McAfee Server Security Suite Advanced

Erweiterte Server-Sicherheit für physische, virtuelle und Cloud-basierte Implementierungen dank Whitelisting

Hauptvorteile

- Zeigt alle physischen sowie virtuellen Server, einschließlich Server in der Cloud, in einer übersichtlichen zentralen Verwaltungskonsole an
- Kombiniert Black- und Whitelists zum Schutz physischer und virtueller Server vor Malware
  - Stellt dynamische Whitelists zum Schutz vor unbekannten Bedrohungen bereit, indem dank McAfee Application Control for Servers gewährleistet wird, dass Hosts keine unerwünschten Anwendungen ausführen
  - Ermöglicht die kontinuierliche Erkennung von Veränderungen auf Systemebene an verteilten und entfernten Standorten zur Erfüllung von Compliance-Anforderungen
- Bietet dank McAfee MOVE AntiVirus optimale Sicherheit für virtuelle Umgebungen bei minimalen Leistungseinbußen

Die von Rechenzentren bereitgestellten Speichersysteme, Server, Netzwerke und Anwendungen haben sich in den vergangenen Jahren erheblich verändert. Die Vielseitigkeit aktueller Rechenzentren und die schnelle Entwicklung in Richtung Cloud Computing erfordern neue Ansätze für die Absicherung dieser Umgebungen. Die Herausforderung für die IT-Abteilungen von Unternehmen sowie Sicherheitsexperten besteht darin, einen einheitlichen und gleichzeitig zuverlässigen Sicherheitsansatz zu entwickeln, mit dem die Flexibilität sowie der kostengünstige Betrieb physischer und virtueller Umgebungen sowie von Cloud-Umgebungen ermöglicht werden können. Als Teil der Intel Security®-Produktpalette bietet McAfee® Server Security Suite Advanced den umfassendsten Server-Schutz sowie Verwaltungsfunktionen für physische, virtuelle und Cloud-Umgebungen. Daneben beinhaltet die Lösung zusätzliche erweiterte Server-Sicherheitsfunktionen wie Whitelists und Änderungskontrollen, um Sie bei der Einhaltung von Compliance-Vorschriften zu unterstützen.

Erkennung aller Workloads

Die Erkennung aller Workloads und die anschließende Umsetzung angemessener Sicherheitsrichtlinien in physischen, virtuellen sowie Cloud-Bereitstellungen ist häufig schwierig. Dank Scan-Berichten, die ungeschützte Endgeräte aufdecken und den Status der Sicherheits-Compliance bestimmen, wird die Verwaltung vereinfacht. Über die Konnektoren für McAfee® ePolicy Orchestrator® (McAfee ePO™) ermöglicht McAfee Server Security Suite Advanced die Erkennung aller physischen und virtuellen Server, einschließlich solcher in privaten und öffentlichen Clouds.

Im Lieferumfang der Lösung enthalten sind die Konnektoren McAfee Data Center Connector for VMware vSphere, Amazon AWS, OpenStack sowie Microsoft Azure. Dadurch können Sie alle virtuellen Maschinen sowohl vor Ort als auch aus der Ferne überwachen und detaillierte Sicherheitsrichtlinien anwenden, die starke Sicherheit gewährleisten. Die Dashboards stellen die Sicherheitslage dar und bieten Informationen zum Speicherschutz des Betriebssystems, den Beziehungen zwischen dem Hypervisor-Host und virtuellen Maschinen, dem Standort jeder virtuellen Maschine uvm.

intel Security

Hauptvorteile (Fortsetzung)

- Bietet mithilfe von McAfee Data Center Connector for VMware vSphere, Amazon Web Services, OpenStack und Microsoft Azure eine vollständige Übersicht des Sicherheitsstatus aller virtueller Maschinen in der privaten und öffentlichen Cloud
- Agentenlose Host-basierte Firewall organisiert mithilfe von VMware vCNS App virtuelle Maschinen in sichere Netzwerkgruppen oder isoliert sie

Server-Schutz

McAfee Server Security Suite Advanced bietet den umfassendsten Schutz für Ihre physischen, virtuellen oder Cloud-basierten Server. Zudem stellt die Lösung Änderungskontrollen sowie eine einmalige Kombination aus Black- und Whitelist-Schutztechnologien bereit, die branchenweit unerreicht sind.

