McAfee Public Cloud Server Security Suite

Umfassende Sicherheit für AWS- und Azure-Cloud-Workloads

Wenn Unternehmen ihre Rechenzentrumstrategie dahingehend ändern, dass sie Server-Instanzen in öffentlichen Clouds einsetzen und auch bevorzugt nutzen, sind sie sich der Bedeutung des gemeinsamen Verantwortungsmodells[1] bewusst. 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 zukunftsorientierte Unternehmen ihre Cloud-Workloads vor Zero-Day-Attacken und hochentwickelten hartnäckigen Bedrohungen schützen, gleichzeitig aber ihre Kosten im Rahmen halten, um die Vorteile ihrer Cloud-Strategie auszuschöpfen? Unternehmen stehen bei der Einführung der Cloud vor einigen großen Herausforderungen:

- Es wird immer schwieriger, mit Zero-Day-Attacken und hochentwickelten Bedrohungen Schritt zu halten.
- Fehlende Transparenz und zentrale Verwaltung erschweren in hohem Maß den Einsatz einer Multi-Cloud-Infrastruktur.
- Leistungsbeeinträchtigung ist ein Problem für die Sicherheit von Cloud-Workloads.

Hauptvorteile

- Konzipiert für Workloads in AWS und Azure
- Sofortige Erkennung
- Sicherheitsanalyse und Bedrohungsabwehr
- Skalierbare Sicherheit
- Umfassender Schutz
- Nutzung der Verwaltungskonsole von McAfee® ePolicy Orchestrator® (McAfee ePO™)
- Möglichkeiten zur Bereitstellung mit Chef, Puppet und OpsWorks
- Compliance-Nachweis
- In andere McAfee-Lösungen integriert

Abbildung 1. Zentrale Konsole zur Verwaltung von Multi-Cloud-Infrastrukturen und mehreren McAfee-Technologien

McAfee® Public Cloud Server Security Suite ermöglicht die sofortige Erkennung und Kontrolle von AWS- und Azure-Workloads sowie Bedrohungen und dadurch vollständigen, konsistenten und dauerhaften Schutz bei minimalen Leistungsbeeinträchtigungen. Außerdem können Sie mehrere Cloud-Rechenzentren, Cloud-Konten sowie virtuelle Maschinen identifizieren und neue Bedrohungen aufspüren.

Dank grundlegendem Viren- und Eindringungsschutz sowie fortschrittlicher Whitelists zur Abwehr von Zero-Day-Bedrohungen erhalten Sie mit McAfee Public Cloud Server Security Suite umfassende Sicherheit. Zudem setzen Änderungskontrollen die Einhaltung von Compliance-Vorschriften durch, während der Datenschutz durch Verschlüsselungsverwaltung gewährleistet wird. Eine zentrale Verwaltungskonsole erleichtert die Verwaltung mehrerer Clouds und die Durchsetzung von Richtlinien. Flexible Bereitstellungsoptionen mit den DevOps-Tools Chef, Puppet und OpsWorks ermöglichen ein nahtloses Arbeiten mit minimalen Beeinträchtigungen.

Erkennung von Cloud-Infrastrukturen und Bedrohungen

Zur besseren Kontrolle über die Cloud-Infrastruktur sowie zur Erkennung von Bedrohungen benötigen Sie eine bessere Übersicht der gesamten Umgebung.

- Erkennen Sie alle virtuellen Netzwerke oder virtuellen privaten Clouds (VPCs), Vorlagen und Workloads in AWS- und Azure-Cloud-Infrastrukturen innerhalb von Minuten. Detaillierte Informationen über Cloud-Infrastrukturkonten, Daten über die

