



**eEye Digital Security Whitepaper**  
Enterprise Vulnerability Assessment Selection Criteria

---

For more information about eEye's Enterprise Vulnerability Assessment  
and Remediation Management Solution, visit:  
[www.eeye.com](http://www.eeye.com)

**© 2003 eEye Digital Security  
All Rights Reserved.**

This document contains information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of eEye Digital Security.

**Collateral Information**

eEye Digital Security Whitepaper  
*Enterprise Vulnerability Assessment  
Selection Criteria (WPEVA0403)*  
Revision level 1.3

For the latest updates to this document, please visit:

**<http://www.eeye.com>**

**Warranty**

This document is supplied on an "as is" basis with no warranty and no support.

**Limitations of Liability**

In no event shall eEye Digital Security be liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained in this document is subject to change without notice.

No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this whitepaper.

**Disclaimer**

All brand names and product names used in this document are trademarks, registered trademarks, or trade names of their respective holders. eEye Digital Security is not associated with any other vendors or products mentioned in this document.

## Overview

Selecting an enterprise vulnerability assessment solution is a complex decision that involves a unification of technology and process to proactively guard the organization's network infrastructure. Combining ongoing vulnerability audits with a proven remediation methodology is the most effective approach in threat prevention and controlling network security.

A survey of 223 enterprises found that 90% had suffered some sort of network intrusion. The average company loss of \$2 million for an intrusion was up from \$400,000 just several years ago.

Source: 2002 CSI/FBI Survey

As reported by CERT, greater than 95% of all network security issues involve the exploitation of known vulnerabilities and can be avoided. For an enterprise, preventing just one security breach could mean hours in saved downtime and millions in averted fiscal damage. The challenge for a large, distributed organization is to first understand the constantly evolving network, identify vulnerabilities, and manage the vulnerability data so that corrective actions can be taken systematically to prevent system compromise.

Selecting the best security technology to incorporate into an enterprise-wide process is a daunting challenge. In selecting an enterprise vulnerability assessment solution, there are several key criteria that must be properly weighed and considered. This paper identifies the most common technology-related decision criteria for enterprise-wide vulnerability assessment solution deployments.

## Goals of an Enterprise Vulnerability Assessment Implementation

Every project has a reason for implementation. For an enterprise-wide deployment of a process that seeks to reduce network risks, the mission should be quite clear and provide both high-level and specific goals. The project should be defined so the goals are achievable and the results are measurable based on organization-specific metrics. Examples of high-level goals for an enterprise vulnerability assessment implementation include:

- **Provide accurate network discovery detail**  
What is the current network topology? How many wireless access points are connected at each office location? Are there unauthorized web servers on the network?
- **Identify network risks and prioritize issues**  
How many high-risk vulnerabilities exist on the network? How many low-risk issues remain from last week? How many web servers are without the latest security patches?
- **Enable efficient network-wide remediation**  
What is the remediation process for each network segment? Who is the responsible team member for fixing mail server issues?

As reported by CERT, greater than 95% of all network security issues involve the exploitation of known vulnerabilities and can be avoided.

Source: 2002 CERT/CC

- **Reduce manhours through correct delegation**  
Are the outstanding security events immediately translated into tasks for resolution? Are multiple tasks assigned to the most competent team members for proper resolution? Are remediation instructions accurate and clear?
- **Analyze the security level of the network**  
What is the baseline of network threat levels for any given segment of the network? Are corporate security policies being adhered to?
- **Implement ongoing network threat reduction**  
Can we automate the process of scheduled threat identification using the most current vulnerability audits? How has the network security profile changed in the last week? Has our exposure been reduced?

### Implementing an Enterprise Vulnerability Assessment and Remediation Management Process

In order for an enterprise vulnerability assessment implementation to be successful, a commitment must be made by the organization to institute vulnerability assessment and remediation as an ongoing process. By establishing a process, it is clear that the security mission is continuous and should be viewed as strategic “preventative maintenance” to assure that the network core is protected against attack.

Ongoing Three-Phase Process of Vulnerability Assessment & Remediation Management



While there is no fail-safe security, reactionary security (i.e. scrambling to implement patches when a worm is propagating) is not a strategy and yields inevitable problems.

Following a best-practice methodology of network discovery and auditing, delegation and remediation of events, and thorough analysis and reporting achieves optimal results. It is critical that this process be ongoing. It is imperative that large organizations select the best technology to simplify the vulnerability assessment and remediation process within the organization.

### Selection Criteria for a Vulnerability Assessment and Remediation Management Implementation

An enterprise deployment of a vulnerability assessment and remediation management solution requires a solid foundation to accomplish the primary task at hand – reducing network risks. To achieve this, the core must be based on proven, best-of-breed network vulnerability assessment technology. From this foundation, organizations have the ability to both correct issues and to further utilize data for reporting, event correlation and analysis.

