CROWDSTRIKE

CrowdStrike Falcon Cloud Security on AWS

aws PARTNER

- Öffentlicher Sektor
- Amazon Linux-fähig
- Marketplace-Verkäufer
- Kompetenter Sicherheitssoftware-Anbieter

CrowdStrike E-Book

Inhaltsverzeichnis

Einführung

Überall auf der Welt nutzen Unternehmen aller Größen die Cloud-Technologie – und immer mehr von ihnen arbeiten mit Amazon Web Services (AWS) oder migrieren zu diesem Cloud-Service. Durch Geschäftsanforderungen wie Flexibilität, Innovation und Gesamtbetriebskosten sehen sich CTOs und CIOs gezwungen, AWS-Technologien einzuführen. Sie vertrauen darauf, dass AWS ihnen dabei hilft, schnell und zuverlässig auf Veränderungen zu reagieren, effektiv zu skalieren und das Unternehmenswachstum voranzutreiben.

Wenn sich Unternehmen weiterentwickeln, müssen sich auch ihre Sicherheitsstrategien verändern, damit sie Bedrohungen immer einen Schritt voraus bleiben. Um angesichts der immer komplexer werdenden Technologien und Cyberangriffe auf alles vorbereitet zu sein, ist es wichtig, rechtzeitig eine Cloud-Sicherheitsstrategie zu entwickeln.

Ganz gleich, ob Ihr Unternehmen auf der Cloud aufbaut oder gerade zur Cloud wechselt, ist es wichtig, Ihre Cloud-Sicherheitsstrategie sorgfältig zu planen. Außerdem sollte der Schutz Ihrer Computing-Umgebung in jeder Phase an erster Stelle stehen.

In einer sich ständig weiterentwickelnden Cloud-Technologielandschaft mit steter Veränderung ist nur Eines gewiss: Die Angreifer wissen, welche Sicherheitsrisiken die Cloud birgt. Kennen Sie die Risiken auch?

52 %

Der Anteil der nordamerikanischen Unternehmen, die davon ausgehen, dass in den nächsten 24 Monaten mindestens 41 % ihrer Workloads in der Cloud ausgeführt werden

Mehr Sicherheit bei der Cloud-Migration

Cloud-Technologie hat neuen Unternehmen zu einem schnellen Start verholfen und laufenden Unternehmen eine Innovationsgrundlage verschafft, aber auch zu neuen Sicherheitskriterien und Bedrohungen geführt. Zu den neuen Sicherheitsrisiken gehören die dezentrale Entwicklung und Richtlinienimplementierung, Transparenzlücken zwischen verschiedenen Technologien und Endgeräten sowie der immer präsente Faktor Mensch, der durch Schatten-IT, undurchdachte Architekturen sowie unzureichende Kompetenzen und Kenntnisse zusätzliche Risiken birgt.

Unternehmen, die Cloud-Technologien zum Aufbau von Infrastruktur und für flexible Skalierung nutzen, müssen den Schutz einer dynamische Umgebung gewährleisten können. Ausgelagerte Anwendungen und Drittanbieter-Lösungen mit unterschiedlichen Sicherheitsstandards und Architekturen können zu Sicherheitslücken führen. Daher ist die frühzeitige Implementierung einer Sicherheitsstrategie der beste Weg, um sich einen zentralen Überblick über verschiedene Cloud-Komponenten und -Services zu verschaffen.

Unternehmen, die von ihrer alten Technologie zur Cloud migrieren, müssen mit Sicherheitsrisiken sowohl im alten als auch im neuen System rechnen. Hybridlösungen sind bei einer Migration besonders anfällig, ebenso wie verbleibende ältere Systeme und Datenbanken, die nicht ordnungsgemäß entfernt werden. Zudem sind in den meisten Fällen Umschulungen oder die Einstellung neuer Mitarbeiter sowie ein Wandel der Unternehmenskultur erforderlich. Dies schafft zwar eine gute Grundlage für die Bewältigung künftiger technologischer Veränderungen, kann aber auch für Unruhe sorgen. Daher ist es während einer großen technischen Umstellung entscheidend, das Thema Sicherheit stets von oben nach unten anzugehen.

