CROWDSTRIKE

Blueprints für sichere AWS-Workloads

Vollständige Transparenz und Sicherheit für Ihre Workloads und Container durch CrowdStrike Falcon Cloud Security sowie ein umfassender Überblick über Warnungen durch AWS Security Hub sind die besten Voraussetzungen für den Aufbau sicherer Cloud-Architekturen.

aws PARTNER

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

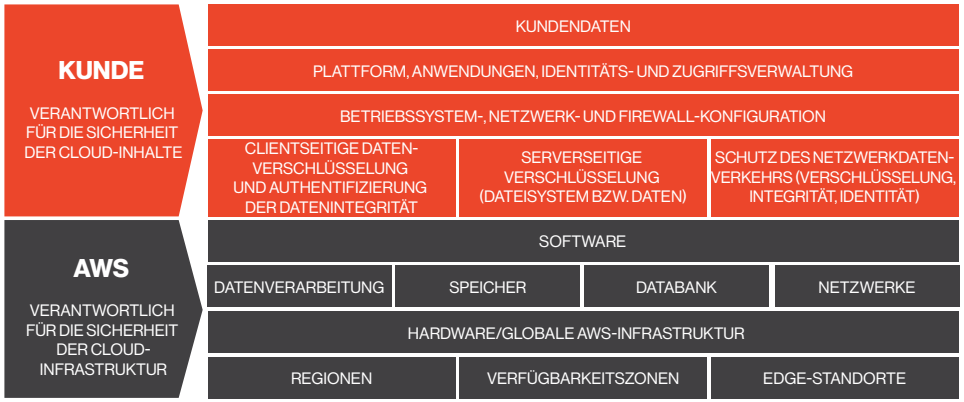
CrowdStrike E-Book

Inhaltsverzeichnis

Aktuelle Cloud-Architekturen durch veraltete Blueprints für Angriffe anfällig

Während immer mehr Unternehmen auf die Nutzung der Cloud umschwenken, entsprechen ihre Sicherheitsmaßnahmen vielfach immer noch den Anforderungen von gestern. Die Nutzung der veralteten lokalen Sicherheitstools in der Cloud führt zu unzureichender Sicherheit und dazu, dass Cloud-Architekten und DevOps-Teams keinen klaren Blueprint für die Absicherung von Anwendungen, Workloads und die Infrastruktur haben.

Bauen Sie mit Amazon Web Services (AWS) und CrowdStrike – einem führenden Unternehmen für cloudbasierten Endgeräte- und Workload-Schutz – ein solides Fundament für Ihre Sicherheit. Die Kombination aus CrowdStrike Falcon und AWS Security Hub ermöglicht die zentrale und automatisierte Verwaltung von AWS-Services-Bedrohungswarnungen, einschließlich Amazon GuardDuty. Und mit CrowdStrike Falcon Cloud Security können Sie die Sicherheit Ihrer AWS-Workloads verbessern und das Modell der geteilten Verantwortung implementieren.



CrowdStrike Falcon Cloud Security schützt Ihre AWS-basierten Workloads

AWS schützt Ihre Cloud-Infrastruktur

AWS Security Hub bietet einen umfassenden Überblick über Sicherheitswarnungen und die Compliance

- Aggregierte Daten aus Falcon und nativen AWS-Services wie Amazon GuardDuty
- Überwachung des AWS-Infrastrukturstatus über grafische Anzeigen
- Durchführung von Compliance-Prüfungen

CrowdStrike Falcon Cloud Security schützt Ihre AWS-Workloads über einen einzigen, schlanken Agenten

- Erweiterte cloudnative Anwendungssicherheit mit Angriffsprävention, Workload-Schutz und Sicherheitsverwaltung für Cloud-Umgebungen
- Vereinfachung des Sicherheitstechnologiebestands durch einen einzigen Agenten, der dank geringem Platzbedarf auf AWS-Ressourcen bessere Leistung ermöglicht
- Reduzierung des Architekturbedarfs für vollständige Sicherheitstransparenz und Verringerung der Komplexität – und dadurch mehr Vorteile durch Ihre AWS-Investitionen

