DATENBLATT

McAfee Security Suite for Virtual Desktop Infrastructure

Die Sicherheit, die Sie benötigen – bei minimalen Auswirkungen auf die Leistung

Virtuelle Desktops finden zunehmend stärkere Verbreitung, sodass Sie in die Lösung integrierte starke Desktop-Sicherheit benötigen, die Ihr Unternehmen schützt, ohne die Leistung oder die gewünschte Server-Dichte zu beeinträchtigen. Herkömmliche Virenschutzprogramme sind nicht für den Einsatz in virtualisierten Umgebungen konzipiert. Die Antwort darauf stellt die Lösung McAfee® Security Suite for Virtual Desktop Infrastructure (VDI) dar, die umfassende und speziell für virtuelle Desktops optimierte Sicherheit bereitstellt.

McAfee Security Suite for VDI bietet Malware-Schutz speziell für virtualisierte Umgebungen, Whitelists zum Schutz vor Zero-Day-Bedrohungen, sowie Schutz vor Desktop-Eindringungen und Datenkompromittierungen. Die Lösung warnt Benutzer auch vor böswilligen Webseiten und/oder blockiert den Zugriff darauf.

Optimierte Scan-Architektur

Die Dynamik virtueller Desktops erfordert große Sorgfalt. So lange Abbilder offline sind, müssen sie frei von Malware bleiben. Sobald jedoch Benutzer eine Sitzung starten, müssen sie ohne Verzögerung geprüft werden. Allerdings wird beim Sitzungsstart nicht nur der Malware-Schutz gestartet. Da Benutzer häufig zur gleichen Zeit ihre Arbeit beginnen, können sie dabei „Virenschutz-Blockaden“ auslösen, bei denen der Virenschutz alle Ressourcen verbraucht und das Abrufen von Sitzungen verhindert.

Zur Vermeidung von Scan-Engpässen und Verzögerungen lagert McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) Scans, Konfigurationen und DAT-Aktualisierungen aus den einzelnen Gast-Abbildern in die gesicherte virtuelle Appliance bzw. auf den 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. Dank der Möglichkeit zur bedarfsgerechten Scan-Planung können Sie gewährleisten, dass die Hypervisor-Leistung nicht durch Scans beeinträchtigt wird.

Detaillierte Richtlinienverwaltung

Die Konfiguration der Richtlinien sowie der McAfee MOVE AntiVirus-Kontrollfunktionen erfolgt über die McAfee® ePolicy Orchestrator® (McAfee ePO™)-Konsole. Die Daten aus virtuellen Desktops können über zentrale Dashboards und Berichte mit Informationen aus anderen

Hauptvorteile

- Bietet dank McAfee ePO und Cloud Workload Discovery Funktionen für Erkennung und Transparenz
- Einzigartige Kombination von Blacklists und Whitelists zum Schutz virtueller Desktops vor Malware
- Optimierte Sicherheit für virtuelle Umgebungen, um Leistungs-einschränkungen zu minimieren
- Integration von Eindringungs- und Web-Schutz dank Speicher- und Web-Anwendungsschutz
- Nutzung von McAfee ePO für zentrale Übersichten, Kontrollen und Berichtsfunktionen zu allen Endgeräten
- Unterstützung flexibler Optionen für agentenlose Bereitstellung sowie Bereitstellung auf mehreren Plattformen
- Unterstützung elastischer Bereitstellung von Offline-Scannern zur bedarfsgerechten Skalierung (für mehrere Plattformen)
- Integration lokaler Reputationsdaten zur schnelleren Reaktion auf Bedrohungen (für mehrere Plattformen)

Systemen zusammengefasst werden. Administratoren können über Cloud Workload Discovery für private Clouds individuelle Richtlinien pro VM, Ressourcen-Pool, Cluster oder Rechenzentrum konfigurieren und ihre Sicherheitseinstellungen präzise an den Aufbau des Rechenzentrums anpassen.

Agentenlose Option 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 VMware-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 MOVE AntiVirus in vCNS ermöglicht die Überwachung des SVM-Status innerhalb von VMware vCenter und den Empfang von Warnmeldungen, wenn die SVM die Verbindung verliert. Für den Fall, dass eine VM-Infizierung festgestellt wird, erhält die Software McAfee ePO zudem Ereignisdaten mit Details zur betroffenen VM. Durch die starke Integration mit NSX können in McAfee ePO 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.

Option für mehrere Plattformen für alle Hypervisoren

Bei Installationen auf mehreren Plattformen kommuniziert der McAfee MOVE AntiVirus-Agent – eine Endgeräte-Komponente mit geringem Ressourcen-Verbrauch – mit McAfee MOVE Offload Scan Server, um Virenschutz-Funktionen für den entsprechenden virtuellen Desktop zu koordinieren. Ein McAfee ePO-Agent verwaltet die Richtlinien und Scan-Funktionen. Sie haben auch die Möglichkeit, ein Gold-Abbild zu scannen und als „sauberes Master-Abbild“ zu definieren. Dadurch können Administratoren globale Caches vorab mit sauberen Abbildern auffüllen, um die Startzeiten der virtuellen Desktops zu verkürzen.

Wenn ein Benutzer auf eine Datei zugreift, führt der McAfee MOVE Offload Scan Server einen On-Access-Scan durch und liefert eine Rückmeldung an die VM.

