McAfee Server Security Suite Advanced

Umfassende Sicherheit für physische, virtuelle sowie Cloud-Bereitstellungen einschließlich Whitelisting und Änderungskontrolle

Ohne einen ganzheitlichen Ansatz fällt es in heutigen komplexen IT-Umgebungen zunehmend schwerer, neue Server und Cloud-Workloads vor immer raffinierteren Bedrohungen zu schützen. McAfee® Server Security Suite Advanced bietet einheitlichen und dauerhaften Schutz für Ihre physischen, virtuellen und öffentlichen Cloud-Bereitstellungen. Zu den umfassenden Sicherheitsfunktionen gehören grundlegende Funktionen für Virenschutz, Firewall-Schutz, Eindringungsabwehr und Whitelisting zur Abwehr von Zero-Day-Bedrohungen ebenso wie Änderungskontrollen, mit denen die Compliance mit gesetzlichen Vorschriften gewährleistet wird. Hochentwickelte Schutzmaßnahmen minimieren Leistungseinbußen bei physischen sowie virtuellen Servern und werden automatisch mit Ihren dynamischen Cloud-Workloads skaliert.

Sofortige Erkennung und Kontrolle

Dank Cloud Workload Discovery für Hybrid-Clouds, einer Kernfunktionen von McAfee Server Security Suite Advanced, wird das Aufspüren von Sicherheitslücken in Ihrem wachsenden Hybrid-Rechenzentrum erheblich erleichtert. Diese Funktion, die VMware, OpenStack, AWS und Microsoft Azure abdeckt, erhalten Sie einen umfassenden Überblick über alle Workloads sowie die zugrunde liegenden Plattformen. Informationen über schwache Sicherheitskontrollen, unsichere Firewalls und Verschlüsselungseinstellungen sowie Kompromittierungsindikatoren (z. B. verdächtigen Datenverkehr) ermöglichen eine schnellere Erkennung von Bedrohungen. Mit McAfee® ePolicy Orchestrator® (McAfee ePO™) sowie DevOps-Tools können gefundene Gefahren schnell behoben werden.

Die Gewährleistung von Cloud-Sicherheit wird durch zahlreiche unterschiedliche Cloud-Workloads mit individuellen Risikoprofilen und Sicherheitsanforderungen erschwert. Cloud Workload Discovery vergleicht mithilfe richtlinienbasierter Analysen, welche Sicherheitskontrollen für diese unterschiedlichen Workloads notwendig und welche derzeit vorhanden sind. Dadurch werden ausreichender Schutz und Compliance gewährleistet. Sobald Sie Sicherheitsrisiken entdecken, können Sie mit wenigen Mausklicks vollständigen Schutz einrichten.

Hauptvorteile

- Zentrale Sicherheitsverwaltung für Endgeräte, Netzwerke, Daten und Compliance-Lösungen von McAfee und Drittanbietern über McAfee ePO
- Umfassender Überblick, Risikobewertung und Behebung mit Cloud Workload Discovery für Hybrid-Clouds
- Kombination aus Blacklists und Eindringungsschutz mit hochentwickelten Whitelists und Änderungskontrolle zum Schutz physischer und virtueller Server vor Malware
  - Schutz vor unbekannten Bedrohungen, indem die Ausführung unbekannter Anwendungen verhindert wird
  - Kontinuierliche Erkennung von Veränderungen auf Systemebene an verteilten und entfernten Standorten zur Erfüllung von Compliance-Anforderungen

Dank der Integration von Cloud Workload Discovery in die McAfee ePO-Verwaltungskonsole haben Unternehmen effektive Kontrollmöglichkeiten, um sichere Lösungen in physischen, virtuellen und Cloud-Umgebungen zu implementieren. Diese Integration bietet für Sicherheitsadministratoren einen wichtigen Vorteil: Sie können eine einzige Verwaltungsplattform mit vereinfachten Workflows nutzen, um auf Bedrohungswarnungen zu reagieren sowie Richtlinien durchzusetzen und so die Ermittlung und Behebung von Sicherheitsproblemen zu beschleunigen.

