CROWDSTRIKE

# FALCON CLOUD WORKLOAD PROTECTION

## Schutz gegen Datendiebstahl für Cloud-Workloads und Container

## CLOUD-WORKLOADS IN ALLEN UMGEBUNGEN SCHÜTZEN

CrowdStrike Falcon® Cloud Workload Protection schützt vor Datendiebstahl in privaten, öffentlichen, hybriden sowie in Multi-Cloud-Umgebungen. Die Bereitstellung erfolgt über den schlanken Falcon-Agent, die Verwaltung auf der nativen CrowdStrike® Cloud-Plattform. Die Falcon-Plattform gestattet es Kunden außerdem, Technologien über alle denkbaren Workloads hinweg schnell einzuführen und zu schützen.

## WICHTIGE LEISTUNGSMERKMALE

### UMFASSENDER EINBLICK IN CLOUD-WORKLOADS

Der umfassende Einblick in die Ereignisse von Cloud-Workloads und in die Metadaten von Instanzen ermöglicht die Erkennung, Reaktion und proaktive Bedrohungssuche. So ist sichergestellt, dass potenziell bösartige Aktivitäten nicht unbemerkt bleiben.

- Sammelt Metadaten auf Ebene der Instanzen, sodass die Eigentümer der von einer Warnung betroffen Assets leicht identifizierbar sind
- Gruppiert Hosts nach Konten-ID, was eine schnelle und einfache Visualisierung und Identifizierung von Assets pro Eigentümer ermöglicht
- Erkennt automatisch verdächtige und böswillige Aktivitäten und nimmt eine intelligente Priorisierung vor
- Überwacht kontinuierlich Ereignisse und macht die Aktivitäten der Workloads sichtbar, auch der Aktivitäten in Containern; umfassend ergänzte Daten und Ereignisdetails ermöglichen Untersuchungen gegen flüchtige und außer Dienst gestellte Workloads
- Stellt eine zentrale Konsole bereit für die proaktive Suche nach Bedrohungen über alle Workloads und Endgeräte hinweg
- Erkennt und untersucht Angriffe, die sich über mehrere Umgebungen und verschiedene Arten von Workloads erstrecken, und kann dabei zwischen Endgeräten, Instanzen und Containern wechseln

## WESENTLICHE VORTEILE

- Umfassender Einblick in Workloads über eine einzige Konsole
- Automatische Erkennung der Footprints von Coud-Workloads
- Beseitigung von Reibungsverlusten bei der Integration von wichtigen Clouds
- Workloads mit DevOps-Geschwindigkeit schützen ohne Leistungseinbußen
- Dank verbrauchsabhängiger Abrechnung nur für das zahlen, was genutzt wird
- Nahtlose Migration von Vor-Ort-Ressourcen in die Cloud mit einem einheitlichen Sichtbarkeits- und Schutzniveau
- Bedrohungssuche und Nachforschungen in der Cloud ermöglichen und beschleunigen

# FALCON CLOUD WORKLOAD PROTECTION

- Unterstützt die Eindämmung und Untersuchung kompromittierter Workloads sowie das Ergreifen entsprechender Maßnahmen
- Beinhaltet CrowdScore™ Incident Workbench zur Aufdeckung von Angriffen und zur Verbesserung der Reaktionszeit. Hierbei werden Sicherheitswarnungen mit Vorfällen korreliert. Einordnung, Priorisierung und Hervorhebung dringender Fälle mit sofortigem Handlungsbedarf erfolgen automatisch

## ERKENNUNG VON MULTI-CLOUD-WORKLOADS

Falcon verschafft Einblick in den Umfang und die Art von Footprints in Public und Hybrid Clouds.

- Erkennt vorhandene Workload-Bereitstellungen in der Cloud automatisch – ohne Installation eines Agents – durch Auflisten vorhandener Instanzen für Amazon Web Services (AWS) Elastic Compute Cloud (EC2), Google Cloud Platform (GCP) Compute Engine und virtuelle Maschinen in Microsoft Azure
- Informiert in Echtzeit über Workloads, einschließlich kontextreicher Metadaten über Systemgröße und Systemkonfiguration, Netzwerk sowie Sicherheitsgruppeninformationen für AWS, GCP und Azure
- Identifiziert Workloads, die nicht durch die Falcon-Plattform geschützt sind
- Verschafft Ihnen Einblick in Ihren Cloud-Footprint, sodass Sie alle Workloads schützen, Risiken aufdecken und mindern und die Angriffsfläche reduzieren können

## CONTAINER-SICHERHEIT

Falcon bietet Schutz und Einblick ohne Beeinträchtigung der Containerleistung.

