# McAfee Public Cloud Server Security Suite

## Umfassende Server-Sicherheit für Benutzer öffentlicher Clouds

**Hauptvorteile**

Die McAfee Public Cloud Server Security Suite bietet folgende Vorteile:

- Anzeige flexibler Cloud-Server-Instanzen, die aktiviert und deaktiviert werden; Erkennung von Server-Instanzen in der öffentlichen Cloud mit McAfee Data Center Connector-Modulen für zentrale Richtlinienkonfiguration und -durchsetzung selbst in Unternehmen mit „Schatten-IT"-Problemen
- Schutz von Server-Instanzen mit einer einmaligen Kombination aus Virenschutz, Host-basierter Firewall, Anwendungs-Whitelists, Eindringungsschutz- und Datenschutztechnologien für alle öffentlichen Cloud-Implementierungen, die in Microsoft Windows- oder Linux-Umgebungen ausgeführt werden
- Verwaltung von Sicherheitsrichtlinien für Server-Instanzen in der öffentlichen Cloud über eine zentrale Verwaltungsplattform, damit empfohlene Vorgehensweisen überall durchgesetzt werden

Wenn Unternehmen ihre Rechenzentrumstrategie dahingehend ändern, dass sie Server-Instanzen in öffentlichen Clouds einsetzen und auch bevorzugt nutzen, ist ihnen bewusst, dass das gemeinsame Sicherheitsmodell ein wichtiger Aspekt ist. Anbieter öffentlicher Clouds wie Amazon Web Services (AWS) und Microsoft Azure schützen die Peripherie, während die Benutzer ihre eigenen Inhalte schützen müssen. Doch wie können sich zukunftsorientierte Unternehmen vor Zero-Day- und hochentwickelten hartnäckigen Bedrohungen schützen, gleichzeitig aber ihre Kosten im Rahmen halten, um die Vorteile ihrer Cloud-Strategie auszuschöpfen?

McAfee® Public Cloud Server Security Suite bietet Unterstützung bei der Durchsetzung sowie Verwaltung von Sicherheitsrichtlinien für Server in der öffentlichen Cloud und ermöglicht so umfassende Sicherheit. Die McAfee Public Cloud Server Security Suite gewährt Einblick in die Server-Instanzen der öffentlichen Cloud, stellt dank einer leistungsfähigen Kombination aus Black- und Whitelist-Technologien umfassende Schutzmaßnahmen bereit und erlaubt zusammen mit McAfee® ePolicy Orchestrator® (McAfee ePO™) die dynamische Verwaltung dieser Umgebung zusammen mit Desktop-Computern, Mobilgeräten und physischen Servern.

### Optimiert für die öffentliche Cloud

Sicherheitsbewusste IT-Experten müssen Risiken verwalten können, um der Datensicherheit in der Cloud das gleiche Vertrauen entgegenbringen zu können wie bei ihren physischen Servern vor Ort. McAfee Public Cloud Server Security Suite ist optimiert für den Cloud-Betrieb und bietet die gleichen erstklassigen McAfee VirusScan®- und IPS-Technologien (Intrusion Prevention System, Eindringungsschutz-System) wie unsere Sicherheits-Suites für physische Server.

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

intel Security

### Unterstützte Plattformen

- Windows 2008, 2008 R2, 2012, 2012 R2
- Linux (Red Hat, CentOS, SUSE, Ubuntu, Amazon Linux)

In McAfee Public Cloud Server Security Suite 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.

Eine Firewall für Linux- und Windows-Systeme verhindert, dass Malware und Botnets in die Cloud-Server eindringen und sich dort verbreiten, indem sie nicht autorisierten Netzwerkverkehr blockiert. Amazon EBS-Volumes werden sicher und zuverlässig verschlüsselt. Zusätzlich werden Volumes mit bereits bestehenden Daten verschlüsselt.

