McAfee Virtual Network Security Platform

Umfassende Bedrohungserkennung und Eindringungsschutz für Cloud-Netzwerke

McAfee® Virtual Network Security Platform (McAfee vNSP) ist eine umfassende Lösung für Netzwerkbedrohungs- und Eindringungsschutz (IPS), die für die besonderen Anforderungen privater und öffentlicher Clouds konzipiert wurde. Sie erkennt und blockiert raffinierte Bedrohungen in Cloud-Architekturen schnell, sicher sowie problemlos und bietet Unternehmen die Möglichkeit, Workloads zu schützen und die Compliance zuverlässig wiederherzustellen. Die Lösung bietet fortschrittliche Technologien wie signaturlose Erkennung, Inline-Emulation sowie signaturbasierte Bereitstellung von Schwachstellen-Patches. Dank optimierter Workflows, flexibler Integrationsoptionen sowie vereinfachter Lizenzierung können Unternehmen ihre Sicherheitsmaßnahmen unkompliziert verwalten und skalieren, um aktuelle und zukünftige Anforderungen zu erfüllen.

Vollständige Sicherheit für öffentliche Clouds

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 können. McAfee vNSP unterstützt Amazon Web Services (AWS), Microsoft Azure und Oracle Cloud Infrastructure (OCI), die aktuell führenden öffentlichen Cloud-Dienste, und bietet vollständigen Überblick über Bedrohungen sowie Schutz für Daten, die an ein Internet-Gateway oder von Server zu Server (interner Datenverkehr) übertragen werden.

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 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 Clouds sowie innerhalb der SDDCs (Software-definierten Rechenzentren).

Hauptvorteile

- Vollständiger Schutz für private und öffentliche Clouds (AWS, Azure und OCI)
- Echter Schutz für internen Datenverkehr
- Zentrale Verwaltungskonsole für Kontrolle und Übersicht
- Fortschrittliche Analyse-technologien zum Schutz vor bekannten und unbekannten Bedrohungen
- Hochverfügbarkeit, Wieder-herstellung nach Systemausfall und Lastausgleich für hohe Leistung
- Gemeinsame Nutzung von Cloud-Lizenzen für größere Flexibilität in privaten und öffentlichen Clouds
- Integration in McAfee-Produkt-palette für Gerät-zu-Cloud-Sicherheit
- Verfügbar im **AWS Marketplace**
- Verfügbar im **Azure Marketplace**

Folgen Sie uns

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.

Flexibilität in privaten Clouds

McAfee vNSP integriert sich nahtlos in verbreitete Privat-Cloud-Plattformen wie VMware NSX und OpenStack-basierte SDN-Umgebungen. Tatsächlich ist McAfee Virtual Network Security Platform die 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.

Schutz vor hochentwickelten Bedrohungen

McAfee vNSP basiert auf einer Analysearchitektur der nächsten Generation und führt tiefgehende Untersuchungen des virtuellen Netzwerkverkehrs durch. Die Lösung setzt auf eine Kombination fortschrittlicher Untersuchungstechniken zur Erkennung und Abwehr bekannter Angriffe sowie unbekannter 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 einzelne Technologie zur Malware-Erkennung ist im Stande, sämtliche Angriffe abzuwehren. Aus diesem Grund vereint McAfee vNSP mehrere fortschrittliche Techniken zur Malware-Analyse, um zu verhindern, dass unerwünschte Malware Ihr Netzwerk beschädigt. Die Lösung nutzt 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 vNSP zudem verborgene Dateien, die zur 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. McAfee bietet auch systemeigene Unterstützung für Snort-Signaturen zur Erkennung und Abwehr von Malware.

Flexible gemeinsame Nutzung von Cloud-Lizenzen

Viele Unternehmen verteilen 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

Weitere Informationen

- **Absicherung Ihrer virtuellen Amazon Web Services-Netzwerke**
- **Absicherung Ihrer virtuellen Microsoft Azure-Netzwerke**

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 gemeinsamer Nutzung von Cloud-Lizenzen, sodass Kunden ihre Lizenzen für McAfee vNSP und den Durchsatz für jede Kombination aus öffentlichen und privaten Cloud-Plattformen gemeinsam nutzen können. Durch die gemeinsamer Nutzung von Cloud-Lizenzen verbessert sich außerdem die Flexibilität und Sicherheit, da Administratoren schnell Untersuchungen von internem Datenverkehr durchführen und die Mikrosegmentierung für virtuelle Workloads unabhängig von deren Speicherort ermöglichen können – die komplexe Lizenzierung und der zeitaufwändige Beschaffungsprozess entfallen dabei.

Optimierung von Workflows und Analysen

Moderne Bedrohungen können eine große Anzahl an Warnmeldungen generieren, die schnell die Möglichkeiten der Sicherheitsverantwortlichen zur Priorisierung und Nachverfolgung übersteigen. Wenn die Reaktion zu langsam erfolgt, können echte Bedrohungen unerkannt Fuß fassen. Die in McAfee vNSP enthaltenen hochentwickelten Analysefunktionen und umsetzbaren Workflows korrelieren mehrere IPS-Warnmeldungen zu einem einzigen Ereignis, damit Administratoren schnell relevante Informationen erhalten. Zudem entsteht durch die Integration in weitere McAfee-Sicherheitslösungen eine wirklich umfassende und vernetzte Plattform zur Erkennung und Beseitigung von Netzwerkbedrohungen.

