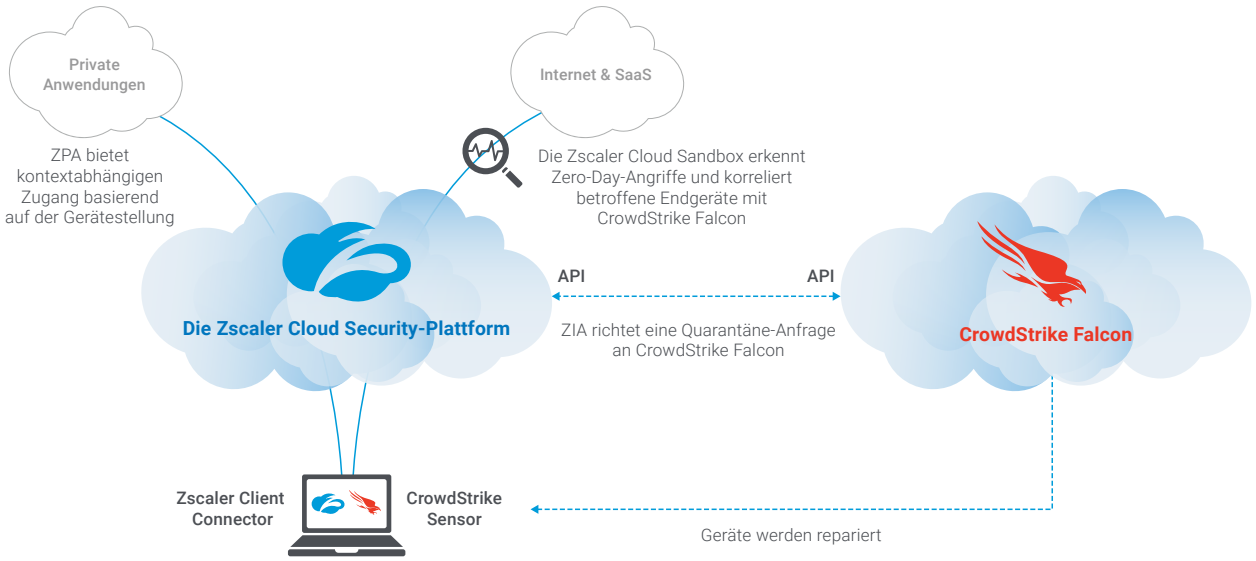
PARTNER-INFORMATION

Modernisierung der Sicherheit vom Endgerät zur Applikation

Die Zscaler™ Cloud-Sicherheitsplattform kann in die CrowdStrike Falcon-Plattform integriert werden, um Ende-zu-Ende-Schutz vom Gerät zum Netzwerk zur Applikation zu erhalten, einschließlich von der Gerätestellung gesteuerter Zugangskontrolle, plattformübergreifender Datenkorrelation und Erkennung von Bedrohungsauswirkungen zur schnelleren Reaktion.

Die Probleme

Benutzer arbeiten zunehmend von Remote-Standorten aus und Anwendungen werden in die Cloud verlagert. Das Internet ist das neue Unternehmensnetzwerk. Herkömmliche Sicherheitsmodelle, die für das Zeitalter der Rechenzentren vor Ort entwickelt wurden, können nicht mehr mithalten. Erstens sind Sicherheitslösungen für den On-Premise-Einsatz komplex in Bezug auf die Bereitstellung, Verwaltung und Wartung. Sie erfordern die Schulung von IT- und Sicherheitsexperten, um korrekt konfiguriert zu werden, und können nicht dynamisch skalieren. Appliance-basierte Hardware hat verschiedene Aktualisierungszyklen, die Vorabinvestitionen erfordern und während des Uprade-Prozesses ständig vom Kerngeschäft ablenken. Zweitens steigt durch direkte Verbindungen von Remote-Benutzern zur Cloud das Risiko für das Unternehmen, da diese Aktivitäten nicht sichtbar sind. Der herkömmliche VPN-Ansatz beeinträchtigt die Nutzererfahrung, da Benutzer wiederholt mit dem VPN verbunden und von ihm getrennt werden, um ein Gleichgewicht zwischen Produktivität und dem erforderlichen sicheren Zugriff auf geschäftskritische Anwendungen herzustellen. Ein BYOD-Ansatz (Bring-Your-Own-Device) lässt nicht verwaltete



Geräte auf das Unternehmensnetzwerk zugreifen und erhöht so das Risiko von Datenoffenlegung und Datenverlust. Das Schlimmste ist, dass herkömmliche Sicherheitslösungen moderne Bedrohungen nicht effektiv und rechtzeitig erkennen können. Während die Menge der Angriffe täglich zunimmt und Taktiken immer ausgefeilter werden, können Organisationen nicht schnell genug Sicherheitsexperten einstellen, um angemessen darauf zu reagieren.