Common selection criteria of large, distributed organizations that have implemented enterprise vulnerability assessment and remediation management solutions include:

- **Distributed Architecture**  
Local host scanning within remote subnets in a distributed network.
- **Scanning Capability**  
Breadth and depth of vulnerability scanning technology including multi-platform scanning of operating systems.
- **Centralized Management**  
Centralized management of all the remote scanning engines.
- **Scalability**  
Ability to scan large subnets and grow with network evolution.
- **Integration with Existing Technology**  
Component-based solution that integrates with and protects existing events management infrastructure (e.g. Tivoli or HP OpenView).
- **Stability**  
Vulnerability scanning application should be stable so that the network resources are not choked.
- **Performance**  
Scan should be completed efficiently and not impede or disrupt system resources.
- **Non-Intrusiveness**  
Scanner should not utilize intrusive testing or exploit code to determine vulnerabilities.
- **Customized Audit Capability**  
Customizable audit creation and an open API architecture to meet varied needs.
- **Reporting**  
Flexible, customizable that is able to accommodate executive and technical needs respectively.
- **Updates**  
New vulnerabilities and threat exposures should be updated regularly and be provided by a leading authority on security vulnerabilities.
- **Confidentiality**  
Reports and alerts should be confidential within the organization; hence role-based user profiles for issue resolution are imperative.
- **Remediation**  
Remediation should include elements of workflow automation from a security perspective. Identified vulnerabilities should be resolved according to the stipulated resources and policies.
- **Verification via Iterative Scans**  
Delta reports comparing sequential scans are essential for showing remediation progress.

### Achieving Threat Reduction Goals with Proven Technology

Utilizing the previously described selection criteria establishes a solid baseline for defining specific vulnerability assessment and remediation management requirements. Organizations seeking to implement a best-practice solution need to consider these criteria as they relate to interoperability within their specific organization. Therefore, some criteria will be of more importance and should be met first in order to achieve organizational goals.

In the end, the entire process needs to be practical, efficient, and effective in reducing network vulnerabilities.

### eEye's Enterprise Vulnerability Assessment Solution

eEye Digital Security's Enterprise Vulnerability Assessment solution is one such offering that is capable of meeting the complex challenge of enterprise-wide threat identification and reduction.

Based on best-of-breed technology and specifically designed to meet the diverse needs of enterprise network security initiatives, eEye's solution is proven, accurate, and effective. The power of eEye's Enterprise Vulnerability Assessment solution is a result of its vulnerability assessment scanning expertise, enterprise management capabilities, and renowned vulnerability research team. As a modular offering, eEye's solution is both powerful and flexible to meet the varied needs of any organization.

The following is a brief snapshot of how eEye's Vulnerability Assessment solution applies to some specific needs common in large, distributed enterprises:

#### **Requirement: Top-rated scanner engine in the categories of accuracy, safety, and bandwidth utilization**

eEye's Vulnerability Assessment Solution incorporates Retina® Network Security Scanner as the scanning engine. Retina is the industry's leader in the vulnerability assessment market, recognized for its accuracy, non-intrusiveness, speed, and ability to perform custom audits. Retina utilizes no exploit code (nor partial exploit code) in the scanning process, and incorporates third-party confirmation, resulting in fewer false-positives and higher accuracy. Retina's scanning engine utilizes appropriate bandwidth when performing audits, and recognizes and adapts to network/host saturation. Furthermore, Retina's audits are specially designed to be non-intrusive, accurate, and fast – further reducing network stress and bandwidth.

"[eEye's Enterprise Vulnerability Assessment solution] becomes more than just useful for the enterprise; it becomes an asset. This is a product worth having."

Source: *InfoWorld* (2/21/03)

**Requirement: Component-based solution architecture protects current IT investment**

eEye's solution incorporates several modular components, which may or may not be necessary depending on the customer's environment. This architecture enables existing IT assets to be leveraged. With data bridges, existing network management consoles or help desk ticketing systems (e.g. Tivoli, CA, and Remedy) can manage vulnerability information.

**Requirement: Flexible reporting: executive summary level, technical detail level, and remediation-focused reports**

Via the centralized data repository in eEye's Enterprise Vulnerability Assessment solution, and through the management console, varying report types are readily available to the executive, security administrators, and systems administration personnel. Report access can be customized based on user level. Reports include the SANS Top 20, delta, Top 20 ports, services, users, and many more. Remediation management tracking by user or group is also available.

**Requirement: Extensibility of Retina with built-in audit creation wizard and open API architecture**

Custom audits may be swiftly created through Retina's Audit Wizard feature. More sophisticated Audit Modules, including those with remediation-oriented activities or policy-enforcement capabilities, may be incorporated into the assessment process using Retina's API functions.

**Requirement: Distributed Retina scanner deployments for protected network segments**

This capability allows discrete subnets to be scanned locally without interference from firewalls. Remote management of scanner engines is securely accessed from any web browser. Scan data is delivered to a central repository via an encrypted channel.

**Requirement: Completely automated scan scheduling and updating of scanning engine updates**

eEye's Enterprise Vulnerability Assessment solution provides true *set-and-forget* functionality. All aspects of the scanner engine's operation can be pre-determined and timed to execute at will. Updates to the vulnerability identification database occur automatically, ensuring that the latest threats are accurately identified for correction.

To learn more about eEye Digital Security's Enterprise Vulnerability Assessment and remediation management solution, visit:

<http://www.eeye.com/html/Solutions/EnterpriseVA/index.html>