Falcon und AWS ermöglichen nahtlose Sicherheit für Ihre Workflows

Durch die Integration von CrowdStrike mit AWS Security Hub erhalten Sie einen umfassenden Echtzeit-Überblick über Sicherheitswarnungen mit hoher Priorität. Der API-zentrierte Ansatz von CrowdStrike führt dabei Falcon Cloud Security und AWS Security Hub zusammen, damit Ihr gesamtes Team (einschließlich DevOps, CISO, Cloud-Architekten und Operations) Sicherheitsaufgaben automatisch durchführen und den Schutz insgesamt verbessern kann.

TRANSPARENZ – MIT EINEM VOLLSTÄNDIGEN ÜBERBLICK

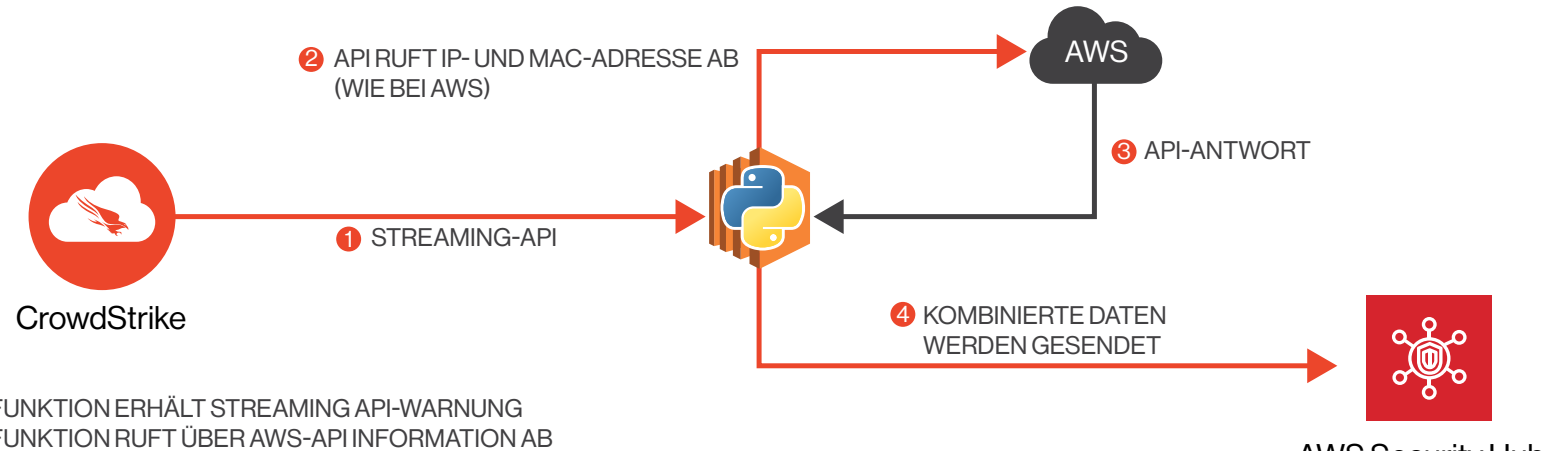
Falcon Cloud Security schützt Ihre AWS-Workloads während des gesamten Bedrohungslebenszyklus, indem Machine Learning, künstliche Intelligenz, Verhaltensanalysen und proaktive Bedrohungssuche in einer einzigen Lösung kombiniert werden.

SCHUTZ – MIT BESSERER LEISTUNG

Falcon Cloud Security funktioniert überall – für Amazon EC2-Instanzen (Amazon Elastic Cloud Compute), für Amazon ECS (Amazon Elastic Container Service) auf Amazon EC2 und für Amazon EKS (Amazon Elastic Kubernetes Service) auf Amazon EC2 – und bietet Endgeräte- und Workload-Schutz, selbst wenn diese offline sind.