Unterstützte Plattformen

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

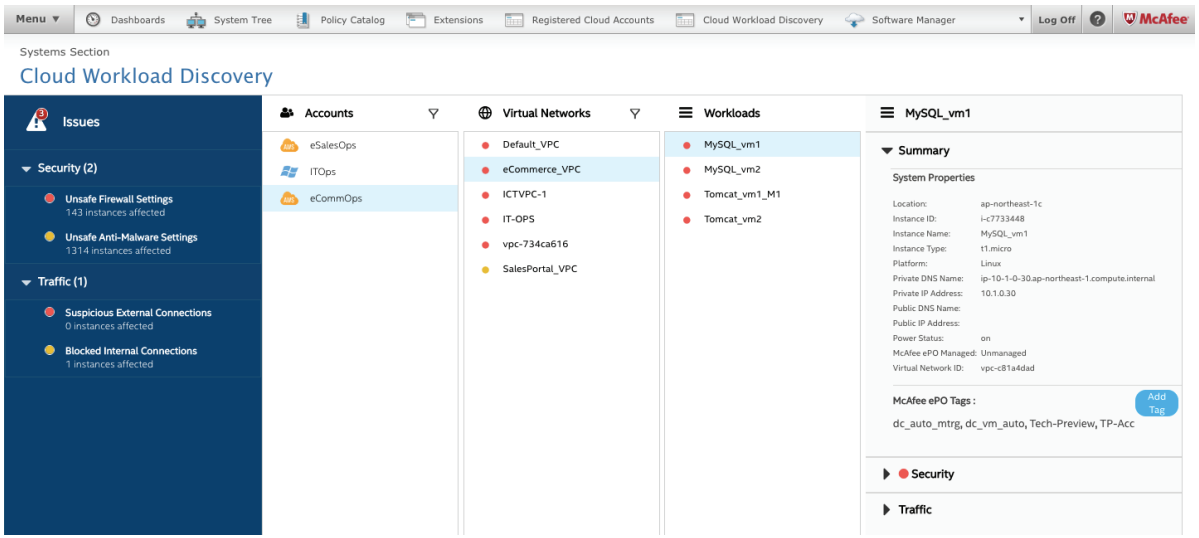

Abbildung 2. Erkennung und Überwachung mehrerer Cloud-Infrastrukturen und neuer Bedrohungen

Zugriffsberechtigungen einzelner Benutzer auf die Cloud-Infrastruktur, Informationen zur Zuweisung von Workloads für Vorlagen und VPCs sowie die Möglichkeit zur schnellen Erstellung von Snapshots der Systemstruktur innerhalb der Cloud-Infrastruktur sind die ersten Schritte zum angemessenen Schutz Ihrer Cloud-Infrastruktur.

- Erhalten Sie einen Überblick über die Sicherheit mehrerer Clouds an einem zentralen Ort. Dank der End-to-End-Bedrohungsinformationen (z. B. zu Angriffsquellen) können Sie die Sicherheit besser kontrollieren.
- Zeigen Sie den Datenverkehr von Workloads an, und kontrollieren Sie den Informationsaustausch zwischen den Workloads sowie den Datenabruf von außerhalb des Unternehmens.

Überwachung der Cloud und schnellere Maßnahmen bei Sicherheitswarnungen

Da die schnelle Problembehebung immer wichtiger wird, können Sie mit dieser Lösung Sicherheitsprobleme auf einer tieferen Ebene schnell analysieren und sofort Maßnahmen durchführen.

- Erkennen Sie Probleme, die dringende Maßnahmen erfordern, und führen Sie bei farblich gekennzeichneten Bedrohungen entsprechende Aktionen durch.
- Erstellen Sie benutzerdefinierte Tags, und weisen Sie diese entsprechend Ihren individuellen Anforderungen den Workloads zu.
- Führen Sie Behebungsmaßnahmen zur Eindämmung von Sicherheitsproblemen durch, und nutzen Sie Richtlinien sowie Definitionen zur Bedrohungsreputation, um Ihre Infrastruktur vor zukünftigen Sicherheitsvorfällen zu schützen.

Umfassende Host-basierte Sicherheitskontrollen

Für Windows und Linux

Abbildung 3. Umfassende Sicherheit für Workloads in öffentlichen Clouds

- Verwalten Sie die Cloud-Firewall mit benutzerdefinierten Richtlinien für individuelle Workloads oder Workload-Gruppen. Verwalten Sie Richtlinien für AWS-Sicherheitsgruppen, um den Datenverkehr für eine oder mehrere Instanzen zu kontrollieren.
- Erkennen Sie verdächtigen Datenverkehr in VPCs und führen Sie Behebungsmaßnahmen durch, die eine Exfiltrierung wichtiger Informationen in die falschen Hände verhindern.