Um diese Probleme anzugehen, brauchen wir Transformation. Um Unternehmen diese Transformation zu erleichtern, bieten Zscaler und CrowdStrike ihre Sicherheitsdienste als zu 100 Prozent Cloud-native Sicherheit-als-Service-Plattformen an. Die Partnerschaft unserer beiden marktführenden Lösungen trägt zu einem einfacheren, schnelleren, effektiveren und überschaubaren Übergang bei.

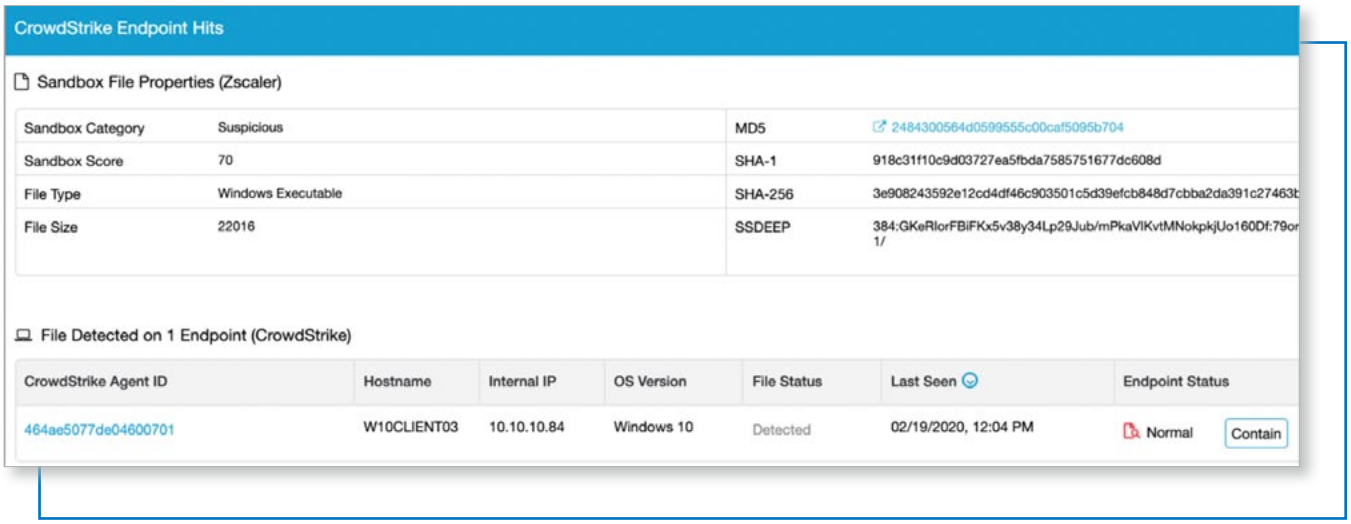
Die Integration von Zscaler und CrowdStrike

Zscaler Private Access™ (ZPA™) und CrowdStrike Falcon-Plattform

Bedingter Zugang basierend auf der Gerätestellung: Zscaler ZPA gewährt bedingten Zugriff auf geschäftskritische interne Anwendungen nur über Geräte, auf denen CrowdStrike ausgeführt wird. Dadurch wird verhindert, dass nicht konforme oder fehlerhafte Geräte auf sensible Anwendungen und Daten zugreifen. Anstelle der traditionellen, allein auf Authentifizierung basierten Alles-oder-Nichts-Zugangskontrolle, wird durch diese Integration unter Einbeziehung der Gerätestellung eine Zero-Trust-Zugangskontrolle implementiert, und Administratoren können anhand dieser Richtlinie entscheiden, welche Anwendungen geschützt werden sollen.

Zscaler Internet Access™ (ZIA™) und CrowdStrike Falcon-Plattform

Korrelation der Zero-Day-Erkennung mit der Endgeräteumgebung für eine schnellere Reaktion: Die Zscaler Cloud Sandbox befindet sich inline an der Cloud-Edge, um Zero-Day-Bedrohungen zu entdecken. Durch API-Integration wird das resultierende Reporting mit den Endgerätedaten von CrowdStrike korreliert, um infizierte Endgeräte innerhalb der gesamten Umgebung automatisch zu identifizieren und per One-Click zur Falcon-Plattform das Auslösen einer sofortigen Quarantäneaktion zu ermöglichen. Darüber hinaus kann der Administrator vom Zscaler Insight Log zur Falcon-Konsole mit automatisch verfügbaren Daten zur Endgeräteuntersuchung umschalten.



