



RETINA® Web Security Scanner

Integrated Threat & Security Management.

SOLUTION OVERVIEW

- Vulnerability Assessment for Web Applications
- Fully Automated Web Crawling and Reporting
- Minimal Website Training or Learning Required
- Most Accurate and Automated Scanning Tool on the Market
- Supports Credentials, Proxies, and Custom Applications
- Policy, PCI and Regulatory Compliance and Best Practice Recommendations for Web Security



Product Overview

The Retina Web Security Scanner is the best-in-class web scanning solution that rapidly and accurately scans large, complex web sites and web applications to tackle web-based vulnerabilities. The Retina Web Security scanner is able to provide you with a complete picture of the performance and security status of deployed web applications plus on-demand inventory and diagnostic capabilities, ensuring privacy and compliance. Retina Web Security Scanner identifies application vulnerabilities as well as site exposure risk, ranks threat priority, produces highly graphical, intuitive HTML reports, and indicates site security posture by vulnerabilities and threat level.

Web Application Facts

- The uniqueness of most websites requires that artificial intelligence be used for automated assessment, web application scanning is a very challenging problem in computer science
- Most security tools use signature-based technologies (IDS/IPS, network security, antivirus) which is a relatively simple technology. The eEye research team has created a tool that works like a human consultant: it profiles a web application, creates custom attacks and determines if the website is vulnerable to these attacks
- There is a wide range of measured effectiveness across web scanners in terms of accuracy and automation
- The only third-party study done on these tools concluded that the Retina Web engine found 10-20 times more vulnerabilities than competing tools, with a lower false positive rate
- Competing tools are designed to be used with significant and time consuming manual training
- Using another tool can cause you to miss a large number of vulnerabilities, leaving your applications vulnerable and requiring multiple costly cycles of development to repair



RETINA® Web Security Scanner

Benefits and Features

1. “Accuracy, Accuracy, Accuracy”

In real estate, there are only three important things to consider: location, location, location. In Web application scanning, they are: accuracy, accuracy, and accuracy.

- False negatives leave enterprises exposed to vulnerabilities that can result in loss of confidential data
- False positives destroy the credibility of the security team and can cripple an application security program

2. Fully Automated Solution

Security teams do not have the time to teach tools how to scan a website

- In web application scanning you are only given the home page and then required to crawl the rest of the site unlike network scanning where you know the problem space ahead of time (an IP/Port range)
- If you don't crawl a page, you can't test it
- Competing tools require significant manual effort to function: “In order to achieve good results, web application scanners should be used in conjunction with manual security assessment, which requires close acquaintance with the web application and its different functionalities.” Ory Segal, Watchfire Director of Research

3. Retina Web Reports Help you Solve the Problem

Finding Vulnerabilities is only the first step; fixing them is the goal:

- Web application attacks are polymorphic; they can be made in a number of ways
- A single coding error can create hundreds or thousands of vulnerabilities
- Retina Web Reports group vulnerabilities by their root cause, speeding remediation
- All HTML Retina Web Reports allow developers and security teams to validate vulnerabilities by replaying them against the website - no more arguing whether something is vulnerable or how to replicate it

4. Proactively Guard Against Application Flaws in Development and in Production

The eEye development and research teams encourage clients to test web applications during development and throughout a solutions production life cycle. This provides a baseline for secure application testing and assists with best practice security assessment and regulatory compliance.

5. Quickly Identify Links and Pages Within your Website and Web Application

Retina Web can reliably and non-intrusively identify all of the pages within your web site and web application and document them graphically by hierarchy and risk. Essentially, if the web site has links, Retina Web will document and assess with the highest accuracy in the industry.

6. Safely Scan your Web Application Without Causing Business Interruptions or Crashing the Application

Retina Web does not scan and test with exploit code and will not crash your systems during a scan. With Retina Web, you can safely scan production environments and obtain accurate results without business interruption.

