DATENBLATT

McAfee Virtual Network Security Platform

Umfassende Bedrohungserkennung für Cloud-Netzwerke

McAfee® Virtual Network Security Platform ist eine umfassende Lösung für Netzwerkbedrohungs- und Eindringungsschutz (IPS), die für die besonderen Anforderungen privater und öffentlicher Clouds konzipiert wurde. Die Lösung erkennt und blockiert raffinierte Bedrohungen in Cloud-Architekturen sicher sowie problemlos und bietet Unternehmen die Möglichkeit, die Compliance wiederherzustellen sowie zuverlässige Cloud-Sicherheit zu erhalten. Zu den hochentwickelten Technologien gehören signaturlose Erkennung, Inline-Emulation, signaturbasierte Schwachstellen-Patches sowie Unterstützung für Amazon Web Services (AWS) und Netzwerkvirtualisierung. Dank optimierter Workflows, mehrerer Integrationsmöglichkeiten sowie vereinfachter Lizenzierung können Unternehmen ihre Sicherheitsfunktionen auch in äußerst komplexen Cloud-Architekturen problemlos verwalten und skalieren.

Vollständige Sicherheit für die öffentliche Cloud dank hochentwickelter Sicherheitstechnologien

Öffentliche Clouds bieten Komfort, Kosteneinsparungen und die Möglichkeit, die Infrastrukturausgaben in ein Betriebskostenmodell zu verwandeln. Sie bringen jedoch auch neue Risiken mit sich, da Schwachstellen in öffentlich zugänglicher Software Angreifern das Eindringen in die Cloud und das Exfiltrieren sensibler Informationen oder die versehentliche Kompromittierung von Kundendaten durch andere Mandanten des Cloud-Anbieters ermöglichen könnten. McAfee Virtual Network Security Platform unterstützt AWS, den derzeit führenden öffentlichen Cloud-Dienst, und bietet einen vollständigen Überblick über die Daten, die das Internet-Gateway passieren oder innerhalb des Netzwerks übertragen werden. So können Sie nicht nur den Überblick über Bedrohungen wiederherstellen, sondern dank der Eindringungsschutzplattform (IPS), die den netzwerkinternen Datenverkehr überprüft, zudem die Compliance der öffentlichen Cloud-Architekturen gewährleisten.

Hauptvorteile

Unerreichter Schutz vor hochentwickelten Bedrohungen

- Signaturlose fortschrittliche Malware-Analyse
- Schutz vor Cross-Site-Scripting und SQL-Einschleusung
- Fortschrittliche Botnet-Callback- und Malware-Erkennung
- Verhaltensbasierte Analysen und Schutz vor Distributed Denial-of-Service-Angriffen (DDoS)
- Integration von McAfee Advanced Threat Defense
- System zur Entdeckung von Eindringversuchen (IDS) sowie zu ihrer Erkennung (IPS)
- Permanent aktive McAfee Virtual Network Security Platform-Lösung für VMware ESX

Cloud-fähige Architektur

- Überwachung des Durchsatzes jeder Kombination aus öffentlichen und privaten Clouds mit nur einer Lizenz

Sicherung virtueller Umgebungen

Unternehmen wechseln schnell zu virtualisierten IT-Infrastrukturen, wie privaten und öffentlichen Clouds, bei denen physische Server gleichzeitig mehrere virtuelle Maschinen (VMs) und sogar komplette virtualisierte Workloads hosten können. Die dadurch resultierende Kommunikation zwischen den VMs in Kombination mit Sofort-Migrationen, -Replikationen sowie Backups dieser Workloads vergrößert den Datenverkehr innerhalb der privaten und öffentlichen Cloud sowie innerhalb der SDDCs. Dieses Chaos wird durch die flexiblen Möglichkeiten der Netzwerkvirtualisierung verstärkt, die die wachsenden Datenverkehrsflüsse dynamisch und unvorhersehbar machen. Um in dieser Situation Schritt halten zu können, müssen virtualisierte Sicherheitslösungen flexibel sowie skalierbar sein und – was noch wichtiger ist – nahtlos mit den Plattformen für Software-definierte Netzwerke (SDN) zusammenarbeiten, die diese häufig kurzlebigen VMs und Workloads koordinieren.