Konfiguration von McAfee Security Suite for VDI

- McAfee MOVE AntiVirus
  - Implementierung auf mehreren Plattformen
  - Agentenlose Implementierung
- Cloud Workload Discovery für private Clouds (VMware und OpenStack)
- McAfee VirusScan® Enterprise for Windows
- McAfee VirusScan Enterprise for Linux
- McAfee Host Intrusion Prevention for Desktops
- McAfee Application Control for Desktops
- McAfee SiteAdvisor® Enterprise (Technologie)
- McAfee ePolicy Orchestrator

Im Fall von Problemen können die Benutzer über eine Pop-Up-Warnmeldung informiert und die Datei bis zur Entscheidung über geeignete Maßnahmen in die Quarantäne verschoben werden. Für jeden virtuellen Desktop können in der McAfee ePO-Konsole individuelle Richtliniensätze konfiguriert werden. Alternativ lassen sich die virtuellen Desktops als Gruppe verwalten.

Da Workloads in Mehrplattformumgebungen aktiviert und deaktiviert werden, 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 in Mehrplattform-umgebungen die globalen Bedrohungsinformationen aus McAfee Global Threat Intelligence 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 virtuellen Desktops automatisch gegen die neu entdeckte Malware zu immunisieren.

Funktion	Warum Sie sie benötigen
Schutz virtueller Umgebungen	▪ Verbessert die Sicherheit von Arbeitsabläufen auf virtuellen Desktop-Infrastrukturen, ohne dass die Leistung beeinträchtigt und der Ressourcenbedarf erhöht werden. ▪ Für VMware optimierte agentenlose Bereitstellung ermöglicht hervorragende Leistung und VM-Dichte. Keine Notwendigkeit zur Installation/Aktualisierung unserer Agenten auf jedem virtuellen Desktop, sodass die Komplexität reduziert und die Benutzerfreundlichkeit erheblich verbessert werden. ▪ Bereitstellung auf mehreren Plattformen für alle Hypervisoren unterstützt die flexible Bereitstellung von Offline-Scannern, um bedarfsgerechte Skalierung zu ermöglichen und lokale Reputationsdaten für schnelle Reaktionen auf Bedrohungen einzubeziehen.
Grundlegender Endgeräteschutz	▪ Die McAfee-Virenschutzlösung scannt schneller, verbraucht weniger Speicher, benötigt weniger CPU-Zyklen und schützt Benutzer besser als andere Produkte. ▪ Host-Eindringungsschutz schützt Unternehmen vor komplexen Sicherheitsbedrohungen, die andernfalls unbeabsichtigt auf Systeme gelangen oder dort zugelassen werden könnten. ▪ McAfee SiteAdvisor® Enterprise verhindert, dass Benutzer mit gefährlichen Webseiten interagieren, und ermöglicht die Anpassung entsprechender Richtlinien, um so die Einhaltung von Compliance-Vorschriften zu gewährleisten.

Funktion	Warum Sie sie benötigen
Anwendungs-Whitelists	▪ Reduziert im Vergleich mit herkömmlichen Endgerätesicherheitskontrollen erheblich den Leistungsbedarf auf dem Host. ▪ Schützt auch ohne Signaturaktualisierungen vor Zero-Day-Bedrohungen und hochentwickelten hartnäckigen Bedrohungen (APTs), sodass die Schutzwirkung schneller erreicht wird. ▪ Dynamische Whitelists erfordern geringeren Verwaltungsaufwand im Vergleich zu veralteten Whitelist-Techniken.
Cloud Workload Discovery	▪ Bietet einen vollständigen Überblick über Privat-Cloud-Workloads und die zugrundeliegenden Plattformen, um schwache Sicherheitskontrollen zu identifizieren.
Schutz für Dateien und Wechselmedien (Verschlüsselung)	▪ Dank Schutz für Dateien und Wechselmedien kann Verschlüsselung erheblich einfacher und weniger riskant bereitgestellt werden. ▪ Ermöglicht dank optimierter Implementierung der Intel® AES-NI-Technologie beinahe ungebremste Leistung auf verschlüsselten Hosts. ▪ Ermöglicht die Bereitstellung automatischer und transparenter Verschlüsselung für Dateien/Ordner sowie Wechselmedien (USB-Laufwerke, CDs, DVDs), die durch Richtlinien durchgesetzt wird. ▪ Bietet Benutzern die Möglichkeit zur Verschlüsselung von USB-Medien und sicheren Übertragung von Informationen. ▪ Ermöglicht den sicheren Zugriff auf Daten in Netzwerkfreigaben.
Zentrale Verwaltung durch die Software McAfee ePO	▪ Zentrale Verwaltung physischer, virtueller und Cloud-Bereitstellungen für bessere Sicherheitskontrollen, einschließlich Richtlinienverwaltung, Bereitstellung, Transparenz und Sicherheitsverwaltung für alle Plattformen. ▪ Vereinfacht Betriebsabläufe und verringert den Zeitaufwand für die Administratoren. ▪ Verringert die Hardware-Kosten aufgrund von geringerem Server-Ressourcenbedarf.

Weitere Informationen

McAfee-Lösungen bieten die von Ihnen geforderte Sicherheit bei minimalen Auswirkungen auf die Leistung. Weitere Informationen finden Sie unter **www.mcafee.com/de/products/data-center-security-suite-for-vdi.aspx**.

McAfee
Together is power.

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