# McAfee Cloud Workload Security

## Sichern Sie Ihre Hybrid-Infrastruktur-Workloads: 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 (McAfee® CWS) 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 Schutz sowie die Möglichkeit, Ihre Workloads mit nur einer einzigen automatisierten Richtlinie zu schützen, während sie Ihre virtuellen privaten, öffentlichen und Multi-Cloud-Umgebungen durchlaufen. Dadurch wird die Effektivität Ihres Cyber-Sicherheitsteams erheblich verbessert.

## Moderne Workload-Sicherheit: Anwendungsszenarien

### Automatische Erkennung

Nicht verwaltete Workload-Instanzen und Docker-Container reißen Lücken in die Sicherheitsverwaltung und sind für Angreifer der geeignete Ansatzpunkt zur Infiltrierung Ihres Unternehmens. McAfee CWS erkennt flexible Workload-Instanzen und Docker-Container in Umgebungen von Amazon Web Services (AWS), Microsoft Azure, OpenStack und VMware. Die Lösung sucht zudem permanent 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.

### Einblicke in Netzwerkverkehr

Durch die Auswertung des systemeigenen Netzwerkverkehrs aus den Cloud-Workloads kann McAfee CWS die Bedrohungsdaten ergänzen und Bedrohungsdaten aus Daten-Feeds von McAfee® Global Threat Intelligence (McAfee® GTI) anwenden.

## Hauptvorteile

- Kontinuierlicher Überblick über flexible Workload-Instanzen zur Vermeidung blinder Flecken im Betrieb sowie Automatisierung arbeitsaufwändiger Richtlinienimplementierungen
- Zentrale Verwaltung und automatisierte Workloads verringern Komplexität hybrider und Multi-Cloud-Umgebungen erheblich
- Visualisierung und Erkennung von Netzwerkbedrohungen ohne Installation eines Agenten
- Für virtuelle Maschinen optimierte Bedrohungsabwehr mit mehrstufigen Gegenmaßnahmen
- 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

Die ergänzten Informationen können Eigenschaften wie Risikowert, geografischer Standort und weitere wichtige Netzwerkinformationen enthalten, die für automatische Behebungsaktionen zum Schutz von Workloads verwendet werden können.

### Integration in Bereitstellungs-Frameworks

McAfee CWS erstellt Bereitstellungsskripte, die die automatische Bereitstellung und Verwaltung des McAfee®-Agenten in Cloud-Workloads ermöglichen. Mithilfe dieser Skripte ist die Integration in Tools wie Chef, Puppet und andere DevOps-Frameworks möglich, sodass der McAfee-Agent in Workloads bei Cloud-Anbietern wie AWS und Microsoft Azure bereitgestellt werden kann.

### Konsolidierung von Ereignissen

Dank McAfee CWS können Unternehmen die Verwaltung der zahlreichen Schutztechnologien für ihre lokalen und Cloud-Umgebungen über eine einzige Benutzeroberfläche erledigen. Dazu gehört auch die Integration in weitere Technologien wie AWS GuardDuty, McAfee® Policy Auditor und McAfee® Network Security Platform.

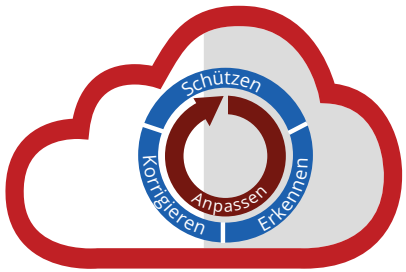
- Administratoren können die von AWS GuardDuty erfassten Daten aus der kontinuierlichen Überwachung sowie zu nicht autorisiertem Verhalten nutzen, um zusätzliche Einblicke in Bedrohungen zu erhalten. Durch diese Integration können McAfee CWS-Kunden GuardDuty-Ereignisse direkt innerhalb der McAfee CWS-Konsole anzeigen, einschließlich Netzwerkverbindungen, Port-Prüfungen sowie DNS-Anfragen zu EC2-Instanzen.
- McAfee Policy Auditor führt agentenbasierte Überprüfungen auf bekannte oder benutzerdefinierte Konfigurations-Audits durch. Damit wird die Einhaltung von Vorschriften wie HIPAA (Health Insurance Portability and Accountability Act), PCI-DSS (Payment Card Industry Data Security Standard), CIS Benchmark (Center for Internet Security Benchmark) oder weiteren Branchenstandards sichergestellt. McAfee CWS meldet alle nicht bestandenen Audits und ermöglicht dadurch eine sofortige Übersicht über Fehlkonfigurationen von Workloads in der Cloud.
- McAfee Network Security Platform ist eine weitere Cloud-Sicherheitsplattform, die den Netzwerkverkehr in Hybrid-Umgebungen sowie AWS- und Microsoft Azure-Umgebungen untersucht. Sie führt Deep Packet Inspection des Datenverkehrs durch und meldet alle Unregelmäßigkeiten oder Warnungen an McAfee CWS. Dadurch erhalten Sie eine zentrale Übersicht aller Multi-Cloud-Umgebungen und können Behebungsmaßnahmen starten.