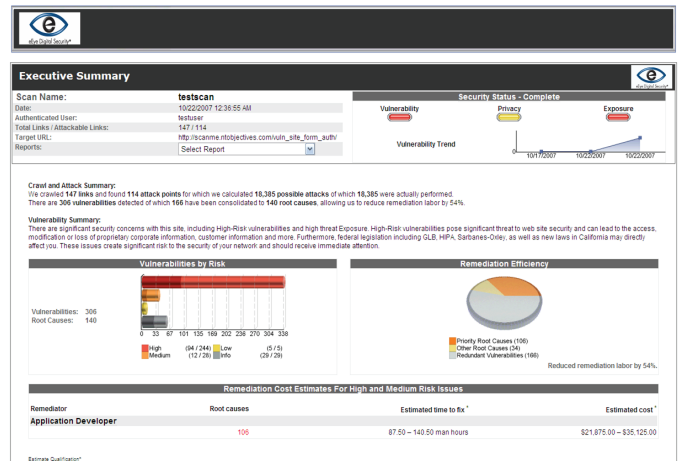
7. Extensive Web Application Support

Retina Web provides extensive support for any operating system hosting a web application and can scan web applications developed in ASP, .NET, PHP, Java, AJAX, ActiveX and HTML

8. Test your Website to see if it is Being Used to Hack your Users

With recent advances in hacking techniques, hackers are using websites to attack users, installing malware like keystroke loggers and rootkits.

- The Bank of India Attack, where an invisible iframe infected user machines, made these attacks famous
- Retina Web is the only tool that can detect if a website is already infected with malware attacks such as the iframe attack (where a hacker inserts code that calls another website to upload malware, such as keystroke loggers, to users of the website)





eEye Digital Security®

RETINA® Web Security Scanner

Key Advantages

- o Independent testing confirms Retina Web finds 10-20 times more vulnerabilities than competing tools
- o Independent testing confirms the lowest false positive rate for a web application scanner
- o Fully automated testing without the need to train the solution on the target website
- o Reports are interactive HTML – they consolidate vulnerabilities by root cause, saving time and money and allow 20 users to validate vulnerabilities through the reports without requiring a license of the tool.
- o Effectively audits more code base than the leading competitors
- o Complete web site and link crawling to document an entire website or web application
- o Comprehensive reporting for executives, developers, database administrators and security experts
- o Backed by an unrivaled vulnerability research and development team
- o Platform independent scanning architecture for auditing any web application regardless of host operating system
- o Innovative, non-intrusive, and safe scanning technology
- o User definable custom audits, programming skills not required
- o Identifies known, unknown, and zero-day vulnerabilities at the application layer
- o Accurate vulnerability detection using multiple engines for verification and analysis
- o Easily identifies common flaws down to the root cause within a web page
- o Runs on Windows 2000, XP, or 2003

Why Use Retina Web Security Scanner

1. Department or enterprise-wide web application security verification

Retina Web scales to meet the requirements of any web application and supports scanning in distributed environments by allowing reports to be managed using any web browser from a central location.

2. Compliance with industry or federal regulations

Retina Web 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 verifying the security and integrity of web applications.

3. Identify security risks and eliminate business interruptions

Less sophisticated and intrusive scanners can crash an application as a result of their scanning by identifying a flaw and executing full exploit code to penetrate the vulnerability. Retina Web does not run any type of exploit code to conduct a scan and accurately identifies vulnerabilities without compromising an application.

4. Link and risk identification

Retina Web can accurately crawl and document all links within a website and determine pages and links connected throughout the application. Vulnerability assessment determines which pages and code pose the greatest risk to the site from hackers to data leakage and appropriately document the risk and severity for prioritized remediation.

Organizations

RETINA WEB – Small to Medium Business (SMB), Large to Enterprise Organizations

Regulated Organizations such as healthcare and financial, manufacturing, and education

Any enterprise using credit cards and subject to PCI

Resellers, VARs, Systems Integrators, Consultants, PCI ASVs

User Environment

PRIMARY

Security, network managers, and developers responsible for the security of critical data and web applications for regulatory compliance, service availability, and business continuity.

SECONDARY

Technology and solution owners within a reseller organization or a technology consultant looking to offer a full-featured solution for web application security verification.