ABWEHR – MIT EINER VEREINFACHTEN ARCHITEKTUR

Falcon Cloud Security vereinfacht komplexe DevSecOps-Pipelines und verbessert die operative Zuverlässigkeit, da Cloud-Architekturen vereinfacht werden. Falcon konsolidiert Ihre Endgeräte- und Workload-Agenten mit einer umfassenden Plattform, die mit Ihrem Bestand wächst und sich ohne zusätzliche Komplexität an Ihre Anforderungen anpasst.



1. LAMBDA-FUNKTION ERHÄLT STREAMING API-WARNUNG
2. LAMBDA-FUNKTION RUFT ÜBER AWS-API INFORMATION AB
3. BEI ÜBEREINSTIMMUNG MIT EINER EC2-INSTANZ WERDEN DATEN ZURÜCKGEGEBEN
4. EC2- UND CROWDSTRIKE-DATEN WERDEN KOMBINIERT, FORMATIERT UND AN AWS SECURITY HUB GESENDET

Transparenz – mit einem vollständigen Überblick

Durch die Warnungen aus Amazon GuardDuty und Falcon Cloud Security, die über AWS Security Hub aggregiert werden, erhält Ihr Team eine zentrale Ansicht und damit den Sicherheitsüberblick, den es für strategische Sicherheits- und Ressourcenentscheidungen benötigt. Und dank der Automatisierung routinemäßiger Sicherheitsanalysen können Sie besonders kritische Zwischenfälle trotz der enormen Datenmengen schneller finden und beheben.

Nutzung von Threat Graph-Daten

Mit den KI-gestützten Threat Graph-Analysedaten erkennen Sie potenzielle Bedrohungen schnell und zuverlässig und erreichen ein Schutzniveau für Ihre AWS-Workloads, das vorher nicht möglich war.

Automatisierung von Sicherheitsaufgaben

Ohne Threat Graph müssen Analysten Telemetriedaten von Endgeräten und Workloads manuell zusammentragen, Bedrohungsdaten-Feeds hinzufügen, Korrelationsregeln definieren und anschließend die Daten hin und her verschieben, um festzustellen, ob Sicherheitsereignisse miteinander verknüpft sind. Bei Falcon Cloud Security werden alle diese Analyseergebnisse, Ereignisse und deren Beziehungen zentral erfasst, sodass Sicherheitsadministratoren die Analysen automatisieren können und bei der Untersuchung potenzieller Kompromittierungen einen zuverlässigeren und detaillierteren Überblick erhalten.

Integration von Sicherheit in CI/CD-Pipelines

Mit Falcon Cloud Security können Cloud-Sicherheitsteams mit der Dynamik und Flexibilität von AWS-Workloads Schritt halten. Die nahtlose Unterstützung für CI/CD-Bereitstellungs-Workflows wird durch leistungsstarke APIs und die optimierte Integration mit AWS Security Hub ermöglicht.

DevOps-Teams erweitern die Automatisierung

- Automatisierte Bereitstellung von Entwicklungspipelines
- Reduzierung der Komplexität von Bereitstellungs- und Verwaltungsaufgaben
- Bereitstellung von Sicherheit parallel zu bereitgestellten Anwendungen

Sicherheitsteams gewinnen tiefere Einblicke

- Mehr Kontext zu Ihren AWS-Sicherheitswarnungen
- Verständnis der Auswirkungen von Sicherheitsereignissen
- Vereinfachte Reaktion auf Zwischenfälle
- Identifizierung der Absicht basierend auf Angriffsindikatoren
- Reduzierung von False Positives und Steigerung der Sicherheitseffizienz

>7 Billionen
Ereignisse pro Woche

200.000
neue IOCs täglich veröffentlicht

>200
Bedrohungsakteure überwacht

>1,2 Mio.
Malware-Varianten täglich verarbeitet

Schutz – mit besserer Leistung

Mit CrowdStrike benötigen Sie nur einen Sensor, um alle Ihre Endgeräte und Workloads zu schützen – von IoT-Geräten über Laptops bis zu Cloud-Computing-Instanzen. Mit AWS Security Hub als Dashboard können Sie Sicherheitswarnungen von Falcon Cloud Security und Amazon GuardDuty aggregieren und priorisieren, um Amazon EC2-Instanzen oder -Container zu schützen, die auf Amazon ECS und Amazon EKS ausgeführt werden.

