McAfee Cloud Workload Security

Schutz für Ihre Workloads in privaten und öffentlichen Clouds: Sicherer. Schneller. Einfacher.

Unternehmensrechenzentren entwickeln sich weiter, und im gleichen Zuge werden jeden Tag immer mehr Workloads in Cloud-Umgebungen migriert. Die meisten Unternehmen nutzen eine hybride Umgebung mit einer Mischung aus lokalen und Cloud-Workloads, einschließlich Containern, die ständig im Fluss sind. Daraus ergeben sich neue Sicherheitsherausforderungen, da für den Schutz der Workloads in Cloud-Umgebungen (ob privat oder öffentlich) neue Ansätze und Tools erforderlich sind. Unternehmen benötigen einen zentralen Überblick über alle Cloud-Workloads sowie lückenlosen Schutz vor Risiken durch fehlerhafte Konfigurationen, Malware und Datenkompromittierungen.

McAfee® Cloud Workload Security automatisiert die Erkennung sowie den Schutz flexibler Workloads und Container um Sicherheitslücken zu schließen, hochentwickelte Bedrohungen abzuwehren und die Verwaltung von Multi-Cloud-Umgebungen zu vereinfachen. McAfee liefert unübertroffenen Schutz sowie die Möglichkeit, Ihre Workloads mit nur einer einzigen automatisierten Richtlinie zu schützen, während sie Ihre virtuellen privaten, öffentlichen und hybriden Umgebungen durchlaufen. Dadurch wird die Effektivität Ihres Cyber-Sicherheitsteams erheblich verbessert.

Echtzeittransparenz

Automatische Erkennung

Nicht erfasste Workload-Instanzen und Docker-Container reißen Lücken in die Sicherheitsverwaltung und sind für Angreifer der geeignete Ansatzpunkt zur Infiltrierung Ihres Unternehmens. McAfee Cloud Workload Security erkennt dynamische Workload-Instanzen und Docker-Container in Amazon Web Services (AWS)-, Microsoft Azure- sowie VMware-Umgebungen und sucht kontinuierlich nach neuen Instanzen. Dadurch erhalten Sie einen zentralen, vollständigen Überblick über Ihre Umgebungen und vermeiden blinde Flecken in Betrieb und Sicherheit, die zu Risiken führen können.

Hauptvorteile

- Kontinuierlicher Überblick über flexible Workload-Instanzen zur Vermeidung blinder Flecken im Betrieb sowie Automatisierung arbeitsaufwändiger Richtlinienimplementierungen
- Erkennung und Überwachung von Docker-Containern und deren Absicherung durch Mikrosegmentierung
- Für virtuelle Maschinen optimierte Bedrohungsabwehr mit mehrstufigen Gegenmaßnahmen
- Zentrale Verwaltung und automatisierte Workflows verringern Komplexität hybrider und Multi-Cloud-Umgebungen erheblich
- Integration von Automatisierungs-Tools (z. B. Chef und Puppet) zur Anwendung von Sicherheitsfunktionen für Workloads in öffentlichen und privaten Clouds zum Zeitpunkt der Bereitstellung

Folgen Sie uns

Moderne Workload-Sicherheit

Schutz vor hochentwickelten Bedrohungen

McAfee Cloud Workload Security integriert umfassende Gegenmaßnahmen, die von Machine Learning- und Whitelisting-Funktionen, Eindämmung von Anwendungsprozessen bis zu für virtuelle Maschinen optimierten Malware-Schutz, Dateiintegritätsüberwachung sowie Mikrosegmentierung reichen und Workloads vor Bedrohungen wie Ransomware und gezielten Angriffen schützen können. Die Funktionen zum Schutz vor hochentwickelten Bedrohungen, einschließlich Machine Learning, erkennen bislang unbekannte Bedrohungen mittels Machine Learning-Techniken, die böswillige Inhalte aufgrund ihrer Code-Attribute und ihres Verhaltens entlarven.

Konsolidieren von Ereignissen

Dank McAfee Cloud Workload Security können Unternehmen die Verwaltung der zahlreichen Schutztechnologien für ihre lokalen und Cloud-Umgebungen über eine einzige Benutzeroberfläche erledigen. Dies schließt Drittanbietertechnologien wie AWS GuardDuty mit ein. Administratoren können die von AWS GuardDuty erfassten Daten aus der kontinuierlichen Überwachung sowie zu nicht autorisiertem Verhalten nutzen, um zusätzliche Einblicke in Bedrohungen zu erhalten. Durch diese Integration können McAfee Cloud Workload Security-Kunden GuardDuty-Ereignisse direkt innerhalb der McAfee Cloud Workload Security-Konsole anzeigen, einschließlich Netzwerkverbindungen, Port-Prüfungen sowie DNS-Anfragen zu EC2-Instanzen. Die GuardDuty-Netzwerkverbindungsereignisse werden in einem Flussdiagramm zugeordnet, wenn der Datenverkehr dem von McAfee Cloud Workload Security erkannten Datenverkehr entspricht.

Überragender Schutz virtueller Umgebungen

McAfee Cloud Workload Security schützt Ihre virtuellen Maschinen in der privaten Cloud vor Malware, ohne dabei die zugrunde liegenden Ressourcen zu belasten oder zusätzliche Betriebskosten zu verursachen. Sie erhalten Malware-Schutz, der ressourcenintensive Aufgaben wie etwa On-Demand-Scans dann ausführt, wenn der Hypervisor nicht überlastet ist.