Zentrale Verwaltung für Echtzeittransparenz und Kontrolle

Eine einzelne McAfee Network Security Manager-Appliance ermöglicht zentrales, webbasiertes Management für Echtzeittransparenz und -kontrolle. Die moderne Konsole gibt Ihnen in einer zentralen Übersicht 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. Diese sind für Ihre herkömmlichen Ressourcen sowie für Ihre privaten und öffentlichen Clouds-Umgebungen verfügbar. Die intuitive Benutzeroberfläche skaliert problemlos und kann weit verteilte geschäftskritische Cluster verwalten.

McAfee Network Security Manager kann auch als virtuelle Instanz auf VMware ESX-Servern und in AWS- oder Azure-Umgebungen bereitgestellt werden. McAfee vNSP unterstützt AWS IAM (Identity and Access Management), sodass Administratoren den Zugriff auf AWS-Services und -Ressourcen basierend auf Berechtigungen für bestimmte Benutzer und Gruppen unkompliziert und sicher verwalten können.

Hochverfügbarkeit, Wiederherstellung nach Systemausfall und Lastausgleich

McAfee vNSP stellt mithilfe mehrerer Methoden automatisch unterbrechungsfreie Kontrollen, Schutzmaßnahmen und Leistung bereit.
McAfee Network Security Manager unterstützt dank proaktiver Umgebungsüberwachung Hochverfügbarkeit.

Wenn ein aktiver Controller ausfällt, führt McAfee Network Security Manager automatisch ein Failover zu einem Standby-Controller durch, um unterbrechungsfreie Übersicht und Sicherheit zu gewährleisten. Außerdem kann McAfee Network Security Manager Funktionen zur Wiederherstellung nach einem Systemausfall in AWS-, Azure- und OCI-Umgebungen bereitstellen.

McAfee vNSP bietet zudem Hochverfügbarkeit für IPS-Sensoren. Wenn ein Sensor ausfällt, erstellt die Automatik-Skalierungsfunktion automatisch einen neuen virtuellen IPS-Sensor für nahtlosen und unterbrechungsfreien Schutz. Wenn außerdem der Netzwerkverkehr zunimmt, gewährleistet der automatische Lastausgleich zwischen Sensoren eine optimale Leistung. Zusätzliche Sensoren können automatisch bereitgestellt werden, um die erforderliche Durchsatzleistung zu gewährleisten.

Integrierte Sicherheit

Raffinierte Angriffe interessieren sich nicht für Produktgrenzen und nutzen sehr schnell alle Infrastrukturlücken aus, insbesondere die zwischen Sicherheitsprodukten. McAfee vNSP ist das einzige IPS, das sich in mehrere Sicherheitsprodukte integriert und für hervorragende Sicherheit, Schutz und höhere Rendite Daten sowie Workflows aus mehreren Lösungen nutzt. Beispiele für die Integration in McAfee-Sicherheitslösungen:

- **McAfee ePolicy Orchestrator® (McAfee ePO™):** Vollständiger Überblick über alle IPS-Ereignisse und Warnmeldungen
- **McAfee Endpoint Intelligence Agent:** Kombination der Netzwerk- und Endgerätedaten zum Schließen von Datenlecks
- **McAfee Enterprise Security Manager:** Austausch umfassender Daten und IPS-Quarantäne bei IPS-Warnmeldungen
- **McAfee Threat Intelligence Exchange:** Austausch der Erkenntnisse aus verschiedensten Gerätetypen
- **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:** Tiefgehende Analysen zur Erkennung schwer aufspürbarer Bedrohungen
- **McAfee Cloud Threat Detection:** Ein Dienst, der sich in bereits vorhandene McAfee-Sicherheitslösungen integriert, um raffinierte Malware-Varianten zu erkennen
- **McAfee Management for Optimized Virtual Environments (McAfee MOVE):** Virenschutz-Lösung für virtuelle Umgebungen
- **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 JavaScript in PDF-Dateien (ressourcenschonende Sandbox)
- Modul zur Adobe Flash-Verhaltensanalyse
- Erweiterter Umgehungsschutz

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)
- Whitelist/Blacklist-Verbesserungen bei der Unterstützung von STIX (Structured Threat Information eXpression)
- Grenzwert- und heuristikbasierte Erkennung
- Host-basierte Verbindungsbegrenzung
- Native Unterstützung von Snort-Signaturen
- Selbstlernende, profilbasierte Erkennung

McAfee Global Threat Intelligence

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

	Sensortyp 1	Sensortyp 2
Plattform	VMware ESX 5.5/6.0/6.5	AWS Azure OCI VMware vSphere 6.5 und NSX 6.3
Modell des virtuellen IPS-Sensors	**IPS-VM600**	**IPS-VM600-VSS**
Typ der virtuellen IPS-Bereitstellung	Eigenständig	Verteilt
Unterstützung für VMware NSX	Nein	Ja
AWS-Unterstützung	Nein	Ja
Unterstützung für Azure	Nein	Ja
OCI-Unterstützung	Nein	Ja
Anzahl an logischen Prozessoren	4	AWS 4, Azure 5
Erforderlicher Speicher	7 GB	7 GB
Speicherung	8 GB	8 GB
Spezifikationen für den virtuellen Sensor		
Maximaler Durchsatz	bis 1 Gbit/s	bis 1 Gbit/s
Anzahl überwachter Port-Paare	3	1 (Überwachungsport, kein Port-Paar)
Virtuelle Schnittstellen (VIDS) pro Sensor	100	100
DoS-Profile	300	300
Management-Port	Ja	Ja
Response-Ports	Nein	Nein
Bereitstellungsvarianten	Überwachung zwischen VMs, Überwachung zwischen physischem System und VM, Überwachung zwischen physischen Systemen, SPAN-/Inline-Port-Überwachung	

McAfee
Together is power.

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