VERTICAL

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



eEye Digital Security®

RETINA® Web Security Scanner

Questions to Consider

1. Do you currently perform web based application scans?
2. Do you currently have, or are you planning to initiate a web application vulnerability assessment project as it relates to security or compliance?
 - If so, what are you looking to improve over your current tool in terms of performance?
 - If so, what challenges are you facing in your application security program?
3. Do you have unknown web servers and web pages appearing on your website or within your infrastructure? How do you know?
4. Have you been exploited or attacked due to a web application flaw?
5. Do you know the financial impact of data loss or a successful web application attack? Do you know how much it costs to remediate this type of problem?

Key Features

◦ Reliable, Non-Intrusive Scanning Technology

Most web application scanners rely on exploit code to verify web application vulnerabilities, frequently exposing services data and databases supporting the solution. Retina Web tests without using exploit code and will not harm your web application even if it is in production.

◦ HTML Reports

Retina Web HTML reports group vulnerabilities by root cause, facilitating remediation efforts. The reports also allow users to validate vulnerabilities by replaying attacks against the website.

◦ Test for Persistent Cross-Site Scripting

Persistent Cross-Site Scripting (where a hacker can permanently inject an attack into the website) is very dangerous because these attacks can be used to upload malware to other machines. Retina Web investigates if a site is susceptible to this form of attack.

◦ Checks for Existing Malware

Retina Web checks user sites for existing instances of links that can upload malware and verifies if a site has already been hacked.

◦ Comprehensive and Current Testing Philosophy

The most advanced and comprehensive scan engine available. Critical vulnerabilities are fully documented and all known exploit methods are fully automated for testing. The amount of techniques used to verify security and integrity far exceeds the leading competition.

◦ Superior Research Team

No security vendor can match the expertise of the eEye Research and Development Teams. Over the last 10 years, eEye has discovered more critical vulnerabilities than all other research group and leads the way in managing the latest threats like web application vulnerabilities.

◦ Extensive Application Support

Retina Web's flexible architecture allows for scanning of any web application regardless of host operating system, database, or web server. Regardless of the technology implemented: ASP, .NET, PHP, Java, AJAX, ActiveX, and HTML, Retina Web can perform fully-automated scans to document vulnerabilities within your business solutions.

◦ Best Practice Approach to Web Application Vulnerability Assessments

Retina Web guides users through the logical steps of setting up a scan, crawling the website, documenting configuration issues, recommending remediation actions and reporting on the entire vulnerability management process using industry accepted best practices for code and web application mitigation.



eEye Digital Security®

RETINA® Web Security Scanner

Key Features con't.

◦ Unrestricted HyperLink Discovery

Retina Web allows for the discovery of a website without restrictions. At a glance, administrators can determine the number and depth of pages and links on their website and review design parameters for usability and functionality for any given web application.

◦ Flexible Remediation Reporting

Within the workflow of Retina Web, users can review targeted reports to identify specific vulnerabilities for remediation by risk, vulnerability or even by function for executives, developers, auditors, and administrators. Retina Web also provides a costing estimate for remediation so that the business can budget accordingly for remediation versus the cost of an exposure.

◦ Wizard Based Auditing

Configuration wizards help ensure corporate policies with regards to credentials, proxies, test criteria, cost estimates, and third party authentication are being correctly simulated against the entire web application.

◦ Granular Attack Control

Administrators can configure simulated attacks within Retina Web by class or build on custom attack policy. Retina Web provides the ability to target scanning efforts where granular results are required and build tests for verification based on your own security needs.

◦ Configurable High-Speed Scanning

Retina Web can scan an entire website with unprecedented accuracy. Retina Web's secret for speed lies in the ability to configure timeouts and retries by using both minimum and maximum value settings. This ensures that the next result is sent as soon as the session is available without artificially padding delays based on the worst case response scenario.

Other eEye Solutions

RETINA

Do you need to perform network based vulnerability assessment scans as well as web application scans?

SECURE IIS

Do you use MS IIS to host web applications? Do you want to protect against web application flaws that have no defined remediation?

RETINA ENTERPRISE

Do you need to centrally manage and report on distributed network scanning and vulnerability assessment initiatives?

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.**