- Schützt Host und Container über einen einzigen Falcon Agent, der auf dem Host ausgeführt wird
- Erleichtert die Untersuchung von Container-Vorfällen, wenn Erkennungen mit einem bestimmten Container in Verbindung stehen und nicht mit den Host-Ereignissen gebündelt sind
- Erfasst Start-, Stopp-, Image- und Laufzeitinformationen des Containers sowie alle Ereignisse, die innerhalb des Containers erzeugt werden, selbst wenn dieser nur wenige Sekunden läuft
- Verschafft Einblick in den Container-Fußabdruck – einschließlich der Bereitstellungen vor Ort und in der Cloud – und zeigt die Containernutzung auf, einschließlich Trends, Betriebszeit, verwendete Images und Konfiguration zur Identifizierung riskanter und falsch konfigurierter Container
- Beinhaltet verhaltensbasierte Angriffsindikatoren (IOAs), die versierte Bedrohungen erkennen, wie Angriffe ohne Dateien und ohne Malware
- Stellt eine zentrale Verwaltungskonsole für Host- und Containersicherheit bereit

## SCHUTZ ZUR LAUFZEIT

Die Falcon-Plattform kombiniert die besten und neuesten Technologien zum Schutz vor aktiven Angriffen und Bedrohungen, und zwar auch dann, wenn Workloads besonders gefährdet sind: zur Laufzeit.

- Arbeitet mit maschinellem Lernen (ML) und künstlicher Intelligenz (KI) zur Erkennung bekannter und unbekannter Malware
- Bietet Schutz vor Exploits
- Umfasst kundenspezifische IOAs, Whitelisting und Blacklisting zur bedarfsgerechten Erkennung und Prävention
- Arbeitet mit integrierten Bedrohungsdaten, um bösartige Aktivitäten zu blockieren und einen vollständigen Angriffskontext bereitzustellen, einschließlich Zuschreibung
- Schützt rund um die Uhr mit verwalteter Bedrohungssuche, damit verdeckte Angriffe nicht unentdeckt bleiben

## UNTERSTÜTZUNG MEHRERER CLOUDS UND BETRIEBSSYSTEME

Die CrowdStrike Falcon-Plattform leistet einen umfassenden Schutz unter Windows und Linux (Amazon, Red Hat, CentOS, Oracle, SUSE, Ubuntu und Debian). Sie ist kompatibel mit AWS, Microsoft Azure und GCP und funktioniert mit jedem Hypervisor, einschließlich vSphere und Hyper-V.

## UNTERSTÜTZTE CONTAINER

Falcon unterstützt OCI-konforme Container (Open Container Initiative), wie Docker, Orchestrierungsplattformen, wie selbstverwaltete Kubernetes, und gehostete Orchestrierungsplattformen, wie GKE (Google Kubernetes Engine), EKS (Amazon Elastic Kubernetes Service), ECS (Amazon Elastic Container Service), AKS (Azure Kubernetes Service) und OpenShift.

FALCON CLOUD WORKLOAD PROTECTION

## API-GELEITETE CLOUD-INTEGRATIONEN

Falcon beseitigt Reibungsverluste und macht so die Cloud-Sicherheit effizienter.

- Leistungsstarke APIs ermöglichen die Automatisierung der Funktionalität von CrowdStrike Falcon, einschließlich Erkennung, Verwaltung, Reaktion und Aufklärung
- Die Integrationen für Chef, Puppet und AWS Terraform unterstützen Continuous Integration/Continuous Delivery (CI/CD) von Deployment-Workflows
- Die Integration der Konfigurationsverwaltung in das Google Cloud Operating System (OS) automatisiert die Bereitstellung von Falcon Agents direkt von GCP aus, ohne dass benutzerdefinierte Skripts erforderlich sind
- Die Integration für AWS PrivateLink unterstützt den Verkehr von Sensor-zu-Cloud über PrivateLink, wodurch die Exposition im Internet reduziert und die Netzwerkarchitekturen vereinfacht werden

## EINFACHHEIT UND LEISTUNG

Falcon wurde in der Cloud für die Cloud entwickelt. Das macht den Schutz von Workloads einfacher, effizienter und sicherer.

- Eine Plattform handhabt sämtliche Workloads und funktioniert überall: ob Private, Public oder Hybrid Cloud
- Eine zentrale Konsole verleiht Einblick in Cloud-Workloads unabhängig von deren Standort
- Falcon gewährt eine vollständige Flexibilität bei den Richtlinien. Diese werden auf Ebene individueller Workloads, auf Gruppeebene oder auf höherer Ebene angewandt
- Automatische Skalierung bei wachsenden Cloud-Workloads, ohne dass zusätzliche Infrastruktur erforderlich ist
- Die Lösung beansprucht sehr wenige Ressourcen auf dem Host. Es erfolgt keine Beeinträchtigung der Laufzeit-Performance – auch nicht bei Analyse, Suche und Ermittlung
- Flexible verbrauchs- und zeitraumbasierte Abonnementmodelle unterstützen eine flexible Geschäftsplanung

## ÜBER CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq:CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit seinervon Grund auf neu konzipierten Endgeräteschutzplattform die Sicherheit im Cloud-Zeitalter neu. Die Plattform CrowdStrike Falcon® verfügt über eine einzigartige, Cloud basierte, schlanke Agentenarchitektur, die von künstlicher Intelligenz (KI) unterstützt wird und unternehmensweit für Schutz und Transparenz in Echtzeit sorgt. 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 3 Billionen endpunktbezogene Ereignisse pro Woche. Damit ist die CrowdStrike Falcon Plattform eine der weltweit fortschrittlichsten Datenplattformen für Cyber-Sicherheit.

**Testen Sie jetzt kostenlos den Virenschutz der nächsten Generation**

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