Mehr Flexibilität in privaten Clouds

McAfee Virtual Network Security Platform wurde für die zuverlässige Absicherung virtualisierter Umgebungen konzipiert und integriert sich daher nahtlos in verbreitete Plattformen für private Clouds, z. B. VMware NSX und OpenStack-basierte SDN-Umgebungen. Genau genommen ist McAfee Virtual Network Security Platform die derzeit einzige dedizierte virtuelle IPS-Lösung, die für VMware NSX zertifiziert ist. Die Mikrosegmentierung der VMs und die tiefgehende Untersuchung des internen Datenverkehrs werden automatisch in virtualisierten Umgebungen durchgeführt. Das gilt auch dann, wenn Workloads schnell bereitgestellt, migriert und eingestellt werden.

Einzigartiger Bedrohungsschutz

McAfee Virtual Network Security Platform basiert auf einer Untersuchungsarchitektur der nächsten Generation und führt tiefgehende Analysen des virtuellen Netzwerkverkehrs durch. Die Lösung setzt auf eine Kombination fortschrittlicher Untersuchungstechniken zur Erkennung und Abwehr bekannter Angriffe sowie Zero-Day-Attacken im Netzwerk. Diese Techniken umfassen unter anderem die vollständige Analyse der Protokolle, der Bedrohungsreputation und des Verhaltens sowie fortschrittliche Malware-Analyse.

Keine Technologie zur Malware-Erkennung ist allein im Stande, sämtliche Angriffe abzuwehren. Aus diesem Grund kombiniert die McAfee Virtual Network Security Platform mehrere signaturbasierte und signaturlose Erkennungsmodule, um zu verhindern, dass unerwünschte Malware Ihre Clouds beschädigt. Die Lösung umfasst mehrere Untersuchungstechnologien, darunter Inline-Emulation von Browser-, JavaScript- und Adobe-Dateien, Botnet- und Malware-Callback-Erkennung, verhaltensbasierte DDoS-Erkennung sowie Schutz vor hochentwickelten Angriffen mit webseitenübergreifenden Skripts und SQL-Injektion. Dank der Integration von McAfee Advanced Threat Defense erkennt und blockiert McAfee Virtual Network Security Platform zudem verborgene Dateien, die zur genaueren Verhaltensanalyse an McAfee Advanced Threat Defense gesendet werden. McAfee Advanced Threat Defense kombiniert gründliche statische und dynamische (Malware-Sandbox-)Analysen sowie Machine Learning, um die Erkennung von Zero-Day-Bedrohungen einschließlich der Bedrohungen zu erhöhen, die Umgehungstechniken und Ransomware nutzen.

- Innovativer AWS-Untersuchungsansatz für echten Schutz des Datenverkehrs innerhalb der öffentlichen Cloud
- Unterstützung bei der Koordinierung von VMware NSX- und OpenStack-basierten SDN-Umgebungen zur automatischen Mikrosegmentierung sowie Untersuchung des Datenverkehrs zwischen Privat-Cloud-Workloads
- VM-fähiges, in VMware integrierbares Dashboard mit Quarantäne-Erzwingungsfunktion
- Zentrale Verwaltungskonsole für physische und virtuelle Sensoren – lokal und in der Cloud

Intelligente Sicherheitsverwaltung

- Zentrale Konsole verwaltet die lokalen und Cloud-Sensoren
- Intelligente Warnungskorrelation und -priorisierung
- Zuverlässige Dashboards für Malware-Untersuchungen
- Vorkonfigurierte Untersuchungs-Workflows
- Skalierbare webbasierte Verwaltung

Transparenz und Kontrolle

- Identifizierung von Anwendungen
- Identifizierung von Benutzern
- Identifizierung von Geräten
- Sicherheitsstatus aller VMs in AWS

Vereinfachung durch Cloud License Sharing

Heute verteilen viele Unternehmen ihre IT-Ressourcen und Infrastrukturen über mehrere Clouds sowie Plattformen, um ältere Anwendungen zu unterstützen, die Abhängigkeit von einem Anbieter zu reduzieren, die Systemredundanz zu erhöhen oder Kosten einzusparen. Die Lizenzierung von Sicherheitslösungen für virtualisierte Umgebungen ist mitunter kompliziert und teuer, da die meisten Anbieter den Kauf separater Lizenzen für private und öffentliche Clouds sowie für unterschiedliche SDN-Plattformen verlangen.

McAfee vereinfacht die Lizenzierung und senkt die Kosten dank Cloud License Sharing, einem neuen Konzept, das Kunden die gemeinsame Nutzung des Durchsatzes und der Lizenzen für McAfee Virtual Network Security Platform für jede Plattformkombination aus öffentlichen und privaten Clouds ermöglicht. Cloud License Sharing verbessert außerdem die Sicherheit, da Administratoren schnell Untersuchungen für internen Datenverkehr bereitstellen und die Mikrosegmentierung für virtuelle Workloads unabhängig von deren Speicherort ermöglichen können – der zeitaufwändige Beschaffungsprozesses entfällt dabei.

