DATENBLATT

McAfee Management for Optimized Virtual Environments AntiVirus

Sicherheit für Ihre Privat-Cloud ohne Leistungsbeeinträchtigung

Herkömmliche Virenschutzprogramme sind nicht für den Einsatz in virtualisierten Umgebungen konzipiert. McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) bietet optimierten, erweiterten Malware-Schutz für Ihre virtualisierten Desktops und Server. Sie können die Lösung wahlweise auf Hypervisoren verschiedener Anbieter bzw. bei Verwendung mit VMware NSX oder VMware vCNS agentenlos einsetzen. In jedem Fall erhalten Sie bestbewertete Sicherheit, die sofortige Bedrohungserkennung und -eindämmung bei minimalen Auswirkungen auf die Leistung virtueller Maschinen (VMs) bietet. McAfee MOVE AntiVirus optimiert den Malware-Schutz für virtualisierte Umgebungen, entlastet Hypervisor-Ressourcen und gewährleistet gleichzeitig, dass die regelmäßigen Sicherheits-Scans den Richtlinien entsprechen.

Optimierte Scan-Kontrolle

Die Dynamik von Gast-Desktops und virtuellen Servern erfordert große Sorgfalt. Abbilder müssen frei von Malware sein, wenn Benutzer eine Sitzung starten. Das zu gewährleisten ist jedoch nicht immer einfach, da Benutzer häufig ihre Arbeit zur gleichen Zeit beginnen und dadurch „Virenschutz-Blockaden“ auslösen können, bei denen der Virenschutz Ressourcen bindet und das Abrufen von Sitzungen verhindert.

Zur Vermeidung von Scan-Engpässen und Verzögerungen lagert McAfee MOVE AntiVirus Scans, Konfigurationen sowie DAT-Aktualisierungen aus den einzelnen Gast-Abbildern auf einen separaten Scan-Server aus. Dank eines globalen Caches, über den gescannte Dateien verwaltet werden, müssen bereits geprüfte und als sicher bestätigte Dateien bei späteren Zugriffen durch virtuelle Maschinen (VMs) nicht erneut geprüft werden. Für die einzelnen VMs wird weniger Speicherplatz benötigt, sodass der Ressourcen-Pool effektiver genutzt werden kann.

McAfee MOVE AntiVirus erlaubt die Verwendung separater Richtlinien für On-Access- und On-Demand-Scans für angepasste Sicherheitsmaßnahmen. Beispielsweise können Administratoren ein akzeptables Risikoniveau für Echtzeit-On-Access-Scans definieren und auf diese Weise Leistungseinbußen verhindern. Zu einem

Hauptvorteile

- **Auslagerung der Malware-Scans aus den VMs:** Sofortschutz mit geringer Speicher- und Prozessor-Belastung
- **Schutz vor Virenschutz-Blockaden:** Scans können On-Demand oder On-Access stattfinden
- **Flexible Bereitstellungsoptionen:** Wahl zwischen Bereitstellung für mehrere Plattformen (alle gängigen Hypervisoren und Windows-VMs) und agentenloser Bereitstellung (VMware-, Windows- und Linux-VMs)
- **Verbesserte Ressourcen-optimierung:** Flexible Bereitstellung von Offline-Scannern mit Ereignis-benachrichtigungen (bei mehreren Plattformen)
- **Blockierung von Zero-Day- und unbekannten Bedrohungen in Sekunden:** Lokale Reputations-bewertung in Kombination mit Verhaltensanalyse in einer Sandbox (bei mehreren Plattformen, separat erhältliches Zusatzmodul)
- **Nutzt die McAfee® ePolicy Orchestrator® (McAfee ePO™)-Konsole:** Vollständiger Überblick und Kontrolle für physische, virtuelle und Cloud-Bereitstellungen

späteren Zeitpunkt, wenn die Ressourcen weniger stark belastet sind, können sie On-Demand-Scans mit strengeren Richtlinien ausführen.

Umfassende Transparenz für alle Clouds

Unzureichende Transparenz erschwert die Implementierung angemessener Sicherheitsrichtlinien für virtualisierte Umgebungen. McAfee Cloud Workload Discovery für private Clouds mit VMware und OpenStack bietet eine umfassende Übersicht über virtuelle Rechenzentren und stellt wichtige Elemente wie Server, Hypervisoren und VMs in der McAfee ePO-Konsole dar. Sobald Administratoren einen Überblick über den Sicherheitsstatus aller VMs haben und Hypervisor-zu-VM-Beziehungen nahezu in Echtzeit überwachen können, erleichtert das die Absicherung Ihres virtuellen Rechenzentrums erheblich. Ein anpassbares Übersichts-Dashboard zeigt den Status des Sicherheits-Scans, zusammenfassende Übersichten sowie Verlaufs-Sicherheitsdaten für Ressourcen an.