Der strategische Sicherheitsansatz von CrowdStrike

Für den Schutz Ihrer Cloud-Systeme können Sie beispielsweise mit einem Sicherheitspartner wie CrowdStrike zusammenarbeiten. Mit CrowdStrike Falcon Cloud Security und der Unterstützung von Cybersicherheitsexperten erhalten Sie umfassenden Schutz vom Host bis zur Cloud für Workloads und Container auf AWS.

Der CrowdStrike-Ansatz:

- Fokus auf die Angreifer
- Reduzierung des Risikos
- Überwachung der Angriffsfläche
- Schutz während der Laufzeit
- Integration in CI/CD-Pipeline

Die Bedrohungsakteure haben die üblichen IT-basierten Angriffe (z. B. die Erweiterung von Zugriffsrechten, Ransomware sowie das Ausspähen von Daten und Paketen) an die Cloud angepasst und werden darüber hinaus wahrscheinlich auch neue cloudbasierte Angriffstechniken entwickeln. Die CrowdStrike-Lösungen für Cloud-Sicherheit verfügen über integrierte Echtzeitwarnungen und Berichte über mehr als 200 Angreifer, sodass Sie sofort auf neue Bedrohungen reagieren können.

Um im Bereich der Cloud-Sicherheit Risiken zu minimieren und die Angriffsfläche zu reduzieren, müssen Workloads segmentiert, lose Enden verbunden (besonders bei Unternehmen, die alte Systeme aufgeben) und die Sicherheit in der Cloud in den Vordergrund gerückt werden. Dies wird auch als „Shift Left“ bezeichnet. Wenn die Angriffsfläche definiert wurde, sind Überwachungsmaßnahmen mit höchstmöglicher Transparenz die beste Möglichkeit, sich gegen potenzielle Angreifer zu verteidigen. Falcon Cloud Security bietet automatisierte Analysen, Schutz zur Laufzeit und am Speicherort, cloudnative Angriffsindikatoren (IOAs) und Machine Learning (ML), um Untersuchungen zu beschleunigen.

Falcon Cloud Security für DevSecOps und Überwachung

Für Unternehmen, die mit mehreren Umgebungen arbeiten, vereinfacht Falcon Cloud Security die Sicherheitsverwaltung durch die Schaffung einer zentralen Informationsquelle für alle Cloud-Assets und Sicherheitskonfigurationen. Mit IOA-Schutz und ML-basierten geführten Behebungsmaßnahmen, die direkt in die Kontrollebene integriert sind, unterstützt Falcon Cloud Security das Sicherheitsteam bei der Verwaltung der Compliance sowie beim sicheren und effizienten Rollout von AWS-Integrationen.

Falcon Cloud Security für umfassenden Angriffsschutz

Während Sie mit der Cloud-Technologie Systeme neu aufbauen oder ersetzen, bietet Falcon Cloud Security umfassenden Angriffsschutz für Private-, Public-, Hybrid- und Multi-Cloud-Umgebungen, sodass unsere Kunden Technologien für Workloads aller Art schnell und sicher einsetzen können. Mit Falcon Cloud Security können Sie Anwendungen schnell und zuverlässig entwickeln, ausführen und absichern.