Gewährleistung der Sicherheit und Leistung von Amazon EC2-Instanzen

Falcon Cloud Security verwendet cloudnative Skalierung, um Amazon EC2-Instanzen mit minimalen Auswirkungen auf die Laufzeit-Leistung zu schützen – ganz ohne rechenintensive Scans oder invasive Signatur-Updates. Auf diese Weise erhalten Sie Schutz vor allen erweiterten Angriffen, die den klassischen Perimeter und signaturbasierte Ansätze umgehen.

1
schlanker Agent

Schutz von Containern, die auf Amazon ECS und Amazon EKS ausgeführt werden

Falcon Cloud Security wird auf dem Amazon EC2-Instanzknoten ausgeführt und schützt alle darauf ausgeführten Container, einschließlich der von Amazon ECS und Amazon EKS verwalteten. Durch Workload-Überwachung und -Erkennung schützt Falcon Ihre Container vor bekannter Malware sowie vor äußerst raffinierten Angriffen. Dazu untersucht die Lösung Parameter wie die eindeutige Kennung und den Konfigurationstyp des Containers und leitet dann Warnungen an AWS Security Hub weiter.

0
Neustarts erforderlich

Shift-Left-Ansatz für Container-Sicherheit in CI/CD-Pipelines

Durch die Verlagerung der Sicherheitsaufgaben in eine frühere Phase des Software-Entwicklungszyklus können Teams Fehler erkennen, bevor erheblicher Schaden entsteht. Durch das Hinzufügen von Falcon Cloud Security zu Ihren CI/CD-Bereitstellungs-Workflows erhalten Sie Laufzeit-Schutz für Ihre Amazon ECS- und Amazon EKS-Workloads sowie Transparenz zu Ihren containerisierten Anwendungen. Die Anzeige und Verwaltung von Ereignissen wie riskanten Container-Images erfolgt über das AWS Security Hub-Dashboard.

DevOps-Teams können einfacher programmieren

- Malware-Schutz ohne Integration einer Legacy-Appliance
- Vereinfachte Code-Entwicklung und Skript-Erstellung, da nur ein Agent benötigt wird, der sich nahtlos einbindet

Mehr Informationen für Sicherheitsteams

- Korrelation von AWS-Warnungen mit der Falcon Cloud Security-Erkennung, um die Triage und Behebung zu beschleunigen
- Bereitstellung einer Threat-Hunting-Plattform für das Operations-Team

Abwehr – mit einer vereinfachten Architektur

Durch die Effizienzsteigerung bei der parallelen Verwendung von Falcon Cloud Security und AWS Security Hub können Sie die Zeit zur Erkennung, Untersuchung und Behebung verkürzen und so mehr Angriffe stoppen. Dank des integrierten Services für vollständige Sicherheit arbeitet Ihr Team effizienter und verbringt weniger Zeit mit der Verwaltung separater Workstreams. Nutzen Sie die Bedrohungsanalyse und vereinfachte Architektur von CrowdStrike, um die Möglichkeiten von AWS Security Hub zur Aggregation von Ereignissen maximal auszuschöpfen.

Vereinfachte AWS-Architekturen

Andere Sicherheitsanbieter benötigen häufig komplexes Routing für Legacy-Anwendungen, das in den Paketfluss eingefügt werden muss, sowie zahlreiche Workload-Agenten für Virenschutz, EDR und Container-Schutz, die zudem separat installiert und verwaltet werden müssen. Dies kann Ihre AWS-Umgebungen komplexer machen und Ausfallzeiten verlängern. Falcon bietet mit einem einzigen Agenten das gleiche Sicherheitsniveau bei weniger Aufwand.

Kürzere Reaktionszeiten

Die Priorisierung von Zwischenfällen innerhalb von AWS Security Hub vereinfacht die Triage, sodass Ihr Team die schwerwiegendsten Bedrohungen zuerst angehen kann.

Steigerung der Effizienz für größere Kosteneinsparungen

Durch die Möglichkeit, Falcon Cloud Security im AWS Marketplace zu erwerben, können Sie die Vorteile der integrierten Messung und Abrechnung nutzen und gleichzeitig die Ausgaben für elastische Workloads optimieren.

