CROWDSTRIKE

CROWDSTRIKE CLOUD SECURITY

Konzipieren... Konfigurieren... Schützen...

Als Cybersecurity-Unternehmen, das selbst eine der weltweit größten Cloud-Architekturen aufgebaut hat, konnte CrowdStrike wertvolle Erkenntnisse gewinnen und weiß, was zum Schutz von Cloud Workloads und Anwendungslebenszyklen erforderlich ist.

Die Cloud kann verschiedene Sicherheitsrisiken mit sich bringen. So ist die Cloud im Unterschied zu Umgebungen vor Ort anfälliger für menschliche Fehler und inoffizielle IT-Strukturen (Schatten-ITs). Wie jede andere IT-Umgebung ist sie auch Laufzeit-Bedrohungen ausgesetzt. Und nicht zuletzt mangelt es manchen Teams, die für die Implementierung von Cloud Workloads zuständig sind, am notwendigen Know-how über aktuelle Sicherheitsmechanismen.

CrowdStrike schützt seine Cloud-Infrastruktur, indem das Unternehmen seinen Angreifern immer einen Schritt voraus ist, die Angriffsfläche konsequent verkleinert und in seiner Umgebung die volle Transparenz über alle Ereignisse wahrt. Wer Datendiebstähle mithilfe von Cloud-Daten und Analysen stoppen will, braucht eine eng integrierte Plattform, die über entsprechende Fähigkeiten zur Erkennung moderner Bedrohungen verfügt und konsequent auf Schnelligkeit, Skalierbarkeit und Zuverlässigkeit ausgelegt und konfiguriert ist.

MODERNE CLOUD-INFRASTRUKTUR VERLANGT MODERNE CLOUD-SICHERHEIT

Mit dem Siegeszug der Cloud hat sich auch die Art und Weise verändert, wie Unternehmen auf den Markt gehen und moderne Anwendungen entwickeln. Für den Anwendungslebenszyklus ist heute Schnelligkeit wichtig. Die für die Cloud zuständigen Teams müssen daher Cloud-native Anwendungen für eine programmierbare Infrastruktur erstellen, die sich ihrerseits schnell verändern und umkonfigurieren lässt. Im Rahmen des CI/CD-Konzepts (Continuous Integration/ Continuous Deployment) erfolgen zudem eine fortlaufende Automatisierung und kontinuierliche Überwachung während des gesamten Anwendungslebenszyklus: Von Integration und Test bis hin zu Bereitstellung und Deployment – was wiederum zu schnellerer Innovation führt.

Diese Verlagerung in Richtung CI/CD hat ihren Preis. Die für Infrastruktur, DevOps und Sicherheit Verantwortlichen suchen daher nach Wegen, wie Cloud-Ressourcen weiterhin geschützt und die Compliance gewährleistet werden können.

Während Unternehmen immer mehr Cloud-native Toolsets einführen, fällt es Sicherheitsverantwortlichen zunehmend schwerer, damit Schritt zu halten. Das Ergebnis: mangelnde Sichtbarkeit und Kontrolle von Cloud-Ressourcen, fragmentierte Konzepte für Erkennung und Vermeidung von Fehlkonfigurationen, ineffektiver Schutz von Cloud Workloads und Containern und schließlich fehlende Compliance. Dies alles bringt erhöhte Risiken für das Unternehmen mit sich.