Netzwerkvisualisierung mit Mikro-Segmentierung

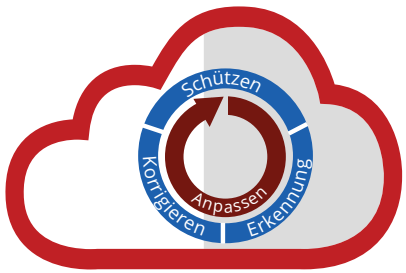
Cloud-eigene Netzwerkvisualisierungen, priorisierte Warnungen vor Risiken sowie Mikrosegmentierungen liefern die Erkenntnisse und Kontrollen, mit deren Hilfe die Ausbreitung von Angriffen sowohl innerhalb virtueller Umgebungen als auch von externen böswilligen Quellen abgewehrt werden kann. Dank der Möglichkeit, Systeme mit einem Mausklick auszuschalten oder zu isolieren, können Probleme durch Konfigurationsfehler verringert und die Behebung beschleunigt werden.

Dateiintegritätsüberwachung

Dank der Dateiintegritätsüberwachung können Sie sicherstellen, dass Ihre Systemdateien und -verzeichnisse nicht durch Malware, Hacker oder böswillige Insider kompromittiert wurden. Umfassende Audit-Protokolle liefern Informationen zu Veränderungen der Dateien auf Server-Workloads und warnen Sie bei einem aktiven Angriff.

Hauptvorteile (Fortsetzung)

- Benutzerfreundlicher und mehrstufiger Schutz vor hochentwickelter Malware sowie Eindringungsschutz
- Visualisierung und Erkennung von Netzwerkbedrohungen ohne Installation eines Agenten
- Korrekturmaßnahmen zum Schutz Ihrer Umgebung direkt aus der Lösung heraus



Cloud Workload Security

Volle **Transparenz** und **Kontrolle**

Anwendungskontrollen

Whitelists für Anwendungen verhindern sowohl bekannte als auch unbekannte Angriffe, indem sie ausschließlich die Ausführung vertrauenswürdiger Anwendungen zulassen und alle nicht autorisierten Inhalte blockieren. Zudem bieten sie dynamischen Schutz basierend auf lokalen und globalen Bedrohungsdaten sowie die Möglichkeit, Systeme stets auf den aktuellen Stand zu halten. Hierfür müssen keine Sicherheitsfunktionen deaktiviert werden.

Vereinfachte Verwaltung

Konsistenz durch zentrale Verwaltung

Eine zentrale Konsole ermöglicht in Multi-Cloud-Umgebungen die zentrale Verwaltung sowie die Nutzung konsistenter Sicherheitsrichtlinien für Server, virtuelle Server und Cloud-Workloads.

Automatisierte Bereitstellung

Durch die Unterstützung von Bereitstellungs-automatisierungs-Tools von Anbietern wie Chef, Puppet und Ansible können Sie Sicherheitstechnologien in mehreren Cloud-Umgebungen automatisch bereitstellen.

Verbesserte Sicherheitsabdeckung

McAfee Cloud Workload Security sorgt für höchste Sicherheitsqualität, während Sie die Vorteile der Cloud nutzen. Die Lösung deckt mehrere Schutz-technologien ab, vereinfacht die Sicherheitsverwaltung und verhindert, dass Cyber-Bedrohungen Ihren Geschäftsbetrieb beeinträchtigen – damit Sie sich auf das Wachstum Ihres Unternehmens konzentrieren können. Im Folgenden finden Sie einen Vergleich der Eigenschaften der verfügbaren Paketoptionen.

Funktionen	Cloud Workload Security Basic	Cloud Workload Security Essentials	Cloud Workload Security Advanced
Zentrale Verwaltung (McAfee® ePO™-Plattform)	✓	✓	✓
Unterstützung von Multi-Cloud-Umgebungen (AWS, Azure, VMware)	✓	✓	✓
Verwendung von Mikrosegmentierung zur Isolierung von Workloads und Containern	✓	✓	✓
Bedrohungsschutz für das Server-Betriebssystem (Windows und Linux)	✓	✓	✓
Schutz vor Host-Eindringungen und Exploits	✓	✓	✓
Cloud-Verschlüsselungsverwaltung	✓	✓	✓
Native Firewall-Verwaltung für AWS und Azure (Sicherheitsgruppen)	✓	✓	✓
McAfee® Management for Optimized Virtual Environments (agentenlos und für mehrere Plattformen)	✓	✓	✓
Host-basierte Firewall	✓	✓	✓
Adaptiver Bedrohungsschutz mit Machine Learning		✓	✓
Visualisierung des Netzwerkverkehrs mit Mikrosegmentierung		✓	✓
Cloud-eigene Netzwerkverkehrsanalyse in Verbindung mit Global Threat Intelligence-Reputationsfaktor		✓	✓
Application Control for Servers			✓
File Integrity Monitoring			✓
Change Control for Servers			✓
McAfee® Virtual Network Security Platform-Integration		✓	✓

Weitere Informationen

Weitere Informationen hierzu finden Sie unter **www.mcafee.com/de/products/cloud-workload-security.aspx**.

McAfee
Together is power.

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