DevOps-Teams können schneller starten

- Integration von Sicherheit und Behebung im Endgerätesensor
- Keine Installation erforderlich – CrowdStrike stellt die Verbindung von einer SaaS-basierten Konsole her
- Einbindung eines einzigen Sicherheitsservices für vollständigen Schutz

Cloud-Architekten profitieren von vereinfachten Designs

- Konsolidierung der Architektur für vereinfachte Builds
- Skaliert mit der wachsenden Cloud-Workload-Umgebung, ohne dass zusätzliche Infrastruktur benötigt wird
- Leistungsstarke APIs zur Automatisierung aller Funktionsbereiche für mehrschichtigen Schutz

100.000 Knoten
pro Tag zur sofortigen Bereitstellung

75 %
höhere Effizienz

Hervorragende Abläufe

Cybersicherheit ist nicht nur ein Technologieproblem – für den Schutz Ihrer AWS-Workloads benötigen Sie auch effektive Mitarbeiter und Prozesse. Die Nichtbeachtung von Sicherheitsabläufen kann zu Schäden führen und Behebungsmaßnahmen erzwingen, die DevOps verlangsamen und die Betriebszeit Ihrer kritischen Anwendungen verkürzen. Diese Folgen können verhindert werden, wenn die Sicherheitstechnologien ordnungsgemäß konfiguriert und auf dem neuesten Stand gehalten werden und die Sicherheitswarnungen, die einem Zwischenfall vorausgehen, zeitnah triagiert, untersucht und behoben werden.

Vielen Unternehmen fällt es schwer, diese operativen Sicherheitsaspekte zu berücksichtigen, da es schwierig und teuer sein kann, qualifiziertes Personal einzustellen, das täglich rund um die Uhr für die Cybersicherheit erforderlich ist.

Erweiterung Ihres Teams mit einem Service für Managed Detection and Response

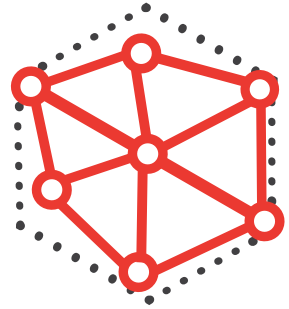
CrowdStrike Falcon Complete umfasst einen Service für verwaltete Erkennung und Reaktion (Managed Detection and Response, MDR), der von einem dedizierten Sicherheitsexpertenteam bereitgestellt wird und die Effektivität der Falcon-Plattform weiter steigert. Falcon Complete konzentriert sich unermüdlich auf die Verwaltung und Überwachung Ihrer Endgeräte- und Workload-Sicherheit und reagiert schnell und präzise auf Bedrohungen – damit Sie das nicht tun müssen.

DevOps-Teams stellen weniger Unterbrechungen fest

- Überwachung rund um die Uhr mit präziser Behebung reduziert Bedrohungen schnell, ohne den betroffenen Workload zu beeinträchtigen

Sicherheitsteams profitieren sofort von Fachwissen und Effektivität

- Kontinuierlich optimierte Sicherheitsrichtlinien für maximale Effektivität
- Erkennung und Beseitigung von Bedrohungen innerhalb von Minuten
- Zuverlässige Sicherheit mit Garantie für die Verhinderung von Kompromittierungen



Das 1-10-60-Framework ist unsere Empfehlung für Unternehmen, die schneller sein möchten als die Angreifer:

<1 Minute
zum Erkennen der Bedrohung

<10 Minuten
zum Verständnis der Bedrohung

60 Minuten
zum Beheben der Bedrohung

Erste Schritte mit CrowdStrike on AWS

Weitere Informationen zu CrowdStrike- und AWS-Lösungen erhalten Sie hier:

- **CrowdStrike Falcon Cloud Security**
- **CrowdStrike-Seite im AWS Marketplace**
- **Vereinbaren Sie eine individuelle Bewertung der Cloud-Sicherheitsrisiken in Ihrem Unternehmen**