DIE VORTEILE IM ÜBERBLICK

- Multi-Cloud-Transparenz mit zentraler Datenquelle für die Cloud-Ressourcen
- Senkung von Kosten und Komplexität durch eine einzige, einheitliche Plattform für On-Premises-, Private-, Public-, Hybrid- und Multi-Cloud-Umgebungen
- Beschleunigung einer sicheren Migration in die Cloud
- Vorhersage und Abwehr moderner Bedrohungen in Echtzeit durch die branchenweit umfassendsten Telemetriedaten für Endgeräte und Cloud Workloads, Bedrohungsaufklärung und KI-gestützte Analytik
- Einhaltung und Bewahrung von Compliance
- Frei skalierbar – keine neue Architektur oder zusätzliche Infrastruktur erforderlich
- Entlastet bei der schwierigen Suche nach Mitarbeitern mit gefragten Qualifikationen für den Schutz der Cloud und verbessert die betriebliche Effizienz

CROWDSTRIKE CLOUD SECURITY

Übliche Herausforderungen für die Cloud-Sicherheit sind:

- Mangelnde Sichtbarkeit wegen ausufernder Cloud-Strukturen
- Zunehmende Zahl von Sicherheitsvorfällen in der Cloud aufgrund von Fehlkonfigurationen
- Bedrohungen für Workloads und Container in öffentlichen, privaten und hybriden Umgebungen erkennen, verhindern und abwehren
- Compliance in Multi-Cloud-Umgebungen herstellen und einhalten sowie Sicherheitsrichtlinien durchsetzen
- Exponierte und verwundbare Workloads aufgrund wachsender Angriffsflächen und mangelnder Kenntnisse über Cloud-Sicherheit

Manuelle Prozesse und herkömmliche Lösungen vertragen sich nicht mehr mit dem schnellen Wandel und den besonderen Herausforderungen, denen Organisationen heute gegenüberstehen. Alternativen sind komplexe Cloud-Sicherheitsplattformen oder isolierte Tools, die allerdings die Komplexität der Schutzmaßnahmen einer Organisation insgesamt weiter steigern. Sicherheitsverantwortliche müssen mit der Geschwindigkeit der agilen Softwareentwicklung Schritt halten und Cloud-Risiken kontinuierlich verwalten können. Hierzu ist es notwendig, die Konfiguration von Cloud-Ressourcen, die Durchsetzung von Sicherheitsrichtlinien und die Compliance proaktiv bewerten und überwachen zu können. Gleichzeitig müssen die Verantwortlichen die Workloads und Container in jeder Cloud umfassend vor Datendiebstahl schützen – und das alles, ohne die Unternehmensabläufe zu beeinträchtigen.

CROWDSTRIKE FALCON: EINE CLOUD-NATIVE PLATTFORM FÜR DEN SCHUTZ JEDER CLOUD

Die CrowdStrike Falcon®-Plattform ist so konzipiert, dass sie Workloads unabhängig von deren Standort unterstützt. Falcon schützt Instanzen in allen Arten von Public Clouds, ob Amazon Web Services (AWS), Google Cloud Platform (GCP) oder Microsoft Azure. Dies gilt für physische Server und virtuelle Maschinen gleichermaßen, und zwar sowohl im eigenen Rechenzentrum als auch für Instanzen in der Public Cloud.

Die Plattform baut auf zwei gemeinsamen Komponenten auf: einem einzelnen, schlanken Agent und einer verteilten Cloud. Die Single-Agent-Architektur unterstützt alle Arten von Workloads. Sie sammelt allerdings gezielt Daten für die Cloud-Infrastruktur und für die Workload, die darauf ausgeführt wird. So ist Falcon für AWS beispielsweise darauf ausgelegt, zusätzliche Metadaten von AWS zu sammeln.

Über diesen Mechanismus kann CrowdStrike seinen Kunden mehrere Anwendungen zur Verfügung stellen, ohne dass mehrere Agents, mehrere Konsolen oder weitere Verwaltungskomponenten erforderlich sind. Mit dieser einzigartigen Cloud-nativen Architektur lässt sich der gewünschte Schutz nahtlos bereitstellen – unabhängig von der Anzahl der verwendeten Virtual Private Clouds (VPCs).

