

# McAfee Vulnerability Manager

Evaluate 100 percent of your network 100 percent of the time

When scanning for vulnerabilities, coverage counts. The McAfee® Vulnerability Manager solution delivers unrivaled scalability that canvasses everything your network can serve up. If it has an IP address or URL, the McAfee Vulnerability Manager solution can discover and assess it. In addition, more than 400 researchers and millions of sensors around the globe deliver continuous vulnerability and threat research to protect you ahead of new or evolving threats. Guard your business with the industry's most flexible, proven, and scalable solution—comprehensive vulnerability management made simple.



## Key Differentiators

- Ultimate flexibility in reporting, scanning, and deployment options
- Unmatched vulnerability coverage and scanning accuracy
- Unrivaled data integration with home-grown and third-party applications
- Unprecedented response to threats via McAfee Global Threat Intelligence
- Unique capability to prove “not vulnerable” to threats

## Breadth of Coverage

- Supports leading enterprise operating systems, including Microsoft Windows, UNIX, Cisco, Linux, Mac, and VMware platforms
- Deep scans Web applications (OWASP Top 10 and CWE Top 25)
- Looks for vulnerabilities in enterprise infrastructure such as Adobe, AOL, Apple, Microsoft (Office, IIS, Exchange), Blue Coat, CA, Cisco, Citrix, Facebook, Google, HP, IBM (Lotus Notes and Websphere), Novell, Oracle, Real Networks, RIM (Blackberry Enterprise Server), SAP, Sun Java, Symantec, VMware, Yahoo, and more
- Scans leading databases, including DB2, MySQL, Oracle, Postgress, Microsoft SQL Server, and Sybase

Thousands of organizations rely on the McAfee Vulnerability Manager solution to quickly find and fix vulnerabilities, from organizations with a few hundred nodes to one continuously scanning over four million IPs.

The McAfee Vulnerability Manager solution sets the market standard by working with the realities that define your business, canvassing all types of network and asset configurations. It can scan nonstop or exactly when and where you need it, allowing you to automatically discover, assess, remediate, and report on all your assets.

## Easy to Implement—In Your World

McAfee makes it simple to implement reliable scanning. The McAfee Vulnerability Manager solution easily installs on your physical or virtualized hardware, or you can use our hardened appliances. Within minutes, you are starting your first scan.

Loading and maintaining your asset inventory is simple, too. Since we integrate directly with enterprise asset management tools, including LDAP, Microsoft Active Directory, and the McAfee ePolicy Orchestrator® (McAfee ePO™) management platform, you can maintain one central repository for asset data. We can also discover and map everything on your network. The rogue devices, forgotten VMware hosts, and other systems that drift on and off your network will surprise you.

For fast policy definition, scan a “gold standard” system to establish a baseline, use the compliance templates we provide, or load policies leveraging our Security Content Automation Protocol (SCAP) support.

These policy-based scans help you benchmark and document compliance with industry regulations.

## Precision Coverage—Made Convenient

Through penetration testing, authenticated scanning, and non-credentialed scanning, the McAfee Vulnerability Manager solution accurately scans everything on your network. This breadth and depth lets you pinpoint vulnerabilities and policy violations with the highest level of precision.

We scan all networked assets, from smartphones to printers, and everything in between. We even scan tricky assets located in air-gapped and critical infrastructure environments. For instance, secure networks are often not allowed an external connection. A laptop or virtual scanner can be used to discover and scan these assets. The results can remain in the restricted environment or, if needed, be rolled up to report data to a centralized system.

For dynamic or portable assets, our asset-centric scanning makes it easy to define scan groups in terms that make sense to your business while reducing the need for repeated scans. You can target each scan with combinations of IP ranges, organizations, system types, and other tags.

Most operating systems require asset credentials before they reveal sensitive configuration information, but these credentials are a management nightmare. Our shared, centralized credentials cut time and hassle when scanning credentialed systems.