McAfee Server Security Suite Advanced gewährleistet, dass Sie dynamische Cloud-Umgebungen für DevOps nutzen können, ohne zwischen Sicherheit und Flexibilität wählen zu müssen. Unsere Sicherheitsfunktionen sind elastisch mit den Cloud-Workloads skalierbar, sodass Ihre Benutzer und Daten jederzeit geschützt sind. Durch die elastische Bereitstellung in Privat-Clouds können Offline-Scan-Server bei der Aktivierung oder Deaktivierung von Workloads automatisch zum Ressourcen-Pool hinzugefügt oder daraus entfernt werden. Für AWS- und Azure-Workloads können Benutzer Sicherheitsfunktionen auf Vorlagenebene konfigurieren, damit die Sicherheit bei Workload-Veränderungen automatisch skaliert wird.

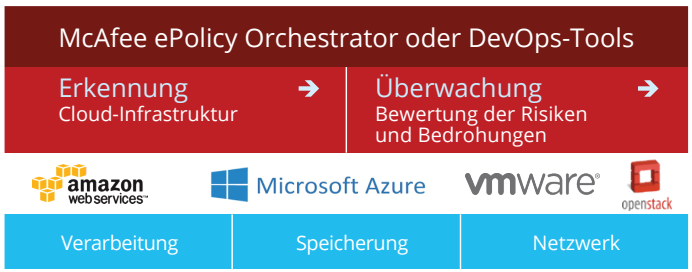

Abbildung 1. Vorteile von Cloud Workload Discovery

Umfassender Schutz

McAfee Server Security Suite Advanced bietet den umfassendsten Schutz für Ihre physischen, virtuellen oder Cloud-basierten Server. Außerdem ist der Schutz vor Buffer Overflow-Angriffen auf 32- und 64-Bit-Windows-Systemen zusammen mit der einzigartigen Kombination aus Black- und Whitelists sowie Änderungskontrollen in der ganzen Branche einmalig. Die Suite enthält folgende Anwendungen:

- **McAfee Application Control for Servers:** Diese Whitelist-Lösung gewährleistet, dass ausschließlich autorisierte Software auf Servern ausgeführt werden kann, damit unbekannte Malware und Zero-Day- sowie hochentwickelte Bedrohungen keine Chance haben. Diese zentral verwaltete Whitelist-Lösung nutzt ein dynamisches Vertrauensmodell, sodass die arbeitsintensive Listenverwaltung entfällt.
- **McAfee Change Control for Servers:** Erkennt kontinuierlich Änderungen auf Systemebene in verteilten und entfernten Standorten, sodass die Compliance mit Gesetzen und Vorschriften wie SOX (Sarbanes-Oxley Act) und PCI DSS (Payment Card Industry Data Security Standard) gewährleistet ist.
- **Bedrohungsschutz-Modul von McAfee Endpoint Security:** Komponente eines kooperativen und erweiterbaren Frameworks, das Microsoft Windows- und Linux-Server vor Zero-Day-Exploits und hochentwickelten Angriffen schützt.
- **McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus):** Diese Malware-Schutzlösung wurde speziell für virtuelle Umgebungen entwickelt. Für reine VMware NSX- und VMware vCNS-Umgebungen steht eine

Hauptvorteile (Fortsetzung)

- Blockierung von Zero-Day- und unbekannten Bedrohungen innerhalb von Sekunden dank der Kombination lokaler Reputationsdaten mit Sandbox-Analysen
- Optimierte Sicherheit für physische und virtuelle Umgebungen mit minimalen Leistungseinbußen

agentenlose Option zur Verfügung. Bei Verwendung in Umgebungen mit mehreren Plattformen kann eine agentenbasierte Variante genutzt werden, die alle gängigen Hypervisor-Anbieter (z. B. Microsoft Hyper-V, VMware, KVM und Xen) abdeckt.

- **McAfee Host Intrusion Prevention for Server:** Überwacht das Verhalten von Code auf Ihrem Server und kontrolliert Ereignisse auf verdächtige Aktivitäten, um Ihr Unternehmen vor komplexen Sicherheitsbedrohungen zu schützen.
- **Firewall-Modul von McAfee Endpoint Security:** Überwacht den Netzwerk- sowie Internet-Datenverkehr und fängt verdächtige Kommunikationsvorgänge ab.

McAfee Server Security Suite Advanced kann die 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 koordinieren sich die in der Suite enthaltenen Lösungen 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.