Absicherung von Containern auf AWS

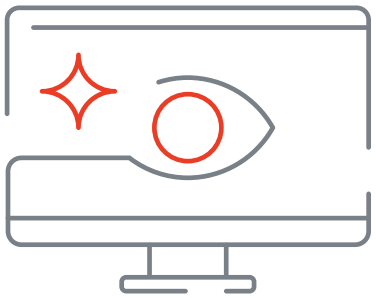
Ein weiteres wichtiges Element einer effektiven Cloud-Sicherheitsstrategie ist der zuverlässige Schutz von Containern. Da Container grundsätzlich isoliert und unabhängig sind, ist es schwierig, einen vollständigen Überblick zu erhalten. Häufig werden sie einmal eingerichtet und dann vergessen – und die langfristige Einhaltung von Sicherheitsvorschriften spielt erst im Nachhinein eine Rolle. Doch selbst mit den besten Überwachungspraktiken können Container aufgrund der schieren Datenmenge, die sie bei Schwachstellenscans erzeugen, Probleme bei der Sicherheitsanalyse verursachen.

Falcon Cloud Security löst diese Probleme. Der schlanke CrowdStrike-Agent bietet einen vollständigen Überblick über Container – unabhängig davon, ob es sich um lokale oder Cloud-Bereitstellungen handelt. Kontinuierliche Überwachung und die Integration der CI/CD-Pipeline erleichtern die Überprüfung und Zurücksetzung von Containern. Darüber hinaus bietet Falcon Cloud Security Überwachung und automatisierte kontinuierliche Bedrohungserkennung, wodurch flexible KI- und ML-gestützte Analysen von Schwachstellendaten in großem Maßstab sowie Laufzeitschutz mit Echtzeitwarnungen ermöglicht werden.

Einfacher und unkomplizierter Schutz Ihrer Computing-Umgebung mit Falcon

Unternehmen, die mit AWS arbeiten, kennen die Vorteile von Cloud-Technologie bei der Migration veralteter Systeme und Entwicklung moderner Anwendungen. Zudem wissen sie, wie wichtig die Zusammenarbeit mit Spitzentechnologie-Unternehmen für den Betrieb von Systemen und das Unternehmenswachstum ist.

CrowdStrike Falcon Cloud Security lässt sich nahtlos mit AWS Security Hub integrieren, wurde mit Blick auf AWS-Services wie Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS) und Amazon Linux 2 entwickelt und wird über AWS Systems Manager bereitgestellt. AWS-Kunden, die mit CrowdStrike zusammenarbeiten, sind in Minutenschnelle einsatzbereit und haben über eine zentrale Konsole sofort Zugriff auf Einblicke und Analysen zu allen ihren Services. Außerdem benötigt CrowdStrike Falcon Cloud Security nur wenig Speicherplatz und wirkt sich auch bei Analysen, Suchen und Untersuchungen nicht negativ auf die Laufzeitleistung aus.



Wo AWS und CrowdStrike zusammenarbeiten

CrowdStrike- und AWS-Computing-Services

- Container-Workloads
- Amazon EC2-Instanzen (z. B. Graviton)
- Amazon WorkSpaces
- Amazon Elastic Kubernetes Service
- Amazon Elastic Container Service
- AWS Fargate
- AWS Outposts

Integrationen von CrowdStrike- und AWS-Cloud-Services

- AWS Verified Access
- AWS Account Factory Customization
- AWS Control Tower
- AWS Security Hub
- AWS Systems Manager
- AWS PrivateLink
- Amazon GuardDuty
- AWS Network Firewall
- AWS CloudEndure Disaster Recovery

Jetzt ist der richtige Zeitpunkt für die Entwicklung einer Cloud-Sicherheitsstrategie

Beim Thema Cloud-Sicherheit sollten Sie mit Experten zusammenarbeiten, die Ihre Angreifer, deren Ziele und deren Vorgehensweise kennen. Als Branchenführer im Bereich der Cybersicherheit hat CrowdStrike nachweislich bereits zahlreiche Kompromittierungen verhindert.

Weitere Informationen zu CrowdStrike- und AWS-Lösungen erhalten Sie auf diesen Seiten:

- **CrowdStrike Falcon for AWS ›**
- **Anstehende Veranstaltungen mit CrowdStrike und AWS ›**
- **CrowdStrike- und AWS-Partnerseite ›**
- **CrowdStrike im AWS Marketplace ›**