CrowdStrike Solutions

CROWDSTRIKE

CONTAINERSICHERHEIT MIT DER FALCON-PLATTFORM

Schutz gegen Datendiebstahl für Container

CONTAINERSICHERHEIT MIT DER FALCON-PLATTFORM

ENDPUNKTBASIERTE DETEKTION UND REAKTION (EDR), SCHUTZ UND ERKENNUNG VON CONTAINERN ZUR LAUFZEIT

Zur Steigerung von Effizienz und Agilität setzen Organisationen zunehmend auf Containertechnologien, wie beispielsweise Docker und Kubernetes. Mit dem Einsatz von Containern verändert sich die Art und Weise, wie Anwendungen erstellt, getestet und eingesetzt werden. Anwendungen können damit sofort in jeder Umgebung eingesetzt und skaliert werden. Allerdings werden Container mit zunehmender Akzeptanz dieser Technologie auch zu einer neuen Angriffsfläche, der es an Transparenz und Sichtbarkeit mangelt und die die Organisationen somit neuen Risiken aussetzt. Die damit verbundenen „blinden Flecken" führen zu einem unbemerkten Versagen der Schutzmaßnahmen und letztendlich zu Datendiebstählen. In den meisten Organisationen fehlt es aus folgenden Gründen an einem ausreichenden Einblick in Container:

- Herkömmliche Sicherheitswerkzeuge sind nicht darauf ausgelegt, Container sichtbar zu machen
- Tools, wie beispielsweise Linux-Protokolle, erschweren eine eindeutige Unterscheidung von Ereignissen, die von Containern erzeugt werden, und Ereignissen, die vom Host erzeugt werden, da sie auf den Host beschränkt sind
- Container sind kurzlebig. Das erschwert die Datenerfassung und Untersuchung von Vorfällen, da forensische Beweise verloren gehen, wenn ein Container beendet wird
- Eine dezentral organisierte Verantwortung für Container schränkt die Gesamtsicht ein

Sobald ein Container gestartet ist und läuft, kann er kompromittiert werden. Selbst wenn das Image richtig konfiguriert und verifiziert ist, ist es anfällig für neue Schwachstellen und Bedrohungen zur Laufzeit. Dass Container von ihrer Konzeption her dynamisch und portabel sind, erschwert deren Schutz zusätzlich. Schnelle Skalierbarkeit bedeutet auch, dass sich die Angriffsfläche ständig verändert, während die Portabilität über mehrere Umgebungen hinweg die Sichtbarkeit einschränkt und erschwert.

Manuelle Prozesse und herkömmliche Lösungen vertragen sich nicht mehr mit dem schnellen Wandel und den besonderen Herausforderungen, denen Organisationen heute beim Einsatz von Containern gegenüberstehen. Alternativen sind komplexe Cloud-Sicherheitsplattformen oder isolierte Tools, die allerdings die Komplexität der Schutzmaßnahmen einer Organisation insgesamt weiter steigern.

DAS KONZEPT VON CROWDSTRIKE ZUM SCHUTZ VON CONTAINERN

CrowdStrike bietet eine Plattform für alle Workloads. Die CrowdStrike Falcon®-Plattform schützt Workloads in allen Umgebungen. Auch Workloads und Container, die in der Cloud und in privaten, öffentlichen und hybriden Rechenzentren oder vor Ort ausgeführt werden. Die Falcon-Plattform und der intelligente, schlanke Falcon-Agent bieten unübertroffenen Schutz und Sichtbarkeit in Echtzeit. Falcon ist speziell auf Container ausgelegt und gewährt detaillierte Einblicke sowohl in host- als auch in containerspezifische Daten und Ereignisse. Die Falcon-Plattform ermöglicht und beschleunigt kritische Aufgaben zur Erkennung, Untersuchung und Bedrohungssuche, die an Containern durchgeführt werden – auch an kurzlebigen Containern, nachdem diese außer Betrieb genommen wurden. Sicherheitsverantwortliche können Container mit DevOps-Geschwindigkeit schützen, ohne dass es zu Leistungseinbußen kommt.

WESENTLICHE VORTEILE

Sichere Container ohne Installation von Zusatzprodukten und ohne Steigerung der Komplexität

Schutz von Containern zur Laufzeit

Unübertroffene Sichtbarkeit mit detaillierten Ereignissen und Metadaten der Container

Identifizierung von Containern, die in Ihrer Umgebung ausgeführt werden, einschließlich Containern mit potenziell riskanten Konfigurationen