Optimierung der Workflows und Analysen

Mit McAfee Virtual Network Security Platform können Sie auch äußerst raffinierte Bedrohungen problemlos erkennen und blockieren, da die Lösung hochentwickelte Analysen umfasst und weitere Sicherheitslösungen integriert, um eine wirklich umfassende und vernetzte Plattform zur Erkennung und Beseitigung von Netzwerkbedrohungen zu bilden.

Moderne Bedrohungen können eine große Anzahl an Warnmeldungen generieren, die schnell die Möglichkeiten der Sicherheitsverantwortlichen zur Priorisierung und Nachverfolgung übersteigen. Wenn die Zusammenhänge nicht rechtzeitig erkannt werden, können echte Bedrohungen unerkannt Fuß fassen. Die bereits im Lieferzustand von McAfee Virtual Network Security Platform enthaltenen hochentwickelten Analysefunktionen und verwertbaren Workflows korrelieren mehrere IPS-Warnmeldungen zu einem einzigen Ereignis, damit Administratoren schnell wichtige von unwichtigen Informationen trennen und relevante, verwertbare Informationen erhalten.

Zentrale Verwaltung dank Echtzeitkontrolle mit Echtzeitdaten

Eine einzelne McAfee Network Security Manager-Appliance ermöglicht zentrales, webbasiertes Management und einzigartige Benutzerfreundlichkeit. Die moderne Konsole sowie die verbesserte grafische Benutzeroberfläche geben Ihnen die volle Kontrolle über Echtzeitdaten. Sie können problemlos alle virtuellen oder physischen McAfee Network Security Platform- und McAfee Network Threat Behavior Analysis-Appliances verwalten, konfigurieren und überwachen. Dabei benötigen Sie für Ihre herkömmlichen Ressourcen sowie für Ihre privaten und öffentlichen Clouds nur eine Konsole. Über die intuitive, webbasierte Verwaltungsoberfläche behalten Sie die Kontrolle in jeder Umgebung: von einzelnen Geräten bis hin zu weit verteilten, unternehmenskritischen Installationen. McAfee Network Security Manager kann auch als virtuelle Instanz auf VMware ESX-Servern und in AWS bereitgestellt werden.

Hochverfügbarkeit und Notfallwiederherstellung

McAfee Network Security Manager vermittelt zwischen Controllern und legt einen als aktiven und den anderen als Reserve fest. Wenn der aktive Controller ausfällt, wird der Reserve-Controller aktiv. Hochverfügbarkeit für Controller ist bei AWS-Bereitstellungen standardmäßig enthalten, sodass ein Failover-Mechanismus bereitsteht, bei dem ein Controller stets aktiv und erreichbar ist. Zusätzlich dazu stellt McAfee Network Security Manager Funktionen zur Wiederherstellung nach einem Systemausfall für AWS-Umgebungen bereit.

Die McAfee Virtual Network Security Platform ermöglicht Hochverfügbarkeit dank Manager Disaster Recovery (MDR), Controller High Availability (HA) und den Funktionen zur automatischen Skalierung des virtuellen IPS-Sensors. Dadurch arbeitet die McAfee Virtual Network Security Platform nahtlos und ohne Unterbrechungen. Die MDR-Lösung stellt einen sekundären Manager bereit, der beim Ausfall des primären Managers einspringt. Im Controller HA-Paar ist einer der Controller stets aktiv und erreichbar, sodass es keine Ausfälle im Netzwerk gibt. Die Funktion zur automatischen Skalierung für virtuelle IPS-Sensoren erstellt einen neuen IPS-Sensor, wenn eine Instanz des Sensors ausfällt. Wenn der Netzwerkverkehr zunimmt, wird ein Lastausgleich durchgeführt.

Koordinierte Schutzarchitektur

Raffinierte Angriffe interessieren sich nicht für Produktgrenzen und nutzen alle Infrastrukturlücken aus, insbesondere die zwischen Sicherheitsprodukten.

