

## 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 an intelligently updated audits database that includes 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 in 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\*

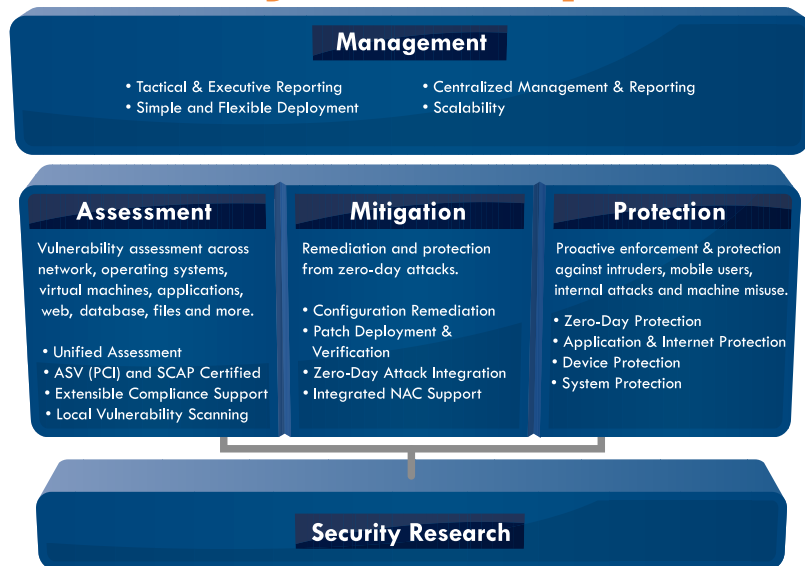
## Secure and Comply with eEye

Retina is a powerful unified vulnerability management and compliance solution designed to help organizations of all sizes with vulnerability assessment, mitigation and protection. Retina, founded from over a decade of technology innovation by eEye's world renowned security research team, is an integrated end-to-end vulnerability and compliance solution designed to help organizations with protection and compliancy by defining and monitoring relevant IT controls.

Retina monitors both patch and configuration vulnerabilities and compliance to pre-defined configuration baselines and provides automated notification of violations. The 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.

Retina's management console is a fully integrated and complete rich internet-enabled application for security and compliance management. Now you can simplify the management of distributed, complex infrastructures while protecting your mission critical assets from evolving threats with a single unified management system.

## Unified Vulnerability Management Security and Compliance



## Assessment

Retina provides industry leading vulnerability assessment, unified configuration and vulnerability scanning across network devices, operating systems, applications, databases, and web applications using a scalable, non-intrusive approach. Organizations can customize their own policies or can import pre-built controls and reports. Retina monitors both vulnerabilities and configuration compliance using nonintrusive agentless scanning and provides automated notification of violations. Optional host based scanning agents are also available for critical assets that require continuous scanning or that cannot be assessed over the wire.

## Mitigation

If computer controls or service levels are impacted by a network problem or intruder, alerts can be issued to a specified user or group, enabling immediate actions be taken to immediate actions in order to re-establish operational and security controls. Retina adheres to broadly accepted industry standards, and the solution includes risk scoring and reporting purposes to ensure reports are easily comprehensible and suitable for our customers, their partners, and auditing services.

## Protection

Retina provides unified zero-day protection for when a vendor supplies security patches which do not yet exist for an operating system or application. Retina adheres to broadly accepted industry standards, and the solution includes risk scoring and reporting purposes to ensure reports are easily comprehensible and suitable for our customers, their partners, and auditing services.

## Depth and Safety of Unified Scan Engines

- Unified scanning across network devices, operating systems, applications, databases, web applications, virtualized environments and much more
- Innovative, nonintrusive scan engine 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)

## Integrated Application and Device Control

- Block approved applications from downloading and installing malware
- Detect and block attacks using vulnerable third-party ActiveX controls installed in Internet Explorer.
- Block sensitive areas of the registry from modifications
- Disable users from using USB storage devices

## Zero-Day Protection and IPS

- Monitor applications behavior of, detect, and block both known and unknown buffer-overflow exploits

- Analyze and decode network protocols looking for signatures of known attacks and signs of intrusion
- Protect the system against known and unknown local and remote buffer overflow exploits

## 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 both 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 patch management vendors

## Product / Integration

- Published Database Schema
- Windows Event Logging
- SNMP Trap Forwarding
- Syslog Daemon
- E-mail Alerts
- Command Line
- Data Export

## Support/ Maintenance

- 24/7 Support Available
- 48-hour SLA for critical vulnerabilities
- Technical Training and Certification Workshops

## Retina for Government

eEye offers a specific solution bundle specifically designed for our Government clients: [Retina.GOV](http://Retina.GOV).

Learn more at [eeye.com/gov](http://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

Sales: [sales@eeye.com](mailto:sales@eeye.com)