McAfee Server Security Suite Essentials und McAfee Server Security Suite Advanced erweitern die Transparenz und Kontrolle auf öffentliche Clouds mit Amazon Web Services (AWS) und Microsoft Azure sowie auf physische Server.

Detaillierte Richtlinienverwaltung

Die Konfiguration der Richtlinien sowie der McAfee MOVE AntiVirus-Einstellungen erfolgt über die vertraute McAfee ePO-Konsole. Sie können virtuelle Daten mit Daten aus Ihren physischen Systemen und öffentlichen Clouds in einheitlichen Dashboards sowie Berichten zusammenführen. Administratoren können über McAfee Cloud Workload Discovery individuelle Richtlinien pro VM, Cluster oder Rechenzentrum konfigurieren und ihre Sicherheitseinstellungen präzise an den Aufbau des Rechenzentrums anpassen.

Weitere McAfee MOVE AntiVirus-Funktionen

Verwaltung und Transparenz:

- Planung eines unmittelbaren On-Demand-Scans für eine VM oder VM-Gruppe
- Genauere Scans mit gezielten On-Demand-Scans
- Dank Integration in VMware NSX Service Composer automatische Bereitstellung eines Offload-Scanners für jeden Hypervisor
- Lösung von Problemen mit Dashboards, Berichten und E-Mail-Warnungen

Vereinfachte Bereitstellung und Konfiguration:

- Bereitstellung und Konfiguration eines Offload-Scanners für mehrere Hypervisoren (agentenlose Variante)
- Wiederherstellung isolierter Dateien über die McAfee ePO-Konsole (Mehrplattform-Variante)
- Detaillierte Diagnose für Virenschutz-Leistungsabstimmung
- Nahtlose Richtlinienverwaltung (agentenlose und Mehrplattform-Variante)

McAfee MOVE AntiVirus-Versionen

McAfee MOVE AntiVirus for Virtual Servers

- McAfee MOVE AntiVirus:
  - Mehrplattform-Variante
  - Agentenlose Variante
- Cloud Workload Discovery für private Clouds (VMware und OpenStack)
- McAfee ePO

McAfee MOVE AntiVirus for Virtual Desktops

- McAfee MOVE AntiVirus:
  - Mehrplattform-Variante
  - Agentenlose Variante
- Cloud Workload Discovery für private Clouds (VMware und OpenStack)
- McAfee Host Intrusion Prevention System
- McAfee SiteAdvisor® Enterprise
- Speicherschutz und Web-Anwendungsschutz
- McAfee ePO

Agentenlose Implementierung für VMware

McAfee MOVE AntiVirus nutzt VMware NSX oder VMware vCNS zur Verbesserung der Effizienz. In agentenlosen Implementierungen verwenden diese Tools den Hypervisor als Hochgeschwindigkeitsverbindung, um der SVM (Security Virtual Machine) von McAfee MOVE AntiVirus das Scannen virtueller Maschinen von außerhalb der Gast-Abbilder zu ermöglichen. Während des Scans erhalten VMware NSX bzw. VMware vCNS von der SVM Informationen über saubere und gefährliche Dateien, damit bei ersteren die Speicherung im Cache erlaubt bzw. bei letzteren der Zugriff gesperrt oder die entsprechende Datei in die Quarantäne verschoben werden kann.

Sie müssen lediglich die SVM sowie die VMware NSX/vCNS-Komponenten auf den VMware ESX-Servern und die VMware NSX/vCNS-Endgerätetreiber auf den Gast-VMs installieren und konfigurieren. Anschließend wird jedes Abbild automatisch geschützt, ohne dass unsere Software hierfür auf jeder Client-VM installiert werden muss. Dank unserer vMotion-fähigen Implementierung können Ihre VMs zwischen Hosts verschoben werden, wobei sie auf dem Ziel-Host nahtlos von der SVM geschützt werden – ohne Beeinträchtigung der Scan- oder VM-Leistung.

Die Integration von McAfee-Produkten in VMware vCNS ermöglicht die Überwachung des SVM-Status innerhalb von VMware vCenter und den Empfang von Warnmeldungen, wenn SVM die Verbindung verliert. Für den Fall, dass eine VM-Infizierung festgestellt wird, erhält die McAfee ePO-Konsole zudem Ereignisdaten mit Details zur betroffenen VM. Durch die starke Integration mit VMware NSX können in der McAfee ePO-Konsole erstellte Richtlinien und in VMware NSX zugewiesene Regeln synchronisiert werden. Wenn gefährdete Maschinen ohne Malware-Schutz bzw. mit Malware infizierte Maschinen gekennzeichnet werden, können diese VMs sofort über die VMware NSX-Firewall isoliert werden.