In McAfee Server Security Suite Advanced enthalten ist auch McAfee Application Control for Servers. Mit dieser Whitelist-Lösung können Sie festlegen, dass auf Servern nur zulässige Software ausgeführt wird. Diese zentral verwaltete Whitelist-Lösung basiert auf einem dynamischen Vertrauensmodell und innovativen Sicherheitsfunktionen, die nicht autorisierte Anwendungen blockieren und hochentwickelte hartnäckige Bedrohungen (APTs) überlisten können – ganz ohne mühsam erstellte und verwaltete Listen. Die Whitelist reduziert erheblich die Leistungsnachteile für Host-Systeme, da sie Schutz vor Bedrohungen bietet, ohne Signatur-Updates zu erfordern.

Die Suite stellt grundlegenden Schutz für Server bereit und bietet dabei herkömmlichen Malware-Schutz für Microsoft Windows- sowie Linux-Server, z. B. die Lösung McAfee VirusScan® Enterprise, die von NSS Labs beim Schutz vor Day-Zero-Exploits und Verschleierungsangriffen die Bestwertung erhielt. Ferner bietet die Suite eine separate Lösung speziell für virtuelle Umgebungen: McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus optimiert den Virenschutz für virtuelle Umgebungen, minimiert die Leistungseinbußen bei sehr großen Umgebungen und unterstützt alle großen Hypervisoren. McAfee MOVE AntiVirus bietet eine agentenlose Variante, die für VMware-Bereitstellungsumgebungen angepasst ist, sowie eine Version für den Einsatz auf mehreren Plattformen, die in KVM-, Microsoft Hyper-V-, VMware- und Xen-basierten Hypervisor-Umgebungen eingesetzt werden kann.

Obwohl Virenschutz für die Gewährleistung der Sicherheit unerlässlich ist, sind zum Schutz hochentwickelter Bedrohungen möglicherweise zusätzliche Lösungen erforderlich. McAfee Host Intrusion Prevention schützt Unternehmen vor komplexen Sicherheitsbedrohungen, die andernfalls unbeabsichtigt auf Systeme gelangen oder dort zugelassen werden könnten.

Zudem ist McAfee Agentless Firewall in VMware vCNS App Firewall integriert. Dadurch können Administratoren eine oder mehrere Instanzen der VMware vShield App Firewall innerhalb der McAfee ePO-Plattform überwachen und Firewall-Richtlinien in virtuellen Rechenzentren über eine zentrale Benutzeroberfläche verwalten. Diese Erweiterung bietet auch einfache Arbeitsabläufe, mit denen Benutzer Gruppen von Ressourcen isolieren können, ohne dazu manuell komplexe Firewall-Regeln erstellen zu müssen. Zudem werden beliebige Veränderungen durch andere Tools ermittelt, und Administratoren können mit einem einzigen Klick den vorherigen Zustand wiederherstellen.

Erweiterung in die Cloud

Je weiter Sie Ihr Rechenzentrum in die Cloud verlegen, desto schwieriger wird es, die Durchsetzung angemessener Sicherheitsrichtlinien für neu bereitgestellte Workloads zu gewährleisten. McAfee löst diese Probleme durch die automatische Erkennung aktiver und angehaltener virtueller Maschinen in privaten und öffentlichen Clouds. Dazu müssen Sie lediglich ein Konto für eine öffentliche Cloud in der Plattform McAfee ePO registrieren. Virtuelle Maschinen können anschließend automatisch mit den Sicherheitsrichtlinien geschützt werden. Zudem bietet das Dashboard für McAfee-Lösungen zum Schutz von Rechenzentren einen vollständigen Überblick über den Schutzstatus sowie Sicherheitsereignisse in Ihren privaten und öffentlichen Clouds.

Optimierung Ihrer Server und Ihres Geschäfts

Das enorme Potenzial von Virtualisierungen und Cloud Computing kann sich erst dann entfalten, wenn diese Technologien ausreichend abgesichert sind. McAfee bietet Server-Sicherheitslösungen, die Ihr Unternehmen auch beim weiteren Wachstum unterstützen. Unabhängig davon, ob Sie physische, virtuelle oder in der Cloud gehostete Systeme schützen möchten – die McAfee-Suite umfasst flexible Lösungen zum Schutz aller Ihrer Server.

