

## What's New in Retina® 5.0

Retina® version 5.0 is the result of exhaustive research and development efforts, combining the award winning technology Retina is known for, with improved functionality in the areas of discovery, remediation and reporting. The following is a partial list of feature enhancements included in this new version. More information can be found at [www.eeye.com/retina](http://www.eeye.com/retina).

### **Workflow Methodology Supported Through User Interface**

Retina's user interface has been enhanced to accommodate a methodical approach to discovery, scanning, remediation and analysis.

The workflow approach to vulnerability assessment and remediation increases the overall efficiency of any security strategy. Discover, Audit, Remediate and Report functions guide users through the logical steps of inventorying network assets, performing vulnerability and policy audits, determining where vulnerabilities are located, prioritizing remediation and lastly, reporting on the process and adapting their strategy accordingly.

### **Discovery Mode**

Retina's discovery scan mode allows for the asset inventory of an entire network (not limited to licensed IP's). Discovery mode features include customizable TCP, UDP and ICMP discovery methods as well as OS detection and general machine data. Discovery results can then be used to create host files, such as address groups, or used to launch a vulnerability assessment scan directly from the discovery interface.

### **Improved OS Detection**

ICMP (Internet Control Messaging Protocol) OS detection method has been incorporated in Retina version 5.0. ICMP delivers an improved detection of Windows devices, which doesn't require domain access. This, combined with existing NMAP fingerprinting database, translates into the utmost accuracy for OS detection. An accurate OS detection is the cornerstone of any vulnerability assessment.

### **Multiple Simultaneous Scans and Scan Scheduling**

Retina now gives users the ability to simultaneously process multiple scan requests, allowing for the scanning of multiple subnets and address groups. Scan jobs can be named and saved to specific output files as well. Additionally, advanced scheduling functionality allows users to schedule scans to be run in accordance with established service windows.



### **Remediation Reporting**

Related to Retina's enhanced interface, specific, detailed remediation reports can be performed, separate from the comprehensive reporting also available. Remediation reports can now be created which group data by vulnerability type, machine criticality or risk level. This allows organizations to run audits and target specific vulnerabilities for remediation, increasing the overall efficiency in responding to worm or virus outbreaks.

### **Wireless Discovery and Auditing**

Using Retina on a device equipped with a wireless network interface card, users can discover active wireless access points broadcasting network traffic. Previously this functionality had required a wired connection. Additionally, Retina determines access point configuration information (SSID, WEP status, IP) and can also test WEP key strength, enforcing critical wireless asset configuration standards.

### **Scan Customization**

User can now configure scan timeouts, OS detection level, tracer levels, etc., allowing them to determine how much information they wish to receive back from a particular scan and increasing the overall speed of scans.

The combination of these feature enhancements with the unique workflow approach to vulnerability assessment and remediation, delivers the most comprehensive security solution available today, backed by the eEye Research Team. This combination of process and technology translates into increased efficiency for the management of network security.

***For more information, or to request an evaluation copy of Retina 5.0, please contact your eEye Sales Representative at 866.339.3732 in the U.S and Canada, 44 0 20 8956.2270 in the U.K or 41 22 718 7700 for rest of Europe.***

