McAfee
An Intel Company

# McAfee Vulnerability Manager

## Kontinuierliche leistungsfähige Ressourcenüberwachung in Echtzeit

### Hauptvorteile

- Unübertroffene Skalierbarkeit, Präzision und Flexibilität
- Echtzeitanalyse neuer Geräte, sobald diese auf das Netzwerk zugreifen; vollständiges Inventar aller Soft- und Hardware-Ressourcen; Zuordnung von Benutzern zu Ressourcen; automatische Netzwerktopologie
- Kombination aus aktiver und passiver Netzwerkerkennung sowie -Überwachung, um virtualisierte, mobile und verborgene Geräte zu entdecken
- Tiefgehende Geräte-Audits, die die Ausführung von Scans steuern und die entsprechenden Informationen in einer verbindlichen Ressourcen-Datenbank speichern
- Dynamische Kennzeichnung von Systemen zur vollautomatischen Schwachstellenanalyse
- Neueste Informationen zu Schwachstellen und Bedrohungen dank McAfee Global Threat Intelligence™
- Höhere auf Anmelde-informationen basierte Sicherheit durch Integration von Cyber-Ark
- Scans von IPv4- sowie IPv6-Netzwerken
- Absolut flexible Berichterstellung – nach einmaligem Scan von Ressourcen können diese jederzeit in Berichte aufgenommen werden
- Automatisierte Arbeitsabläufe bei der Risikoverwaltung mit Berücksichtigung eigener Lösungen sowie Anwendungen von McAfee und von Drittanbietern

Schützen Sie Ihr Unternehmen mit der branchenweit flexibelsten, bewährtesten und skalierbarsten Lösung. Sie bietet Ihnen umfassende Schwachstellenverwaltung, die einfach zu bedienen ist und in Echtzeit erfolgt. McAfee® Vulnerability Manager mit der Funktion McAfee Asset Manager bietet unübertroffene Skalierbarkeit und Leistung bei der aktiven und passiven Überprüfung aller Ressourcen in Ihrem Netzwerk. Alle Geräte oder Ressourcen, die eine IP-Adresse besitzen oder auf Ihr Netzwerk zugreifen, werden von McAfee Vulnerability Manager automatisch und in Echtzeit erkannt sowie analysiert, um die Compliance aller Ressourcen in Ihrem Netzwerk zu ermitteln.

Durch die Berücksichtigung der heutigen Situation von Unternehmen setzt McAfee Vulnerability Manager branchenweit neue Maßstäbe. Die Lösung erfasst sämtliche Netzwerk- und Ressourcenkonfigurationen und kann permanent passiv oder bei Bedarf aktiv Scans durchführen. Dadurch können Sie sämtliche Ressourcen erkennen und analysieren sowie Probleme beheben und Berichte erstellen. Mithilfe von McAfee Vulnerability Manager können Sie in Ihrem Netzwerk verborgene Geräte sowie Smartphones, Tablets und Laptops finden, die zwischen den geplanten Scan-Intervallen auf das Netzwerk zugreifen. Sie werden überrascht sein, was Sie bislang nicht gesehen oder gescannt haben. All diese unkontrollierten Ressourcen könnten Ihre Compliance gefährden. Daher setzen tausende Unternehmen auf McAfee Vulnerability Manager, um Schwachstellen schnell zu finden und nach Priorität zu staffeln. Die überwachten Bereitstellungen umfassen dabei Größenordnungen zwischen einigen hundert Knoten ebenso wie permanente Scans von über vier Millionen IP-Adressen.

### Einfache Implementierung

McAfee vereinfacht die Implementierung zuverlässiger Scans. McAfee Vulnerability Manager lässt sich problemlos auf Ihrer physischen oder virtuellen Hardware installieren. Alternativ werden abgesicherte McAfee-Appliances angeboten. In beiden Fällen können Sie innerhalb weniger Minuten Ihren ersten Scan starten.

Auch das Laden und Verwalten Ihres Ressourcen-Inventars ist einfach. Sobald ein neues Gerät auf das Netzwerk zugreift, aktualisiert das McAfee Asset Manager-Modul sofort die Ressourcen-Datenbank und gewährleistet dadurch den Echtzeitüberblick über sämtliche Geräte in Ihrem Netzwerk. Außerdem integriert sich McAfee Vulnerability Manager direkt in Ressourcen-Management-Tools von Unternehmen, einschließlich LDAP, Microsoft Active Directory und die Verwaltungsplattform McAfee® ePolicy Orchestrator® (McAfee ePO™). Dadurch können Sie ein zentrales Repository für Ressourcen-Daten nutzen.

