McAfee®

Protect what you value.

McAfee Vulnerability Manager

Identify risk exposures and policy violations, prioritize resources, and reduce risk

Quickly and accurately find and prioritize vulnerabilities and policy violations on all of your networked systems. Balance asset value, vulnerability severity, threat criticality, and countermeasures to focus protection on your most important assets.

KEY ADVANTAGES

Make informed decisions

- **Combined vulnerability, asset, and countermeasure information**
- **Threat intelligence and correlation**
- **Customizable reports and predefined audit reports**

Operational efficiency

- **Agentless policy compliance auditing**
- **Automatically discover and prioritize vulnerability and policy violations**
- **Accurate vulnerability and OS identification**
- **Eliminate incorrect patching**

Scalable, enterprise-class protection across any size network

Extended benefits through integration

- Integration with other McAfee products for:
  - **Aggregating vulnerability data from multiple sources**
  - **Automated patching and remediation**
  - **Network-based intrusion prevention system (IPS)**

Priority-based Risk Management

How do you mitigate risks and protect your most valuable assets in the face of changing vulnerabilities and threats? How do you direct IT and security efforts when and where they are most needed? How do you improve workflow and confidently demonstrate compliance at audit time?

Make more informed security decisions using the priority-based approach of McAfee® Vulnerability Manager (*formerly McAfee Foundstone® Enterprise*). Vulnerability Manager increases the accuracy and usefulness of security intelligence by combining vulnerability, asset, and threat criticality information. Our hardened appliances increase the efficiency of your existing resources, resulting in a low cost of ownership. This solution integrates with other McAfee products and with third-party technologies to leverage your investments and extend the benefits of protection and compliance to risk-aware intrusion prevention, monitoring risk scores, countermeasure awareness, and problem resolution.

Measure your exposure to common government and industry regulations with regulation-specific templates for the Sarbanes-Oxley Act (SOX), the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act (HIPAA), BS7799/ISO27002, and the Payment Card Industry Data Security Standard (PCI DSS). Our templates help you see which systems are out of compliance before your auditors arrive.

Broad and Accurate Content Coverage

With Vulnerability Manager, you get a broad selection of checks for IT vulnerabilities and policy violations. Determine how emerging threats and vulnerabilities affect your risk profile—immediately and accurately. And you'll more easily and accurately comply with regulations and policies. In fact, Vulnerability Manager now delivers agentless policy-compliance auditing to your users without the need to deploy additional software or management consoles.

Vulnerability Manager is the only network scanner that incorporates countermeasure intelligence from McAfee ePolicy Orchestrator® (ePO™), our proven, centralized management console with more than 50 million installations at enterprises worldwide. Because ePO data provides a more complete system picture for more accurate assessments, you reduce the sense of urgency and patch only the most vulnerable systems.

DEPLOYMENT OPTIONS

Appliances—purpose-built, hardened appliances

- Vulnerability Manager 1000 and Vulnerability Manager 850
  - Enterprise Manager
  - Vulnerability and asset databases
  - Scan engine
  - Report engine

Software-only

- Deploy on your own hardware; includes Enterprise Manager, vulnerability and asset databases, and scan engine

Minimum requirements

Hardware

- CPU: Dual Xeon 2 Ghz, Dual Core Xeon 2.33 Ghz, or better
- RAM: 2 GB
- Disk space: 80 GB partition
- Ethernet network interface

Operating system

- Microsoft Windows 2000 Server with Service Pack 4
- Microsoft Windows 2003 Server Standard Edition with Service Pack 1

Database

- Microsoft SQL Server 2005 with Service Pack 1 or SQL Server 2000 with Service Pack 4
- All SQL hotfixes and patches

Integrated and Comprehensive Remediation

Need to patch? McAfee Remediation Manager automatically fixes the vulnerabilities and policy violations identified by Vulnerability Manager. Or do you want to block threats at the network level? McAfee Network Security Platform (*formerly McAfee IntruShield®*) correlates Vulnerability Manager data and launches on-demand scans, so that your network security is in synch with your updated risk posture.