VORTEILE

- **Ermöglicht Zero-Trust-Zugangskontrollen** – So wird sichergestellt, dass Benutzer auf geschäftskritische Anwendungen nur über Geräte zugreifen, auf denen CrowdStrike installiert ist und ausgeführt wird. Das Verschleiern von HTTP-Ports verkleinert die Angriffsfläche. Da kein VPN erforderlich ist, wird die Nutzererfahrung erheblich verbessert und gleichzeitig die Sicherheit des Endgeräts erhöht.
- **Effektivere Teams** – Die umfassende Transparenz der Netzwerk- und Endgeräteplattformen vermittelt einen vollständigen Überblick über die Bedrohungslandschaft. One-Click Drill-Down und das Umschalten zwischen Konsolen sowie ein plattformübergreifender Workflow machen Untersuchung und Reaktion schneller und effizienter.
- **Reduziertes Risiko** – Mit dem integrierten Inline-Security-Stack von Zscaler, einschließlich SSL-Überprüfung, Firewall, Web-Proxy, Cloud Sandbox, CASB- und DLP-Schutz, in Kombination mit dem fortschrittlichen Endgeräteschutz und der Analytik von CrowdStrike, können Unterbrechungen und Geschäftsverluste aufgrund von Sicherheitsverstößen und Ausfallzeiten erheblich reduziert werden.
- **Reduzierte Komplexität** – Zscaler und CrowdStrike sind zu 100 Prozent in der Cloud aufgebaut und implementiert. Unser kombiniertes Angebot ist leicht einzurichten, immer aktuell, kosteneffizient, agil und schnell skalierbar. Sicherheitsrichtlinien werden konsistent auf alle Benutzer und Applikationen an jedem Standort angewendet, wodurch das Risiko von Fehlkonfigurationen kompromittierender On-Premise-Anwendungen an mehreren Standorten erheblich reduziert wird. Nicht umsonst werden beide Unternehmen im Gartner MQ als Leader auf ihrem jeweiligen Gebiet genannt.

Weitere Informationen finden Sie unter www.zscaler.com/crowdstrike

Über Zscaler

Zscaler versetzt weltführende Organisationen in die Lage, ihre Netzwerke und Applikationen sicher für eine mobile und Cloud-orientierte Welt zu transformieren. Seine Dienste, Zscaler Internet Access™ und Zscaler Private Access™, bauen schnelle, sichere Verbindungen zwischen Benutzern und Anwendungen, unabhängig von Gerät, Standort oder Netzwerk, auf. Die Dienste von Zscaler werden zu 100% in der Cloud bereitgestellt und bieten eine Einfachheit, Hochsicherheit und Nutzererfahrung, mit der herkömmliche Appliances oder Hybridlösungen nicht konkurrieren können. Die in mehr als 185 Ländern genutzte mandantenfähige, verteilte Cloud-Sicherheitsplattform von Zscaler schützt Tausende von Kunden vor Cyberangriffen und Datenverlust, sodass sie die Agilität, Geschwindigkeit und Kostenvorteile der Cloud sicher nutzen können.

Über CrowdStrike

CrowdStrike® Inc. (Nasdaq: CRWD), ein führender Anbieter von Cybersicherheit, definiert die Sicherheit für das Cloud-Zeitalter mit einer Plattform für den Endgeräteschutz neu, die von Grund auf zur Verhinderung von Verstößen aufgebaut wurde. Die einheitliche, über einen Lightweight-Agent bereitgestellte Plattformarchitektur von CrowdStrike Falcon® nutzt künstliche Intelligenz (KI) im Cloud-Maßstab und bietet Echtzeitschutz und Transparenz für das gesamte Unternehmen, wodurch Angriffe auf Endgeräte innerhalb und außerhalb des Netzwerks verhindert werden. Unter Einsatz des proprietären CrowdStrike Threat Graph® korreliert CrowdStrike Falcon weltweit mehr als zwei Billionen Endgeräte betreffende Events pro Woche in Echtzeit und versorgt damit eine der fortschrittlichsten Datensicherheitsplattformen der Welt.

zscaler™ / CROWDSTRIKE

Zscaler, Inc.
120 Holger Way
San Jose, CA
+1 408 533 0288
www.zscaler.com