### Transparenz für alle Ressourcen

Der zusätzlich erhältliche McAfee Asset Manager verbessert die Transparenz durch permanente passive Erkennung und Überwachung. Dieses System kann innerhalb kürzester Zeit auf einem SPAN-Port bereitgestellt werden und überwacht den Datenverkehr, um sämtliche Ressourcen in Ihrem Netzwerk – nicht autorisierte Geräte, vergessene VMware-Hosts sowie Mobilgeräte – zu erkennen und zu analysieren. Dabei identifiziert das System Geräte, Muster und Kommunikationsvorgänge, also Details, die beim Aufspüren und Beheben von Risiken nützlich sind. Die Informationen zu den Geräten werden zur sofortigen Auswertung an McAfee Vulnerability Manager übermittelt. Die Lösung bietet außerdem die Möglichkeit zur vollständigen Soft- und Hardware-Inventarisierung aller gefundenen Ressourcen.

### Anpassung von Scans an Ihre Anforderungen

McAfee Vulnerability Manager bietet mehrere Möglichkeiten zur Ermittlung und Dokumentierung der Compliance mit Branchenvorschriften. Zur schnellen Richtlinien-Definierung anhand einer Basislinie können Sie ein „Gold-Standard"-System scannen. Alternativ können Sie die bereits im Lieferumfang enthaltenen Compliance-Vorlagen verwenden oder Richtlinien mithilfe von SCAP (Security Content Automation Protocol) laden.

McAfee Vulnerability Manager überprüft alle Netzwerkressourcen und findet auch besonders schwierig zu erkennende Ressourcen in kritischen bzw. solchen Umgebungen, die nicht direkt am Netzwerk angeschlossen sind. Wenn Sie beispielsweise Netzwerke ohne externe Verbindungen betreiben, können Sie einen virtuellen oder auf einem Laptop ausgeführten Scanner ausführen, um diese Ressourcen zu erkennen und zu scannen. Sie haben dann die Möglichkeit, die Ergebnisse in einer eingeschränkten Umgebung zu belassen oder sie in ein zentrales System zu übernehmen.

## Scan-Abdeckung

- Scan von über 450 Betriebssystemvarianten, einschließlich Microsoft Windows, UNIX, Cisco, Android, Linux, Apple Macintosh, Apple iOS und VMware-Plattformen
- Tiefen-Scans von Web-Anwendungen (OWASP Top 10 und CWE Top 25)
- Schwachstellen- und Malware-Suche in Adobe, AOL, Apple, Microsoft (Office, IIS, Exchange), Blue Coat, CA, Cisco, Citrix, Facebook, Google, HP, IBM (Lotus Notes und WebSphere), Novell, Oracle, Real Networks, RIM (BlackBerry Enterprise Server), SAP, Oracle Java, Symantec sowie VMware-Software
- Scan verbreiteter Datenbanken, einschließlich DB2, MySQL, Oracle, Microsoft SQL Server und Sybase

## Standards und Zertifizierungen

- Integrierte Vorlagen für 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 uvm.
- Unterstützung zahlreicher Standards, einschließlich CIS-zertifizierte Audits, COBIT, CPE, CVE, CVSS, DISA STIG, FDCC/SCAP, ISO17799/ISO 27002/FINRA, ITIL, NIST-SP800, NSA, OVAL und SANS Top 20
- Zertifizierung nach Common Criteria
- Konform mit FIPS-140-2-Verschlüsselung

## Technische Daten

Unter www.mcafee.com/de finden Sie aktuelle Hard- und Software-Spezifikationen und -Anforderungen.

Bei den meisten Betriebssystemen müssen vor dem Zugriff auf sensible Konfigurationsinformationen von Ressourcen Anmeldeinformationen angegeben werden. In einigen Fällen kann es jedoch für die Sicherheitsteams schwierig sein, an diese Anmeldeinformationen zu gelangen. Dank der Integration der Privileged Identity Management-Suite von Cyber-Ark können auf Anmeldeinformationen basierte äußerst sichere Erkennungsprozesse und Scans auf einfache und sichere Weise mit hoher Geschwindigkeit erfolgen.

## Risiko-Ermittlung innerhalb von Minuten

Wenn McAfee Asset Manager in Ihrem Netzwerk ein neues System findet, übermittelt das Programm ausführliche Informationen zu diesem System an McAfee Vulnerability Manager für einen gezielten Scan. Innerhalb weniger Minuten kennen Sie den Status dieses Systems sowie das Risiko für Ihre Umgebung.

## Kennzeichnung von Ressourcen für höhere Effizienz

Sie können Kennzeichnungsrichtlinien verwenden, um neue Geräte automatisch anhand ihres Profils und Risikos Scan-Gruppen zuzuordnen. In den Richtlinien können Sie auch festlegen, ob der Scan sofort oder innerhalb des nächsten Scan-Intervalls erfolgen soll.