## Intelligenter Schutz für öffentliche Clouds

Kunden verfügen über wenige inkrementelle Ressourcen, um ein weiteres Sicherheitssystem für ihre Cloud-Server zu verwalten. Und wenn interne Projekte kurzfristig öffentlichen Clouds zugewiesen werden, ohne dass ausreichende IT-Sicherheitsprotokolle eingerichtet sind, können die massiven Sicherheitsmauern plötzlich durchlässig werden und die Kompromittierungswahrscheinlichkeit erheblich steigen. McAfee Public Cloud Server Security Suite nutzt die Leistung und Skalierbarkeit von McAfee ePO, um die gesamte Infrastruktur – physisch, virtuell, für die Cloud und Mobilgeräte – zu erkennen, zu verwalten und in Berichten zu erfassen. McAfee ePO bietet eine zentrale Übersicht über diese Schatten-IT-Instanzen zur äußerst skalierbaren, flexiblen und automatisierten zentralen Verwaltung sowie Durchsetzung der Sicherheitsrichtlinien, damit Sicherheitsprobleme und Bedrohungen erkannt, verwaltet sowie behoben werden.

Gleichzeitig wird mit zunehmender Anzahl von DevOps-Tools die Integration dieser Tools immer wichtiger. McAfee PCS verzahnt sich nahtlos mit den neuesten DevOps-Tools wie Chef und Puppet Labs.

## Kostenschonend und flexibel

Kunden wechseln zu Cloud-basierten Computing-Lösungen, um eine preiswerte Alternative zur Rechenzentrumserweiterung zu nutzen. Flexible Finanzierungsmöglichkeiten müssen diese Migration unterstützen und dem Wunsch der Kunden Rechnung tragen, von einem investitionsbasierten Zahlungsmodell (CapEx) zu einem Betriebskostenmodell (OpEx) zu wechseln. McAfee Public Cloud Server Security Suite wird stundenweise abgerechnet und gibt Kunden die Flexibilität, sich für die Sicherheitslösungen zu entscheiden, die ihre finanziellen Anforderungen bestmöglich erfüllen.