Umfassender Schutz vor Bedrohungen

Die McAfee Public Cloud Server Security Suite nutzt einen einzigen Agenten, der mehrere Sicherheitsebenen bereitstellt, die mit einer zentralen Verwaltungskonsole in mehreren Cloud-Plattformen verwaltet werden können. Diese Lösung kann auch mit DevOps-kompatiblen Tools bereitgestellt werden, was den idealen Nutzungsfall darstellt.

Komponente	Vorteile
Bereitstellungsmöglichkeiten mit Chef, Puppet und AWS OpsWorks	▪ Nutzung von DevOps-Bereitstellungs-Tools zur frühzeitigen Berücksichtigung und einfachen Implementierung der Sicherheit ▪ Möglichkeit zur Integration von Sicherheitsmaßnahmen in die Abläufe
Erkennung von Cloud-Workloads	▪ Sofortige Übersicht über die Cloud-Infrastrukturen mit Anzeige der virtuellen Rechenzentren, Cloud-Workloads und Cloud-Firewalls ▪ Schnelle Bedrohungswarnungen mit automatischer Analyse der Sicherheitslage ▪ Schnellere Behebung von Bedrohungen dank priorisierten Warnungen basierend auf dem Schweregrad von Bedrohungen sowie Schritten zur schnellen Reaktion auf diese Warnungen
Zentrale Verwaltungskonsole für mehrere Cloud-Infrastruktur-Sicherheitslösungen (McAfee ePO)	▪ Optimal geeignet für hybride Umgebungen ▪ Verwaltung der physischen, virtuellen und Cloud-Workloads sowie der Richtlinien über eine einzige Oberfläche ▪ Integriert die Cloud- und lokalen Sicherheitstechnologien von McAfee und Partnern ▪ Geringere Gesamtbetriebskosten dank integrierter Sicherheitsprozesse und schneller Problembehebungsschritte
Malware-Schutz	▪ 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
Host-Firewall	▪ Schutz von Workloads vor nicht autorisierten Zugriffen sowie Angriffen

Komponente	Vorteile
Eindringungsschutz für Hosts	▪ Blockierung von unerwünschtem oder gefährlichem Netzwerkverkehr sowie proaktive Blockierung von Zero-Day- und sonstigen bekannten Angriffen mit patentierter und preisgekrönter Technologie ▪ Verhinderung unerwünschter Änderungen an Ihren Workloads, indem der Zugriff auf bestimmte Ports, Dateien, Freigaben, Registrierungsschlüssel und -werte eingeschränkt wird ▪ Speicherschutz verhindert, dass Programme oder Bedrohungen den Puffer zum Überlauf bringen und Nachbarspeichersegmente überschreiben (ausgenutzte Buffer Overflows können beliebigen Code auf Ihrem Computer ausführen)
Anwendungs-Whitelists	▪ Schutz vor Zero-Day-Bedrohungen und hochentwickelten hartnäckigen Bedrohungen auch ohne Signaturaktualisierungen ▪ Verbesserte Sicherheit und geringere Betriebskosten dank dynamischer Whitelists, die neue Software automatisch akzeptieren, wenn diese über vertrauenswürdige Kanäle hinzugefügt wird ▪ Verringerung der Patch-Zyklen dank sicheren Anwendungs-Whitelists und fortschrittlichem Speicherschutz
Dateiintegritätsüberwachung	▪ Erkennung kontinuierlicher Änderungen auf Systemebene in verteilten und entfernten Standorten ▪ Verhinderung von Manipulationen, indem nicht autorisierte Änderungen an kritischen Systemdateien, Verzeichnissen und Konfigurationen blockiert werden ▪ Erfassung und Überprüfung aller Änderungsversuche am Workload in Echtzeit sowie Durchsetzung von Änderungsrichtlinien nach Zeitfenster, Urheber oder genehmigtem Arbeitsauftrag
Verschlüsselungs-Management	▪ Verschlüsselung von in AWS EBS-Volumes gespeicherten Daten mit dem AWS Advanced Encryption Standard (AES) ▪ Bequeme Verschlüsselung von Volumes mit bereits vorhandenen Daten ▪ Integrierte Verschlüsselung mit Amazon Key Management Service (KMS)

Weitere Informationen

Produktseite: **www.mcafee.com/de/products/public-cloud-server-security-suite.aspx**.

Kann auch über den **AWS Marketplace** erworben werden.

1. http://www.mcafee.com/de/resources/white-papers/wp-cloud-security-primer-techtarget.pdf

McAfee
Together is power.

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