## Erkennung von Schwachstellen und Malware

Während andere Lösungen lediglich oberflächliche Daten wie offene Ports und Konfigurationen abfragen, erfasst McAfee Vulnerability Manager auch tiefergehende Informationen. Die McAfee-Lösung erstellt Analysen auf System- und Anwendungsebene und erfasst Datenbank-Banner, Richtlinieneinstellungen, Registrierungsschlüssel, Datei- und Laufwerksberechtigungen sowie ausgeführte Dienste. Das Produkt überprüft über 450 Betriebssystemversionen, um die größtmögliche Bandbreite von Schwachstellen zu erkennen. Die Analyse deckt außerdem gefährliche Inhalte wie Trojaner, Viren und andere Malware auf.

Sie können vordefinierte Überprüfungen sowie Updates erweitern und auf Zero-Day-Bedrohungen ausdehnen, indem Sie benutzerdefinierte Skripts und Prüfungen erstellen, die auch proprietäre und veraltete Programme erfassen. McAfee Vulnerability Manager analysiert auch Inhalte von Drittanbietern, die XCCDF-, OVAL- und andere SCAP-Standards befolgen.

## Besonderer Fokus auf Web-Anwendungen

McAfee Vulnerability Manager bietet Administratoren die Möglichkeit, Web-Anwendungen auf die gleiche Weise wie traditionelle netzwerkbasierte Ressourcen zu verwalten. Diese Anwendungen können gruppiert werden und besitzen unterschiedliche Wichtigkeiten, Ressourcen-Eigentümer sowie Benutzer. Dank seiner vollautomatisierten Funktionen führt McAfee Vulnerability Manager tiefgehende Scans von Web-Anwendungen durch und kann nach einer großen Bandbreite von Web-Schwachstellen suchen.

## Stets auf dem aktuellen Stand

Millionen Sensoren weltweit weisen Hunderte McAfee Labs-Forscher auf die neuesten Änderungen der Bedrohungssituation hin. McAfee Global Threat Intelligence übermittelt in Echtzeit Risikoanalysen und Hinweise zu Bedrohungen direkt an McAfee Vulnerability Manager, um Sie vor den neuesten Bedrohungen zu schützen.

## Verwaltung, Skalierung und Integration nach Bedarf

McAfee bietet die notwendige Flexibilität, um Ihre Scans, Berichte und Verwaltungsvorgänge auf eine für Sie ideale Weise anzupassen. Sie können in einer zentralen Konsole lediglich die für einen Scanner lokalen Ressourcen überwachen oder den Fortschritt hunderter Remote-Scan-Module anzeigen. Unsere mehrschichtige Architektur kann problemlos skaliert werden, um die Anforderungen von Unternehmen aller Größen zu erfüllen.

Dank der offenen API (Application Programming Interface) lässt sich McAfee Vulnerability Manager mit den meisten Anwendungen integrieren.

## Reaktionen anhand des Risikos

Die zentrale Schwachstellenübersicht, aus der Sie direkt Aktionen ausführen können, senkt die Kosten für Patch-Installationen und Audits. Dadurch können Sie beispielsweise an Patch-Dienstagen schnell erkennen, welche Computer durch eine neue Microsoft Windows- oder Adobe-Schwachstelle gefährdet sind. Innerhalb von Minuten ermittelt McAfee Vulnerability Manager ohne erneute Prüfung die jeweiligen Prioritäten für das gesamte Netzwerk und bewertet das Risikopotenzial neuer Bedrohungen auf Grundlage vorhandener Konfigurationsdaten und Risikowerte.

Dank dieser Informationen können Sie Ressourcen anhand ihrer Wichtigkeit auswählen und per Rechtsklick sofort gezielte Scans starten.

## Zuverlässige Compliance

Überzeugende Nachweise – etwa erwartete und tatsächliche Scan-Ergebnisse, eventuell nicht geprüfte Systeme oder nicht bestandene Scan-Prüfungen – dokumentieren, dass bestimmte Systeme „nicht gefährdet“ sind. Damit wird eine immer häufiger genannte Audit-Anforderung erfüllt. Dank der Kombination aus aktiver und passiver Überwachung sowie Penetrationstests und Scans mit bzw. ohne Authentifizierung kann McAfee Vulnerability Manager Sie mit größtmöglicher Präzision auf Schwachstellen und Richtlinienverletzungen hinweisen. Das macht eine umfassende Schwachstellenverwaltung so einfach wie nie zuvor.

McAfee
An Intel Company

McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de


53000ds_mvm-mam_1012_fnl_ETMG