# McAfee Security Suite for Virtual Desktop Infrastructure

## Sicherheit und Flexibilität für Ihre Unternehmensumgebung

Da virtuelle Desktops (VDIs) zunehmend stärkere Verbreitung finden, muss starke Desktop-Sicherheit in die Lösung integriert werden, um Ihr Unternehmen zu schützen, 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 VDI dar, die umfassende Sicherheit speziell optimiert für virtuelle Desktops bereitstellt.

**Hauptvorteile**

- Erkennung und Transparenz für VMware vSphere-Umgebungen durch McAfee ePO und McAfee Data Center Connector for VMware vSphere. Die einmalige Kombination von Black- und Whitelists schützt sowohl physische als auch virtuelle Umgebungen vor Malware.
- Optimierte Sicherheit für virtuelle Umgebungen, um Leistungseinschränkungen zu minimieren.
- Schutz vor unbekannten Bedrohungen, indem die Ausführung unbekannter Anwendungen auf Ihren virtuellen Desktops verhindert wird.
- Integration von Eindringungs- und Web-Schutz dank Desktop-Firewall sowie Speicher- und Web-Anwendungsschutz.
- Nutzung von McAfee ePO für Überblick, Kontrolle und Berichterstellung zu allen Endgeräten auf einem Blick.

McAfee Security Suite for VDI bietet Malware-Schutz speziell für virtualisierte Umgebungen, Whitelists zum Schutz vor Zero-Day-Bedrohungen, 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 (MOVE) AntiVirus Scans, Konfigurationen und DAT-Aktualisierungen aus den einzelnen Gast-Abbildern in die gesicherte virtuelle Appliance bzw. auf den Offload-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-Einstellungen erfolgt über die McAfee® ePolicy Orchestrator® (McAfee ePO™)-Konsole. Die Daten aus virtuellen Desktops können über zentrale Dashboards und Berichte mit Informationen aus anderen Systemen zusammengefasst werden. Administratoren können eine individuelle Richtlinie pro VM, Ressourcen-Pool, Cluster oder Rechenzentrum über McAfee Data Center Connector konfigurieren und ihre Sicherheitseinstellungen präzise an den Aufbau des Rechenzentrums anpassen.

intel Security

### Konfiguration von McAfee Security Suite for VDI

**McAfee MOVE AntiVirus for Virtual Desktops (VDI)**

- McAfee MOVE AntiVirus
  - Bereitstellung auf mehreren Hypervisoren
  - Agentenlose Implementierung
- McAfee Data Center Connector for vSphere
- McAfee VirusScan® Enterprise for Windows (Software)
- McAfee VirusScan Enterprise for Linux (Software)
- McAfee Host Intrusion Prevention System
- McAfee Application Control for Desktops
- McAfee SiteAdvisor® Enterprise (Technologie)
- McAfee ePolicy Orchestrator (Software)

## Agentenlose Bereitstellung mit VMware vShield für verbesserte Effizienz

In agentenlosen Implementierungen verwendet VMware vShield Endpoint den Hypervisor als Hochgeschwindigkeitsverbindung, um der McAfee MOVE AntiVirus Security Virtual Appliance (SVA) das Scannen virtueller Maschinen von außerhalb der Gast-Abbilder zu ermöglichen. Während des Scans erhält vShield von der SVA 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.

Nach der Installation und Konfiguration der SVA sowie der erforderlichen vShield-Komponenten auf den ESX-Servern und der vShield-Treiber auf den Gast-VMs werden alle Abbilder automatisch bereits bei der Erstellung geschützt. Auf den Client-VMs muss keine McAfee-Software installiert werden. Dank unserer vMotion-fähigen Implementierung können virtuelle Maschinen zwischen Hosts verschoben werden, wobei sie auf dem Ziel-Host nahtlos von der SVA geschützt werden – ohne Beeinträchtigung der Scan- oder VM-Leistung. Die McAfee-Integration ermöglicht die Überwachung des SVA-Status innerhalb von vCenter und den Empfang von Warnmeldungen, wenn die SVA die Verbindung verliert. Für den Fall, dass eine VM-Infizierung festgestellt wird, erhält McAfee ePO zudem Ereignisdaten mit Details zur betroffenen VM.

## Unterstützung mehrerer Hypervisoren für Standard und Komfort

Bei Installationen auf mehreren Hypervisoren kommuniziert der McAfee MOVE AntiVirus-Agent – eine Endgeräte-Komponente mit geringem Ressourcen-Verbrauch – mit dem 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. 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.

## Weitere Informationen

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

| 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.<br>• Agentenlose Bereitstellung auf mehreren Hypervisoren bietet die Möglichkeit zum Einsatz in Virtualisierungsumgebungen mit unterschiedlichen Anbietern (VMware, Citrix, Hyper-V).<br>• Für VMware optimierte agentenlose Bereitstellung ermöglicht hervorragende Leistung und VM-Dichte. Keine Notwendigkeit zur Installation/Aktualisierung von McAfee-Agenten in jedem virtuellen Desktop, sodass die Komplexität reduziert und die Benutzerfreundlichkeit erheblich verbessert werden. |
| **Grundlegender Endgeräteschutz** | • Virenschutz für physische Server, der von NSS Labs beim Schutz vor Zero-Day-Exploits und Verschleierungsangriffen die beste Bewertung erhielt.<br>• Host-Eindringungsschutz schützt Unternehmen vor komplexen Sicherheitsbedrohungen, die andernfalls unbeabsichtigt auf Systeme gelangen oder dort zugelassen werden könnten.<br>• 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. |
| **Anwendungs-Whitelists** | • Reduziert im Vergleich mit herkömmlichen Endgerätesicherheitskontrollen erheblich den Leistungsbedarf auf dem Host.<br>• Schützt auch ohne Signaturaktualisierungen vor Zero-Day-Bedrohungen und hochentwickelten hartnäckigen Bedrohungen (APTs), sodass die Schutzwirkung schneller erreicht wird.<br>• Dynamische Whitelists erfordern geringeren Verwaltungsaufwand im Vergleich zu veralteten Whitelist-Techniken. |
| **Vollständiger Überblick über virtuelle Maschinen in der privaten Cloud** | • Ermöglicht die automatische Erkennung virtueller Maschinen in der privaten Cloud (VMware vSphere). |
| **Schutz für Dateien und Wechselmedien (Verschlüsselung)** | • Dank Schutz für Dateien und Wechselmedien kann Verschlüsselung erheblich einfacher und weniger riskant bereitgestellt werden.<br>• Ermöglicht dank optimierter Implementierung der Intel AES-NI-Technologie beinahe ungebremste Leistung auf verschlüsselten Hosts.<br>• Ermöglicht die Bereitstellung von durch Richtlinien durchgesetzte, automatische und transparente Verschlüsselung für Dateien/Ordner sowie Wechselmedien (USB-Laufwerke, CDs, DVDs).<br>• Bietet Benutzern die Möglichkeit zur Verschlüsselung von USB-Medien und sicheren Übertragung von Informationen.<br>• Ermöglicht den sicheren Zugriff auf Daten in Netzwerkfreigaben. |
| **Zentrale Verwaltung durch die Software McAfee ePO** | • Ermöglicht die Verwaltung physischer Computer und virtueller Maschinen über eine zentrale Übersicht, einschließlich solchen in privaten und öffentlichen Clouds für bessere Sicherheitstransparenz.<br>• Vereinfacht Betriebsabläufe und verringert den Zeitaufwand für die Administratoren.<br>• Verringert die Hardware-Kosten aufgrund von geringerem Server-Ressourcenbedarf. |

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


61145ds_vdi_0614B_fnl