Data Sheet

# McAfee Vulnerability Manager

## Real-time, high-performance continuous asset monitoring

### Key Differentiators

- Unmatched scalability, accuracy, and flexibility.
- Real-time assessment of new devices the moment they appear on the network, full software and hardware asset inventory, user-to-asset mapping, and automatic network topology.
- Combines active and passive network discovery and monitoring to reveal virtualized, mobile, and hidden devices.
- Deep audits of devices guide scans and feed an authoritative asset database.
- Dynamic system tagging can fully automate vulnerability assessment.
- Updated on the latest vulnerabilities and threats through McAfee Global Threat Intelligence.
- Elevated credential-based security with Cyber-Ark integration.
- Scans both IPv4 and IPv6 networks.
- Fully flexible reporting—scan assets once and report against them anytime.
- Automated risk management workflows can include McAfee, home-grown, and third-party applications.

Protect your business with the industry's most flexible, proven, and scalable solution—comprehensive vulnerability management made simple and performed in real time. McAfee® Vulnerability Manager with the McAfee Asset Manager feature—part of the Intel® Security product offering—delivers unrivaled scalability and performance, actively and passively canvassing everything on your network. If a device or asset has an IP address or is using your network, McAfee Vulnerability Manager can discover and assess it, automatically in real time, revealing the compliance of all assets on your network.

McAfee Vulnerability Manager sets the market standard by working with the realities that define your business, canvassing all types of network and asset configurations. It scans passively, nonstop, or actively when and where you need it, allowing you to discover, assess, remediate, and report on all your assets. You can uncover devices hidden on your network as well as smartphones, tablets, and laptops that come and go between scheduled scans. What you haven't been seeing or scanning will surprise you—and could be jeopardizing your compliance. Thousands of organizations rely on McAfee Vulnerability Manager to quickly find and prioritize vulnerabilities, with deployments ranging from a few hundred nodes to one continuously scanning more than four million IP addresses.

### Implement Easily

We make it simple to implement reliable scanning. McAfee Vulnerability Manager easily installs on your physical or virtualized hardware—or you can use hardened McAfee appliances. Within minutes, you can start your first scan.

Loading and maintaining your asset inventory is simple too. With the McAfee Asset Manager module, the asset database updates immediately as new devices go online, ensuring that you know in real time what devices are out there. In addition, McAfee Vulnerability Manager integrates directly with enterprise asset management tools, including LDAP, Microsoft Active Directory, and the McAfee® ePolicy Orchestrator® (McAfee ePO™) management platform, so you can maintain one central repository for asset data.

### Get Visibility into All Assets

The McAfee Asset Manager option increases visibility through always-on passive discovery and monitoring. Quickly deployed on a SPAN port, this system monitors traffic to discover and map everything on your network, including rogue devices, forgotten VMware hosts, and mobile devices. As it watches, it enumerates devices, patterns, and communications—details that help you gauge and mitigate risk. Device details are automatically sent to McAfee Vulnerability Manager for immediate assessment. In addition, McAfee Asset Manager can perform a full software and hardware inventory on each asset it discovers.

intel Security

### Scanning Coverage

- Scans more than 450 varieties of operating systems, including Microsoft Windows, UNIX, Cisco, Android, Linux, Apple Macintosh, Apple iOS, and VMware platforms.
- Deeply scans web applications (OWASP Top 10 and CWE Top 25).
- Searches for vulnerabilities and malware in 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, Oracle Java, Symantec, and VMware software.
- Scans leading databases, including DB2, MySQL, Oracle, Microsoft SQL Server, and Sybase.

### Standards and Certifications

- Includes templates for 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.

## Customize Scans to Your Requirements

McAfee Vulnerability Manager provides several options to help you benchmark and document compliance with industry regulations. For fast policy definition, scan a 'gold standard' system to establish a baseline, take advantage of provided compliance templates, or load policies leveraging the security content automation protocol (SCAP).

McAfee Vulnerability Manager scans all networked assets, even tricky assets located in air-gapped and critical infrastructure environments. For instance, if you have networks without an external connection, you can deploy a laptop-based or virtual scanner to discover and scan these assets. You then have the choice of keeping the results in the restricted environment or, if needed, rolling them up to a centralized system.

Most operating systems require asset credentials before they reveal sensitive configuration information, but some security teams find it challenging gaining access to these credentials. With the integration of Cyber-Ark's Privileged Identity Management Suite, highly secure credential-based discovery and scanning happens easily and securely with excellent performance.

## Determine Risk in Minutes

When McAfee Asset Manager identifies a new system on your network, it passes detailed information about that system to McAfee Vulnerability Manager to trigger a targeted scan. In minutes, you know the status of that system and the risk it poses to your environment.

## Tag Assets for Efficiency

You can also use tagging policies to place new devices in scan groups automatically based on each device's profile and risk. The right scan could be immediate or part of the next periodic scan, depending on the policies you define.

## Detect Both Vulnerabilities and Malware

Where others merely look at superficial open ports and configurations, McAfee Vulnerability Manager goes much deeper. It makes system and application-level assessments that include database banners, policy settings, registry keys, file and drive permissions, and running services. The product tests more than 450 operating system versions to detect the broadest range of vulnerabilities. Our inspections catch malicious content too, including Trojans, viruses, and other malware.

You can augment predefined checks and updates for zero-day threats by writing custom scripts and checks to test proprietary and legacy programs. McAfee Vulnerability Manager also assesses third-party content that follows XCCDF, OVAL, and other SCAP standards.

## Pay Extra Attention to Web Applications

McAfee Vulnerability Manager allows administrators to manage web applications just as they manage traditional network-based assets. Web application assets can be grouped and have their own criticality, asset owners, and personalities. Leveraging fully automated capabilities, McAfee Vulnerability Manager does deep web application scanning across the spectrum of web vulnerabilities.

## Stay Up to Date

Millions of sensors around the world direct hundreds of McAfee Labs researchers to the latest changes in the threat landscape. McAfee Global Threat Intelligence feeds real-time risk assessments and threat advisories directly into McAfee Vulnerability Manager to protect you ahead of emerging threats.

## Manage, Scale, and Integrate as Needed

We offer the flexibility to design your scans. We also offer the reporting and management to work the way you prefer. Monitor just the assets local to a scanner or view the progress of hundreds of remote scanning engines from a single console. Our multitiered architecture scales to meet the needs of any size organization.

Through an open application programming interface (API), McAfee Vulnerability Manager can integrate with most applications.

## Respond Based on Risk

A single actionable view of vulnerabilities drives down patching and audit costs. 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, McAfee Vulnerability Manager prioritizes and ranks the risk potential of new threats based on existing configuration data and risk scores.

With this information in hand, you can select assets based on criticality and right-click to run instant, targeted scans.

## Get Compliant, Be Confident

Conclusive evidence—such as expected and actual scan results, systems not scanned, and failed scans—provides documentation that specific systems are 'not vulnerable,' an increasingly common audit requirement. Through the combination of active and passive monitoring, penetration testing, authenticated scanning, and non-credentialed scanning, McAfee Vulnerability Manager lets you pinpoint vulnerabilities and policy violations with the highest level of precision. Comprehensive vulnerability management has never been simpler.

**McAfee. Part of Intel Security.**
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com