Es ist ganz gleich, ob eine Organisation 10 oder 100 VPCs betreibt. CrowdStrike betreibt eine der größten Cloud-Implementierungen weltweit. Das verschafft uns einzigartige Erkenntnisse über Angreifer und ermöglicht uns die Bereitstellung speziell entwickelter Lösungen, die den Arbeitsaufwand für Sicherheitsverantwortliche senken, Datendiebstähle abwehren und das Cloud-Deployment optimieren.

DEVSECOPS-FÄHIGE CLOUD-SICHERHEIT

Die Cloud-Sicherheit von CrowdStrike® geht über Ad-hoc-Konzepte deutlich hinaus. Sie vereint das Cloud Security Posture Management (CSPM) mit dem Schutz vor Datendiebstahl für Cloud Workloads und -Container in einer einzigen Plattform für jede Cloud. Die Cloud-native Lösung gewährleistet einen durchgängigen Schutz vom Host bis zur Cloud.

- Falcon Horizon verleiht Ihnen Einblick in die gesamte Cloud-Infrastruktur mit kontinuierlicher Überwachung auf Fehlkonfigurationen, Durchsetzung von Sicherheitsrichtlinien und Compliance sowie proaktiver Erkennung von Bedrohungen. So können DevSecOps-Teams schneller agieren und Probleme beheben, bevor die Produktion beeinträchtigt wird. Das spart wertvolle Zeit und Geld.
- Falcon Cloud Workload Protection umfasst automatisierte Erkennung, Laufzeitschutz, Endpunktbasierte Detektion und Reaktion (EDR) für Workloads in der Cloud sowie verwaltete Bedrohungssuche in einem einzigen schlanken Agent für Workloads und Container. Damit werden Anwendungen in der Cloud sicher, schnell und effizient bereitgestellt.

CROWDSTRIKE CLOUD SECURITY

CLOUD-SICHERHEIT VON CROWDSTRIKE IM ÜBERBLICK

ERKENNUNG UND SICHTBARKEIT

- **Zentrale Datenquelle:** Die umfassende Sichtbarkeit von Cloud-Assets, Sicherheitskonfigurationen, Workloads und Containern in Multi-Cloud-Umgebungen mindert Risiken und hilft, die Angriffsfläche zu reduzieren.
- **Erkennung von Cloud-Ressourcen:** Cloud-Ressourcen und Details werden automatisch beim Deployment ermittelt. Dies umfasst Fehlkonfigurationen, Metadaten, Netzwerke, Sicherheitskriterien und Änderungsaktivitäten.
- **Tiefgreifender Einblick:** Der Einblick in Workload-Ereignisse und in die Metadaten von Instanzen ermöglicht die Erkennung, Reaktion und proaktive Bedrohungssuche. So ist sichergestellt, dass potenziell bösartige Aktivitäten in Cloud-Umgebungen nicht unbemerkt bleiben.
- **Mehr sehen, mehr wissen, gezielter handeln:** Sie erkennen und untersuchen auch Angriffe, die sich über mehrere Umgebungen und verschiedene Arten von Workloads erstrecken. Dabei ist der Wechsel von Endgeräten zu Instanzen und Containern möglich.
- **Blinde Flecken beseitigen:** Cloud-Ressourcen, die nicht durch Falcon Horizon geschützt sind, werden schnell erkannt.

BEHANDLUNG UND ANGELEITETE BEHEBUNG VON FEHLKONFIGURATIONEN

- **Bewerten und validieren:** Um Verstöße zu identifizieren und in Echtzeit zu beheben, können Sie gängige ebenso wie hochkomplexe Anwendungskonfigurationen in der Cloud mit den geltenden Benchmarks für Branchen und Organisationen vergleichen.
- **Probleme aufgrund exponierter Cloud-Ressourcen beheben:** Sie beheben Probleme, wie beispielsweise fehlerhafte Konfigurationen, offene IP-Ports und nicht autorisierte Änderungen. Dabei werden Sie mit Anleitungen für Abhilfemaßnahmen und entsprechenden „Leitplanken“ unterstützt, damit sich keine kritischen Fehler einschleichen.
- **Überwachung in Echtzeit und angeleitete Abhilfemaßnahmen:** Dank empfohlener schrittweiser Abhilfemaßnahmen können Sie schnell handeln und Probleme beseitigen.
- **Speicher überwachen:** Sie können Ihre Speichersysteme auf sichere und nicht öffentlich zugängliche Berechtigungen überprüfen.
- **Datenbank-Instanzen überwachen:** Sie prüfen, ob Hochverfügbarkeit, Backups sowie Verschlüsselung aktiviert und Sicherheitsgruppen eingerichtet sind.