Added Help with PCI DSS Compliance

Vulnerability Manager helps customers meet specific mandates outlined in the PCI DSS. Through its ability to verify security patch installations, identify new vulnerabilities, and deliver vulnerability updates, Vulnerability Manager helps companies comply with Requirements 6.1, 6.2, and 11.2. McAfee PCI Certification Services extends this value by meeting another requirement—quarterly external scans performed by a qualified scan vendor. McAfee is an Approved Scan Vendor (ASV), and our PCI Certification Service external scanning supplements the vulnerability and policy auditing assessments performed by Vulnerability Manager.

Features

Priority-based auditing and remediation

- Perform assessments against your security policies and pinpoint your most valuable assets, target high-risk vulnerabilities, and apply remediation to the most critical threats
- Import buffer-overflow protection data from system protection (ePO) to reduce emergency patching during crisis and allow focus on critical vulnerabilities

Comprehensive vulnerability and policy checks

- Uncover unmanaged devices such as rogue wireless access points or forgotten virtualized VMware hosts on your network
- Customizable templates measure compliance with SOX, PCI DSS, HIPAA, ISO27002, FISMA, and the Federal Desktop Core Configuration (FDCC) mandate
- Vulnerability Manager's Foundstone Scripting Language (FSL) scripts allows security professionals to write custom vulnerability checks to test proprietary and legacy programs
- Receive comprehensive, timely vulnerability coverage 24/7 from McAfee Avert® Labs, the world's most respected global threat research center

Policy compliance made easier

- Provide users with expanded scanning capabilities through predefined policy checks; results are captured, stored, and reported
- Define the specific parameters of new policy audit checks with an easy-to-use, wizard-based interface

Configurable rule-based asset identification

- Automatically group and track assets by device type (web server, workstation, mail server), OS type, IP address range, host names, DNS names, or custom rules

Flexible reporting

- Pull reports by platform, business unit, geography, or IP range for insight into policy violations, vulnerabilities, remediation actions, and changing risk profiles
- Predefined templates for government and industry regulations and standards reduce the headache and complexity of demonstrating compliance
- View the results of agentless policy audit scans for Windows and Unix systems with flexible and detailed reporting options
- Detailed compliance reports, such as compliance summary, compliance detail by host, and compliance detail by policy
- FoundScores help you understand, measure, and report on your risk profile over time, showing you changes by scan, risk level, vulnerability, and platform

DEPLOYMENT OPTIONS (continued)

Supplemental applications

- **Vulnerability Manager supports the following applications:**
  - **FSDBUTIL**
  - **Open application programming interface and software development kit (API/SDK)**
  - **Certificate tools**
  - **FSUpdate**
  - **Enterprise resource management (ERM)**

"By enabling a priority-based approach to managing our network security risk, McAfee Vulnerability Manager has enabled CSU, Chico, to significantly mitigate risk and improve our overall security risk posture."
—Jason Musselman, information security analyst, CSU, Chico

For more information, visit *www.mcafee.com.*

Highly scalable open architecture

- Vulnerability Manager's multi-tiered scanner, management, and database are designed to fit your environment
- Features include asset-based discovery, management, scanning, and reporting

Accurate OS and vulnerability checking and immediate threat assessment

- Import asset and operating system data from ePO to the Vulnerability Manager database for improved protection and accuracy, so that patches can be applied correctly
- Identify assets that are already protected by other countermeasures, helping you apply remediation to more vulnerable assets and reduce emergency patching
- Without rescanning your entire network, Vulnerability Manager can visualize and rank risk potential of new threats in minutes by correlating breaking threats to your existing asset and vulnerability data
- Credential-based scans of Microsoft Windows, UNIX, Cisco IOS, and VMware platforms pinpoint vulnerabilities and policy violations with the highest level of precision in the industry

Operational efficiency

- Centralized scan management allows you to increase the speed of scans without having to select the specific scan engine for the run
- Through asset synchronization with Lightweight Directory Access Protocol (LDAP) and Active Directory (AD), you can configure multiple LDAP servers for Vulnerability Manager to import asset information; administrators spend less time creating and grouping IT assets to scan
- Patch, configure, monitor, and manage an entire Vulnerability Manager deployment in a centralized, uniform way with Configuration Manager
- Get automatic software and configuration updates, health and status monitoring, and email notifications
- Manage certificates through a single management console

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

McAfee®