### Durchsetzung von Gruppenrichtlinien für Netzwerksicherheit

Mit McAfee CWS können Benutzer und Administratoren Basislinien für Sicherheitsgruppenrichtlinien erstellen und die bestehenden Workload-Richtlinien auf Einhaltung dieser Basislinien prüfen. Bei allen Abweichungen oder Veränderungen von der Basislinie wird eine entsprechende Warnung in der McAfee CWS-Konsole ausgegeben. Zudem können Administratoren systemeigene Netzwerksicherheitsgruppen manuell in McAfee CWS konfigurieren, um Cloud-eigene Sicherheitsgruppenrichtlinien direkt zu kontrollieren.

## Hauptvorteile (Fortsetzung)

- Unkomplizierter mehrstufiger Schutz vor hochentwickelter Malware und Eindringungsversuchen
- Erkennung und Überwachung von Docker-Containern und deren Absicherung durch Mikrosegmentierung
- Korrekturmaßnahmen zum Schutz Ihrer Umgebung direkt aus der Lösung heraus




Cloud Workload Security

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

## Besondere Eigenschaften von McAfee Cloud Workload Security: Wichtige Funktionen und Technologien

### Unterstützung für Cloud-eigene Versionen

Mit McAfee CWS haben Kunden die Möglichkeit, die Verwaltung mehrerer öffentlicher und privater Clouds – einschließlich AWS EC2, Microsoft Azure (virtuelle Maschinen), OpenStack und VMware Vcenter – in einer einzigen Verwaltungskonsole zusammenzufassen. Mit der in McAfee CWS integrierten neuen Cloud-eigenen Unterstützung für Amazon Elastic Container Service for Kubernetes (Amazon EKS) und Microsoft Azure Kubernetes Service (AKS) können Sie den Import in die Cloud erlauben und Kunden die Möglichkeit geben, Anwendungen in der Cloud auszuführen.

### Einfache, 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. Administratoren können auch mehrere rollenbasierte Berechtigungen in McAfee® ePolicy Orchestrator® (McAfee ePO™) erstellen und Benutzerrollen präziser und passender definieren.

### Netzwerkvirtualisierung mit Mikrosegmentierung

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.

### Hervorragender Virtualisierungsschutz

Die McAfee CWS-Suite schützt die virtuellen Maschinen in Ihrer privaten Cloud mit McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee® MOVE AntiVirus) vor Malware-Angriffen, ohne dabei die zugrunde liegenden Ressourcen zu belasten oder zusätzliche Betriebskosten zu verursachen. Mit McAfee MOVE AntiVirus können Unternehmen ihre Sicherheitsmaßnahmen an spezialisierte virtuelle Maschinen auslagern, die optimierte Scans ihrer virtuellen Umgebung durchführen.

Die Benutzer erhalten Malware-Schutz über McAfee® Endpoint Security for Servers. Diese Lösung kann ressourcenintensive Tasks wie On-Demand-Scans intelligent planen, um eine Beeinträchtigung wichtiger Geschäftsprozesse zu vermeiden.