McAfee arbeitet für die Schwachstellenverwaltung mit Rapid7 zusammen. Die Rapid7-Lösung Nexpose erkennt sowie priorisiert Schwachstellen und meldet behobene Sicherheitslücken.

Minimale Beeinträchtigung der Leistung

Auch wenn Sicherheit in den meisten Unternehmen eine große Rolle spielt, zögern einige die Implementierung von Server-Schutz hinaus, da sie Leistungsbeeinträchtigungen befürchten. McAfee Server Security Suite Advanced bietet Schutz für Ihre physischen sowie virtuellen Server, ohne die Leistung zu beeinträchtigen – selbst bei Malware-Scans.

Im Gegensatz zu anderen Malware-Schutzprodukten stellen McAfee Endpoint Security und McAfee MOVE AntiVirus keine großen Ansprüche an die Rechenleistung. McAfee Endpoint Security bietet schnelle Scans und optimiert die CPU- sowie Speichernutzung – und schützt dennoch besser als vergleichbare Lösungen. McAfee MOVE AntiVirus lagert Malware-Scans aus den virtuellen Maschinen aus, damit sofortiger Schutz gewährleistet wird und die Speicher- und Prozessor-Belastung dennoch gering bleibt. Dank separater Richtlinien für On-Access- und On-Demand-Scans erhalten Sie bessere Möglichkeiten zur Anpassung von Leistung und Sicherheit.

Optimierung Ihrer Server-Sicherheit 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 – unsere Suite umfasst Lösungen zum Schutz aller Ihrer Server und Cloud-Workloads in immer dynamischeren Umgebungen.

Funktion	Warum Sie sie benötigen
Zentrale Konsolen-verwaltung	▪ Zentrale Verwaltung physischer, virtueller und Cloud-Bereitstellungen für bessere Sicherheitskontrollen, einschließlich Richtlinienverwaltung, Bereitstellung, Transparenz und Sicherheitsverwaltung für alle Plattformen ▪ Vereinfachte Betriebsabläufe und geringerer Zeitaufwand für die Administratoren
Sofortige Erkennung und Kontrolle	▪ Erkennung physischer Server und umfassender Überblick über Ihre Workloads und Plattformen, einschließlich VMware vSphere, OpenStack, AWS und Microsoft Azure ▪ Zuverlässiger Schutz dank Sicherheitsmaßnahmen, die flexibel mit Ihren dynamischen Cloud-Workloads skalieren
Schutz virtueller Umgebungen	▪ Optimierung der Sicherheit von Workloads in virtuellen Infrastrukturen, ohne dass die Leistung beeinträchtigt und der Ressourcenbedarf erhöht werden ▪ Wahl zwischen Bereitstellung für mehrere Plattformen (und alle gängigen Hypervisoren) oder agentenloser Bereitstellung für VMware NSX und VMware vCNS, damit hohe Leistung sowie große VM-Dichte gewährleistet werden
Sicherheit für öffentliche Clouds	▪ Kontrolle der Plattform-Sicherheit für AWS und Microsoft Azure, einschließlich Einstellungen für Firewall und Verschlüsselung ▪ Vollständiger Schutz für AWS-Umgebungen durch Überblick über Datenverkehr- und Netzwerkbedrohungen
Anwendungs-Whitelists	▪ Erhebliche Reduzierung des Leistungsbedarfs auf dem Host (im Vergleich mit herkömmlichen Server-Sicherheitskontrollen) ▪ Schützt auch ohne Signaturaktualisierungen vor Zero-Day-Bedrohungen und hochentwickelten hartnäckigen Bedrohungen (APTs), sodass die Schutzwirkung schneller erreicht wird ▪ Geringerer Arbeitsaufwand durch dynamische Whitelists
Änderungskontrolle	▪ 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
Grundlegender Server-Schutz	▪ Implementierung von Malware-Schutz einschließlich Abwehr von Zero-Day-Exploits und hochentwickelten Angriffen ▪ McAfee Host Intrusion Prevention System bietet Schutz vor komplexen Sicherheitsbedrohungen, die sonst unbeabsichtigt auf Ihre Systeme gelangen können
Lokale Reputations-bewertung	▪ Blockierung unbekannter Zero-Day-Bedrohungen innerhalb von Sekunden dank Vernetzung mit McAfee Threat Intelligence Exchange (separat erhältliches Zusatzmodul)

Weitere Informationen

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

McAfee
Together is power.

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