windows Vista and Internet Explorer 7.0.

DIACAP

Retina.GOV enables organizations to become DIACAP compliant.

The Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) is the United States 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.

Unified Vulnerability Management



About eEye Digital Security

Since 1998, eEye Digital Security has made vulnerability management simpler, less expensive, and more effective by providing the only unified vulnerability and compliance management solution that integrates assessment, mitigation, and protection 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

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