

**WELCOME  
TO SECURITY**

**VULNERABILITY  
IS OVER**



**RETINA**

## **RETINA - NETWORK SECURITY SCANNER**

The first network security software application with state-of-the-art artificial intelligence features that allow it to think like a hacker. Retina works like an around-the-clock human network security analyst, giving you the most comprehensive security analysis available.

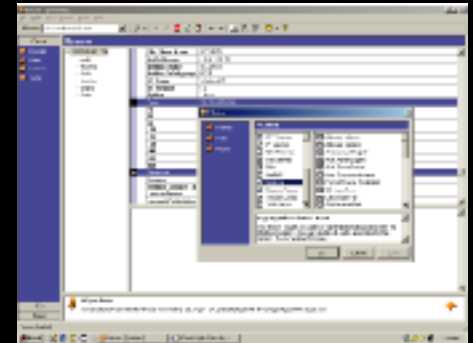
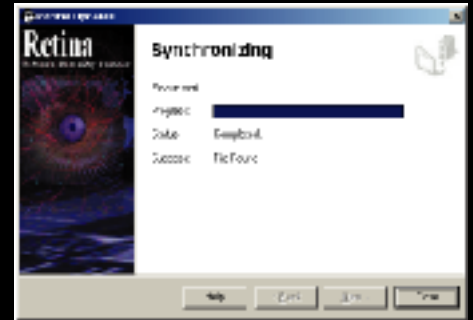
Retina includes easy to navigate reporting tools to help you prioritize and isolate high priority fixes, giving you total control over auditing your network security and open gateways to your internal network.



# RETINA

Retina includes an auto-update feature which provides continuous updates of its modules, allowing users to keep pace with the latest security vulnerabilities.

Retina contains an easy-to-navigate graphical user interface, and executes scans faster than competitive products. Smart scanning enables Retina to run scans for multiple vulnerabilities more efficiently, dramatically cutting down on scan time.



## Retina Features

---

Retina is designed to identify and alert security vulnerabilities, suggest fixes and report possible security holes within a network's Internet, Intranet and Extranet systems.

### Vulnerability Scanning

Vulnerability scanning is the process of checking for all the potential methods that an attacker might use to tamper with an organization's network.

### Graphical User Interface

Retina contains a simple to navigate graphical user interface. This interface can be used to easily control all scanning and reporting features within Retina.

### CHAM (Common Hacking Attack Methods)

This groundbreaking feature is the first of its kind. CHAM employs AI technology in order to simulate the thought process of a hacker or security analyst in finding holes in networks and software packages.

### Fix-It

Retina includes advanced Fix-It technology. This distinct feature allows the network administrator to automatically correct common system security issues including registry settings, file permissions and more.

### Audits

A Retina Audit is a network assessment that identifies and details any problems found that might compromise network security. Retina offers a variety of examples of potential security flaws that can be scanned for.

### Smart Scanning

Retina includes an AI (Artificial Intelligence) module that makes it vastly smarter and intensely thorough about pinpointing real world vulnerabilities.

### Smart Reporting

Retina can produce fully-documented network audit reports based on its security scans.

### Auto Update

Retina encompasses an auto-update feature that provides continuous updates for its modules using an Internet connection. This feature will allow the network administrator to update Retina's modules on a regular basis, thus keeping pace with recently discovered vulnerabilities.

### Open Architecture

Retina has an open architecture that provides the administrator the opportunity to develop vulnerability tests and auditing modules tailored to an organization's precise requirements.

## Audit Modules

---

Retina includes vulnerability auditing modules for the following systems and services:

- Services
- Users and Accounts
- Password vulnerabilities
- Publishing extensions
- Database servers
- Firewalls and Routers
- Proxy Servers
- NetBIOS
- HTTP, CGI and WinCGI
- FTP
- DNS
- DoS vulnerabilities
- POP, SMTP and LDAP
- TCP/IP and UDP
- Registry

## System Requirements

- Windows NT Version 4.0 SP3 or higher
- Internet Explorer Version 4.01 or higher
- 32 MB of memory
- 16 MB of free disk space
- Internet connection  
(optional for remote scanning)