McAfee Vulnerability Manager

Identify 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

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

Integrate with other McAfee products
- Unified IT policy auditing
- Automated patching and remediation
- Network-based intrusion prevention

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, unified IT policy auditing, countermeasure awareness, and problem resolution.

Measure your exposure to common regulations and security standards with templates for the Sarbanes-Oxley Act (SOX), the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Desktop Core Configuration (FDCC) baseline, 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. In fact, Vulnerability Manager delivers agentless policy compliance auditing to your users without the need to deploy additional software or management consoles. It integrates with ePO and McAfee Policy Auditor for simplified auditing across both managed (agent) and unmanaged (agentless) systems.

Vulnerability Manager is the only network scanner that incorporates asset information from McAfee ePolicy Orchestrator® (ePO™), our proven, centralized management console with more than 58 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.

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.

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, scan engine, and utility for operating system hardening

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 2003 Server Standard Edition (x86) with Service Pack 2

Database
- Microsoft SQL Server 2005 with Service Pack 2 or SQL Server 2000 with Service Pack 4
- All SQL hotfixes and patches

Virtualization
- VMware Virtual Infrastructure 3 (VMware ESX 3.x)

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)

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. The McAfee PCI Certification Service 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
- Customizable templates measure compliance with SOX, PCI DSS, HIPAA, ISO27002, FISMA, and the Federal Desktop Core Configuration (FDCC) baseline
- Uncover unmanaged devices such as rogue wireless access points or forgotten virtualized VMware hosts on your network
- Vulnerability Manager FASL Scripts allow security professionals to write custom vulnerability checks to test proprietary and legacy programs
- Vulnerability Manager's assessment capabilities include content built by third parties that follow XCCDF, OVAL and other open standards in the Security Content Automation Protocol (SCAP)

Policy compliance made easier
- Use predefined policy checks for expanded scanning; results are captured, stored, and reported
- Define the specific parameters of new policy audit checks with an easy-to-use, wizard-based interface
- Develop a policy baseline from a "gold standard" system scan, then assess other systems for compliance

Configurable rule-based asset identification
- Configure vulnerability scans based upon individual assets or groups without having to enter IP ranges
- 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
- View vulnerability information, combined with security protection data, in McAfee ePO reports
- Pull reports by platform, business unit, geography, or IP range for insight into policy violations, vulnerabilities, remediation actions, and changing risk profiles
- View the results of agentless policy audit scans for Windows and Unix systems with flexible and detailed reporting options
- Within the ePO console, view the combined results of agent-based and agentless audits
- Detailed compliance reports, such as compliance summary, compliance detail by host, and detail by policy
- Transmit vulnerability assessments in XCCDF report format

Highly scalable open architecture
- Vulnerability Manager's multi-tiered scanner, management, and database are designed to fit your infrastructure needs
- Configure for asset-based discovery, management, scanning, and reporting, based on ePO, AD or LDAP groupings
- Support for deployment in virtualized VMware environments

Immediate threat assessment
Correlate threat information with asset values and vulnerabilities, 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 using threat advisory information delivered automatically

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

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

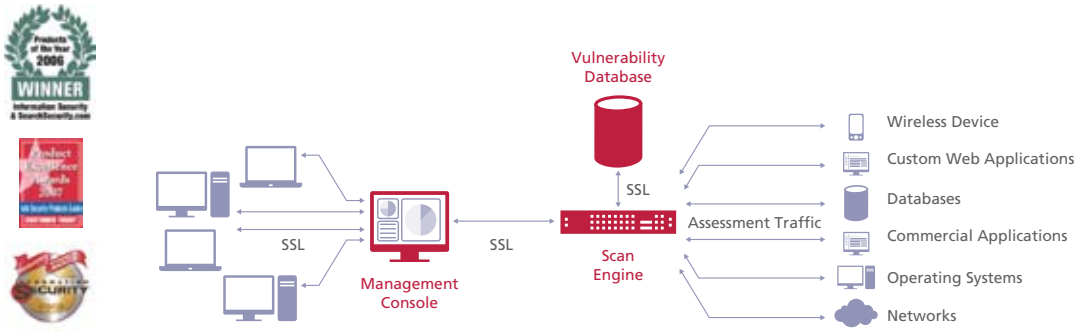
For more information, visit *www.mcafee.com*

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

Integrate with ePO to optimize existing investments in security management infrastructure

- Vulnerability Manager provides ePO with information on unmanaged assets
- Vulnerability Manager scans are performed across asset groups, not just IP ranges
- McAfee Threat Information Service (MTIS) feeds are directed into ePO and are correlated with vulnerability information and security protection provided by other McAfee products
- Quantitative risk scores (using Vulnerability Manager results) are computed and stored within ePO
- Unified policy auditing templates perform agent-based and agentless assessments at the same time



McAfee Vulnerability Manager utilizes a multi-tier architecture to maximize scalability and deployment flexibility.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

5389ds_grc_vm_6.7_0109