CONTAINER-SICHERHEIT UND LAUFZEITSCHUTZ

- **Endgeräteerkennung und Reaktion für Container:** Host und Container werden über einen einzigen Falcon-Agent geschützt, der auf dem Host ausgeführt wird. Der Laufzeitschutz wehrt aktive Angriffe gegen Container ab.
- **Schnelle Untersuchung:** Erleichtert die Untersuchung von Container-Vorfällen, wenn Erkennungen mit einem bestimmten Container in Verbindung stehen und nicht mit den Host-Ereignissen gebündelt sind.
- **Lückenlose Überwachung und Fehlerbehebung:** Erfasst Start-, Stopp-, Image- und Laufzeitinformationen des Containers sowie alle Ereignisse, die innerhalb des Containers erzeugt werden, selbst wenn dieser nur wenige Sekunden läuft
- **Proaktive Bedrohungssuche:** Sofort nach dem Deployment von Falcon stehen Informationen über Container-Details und -Aktivitäten bereit. So wissen Sicherheitsverantwortliche, wo sie nach Bedrohungen suchen können, erhalten Abfrageergebnisse in Sekundenschnelle und können zügig von einem Hinweis zum nächsten wechseln.
- **Fortlaufende Verfügbarkeit:** Details zu den Ereignissen für eine forensische Beweisführung sowie damit verknüpfte Daten sind kontinuierlich verfügbar, auch bei kurzlebigen und ruhenden Containern.
- **Verborgene Bedrohungen aufdecken:** Ein leicht verständlicher Prozessbaum informiert umfassend über Angriffsdetails im Kontext und macht die Untersuchungen damit schneller und einfacher.

IN DER CLOUD FÜR DIE CLOUD ENTWICKELT

Durchgängige Cloud-native Sicherheit

Erkennung, Sichtbarkeit und Compliance für jede Cloud

Schutz von Workloads, Hosts und Containern

Reduziert Ermüdungserscheinungen aufgrund von Fehlalarmen und trägt dazu bei, Probleme schneller zu beheben

Auf Anhieb einsatzbereit – Die Bereitstellung und Inbetriebnahme sind eine Sache von wenigen Minuten. Ohne Neustart, Feinabstimmung oder komplexe Konfiguration

CROWDSTRIKE CLOUD SECURITY

THREAT GRAPH ZUR VERMEIDUNG VON DATENDIEBSTAHL

- **Moderne Bedrohungen vorhersehen und verhindern:** CrowdStrike Threat Graph® schützt in Echtzeit mit den branchenweit umfassendsten Telemetriedaten über Endgeräte und Workloads sowie mit Bedrohungsaufklärung und KI-gestützter Analytik.
- **Zugang zu kontextsensitiver Bedrohungsaufklärung:** Die visuelle Darstellung von Beziehungen zwischen Kontenrollen, Workloads und APIs vermittelt einen tieferen Kontext, der eine schnellere und effektivere Reaktion zulässt.
- **Tiefgreifende KI und Verhaltensanalyse:** Neue und ungewöhnliche Bedrohungen lassen sich in Echtzeit erkennen, um zielgerechte Maßnahmen ergreifen zu können, wodurch wertvolle Ressourcen des Sicherheitsteams geschont werden.
- **Beschleunigte Reaktion:** Die Reaktionsfähigkeit der Mitarbeiter wird in Echtzeit erhöht, da sie dank des Threat Graph in der Lage sind, Bedrohungen sofort zu verstehen und entschlossen zu handeln.
- **Gezielte Identifizierung und Verwaltung von Bedrohungen:** Die gezielte Identifizierung von Bedrohungen wirkt einer Ermüdung durch häufige Fehlalarme in Multi-Cloud-Umgebungen entgegen.