Beschleunigte Bedrohungssuche und Nachforschung in der Cloud

Sofortiger Schutz mit DevOps-Geschwindigkeit ohne Leistungseinbußen

Anpassung an die dynamische Skalierbarkeit von Containern in Echtzeit

CONTAINERSICHERHEIT MIT DER FALCON-PLATTFORM

ENDPUNKTBASIERTE DETEKTION UND REAKTION FÜR CONTAINER

- Die CrowdStrike® Falcon-Plattform verhindert ein unbemerktes Versagen der Schutzmaßnahmen, indem sie containerspezifische Ereignisse aufzeichnet und damit für eine proaktive Bedrohungssuche und forensische Untersuchungen sichtbar macht:
  - **Sichtbarkeit in Echtzeit:** Streaming von Container-Informationen und -Aktivitäten an die Falcon-Plattform in Echtzeit. So erhalten Sie detaillierte Einblicke, um Bedrohungen schnell identifizieren, verfolgen und untersuchen zu können.
  - **Leistungsstarke Suche:** Einfache Filterung von Ereignissen, die in Containern erzeugt wurden. Die Suche kann anhand detaillierter Container-Metadaten erfolgen, wie Bildern, Modus, Konfigurationstyp usw.
  - **Proaktive Bedrohungssuche:** Nach der Bereitstellung beginnt Falcon sofort mit der Aufzeichnung von Containerdetails und -aktivitäten. Das ermöglicht eine proaktive Bedrohungssuche, bei der Sicherheitsverantwortliche in Sekundenschnelle Abfrageergebnisse erhalten und zwischen den jeweiligen Indizien wechseln können.
  - **Fortlaufende Verfügbarkeit:** Details zu den Ereignissen für eine forensische Beweisführung sowie damit verknüpfte Daten sind kontinuierlich verfügbar, auch bei kurzlebigen und ruhenden Containern.
  - **Vollständige Angriffe in einem einzigen Fenster entziffern:** Ein leicht verständlicher Prozessbaum informiert vollständig über Angriffsdetails im Kontext und macht die Ermittlungen damit schneller und einfacher.

SCHUTZ ZUR LAUFZEIT

- Falcon schützt Container kontinuierlich während der Laufzeit, überwacht Ereignisse und analysiert Daten in Echtzeit. So werden Bedrohungsaktivitäten automatisch identifiziert, sodass fortgeschrittene Bedrohungen erkannt und verhindert werden können.
- CrowdStrike Falcon kombiniert die besten Schutztechnologien, wie maschinelles Lernen (ML), künstliche Intelligenz (KI), Angriffsindikatoren (IOAs) und Blockierung individueller Hashwerte zur Abwehr von Malware und komplexen Bedrohungen, die auf Container abzielen:
  - **ML and AI:** Falcon nutzt ML und KI zur Erkennung bekannter und unbekannter Malware in Containern, ohne dass Scans oder Signaturen erforderlich sind.
  - **IOAs:** Falcon verwendet Angriffsindikatoren, um Bedrohungen anhand von Verhaltensweisen zu identifizieren. So kann Falcon Angriffe stoppen, die sich nicht auf Malware stützen – auch dateilose Angriffe.

ERKENNUNG IN CONTAINERN

- Die Falcon-Plattform gewährt einen sofortigen Einblick in die Nutzung von Containern in Ihrer Umgebung. An entsprechenden Dashboards erhalten Sie Übersichten mit Drilldown-Funktionen, mit denen Sie schnell zu detaillierten Anzeigen und Suchvorgängen wechseln können:

IN DER CLOUD FÜR DIE CLOUD ENTWICKELT

Eine Plattform für alle Workloads

Schützt Container, egal wo sie laufen

Funktioniert ab dem ersten Tag: Bereitstellung und Inbetriebnahme sind eine Sache von wenigen Minuten; ohne Neustart, Feinabstimmung oder komplexe Konfiguration

CROWDSCORE WORKBENCH

Kombiniert zusammenhängende Alarme und Indikatoren zu Vorfällen

Rationalisiert den Triage-Prozess

Intelligente Priorisierung von Vorfällen nach Schweregrad und Kritikalität

- **Container-Verwendung:** Verschaffen Sie sich einen Überblick über alle in Ihrer Umgebung verwendeten Container: Anzahl, Anzahl der Hosts, auf denen Container laufen, Anzahl der Registrierungen, Containertypen und Engine-Version. Anhand von Trendgrafiken erkennen Sie schnell Anomalien, wie Spitzen in der Anzahl laufender Container und Container-Verfügbarkeit.
- **Container nach Host:** Durchsuchen Sie die Host-Eigenschaften und finden Sie alle Container, die auf diesem Host laufen.
- **Container-Images:** Zeigen Sie die verwendeten Images an und suchen Sie nach verwundbaren Images.
- **Container-Konfigurationen:** Identifizieren Sie schnell risikoreiche und fehlerhaft konfigurierte Container, wie beispielsweise solche mit eigenartigen Mount-Punkten oder Links, die auf eine Kompromittierung hinweisen können. Überwachen Sie privilegierte Container und solche, die im interaktiven Modus ausgeführt werden, nicht beendet werden können oder mit Root-Zugriff ausgeführt werden.

SCHNELLIGKEIT UND EINFACHHEIT

- **Geringere Kosten und Komplexität:** Falcon arbeitet mit einer zentralen Verwaltungskonsole. In Verbindung damit wird die Containersicherheit durch einen einzigen Agent sichergestellt, der auf dem Worker-Knoten läuft und sowohl den Knoten selbst als auch alle darauf laufenden Container schützt. Die Host- und Containersicherheit werden über dieselbe Konsole verwaltet, unabhängig davon, wo sich die Container befinden.
- **Schnell:** Falcon schützt auf Anhieb und mit DevOps-Geschwindigkeit. Die Lösung passt sich an die dynamische Skalierbarkeit von Containern in Echtzeit an – mit Continuous Integration/Continuous Delivery (CI/CD) über API und Pre-Boot-Skripte.
- **Schlank:** Die Lösung beansprucht sehr wenige Ressourcen auf dem Host. Es erfolgt keine Beeinträchtigung der Laufzeit-Performance – auch nicht bei Analyse, Suche und Ermittlung.
- **Skaliert beim Starten, Stoppen und Beenden von Container-Instanzen:** Die host-basierte Sicherheit schützt Container automatisch beim Hochfahren, ohne dass zusätzliche Infrastruktur, Agents oder dedizierte Sicherheitscontainer erforderlich sind.
- **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.

Testen Sie jetzt kostenlos den Virenschutz der nächsten Generation

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

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.