#### Standards and Certifications

- Includes templates for the most popular compliance templates such as ASCI 33, BASEL II, BILL 198 (CSOX), BSI IT (GR), CoBIT, FDCC, FISMA, GLBA, HIPAA, ISO 27002, JSOX, MITS, PCI, SOX, NIST SP 800-68, SANS Top 20, SCAP, OVAL, and more
- Supports standards, including CIS-certified audits, COBIT, CPE, CVE, CVSS, DISA STIG, FDCC/SCAP, ISO17799/ISO 27002/FINRA, ITIL, NIST-SP800, NSA, OVAL, and SANS Top 20
- Common Criteria certified
- FIPS-140-2 encryption validated

#### Looking for technical specifications?

Visit [www.mcafee.com](http://www.mcafee.com) for current hardware and software specifications and requirements.



#### Unrivaled Detection of Vulnerabilities— And Malware Too

Where others merely look at superficial open ports and configurations, we go deep. We make system and application-level assessments that include database banners, policy settings, registry keys, file and drive permissions, and running services. We test more than 450 operating system versions to detect the broadest range of vulnerabilities.

In addition to our predefined checks and updates for zero-day threats, you can write custom scripts and checks to test proprietary and legacy programs. The McAfee Vulnerability Manager solution also assesses third-party content that follows XCCDF, OVAL, and other SCAP standards.

Leveraging fully automated capabilities, McAfee Vulnerability Manager does deep web application scanning canvassing everything across the spectrum of web vulnerabilities including those checks called for in the 2010 OWASP Top 10 and CWE-25 categories. Since web applications are the doorway to your business they must be treated with the same care and urgency as servers and other critical assets. McAfee Vulnerability Manager allows administrators to manage web applications just as they manage traditional network based assets. Web application assets can be grouped, have their own criticality, asset owners and personalities.

Our inspections catch malicious content, too, including Trojans, viruses, and other malware. Millions of sensors around the world direct hundreds of McAfee Labs™ researchers to the latest changes in the threat landscape. This global threat intelligence feeds directly into the McAfee Vulnerability Manager solution for real-time risk assessments and threat advisories to protect you ahead of the threat.

#### High Performance, Manageable—And Open

Some organizations centralize, some prefer a distributed environment. McAfee offers the flexibility to architect your scans, reporting, and management to work the way you prefer.

Monitor the progress of hundreds of remote scanning engines, not just the assets local to a scanner. Manage it all from a single console for a consolidated view of the vulnerability status for your entire network. You can also construct separate scan environments and aggregate select data after the fact.

Our multitiered architecture scales to meet the needs of any size organization. Through an open application programming interface (API), the McAfee Vulnerability Manager solution can integrate with your applications, from in-house to third-party products. With our fully documented API, vulnerability management can be tightly integrated with the full IT security lifecycle, including trouble ticketing, remediation, security information and event management (SIEM), and configuration and patch management.

#### Find and Fix Fast—With Less Stress

Beyond identifying your vulnerabilities, we're able to direct your patch efforts intelligently and drive down the cost of audits. This insight comes from a single correlated, actionable view.

For instance, on Patch Tuesdays, you can quickly decide which machines could be affected by a new Microsoft Windows or Adobe vulnerability. In minutes, without rescanning your entire network, the McAfee Vulnerability Manager solution visualizes and ranks the risk potential of new threats based on existing configuration data and risk scores.

In addition to standards-based scoring, our patented McAfee FoundScore™ technology—a McAfee risk formula—uses a unique algorithm that takes into account asset criticality, risk rating for discovered vulnerabilities, resource type, and other variables to deliver a usable risk grading.

With McAfee FoundScore technology, you can select assets based on criticality and right-click to run an instant, targeted scan. While the scans run, the McAfee Vulnerability Manager solution will show you each system's software or confirm that appropriate intrusion prevention is in place.

Conclusive evidence—such as expected and actual scan results, any systems not scanned, and any failed scans—documents that specific systems are “not vulnerable,” an increasingly common audit requirement.

As you work, tailor scans and reports with virtually unlimited flexibility. You can also analyze data and use the McAfee ePO query and report engine to aggregate, filter, organize, and distribute results.

Comprehensive vulnerability management has never been simpler.

