Produkte von CrowdStrike

CROWDSTRIKE

aws partner network
Advanced Technology Partner
Security Competency

FALCON FOR AWS

Schutz für AWS-Workloads gegen Datendiebstahl

AWS-WORKLOADS BESSER ANALYSIEREN UND VOR DATENDIEBSTAHL SCHÜTZEN

- **SCHUTZ:** Eine beispiellose Abdeckung schützt vor Datendiebstählen ebenso wie vor Bedrohungen von AWS-Workloads – ob durch Malware oder besonders versierte Angriffe.
- **SICHTBARKEIT:** Die kontinuierliche und umfassende Überwachung der Workloads, einschließlich der Container-Sichtbarkeit, stellt sicher, dass nichts übersehen wird und verdeckte Angriffe gestoppt werden können.
- **EINFACHHEIT:** Die Lösung wurde in der Cloud für die Cloud entwickelt. Das macht den Schutz von AWS-Workloads einfacher, effizienter und sicherer.
- **AUTOMATISIERUNG:** Die Dynamik und Flexibilität der AWS-Workloads bleibt dank der Cloud-Sicherheit uneingeschränkt nutzbar.

DIE CROWDSTRIKE FALCON-PLATTFORM – IN DER CLOUD ZUM SCHUTZ DER CLOUD ENTWICKELT

Die CrowdStrike Falcon-Plattform verhindert dank ihrer einzigartigen Funktionen Datendiebstahl und Sicherheitsverletzungen und trägt zum Schutz der AWS-Workloads bei, ohne Leistungseinbußen hinnehmen zu müssen.

BESSERER SCHUTZ VON AWS-WORKLOADS MIT CROWDSTRIKE

- Unterstützt Instanzen der Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS) & Amazon Elastic Kubernetes Service (Amazon EKS) Container, Windows und Linux, einschließlich Amazon Linux
- Integration in den AWS Security Hub zur zentralen und automatisierten Verwaltung von Bedrohungswarnungen der AWS-Dienste
- AWS Registered Security Competency
- Amazon GuardDuty; Partner für Bedrohungsaufklärung
- Pay-as-you-go-Option

WICHTIGE MERKMALE DER LÖSUNG

SCHUTZ VON EC2 UND CONTAINERN

Falcon for AWS verbindet die besten und neuesten Technologien zum Schutz von Cloud-Workloads vor Datendiebstahl, Malware und versierten Angriffen.

- Maschinelles Lernen und KI schützen vor bekannter und Zero-Day-Malware
- Cloud-Workloads werden vor Bedrohungen geschützt, wie beispielsweise Web-Shells, SQL-Shells und Zugangsdatendiebstahl
- Verhaltensbasierte Angriffsindikatoren (IOAs) verhindern ausgefeilte Angriffe; auch solche ohne Dateien oder Malware
- Schutz und Blockade von Exploits
- Verwaltete Bedrohungssuche rund um die Uhr, damit verdeckte Angriffe nicht unentdeckt bleiben

SICHTBARKEIT

Falcon for AWS übernimmt die volle Endgeräteerkennung und Reaktion (EDR) für Cloud-Workloads und macht Workloads in der gesamten AWS-Umgebung kontinuierlich und umfassend transparent.

- Volle EDR verhindert unbemerkte Ausfälle durch die Erfassung von Rohdaten zur Herstellung vollständiger Transparenz
- Einblick in Vorfälle mit Containern unter Darstellung von Prozessbäumen mit Anzeige der Container-IDs
- Sichtbarkeit auf Kernel-Ebene mit detaillierten und tiefen Einblicken in wichtige Workload-Ereignisse
- Angriffe werden vollständig transparent. Jede Warnung erfolgt unter Angabe von Details, Kontext und Verlauf
- Details zu den Ereignissen sowie damit verknüpfte Daten sind kontinuierlich verfügbar, auch bei kurzlebigen und ruhenden Workloads
- Die Erkennung von verdächtigen Instanzen hilft bei der Identifizierung ungeschützter Instanzen
- Die Kontenüberwachung identifiziert reguläre und privilegierte Konten und bietet eine historische Ansicht der Benutzeranmeldeaktivitäten
- Die Anwendungsnutzung wird überwacht, damit sichtbar wird, was auf Ihren Instanzen ausgeführt wird
- Informationen über die AWS-Umgebung, Konten und Instanzen, wie z. B. Falcon-Abdeckung, Anzahl der AWS-Konten, EC2-Instanzen, Virtual Private Clouds (VPCs), EBS-Speicher. Dies schließt Sicherheitsgruppen (IDs und Namen) und zugehörige ACLs für eingehende und ausgehende Verbindungen ein

EINFACHHEIT

Schützen Sie Ihre Cloud-Workloads ohne Overhead und zusätzliche Komplexität.

- Funktioniert überall; deckt Windows, Linux, einschließlich Amazon Linux und Container ab
- Automatisch auf dem neuesten Stand dank SaaS-Bereitstellung
- Eine zentrale Konsole verleiht Einblick in Cloud-Workloads unabhängig von deren Standort
- Schutzrichtlinien – vollständige Flexibilität bei der Anwendung von Richtlinien auf individuellen Server-, Gruppen- oder Rechenzentren

AUTOMATISIERUNG

Beseitigen Sie manuelle Prozesse in wichtigen und ressourcenintensiven Bereichen und machen Sie so die Cloud-Sicherheit effizienter und besser.