Sie können McAfee MOVE AntiVirus gleichzeitig mit VMware vCNS und VMware NSX agentenlos verwenden, sodass die Lösung extrem einfach und nahtlos von Kunden eingesetzt werden kann, die bereits VMware vCNS nutzen und eine VMware NSX-Umgebung aufbauen möchten.

Option für mehrere Plattformen für alle gängigen Hypervisoren

Bei Installationen auf mehreren Plattformen (z. B. vSphere, Hyper-V, KVM und XenServer) kommuniziert der McAfee MOVE AntiVirus-Agent – eine Endgeräte-Komponente mit geringem Ressourcen-Verbrauch – mit der SVM, um Virenschutz-Funktionen für die entsprechenden VMs zu koordinieren. Der McAfee MOVE AntiVirus-Agent nutzt einen lokalen Cache und verwaltet Richtlinien sowie Scan-Funktionen. Sie können ein Gold-Abbild scannen und als „sauberes Master-Abbild“ definieren. Wenn Sie den lokalen Cache mit sauberen Abbildern auffüllen, können Sie die Startzeit der VMs verkürzen.

Sobald ein Zugriff auf eine Datei stattfindet, führt McAfee MOVE Offload Scan Server einen On-Access-Scan durch und liefert eine Rückmeldung an die VM. Bei Problemen können Benutzer über eine Pop-Up-Warnung benachrichtigt werden und haben die Möglichkeit,

gefährliche Dateien zu löschen, zu sperren oder zu isolieren.

Da der Scan-Bedarf in Mehrplattformumgebungen schwankt, können automatisch SVMs hinzugefügt oder aus dem Ressourcen-Pool entfernt werden, um die Scan-Leistung zu skalieren. Dadurch erreichen Sie unbegrenzte Skalierbarkeit und können die Ressourcen effizient nutzen. Ereignisbenachrichtigungen informieren Administratoren über die Trends der SVM-Nutzung und zeigen auf, wie sich die Ressourcenverwaltung optimieren lässt.

McAfee MOVE AntiVirus kann die weltweiten Bedrohungsinformationen aus McAfee Global Threat Intelligence (McAfee GTI) durch lokale Daten aus McAfee Threat Intelligence Exchange ergänzen. Dieses Zusatzmodul ist separat erhältlich und bietet Soforterkennung sowie -abwehr der stetig zunehmenden Zahl von Malware-Varianten. Mithilfe von McAfee Threat Intelligence Exchange koordiniert sich McAfee MOVE AntiVirus mit McAfee Advanced Threat Defense, um das Verhalten unbekannter Anwendungen in einer Sandbox dynamisch zu analysieren und alle Endgeräte automatisch gegen die neu entdeckte Malware zu immunisieren. Durch die Vernetzung von McAfee MOVE AntiVirus mit der McAfee Network Security Platform über McAfee Threat Intelligence Exchange erhalten Sie einen mehrstufigen Sicherheitsansatz mit einer einheitlichen Peripherie sowie Schutz für virtuelle Maschinen.

Einheitliche Richtlinienverwaltung für agentenlose und Mehrplattform-Bereitstellung

Viele Unternehmen interessieren sich für die Möglichkeit, McAfee MOVE AntiVirus parallel in agentenlosen und Mehrplattform-Bereitstellungen zu verwenden. Dank McAfee MOVE AntiVirus haben Sicherheitsadministratoren die Möglichkeit, einheitliche Richtlinien zu definieren und zu verwalten. Dabei wird ein Erweiterungspunkt in der McAfee ePO-Konsole genutzt, so dass die Verwaltung dieser unterschiedlichen Methoden nahtlos und unkompliziert erfolgt.

Architektur	Mehrplattform-Variante	Agentenlose Variante
Unterstützte Hypervisoren/ Plattformen	Alle wichtigen Hypervisoren: VMware, Citrix, Hyper-V und KVM	VMware
Scan-Plattform	Windows 2008, Windows 2012 R2, Windows Server 2016	Linux Ubuntu 16.04
Skalierbarkeit der Umgebung	Eine SVM kann VMs mehrerer Hypervisoren schützen, SVMs können flexibel bereitgestellt werden.	Eine SVM pro ESX-Host
Kommunikation mit VMs	Über das Netzwerk	Über den Hypervisor
Schutz virtueller Maschinen	Windows	Windows und Linux

Weitere Informationen

McAfee-Lösungen bieten die von Ihnen geforderte Sicherheit und Flexibilität.

Weitere Informationen erhalten Sie unter **www.mcafee.com/de/products/move-anti-virus.aspx**.

McAfee
Together is power.

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