ZENTRALE DATENQUELLE MIT LEISTUNGSSTARKEN API

- **Automatisierung:** Leistungsstarke APIs ermöglichen die Automatisierung der Funktionalität von CrowdStrike Falcon, einschließlich Erkennung, Verwaltung, Reaktion und Aufklärung.
- **Vorteile von SOAR nutzen:** Die Vorteile von SOAR (Security Orchestration, Automation and Response) sowie anderer fortschrittlicher Workflows lassen sich zur Optimierung der Unternehmensleistung nutzen.
- **Unterstützung von CI/CD-Pipelines:** Problemlose Integration von Chef, Puppet und AWS Terraform zur Unterstützung von CI/CD-Workflows.
- **Zentrale Datenquelle:** Dank der zentralen Datenquelle haben Sicherheitsverantwortliche schnellen Zugriff auf alles, was sie zur Reaktion und Untersuchung benötigen.

UNKOMPLIZIERT UND LEISTUNGSSTARK

- **Konsequent für die Cloud entwickelt:** Die Falcon-Plattform wurde in der Cloud für die Cloud entwickelt. Das macht den Schutz von Workloads einfacher, effizienter und sicherer und erleichtert die Einhaltung der Compliance.
- **Eine Plattform für alle Workloads:** Falcon schützt überall – in privaten, öffentlichen und hybriden Cloud-Umgebungen.
- **Einheitliche Sichtbarkeit und Steuerung:** Eine zentrale Konsole verleiht Einblick in die Sicherheitsaufstellung der Cloud Workloads unabhängig von deren Standort.
- **Umfassende Richtlinienflexibilität:** Richtlinien lassen sich auf der Ebene individueller Workloads, Gruppen oder auf höherer Ebene anwenden. Zudem können Richtlinien sowohl in On-Premises- als auch in Multi-Cloud-Implementierungen vereinheitlicht werden.
- **Beliebig skalierbar:** Die Falcon-Plattform lässt sich nahtlos skalieren – ohne Umstrukturierung oder zusätzliche Infrastruktur.
- **Umfassende Unterstützung:** Die Falcon-Plattform unterstützt OCI-konforme Container (Open Container Initiative), wie Docker und Kubernetes, und selbstverwaltete sowie gehostete Orchestrierungsplattformen, wie GKE (Google Kubernetes Engine), EKS (Amazon Elastic Kubernetes Service), ECS (Amazon Elastic Container Service), AKS (Azure Kubernetes Service) und OpenShift.

ÜBER CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit seiner von Grund auf neu konzipierten Endgeräteschutzplattform die Sicherheit im Cloud-Zeitalter neu. Die schlanke Single- Agent-Architektur der CrowdStrike Falcon®-Plattform nutzt Cloud-skalierte Künstliche Intelligenz und sorgt unternehmensweit für Schutz und Transparenz. So werden Angriffe auf Endgeräte sowohl innerhalb als auch außerhalb des Netzwerks verhindert. Mit Hilfe des firmeneigenen CrowdStrike Threat Graph® korreliert CrowdStrike Falcon weltweit und in Echtzeit über 5 Billionen endpunktbezogene Ereignisse pro Woche. Damit ist die CrowdStrike Falcon Plattform eine der weltweit fortschrittlichsten Datenplattformen für Cybersicherheit.

Testen Sie jetzt kostenlos den Virenschutz der neuesten Generation

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

© 2021 CrowdStrike, Inc. Alle Rechte vorbehalten.