SOLUTION OVERVIEW

- Integrated Threat and Security Management
- Vulnerability Assessment Across your Entire Network
- Automated Audit Updates Three Times Faster than the Leading Competitor
- Asset Classification including Rogue, Mobile, and Virtual Machines
- Policy and Regulatory Compliance and Best

Retina Network Security Scanner is designed for any size organization, from large enterprises to small and medium businesses. Retina® is recognized as the industry standard for vulnerability assessment and is designed to identify known network security vulnerabilities and assist in prioritizing threats for remediation. This multi-platform scanner features fast, accurate, and non-intrusive scanning, enabling administrators to effectively and efficiently secure their networks against even the most recent of discovered vulnerabilities and missing patches. Organizations can also leverage Retina for security risk management and for enforcing standards-based policy settings in support of their corporate and regulatory audits. With eEye provided audit groups and reports, regulatory scanning and reporting are streamlined for efficient business implementations. Retina also provides centralized network policy assessment, centralized vulnerability management, and centralized event and scan job control through the REM® Security Management Console allowing the solution to scale for any environment.

Best-of-breed scan engine, comprehensive vulnerability database, and lowest false positive rate makes Retina the most efficient solution for any environment.

1. Confidently identify all vulnerabilities with the lowest false positive rate in the industry; on average less than 1%

The eEye Research Team provides vulnerability audit updates for US Government recognized critical vulnerabilities three times faster than the leading competition. Updates are provided with a service level of 48 hours from public disclosure and are automatically downloaded and incorporated by the solution.

2. Proactively guard against known and newly-identified vulnerabilities with frequent, automated updates from the unrivaled eEye Research Team

Retina can reliably and non-intrusively scan your environment to identify all systems and devices. Essentially, if the device has a TCP/IP address, Retina will scan it and classify it with the highest accuracy in the industry.

3. Quickly identify all machines on your network including rogue, virtual, and wireless devices

Retina does not scan and test with exploit code and will not crash your systems during a scan. With Retina, you can scan an entire Class C network in approximately 15 minutes using our proprietary Adaptive Speed technology.

4. Safely scan your network without crashing system devices and causing business interruptions

Retina provides an extensive command line, and event forwarding through SNMP, Syslogs, email, and Windows Event Logs to integrate into virtually any network management solution, security information manager, or call center.

5. Extensive third party integration support into your existing infrastructure

Retina does not require high-end or high cost servers to perform vulnerability assessments.

6. The only network vulnerability scanner to be available as an appliance, managed service or software supporting Windows 2000, XP, 2003, Vista, and 2008

072009
Key Advantages
- Less than 1% false positive rate
- Audit release 3x faster than the leading competitor
- Complete asset inventory and auditing including installed software
- The most comprehensive vulnerability database with PCI and CVSS scoring
- Independently tested and reviewed by NSS Labs for use with PCI Compliance requirements
- Automated updates for latest vulnerability checks and information
- Backed by an unrivaled vulnerability research team
- Open architecture for third-party integration and compatibility
- Innovative, non-intrusive, and safe scanning technology
- User-definable custom audits using wizards; no programming required
- Identifies known and published zero day vulnerabilities
- Accurate OS detection using multiple engines for verification
- Easily identify common registry, permission, and security problems
- Wireless asset detection, SSID identification, and dictionary WEP cracking
- Distributed and Scalable Management using the REM Security Management Console Exclusion list for devices and ports to never be scanned

Organizations
- RETINA – Small to Medium Business (SMB)
- RETINA ENTERPRISE – Large to Enterprise Organizations (includes REM)
- Regulated Organizations such as healthcare and financial, manufacturing, and education
- Resellers, VARs, Systems Integrators, Consultants, PCI ASVs

User Environment
- PRIMARY
  Security and network managers with responsibility for a LAN or WAN with 512 to 15,000 network assets for vulnerability management, patch assessment, or regulatory compliance.

- SECONDARY
  Technology and product managers within a reseller organization, or a technology consultant looking to offer a full-featured, managed security solution.

- VERTICAL
  Security managers within regulated industries: finance (PCI or Sarbanes Oxley), healthcare (HIPAA)

Why Use Retina Network Security Scanner
1. Department or enterprise-wide vulnerability assessment
   Retina scales to meet the requirements of any size organization and supports scanning in distributed environments using software or appliances.

2. Compliance with industry or federal regulations
   Retina helps companies comply with Payment Card Industry (PCI), Federal Desktop Core Configuration (FDCC), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley (SOX), Gramm-Leach-Bliley Act, Federal Information Security Management (FISM) Act, European Union Data Directive, and others by providing customizable security policies and extensible reports.