### Tag-Nutzung und Automatisierung der Workload-Sicherheit

Dank der Funktion zum Importieren von AWS- und Microsoft Azure-Tag-Informationen in McAfee ePO und der Möglichkeit zur Tag-basierten Richtlinienzuweisung wird gewährleistet, dass allen Workloads automatisch die richtigen Richtlinien zugewiesen werden. Vorhandene AWS- und Microsoft Azure-Tags werden mit McAfee ePO-Tags synchronisiert und automatisch verwaltet.

### Automatische Behebung

Der Benutzer definiert McAfee ePO-Richtlinien. Wenn McAfee CWS ein System entdeckt, das nicht von McAfee ePO-Sicherheitsrichtlinien geschützt ist und Malware oder Viren enthält, wird es automatisch isoliert.

### Adaptiver Bedrohungsschutz

McAfee CWS 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. McAfee® Advanced Threat Protection erkennt bislang unbekannte Bedrohungen mittels Machine Learning-Techniken, die böswillige Inhalte aufgrund ihrer Code-Attribute und ihres Verhaltens entlarven.

### Anwendungskontrolle

Whitelists für Anwendungen verhindern sowohl bekannte als auch unbekannte Angriffe, indem sie ausschließlich die Ausführung vertrauenswürdiger Anwendungen zulassen und alle nicht autorisierten Inhalte blockieren. McAfee® Application Control bietet 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.

### Dateiintegritätsüberwachung

Dank der McAfee®-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.

## Optimierte Sicherheitsmaßnahmen für Ihre Multi-Cloud-Umgebung

McAfee CWS sorgt für höchste Sicherheitsqualität, während Sie die Vorteile der Cloud nutzen. Die Lösung deckt mehrere Schutztechnologien 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 | McAfee Cloud Workload Security Basic | McAfee® Cloud Workload Security Essentials | McAfee® Cloud Workload Security Advanced |
|---|---|---|---|
| Zentrale Verwaltung (McAfee ePO-Plattform) | ✓ | ✓ | ✓ |
| Unterstützung von Multi-Cloud-Umgebungen (AWS, Microsoft Azure, VMware) | ✓ | ✓ | ✓ |
| Verwendung von Mikrosegmentierung zur Isolierung von Workloads und Containern | ✓ | ✓ | ✓ |
| McAfee MOVE (agentenlos und für mehrere Plattformen) | ✓ | ✓ | ✓ |
| McAfee Endpoint-Bedrohungsschutzmodul für Server-Betriebssysteme (Windows und Linux) | ✓ | ✓ | ✓ |
| Host-basierte Firewall | ✓ | ✓ | ✓ |
| Native Firewall-Verwaltung für AWS und Microsoft Azure (Sicherheitsgruppen) | ✓ | ✓ | ✓ |
| Schutz vor Host-Eindringungen und Exploits | ✓ | ✓ | ✓ |
| Import von AWS- und Microsoft Azure-Tag-Informationen in McAfee ePO | ✓ | ✓ | ✓ |
| Automatische Korrektur nicht konformer Workloads | ✓ | ✓ | ✓ |
| Adaptiver Bedrohungsschutz mit Machine Learning | | ✓ | ✓ |
| Visualisierung des Netzwerkverkehrs mit Mikrosegmentierung | | ✓ | ✓ |
| Cloud-eigene Netzwerkverkehr-Analyse kombiniert mit McAfee GTI-Reputationsfaktor | | ✓ | ✓ |
| McAfee® Virtual Network Security Platform (McAfee® vNSP)-Integration | | ✓ | ✓ |
| Dynamische Whitelist für Server mit McAfee Application Control | | | ✓ |
| Kontinuierliche Audit-Protokollierung mit McAfee-Dateiintegritätsüberwachung | | | ✓ |
| Datei- und Ordnerschutz mit McAfee® Change Control for Servers | | | ✓ |

## Weitere Informationen

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

Für die Nutzung der Funktionen und Vorteile der McAfee-Technologien muss das System entsprechend konfiguriert werden, und möglicherweise müssen Hard- bzw. Software oder Services aktiviert werden. Weitere Informationen finden Sie unter www.mcafee.com/de. Kein Computersystem kann absolut sicher sein.



McAfee Together is power.

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