McAfee Virtual Network Security Platform ist das einzige IPS, das sich in mehrere Sicherheitsprodukte integriert und Daten sowie Workflows zum Schließen bestehender Lücken nutzt. Dadurch werden die Rendite gesteigert und die Gesamtbetriebskosten gesenkt. Weitere Integrationen in Sicherheitsprodukte:

- **McAfee ePolicy Orchestrator® (McAfee ePO™):** Vollständiger Überblick über alle IPS-Ereignisse und Warnmeldungen
- **McAfee Endpoint Intelligence Agent:** Kombination der Netzwerk- und Endgerätedaten zum Stoppen von Datenlecks
- **McAfee Enterprise Security Manager:** Austausch umfassender Daten und IPS-Quarantäne bei IPS-Warnmeldungen
- **McAfee Threat Intelligence Exchange:** Austausch der Erkenntnisse aus verschiedensten Geräten
- **McAfee Global Threat Intelligence:** Einer der weltweit umfangreichsten und aktivsten Reputationsdienste
- **McAfee Network Threat Behavior Analysis:** Erweiterung des Überblicks über das Netzwerk
- **McAfee Virtual Advanced Threat Defense**
- **McAfee Cloud Threat Detection**
- **McAfee Management for Optimized Virtual Environments (McAfee MOVE)**
- **Schwachstellen-Scanner von Drittanbietern:** Hosting- und Risikoanalysen für Endgeräte

Zusätzliche Funktionen

Schutz vor hochentwickelten Bedrohungen

- Emulationsmodul McAfee Gateway Anti-Malware Engine
- Modul zur Emulation von in PDF-Dateien enthaltenem JavaSript (ressourcenschonende Sandbox)
- Modul zur Adobe Flash-Verhaltensanalyse
- Schutz vor hochentwickelten Verschleierungstechniken

Schutz vor Botnets und Malware-Callbacks

- Schnelle Callback-Fluss-Erkennung für Domain Name Server (DNS)/Domain Generation Algorithms (DGA)
- DNS-Server-Sinkholes
- Heuristische Bot-Erkennung
- Korrelation unterschiedlicher Angriffe
- Zentrale Steuerungsdatenbank

Erweiterter Eindringungsschutz

- IP-Defragmentierung und Neuordnung des TCP-Datenstroms
- Unterstützung von McAfee-Signaturen, benutzerdefinierten Signaturen sowie Open-Source-Signaturen
- Host-Quarantäne und Bandbreitenbeschränkung
- Überprüfung virtueller Umgebungen
- Schutz vor Denial-of-Service- (DoS) und Distributed Denial-of-Service-Angriffen (DDoS)
- Grenzwert- und heuristikbasierte Erkennung
- Host-basierte Verbindungsbegrenzung
- Selbstlernende, profilbasierte Erkennung

McAfee Global Threat Intelligence

- Datei-Reputation
- IP-Reputation
- Zugriffskontrolle basierend auf dem Standort
- Zugriffskontrolle basierend der IP-Adresse

	Sensortyp 1	Sensortyp 2	Sensortyp 3
Plattform	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 NSX 6.3 AWS
Modell des virtuellen IPS-Sensors	**IPS-VM100**	**IPS-VM600**	**IPS-VM100-VSS**[1]
Typ der virtuellen IPS-Bereitstellung	Eigenständig	Eigenständig	Verteilt
Unterstützung für VMware NSX	Nein	Nein	Ja
AWS-Unterstützung	Nein	Nein	Ja
Anzahl logischer CPU-Kerne[2]	3	4	3
Erforderlicher Speicher[3]	4 GB	6 GB	5 GB
Spezifikationen für den virtuellen Sensor			
Maximaler Durchsatz[4]	bis 500 Mbit/s	bis 1 Gbit/s	bis 500 Mbit/s
Gleichzeitige Verbindungen	200.000	600.000	200.000
Hergestellte Verbindungen pro Sekunde	6.000	20.000	6.000
Unterstützte UDP-Datenflüsse	39.168	254.208	39.168
Anzahl überwachter Port-Paare	2	3	1[5]
Virtuelle Schnittstellen (VIDS) pro Sensor	32	100	32
DoS-Profile	100	300	100
Management-Port	Ja	Ja	Ja
Response-Ports	Ja	Ja	Nein
Bereitstellungsvarianten	Überwachung zwischen VMs, Überwachung zwischen physischem System und VM, Überwachung zwischen physischen Systemen, SPAN-Port-Überwachung		VMware NSX-Inline-Prüfung

1. Nur zur Verwendung als zusätzlicher Service in VMware NSX-Umgebungen.
2. Die Ressourcenanforderungen für die VM können sich bei neuen Releases ändern. Informationen hierzu finden Sie in der Dokumentation zum jeweiligen Release.
3. ebd.
4. Gemessen mit 1.518 Byte-UDP-Paketen unter idealen Testbedingungen.
5. Virtuelle Darstellung der ein- und ausgehenden Datenströme. Überprüfung ist auf Kernel-Ebene eng mit VMware NSX verknüpft.

McAfee
Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de