3. Identify security risks and eliminate business interruptions
   Less sophisticated scanners can crash a server or device as a result of their scanning methods that include running partial or full exploit code. Retina does not run any type of exploit code to conduct a scan and can accurately identify vulnerabilities without compromising a host.

4. Asset and risk identification
   Retina can accurately detect and classify all assets within an environment and determine rogue, wireless, and virtual devices connected to the infrastructure. Vulnerability assessment determines which devices pose the greatest risk to the environment from malware to hackers to unauthorized computing devices.
Questions to Consider

1. Do you currently perform network-based vulnerability assessment scans?
2. Do you currently have, or are you planning to initiate a vulnerability assessment project as it relates to security or compliance?
3. Do you have resources and budget set aside for this project?
4. Do you have rogue and wireless assets appearing on your network? How do you know?
5. Have you been exploited or attacked due to a missing patch?
6. Do you know the financial impact of being hit with an attack?

Key Features

- **Reliable, Non-Intrusive Scanning Technology**
  Most scanners rely on exploit code to test network vulnerabilities, which frequently crashes servers, devices, or even networks in the process. Retina tests without using exploit code and harming your devices and network.

- **Comprehensive and Current Database**
  The most advanced, comprehensive database available. Critical vulnerabilities are updated within 48 hours of public disclosure. This is three times faster than the leading competition.

- **Superior Research Team**
  No security vendor can match the expertise of the eEye Research Team. Over the last 10 years, eEye has discovered more critical vulnerabilities than any other research group.

- **Extensive Third-Party Integration Support**
  Retina's open architecture allows for integration with third-party applications such as event managers, security information managers, network management systems, call centers and many framework based solutions.

- **Best Practice Approach to Vulnerability Assessment**
  Retina guides users through the logical steps of discovering assets, auditing known vulnerabilities and configuration issues, recommending remediation actions and reporting on the entire vulnerability management process using industry accepted best practices.

- **Unrestricted Asset Discovery**
  Retina allows for the discovery of a network's entire infrastructure without restrictions or separate licensing. At a glance, administrators can determine the number and type of hosts on the network and build policies and groups for vulnerability assessment based on the results.

- **Flexible Remediation Reporting**
  Within the workflow or Retina, users can create targeted reports to identify specific vulnerabilities for remediation by risk, vulnerability, host or even export the data to common file formats for inclusion in other reports and management systems.

- **Wizard Based Customizable Audits**
  Custom audits help ensure corporate policies with regard to anti-virus installations, file sharing programs, instant messaging, and third-party applications are being correctly identified and mitigated.

- **Granular Job Scheduling and Job Duration Support**
  Administrators can schedule and run multiple scan jobs against multiple targets and groups (business groups, subnets, for example) for scanning at one time, and control when a job must terminate (scan windows) in order not to impact business requirements like change control windows.

- **Adaptive High-Speed Scanning**
  Recognized as the fastest security scanner available, Retina can scan an entire Class C network in approximately 15 minutes. Retina scans every machine on your network, all types of operating systems, network devices and third-party or custom applications with extreme accuracy and speed.
### Other eEye Solutions

<table>
<thead>
<tr>
<th>RETINA ENTERPRISE</th>
<th>APPLIANCES</th>
<th>BLINK ENTERPRISE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you need to centrally manage and report on distributed network scanning and vulnerability assessment initiatives?</td>
<td>Do you want a turnkey appliance solution or to setup and license servers on their own?</td>
<td>Do you want an agent-based vulnerability assessment solution in lieu of a network-based scanner?</td>
</tr>
</tbody>
</table>

### Market Feedback

“A good product for organizations of most sizes, especially those with widely distributed networks and limited security management resources.”

- SC Magazine, January 2007

“Retina Scanner detected 100% of Attacker Initiated vulnerabilities with 100% of System Exposure and 100% of System and Service Faults. We found this effectiveness to be excellent.”

- NSS Labs, September 2008

“It is apparent that eEye maintains a superior vulnerability research team that focuses on the most widely deployed operating systems and applications.”

- NSS Labs, September 2008

“For its solid performance, good value and its venerable pedigree, we rate this product our Best Buy for the month.”

- SC magazine, August 2008

### About eEye Digital Security

eEye® Digital Security is pioneering a new class of security products: integrated threat management. This next-generation of security detects vulnerabilities and threats, prevents intrusions, protects all of an enterprise's key computing resources, from endpoints to network assets to web sites and web applications, all while providing a centralized point of security management and network visibility. eEye's research team is consistently the first to identify new threats in the wild, and our products leverage that research to deliver on the goal of making network security as easy to use and reliable as networking itself. Founded in 1998 and headquartered in Orange County, California, eEye Digital Security protects more than 9,000 corporate and government organizations worldwide, including half of the Fortune 100. For more information, please visit www.eEye.com.