**Abbildung 1.** Zentrales Übersichts-Dashboard für McAfee Public Cloud Server Security Suite

| Komponente | Vorteil | Kundenvorteile |
|---|---|---|
| **Zentrale Verwaltung durch die Software McAfee ePO** | Umgebung mit einer zentralen Konsole, die umfassende Verwaltung aller McAfee-Endgeräte-Funktionen ermöglicht | • Verwaltung physischer Computer und virtueller Maschinen über eine zentrale Übersicht, einschließlich solchen in privaten und öffentlichen Clouds für bessere Sicherheitstransparenz<br>• Vereinfachte Betriebsabläufe und geringerer Zeitaufwand für die Administratoren<br>• Senkung der Hardware-Kosten durch geringeren Server-Ressourcenbedarf |
| **Cloud-Connector-Module für Amazon AWS, Microsoft Azure und OpenStack** | Vollständiger Überblick über virtuelle Maschinen auch in der privaten Cloud | • Erkennung nicht nur physischer Server, sondern auch von Hypervisoren und virtuellen Maschinen in den Umgebungen von VMware vSphere, Amazon AWS und OpenStack, sodass die zu schützenden Ressourcen vollständig angezeigt werden<br>• Erkennung der Bereitstellung virtueller Maschinen und anschließend automatischer Schutz dieser Instanzen durch Sicherheitsrichtlinien, um zuverlässige Sicherheit zu gewährleisten |
| **Datenschutz für die Cloud** | Einfache Verschlüsselung von Datenvolumes mit der Software McAfee ePO | • Verschlüsselung zur Verbesserung des Schutzes für Daten und geistiges Eigentum vor unbefugtem Zugriff<br>• Bequeme Verschlüsselung von Volumes mit bereits vorhandenen Daten über die Software McAfee ePO<br>• Keine Leistungseinbußen bei Verwendung der Amazon-eigenen EBS-Verschlüsselung |
| **VirusScan Enterprise für Server** | Grundlegender Malware-Schutz für Windows- und Linux-Server sowie Eindringungsschutz und Änderungskontrollen | • Malware-Schutz für physische Server, der von NSS Labs beim Schutz vor Zero-Day-Exploits und Verschleierungsangriffen die Bestwertung erhielt<br>• Stärkster Schutz vor Malware: Schützt Systeme und Dateien vor Viren, Spyware, Würmern, Trojanern und anderen Sicherheitsrisiken; entdeckt sowie löscht Malware und erlaubt Benutzern die unkomplizierte Konfiguration von Richtlinien zur Behandlung isolierter Elemente<br>• Präventiver Schutz vor Angriffen: Dank Echtzeit-Scans sind alle Systeme – auch Systeme an entfernten Standorten – vor aktuellen und neuen Bedrohungen geschützt; VirusScan Enterprise zum Schutz auch vor Buffer-Overflow-Angriffen, die Schwachstellen in Microsoft-Anwendungen ausnutzen |
| **Host-basierter Eindringungsschutz** | Eindringungsschutz für wichtigen und allgemein erforderlichen Schutz vor bekannten und Zero-Day-Bedrohungen | • McAfee Host Intrusion Prevention zum Schutz Ihres Unternehmens vor komplexen Sicherheitsbedrohungen, die andernfalls unbeabsichtigt auf Systeme gelangen oder dort zugelassen werden könnten<br>• Technologie der nächsten Generation für stärkeren Schutz vor Viren, Würmern, Trojanern und anderen Bedrohungen, die Ihre wichtigsten Daten kompromittieren oder Ihr Unternehmen stilllegen können; schützt zuverlässig Ihre verwundbaren Anwendungen vor Angriffen<br>• Schutz Ihrer Geräte vor Viren, die über Wechselmedien, das Web oder entfernte Netzwerke eindringen |
| **Firewall für Linux und Windows** | Netzwerk-Firewalls zur Blockierung von nicht autorisiertem Netzwerkverkehr | • Verhindert, dass Malware in die Cloud-Server eindringt und sich dort verbreitet |

| Komponente | Vorteil | Kundenvorteile |
|---|---|---|
| **Anwendungskontrolle** | Gewährleistet, dass Hosts in einem sicheren Status gehalten werden, indem die Ausführung unerwünschter Anwendungen verhindert wird | • Erhebliche Reduzierung des Leistungsbedarfs auf dem Host im Vergleich zu herkömmlichen Endgerätesicherheitsmaßnahmen<br>• Schutz auch ohne Signaturaktualisierungen vor Zero-Day-Bedrohungen und hochentwickelten hartnäckigen Bedrohungen (APTs), sodass die Schutzwirkung schneller erreicht wird<br>• Geringerer Verwaltungsaufwand dank dynamischer Whitelists (im Vergleich mit veralteten Whitelist-Techniken) |
| **Änderungskontrolle** | Dateiintegritätsüberwachung durch kontinuierliche Erkennung von Änderungen auf Systemebene in verteilten und entfernten Standorten | • Verhinderung von Manipulationen durch Blockierung nicht autorisierter Änderungen an kritischen Systemdateien, Verzeichnissen und Einstellungen, sodass Administratoren bei der Behebung von Sicherheitskompromittierungen Zeit sparen<br>• Erfassung und Überprüfung aller versuchten Änderungen am Server in Echtzeit und Erzwingung von Änderungsrichtlinien nach Zeitfenster, Urheber oder genehmigtem Arbeitsauftrag<br>• Kontinuierliche Kontrolle zur Minimierung der Auswirkungen spontaner oder nicht autorisierter Änderungen |

Weitere Informationen zu den Vorteilen der McAfee Public Cloud Server Security Suite erhalten Sie unter **www.mcafee.com/de/products/public-cloud-server-security-suite.aspx**.

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