McAfee Server Security Suite Advanced bietet mit hochentwickelten Lösungen Sicherheit für physische, virtuelle sowie in der Cloud gehostete Server, damit Ihr Unternehmen zuverlässig geschützt ist.

Weitere Informationen zu den Vorteilen von McAfee Server Security Suite Advanced finden Sie unter **www.mcafee.com/de/products/server-security-suite-advanced.aspx**.

Funktion	Warum Sie sie benötigen
Anwendungs-Whitelists	• Erhebliche Reduzierung des Leistungsbedarf auf dem Host (im Vergleich mit herkömmlichen Endgerätesicherheitskontrollen) • Schutz auch ohne Signaturaktualisierungen vor Zero-Day-Bedrohungen und hochentwickelten hartnäckigen Bedrohungen (APTs), sodass die Schutzwirkung schneller erreicht wird • Geringerer Verwaltungsaufwand dank dynamischer Whitelists (im Vergleich mit veralteten Whitelist-Techniken)
Kontrolle über Änderungen	• Verhinderung von Manipulationen durch Blockierung nicht autorisierter Änderungen an kritischen Systemdateien, Verzeichnissen und Einstellungen, sodass Administratoren bei der Behebung von Sicherheitskompromittierungen Zeit sparen • Erfassung und Überprüfung aller versuchten Änderungen am Server in Echtzeit und Erzwingung von Änderungsrichtlinien nach Zeitfenster, Urheber oder genehmigtem Arbeitsauftrag • Kontinuierliche Kontrolle minimiert die Auswirkungen spontaner oder nicht autorisierter Änderungen
Zentrale Konsolenverwaltung	• Verwaltung physischer Computer und virtueller Maschinen über eine zentrale Übersicht, einschließlich solchen in privaten und öffentlichen Cloud für bessere Sicherheitstransparenz • Vereinfachte Betriebsabläufe und geringerer Zeitaufwand für die Administratoren • Senkung der Hardware-Kosten durch geringeren Server-Ressourcenbedarf
Grundlegender Server-Schutz	• Malware-Schutz für physische Server, der von NSS Labs[1] beim Schutz vor Zero-Day-Exploits und Verschleierungsangriffen die beste Bewertung erhielt • Host Intrusion Prevention schützt Unternehmen vor komplexen Sicherheitsbedrohungen, die andernfalls unbeabsichtigt auf Systeme gelangen oder dort zugelassen werden könnten
Schutz virtueller Umgebungen	• Optimierung der Sicherheit von Arbeitsabläufen in virtuellen Infrastrukturen, ohne dass die Leistung beeinträchtigt und der Ressourcenbedarf erhöht werden • Schutz für mehrere Hypervisoren im Rechenzentrum, sodass ein identischer Sicherheitsstatus auf allen eingesetzten Hypervisoren gewährleistet wird • Für VMware-Umgebungen optimierte agentenlose Bereitstellung ermöglicht hervorragende Leistung und VM-Dichte
McAfee Agentless Firewall	• Anzeige einer Übersicht aller isolierten virtuellen Netzwerke in McAfee ePO-Berichten • Kontrolle und Isolierung virtueller Maschinen und Daten durch Integration in die VMware vCNS App Firewall
Vollständiger Überblick über virtuelle Maschinen in der privaten und öffentlichen Cloud	• Erkennung nicht nur physischer Server, sondern auch von Hypervisoren und virtuellen Maschinen in den Umgebungen von VMware vSphere, Amazon AWS, OpenStack und Microsoft Azure, sodass die zu schützenden Ressourcen vollständig angezeigt werden • Erkennung der Bereitstellung virtueller Maschinen, die anschließend automatisch durch Sicherheitsrichtlinien geschützt werden können, um die zuverlässige Sicherheit dieser virtuellen Maschinen zu gewährleisten

1. NSS Labs, Inc., Protection & Evasion Test (NSS Labs-Testbericht zu Schutz und Verschleierung), 2013.

McAfee. Part of Intel Security
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com