- Automatische Erkennung des Angreiferverhaltens mit priorisierten Warnungen bei Gewichtung der Angriffsschwere; zeitaufwendige manuelle Suchläufe und Bewertungen können entfallen
- Integration in CI/CD-Bereitstellungs-Workflows

CONTAINER-SICHERHEIT

- Ein singulärer Agent auf dem betreffenden Knoten schützt die Instanz selbst sowie alle darauf laufenden Container
- Für Container gefährliche und böswillige Aktivitäten werden erkannt
- Vorfälle mit Containern werden transparent gemacht, wobei entsprechende Prozessbäume die Container-IDs anzeigen

WESENTLICHE VORTEILE

- AWS-Workloads werden vor Datendiebstahl, Malware und versierten Angriffen geschützt
- Eine Konsole verleiht Einblick in die AWS-Umgebung, ohne die Systemleistung zu beeinträchtigen
- Die Komplexität der Sicherheitsmaßnahmen sinkt: Die Plattform ist in die Cloud zum Schutz der Cloud integriert

FALCON FOR AWS

- Leistungsstarke APIs zur Automatisierung aller Funktionsbereiche, einschließlich Erkennung, Verwaltung, Reaktion und Aufklärung
- Automatischer Schutz von virtuellen Workloads, sobald diese hochfahren
- Automatische Skalierung bei wachsenden Cloud-Workloads, ohne dass zusätzliche Infrastruktur erforderlich ist
- Als native Cloud-Lösung stets auf dem neuesten Stand
- Automatisierte Untersuchungen und Bedrohungsanalysen zur Beschleunigung der Reaktion auf Vorfälle

LEISTUNG

Falcon for AWS ist der ultimative Schutz vor Datendiebstählen und Sicherheitsverletzungen, ohne die Leistung der Cloud zu beeinträchtigen.

- Keine Neustarts, daher keine lästigen Workload-Ausfallzeiten
- Schlank – auf dem Endgerät läuft lediglich ein kleiner Agent
- Keine invasiven Updates – neue Funktionen werden der Cloud hinzugefügt, ohne dass Cloud-Workloads belastet oder unterbrochen werden müssen
- Keine Signaturen – keine Unterbrechungen oder Leistungseinbußen wegen täglicher oder stündlicher Signatur-Updates
- Keine leistungshungrigen Scan-Läufe – maschinelles Lernen und Pre-Execution Prevention in Falcon for AWS machen AV-Scans überflüssig, sodass die damit verbundenen Leistungseinbußen auf virtuellen Systemen entfallen
- Keine Beeinträchtigung der Laufzeit-Performance – auch nicht bei Analyse, Suche und Ermittlung

ÜBER CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), ein weltweit führender Spezialist für Cybersecurity, definiert Sicherheit für die Cloud-Ära neu: Mit einer Plattform für den Endgeräteschutz, die konsequent dazu entwickelt wurde, Datendiebstähle zu stoppen. Die Architektur der CrowdStrike Falcon®-Plattform beruht auf einzelnen schlanken Agents. Sie nutzt künstliche Intelligenz (KI) in der Cloud und sorgt auf Anhieb für Transparenz und Schutz im gesamten Unternehmen, um Angriffe auf Endgeräte innerhalb und außerhalb des Netzwerks zu verhindern. Über den proprietären CrowdStrike Threat Graph® korreliert CrowdStrike Falcon über zwei Billionen endgerätebezogene Ereignisse pro Woche in Echtzeit aus aller Welt und überführt sie in eine der weltweit modernsten Datenplattformen für Sicherheitsaufgaben.

Mit CrowdStrike profitieren Kunden von besserem Schutz, besserer Leistung und sofortiger Time-to-Value – und das alles auf der cloud-nativen Falcon-Plattform.

Sie sollten vor allem eines über CrowdStrike wissen: **Wir stoppen Datendiebstahl.**

FALCON FOR AWS BIETET

- Details zu Instanzen für Ihr Operations-Team, insbesondere für diejenigen, die keinen direkten Zugang zu Ihren EC2-Instanzen haben
- Einblick in Ihre AWS-Instanzen mit zusätzlichem Kontext – Falcon for AWS identifiziert und katalogisiert Metadaten zu allen Ihren EC2-Instanzen in allen Regionen, einschließlich der Instanzen ohne installierten Falcon-Sensor, für die von Ihnen bereitgestellten AWS-Konten
- Erweitert den Schutz auf Container, die auf geschützten Host-rechnern laufen
- Sofortansicht der Falcon-Agent-Abdeckung in der AWS-Umgebung
- Gesamtzahl der AWS-Konten und EC2-Instanzen – auch EC2-Instanzen, die Zugang zum Internet haben – sowie gesamter Elastic Block Store
- Auflistung aller Sicherheitsgruppen (IDs und Namen) und zugehörige ACLs für eingehende und ausgehende Verbindungen
- Liste der Virtual Private Clouds (VPCs)

Testen Sie jetzt kostenlos den Virenschutz der nächsten Generation

Erfahren Sie mehr unter **www.crowdstrike.de**