CrowdStrike, Okta und Zscaler vereinheitlichen die Sicherheit mit domänenübergreifendem Schutz zur Verbesserung der Cyber-Resilienz im KI-Zeitalter

Herausforderungen

Angreifer agieren heute so schnell wie nie zuvor. Die durchschnittliche Dauer eines Cyberangriffs sank 2024 auf einen historischen Tiefstand von 48 Minuten, der schnellste Angriff dauerte lediglich 51 Sekunden.[1] Gleichzeitig erfolgten 79 % der Angriffe ohne Malware und nutzten Identitätsmissbrauch, Social Engineering und Cloud-Fehlkonfigurationen, um einer Erkennung zu entgehen.[1] Mit herkömmlichen reaktiven Sicherheitsstrategien ist den dynamischen Taktiken heutiger Angreifer nicht mehr beizukommen. Bedrohungsakteure nutzen immer raffiniertere Methoden, darunter KI-gesteuerte Automatisierung und Stealth-Taktiken, um sich unbefugten Zugriff auf Umgebungen zu verschaffen und sich dort unentdeckt zu bewegen. Um diese Herausforderungen zu meistern, müssen Unternehmen über einen fragmentierten Sicherheitsansatz mit Einzellösungen hinausgehen, der die Komplexität erhöht, Reaktionen verzögert und letztlich die allgemeine Sicherheit schwächt.

Anforderungen

Es ist höchste Zeit, bisherige Sicherheitsansätze zu überdenken und uns die Leistungsfähigkeit der KI in puncto Geschwindigkeit und Skalierbarkeit zunutze zu machen. Unternehmen benötigen fortschrittliche Sicherheitsplattformen, die nahtlos zusammenarbeiten, um einen mehrschichtigen Schutz zu gewährleisten, die Komplexität zu reduzieren und die Betriebseffizienz zu steigern.

Lösung

Um neuartigen Bedrohungen zu begegnen, die durch KI verstärkt werden, stellen CrowdStrike, Okta und Zscaler eine vollständig integrierte, domänenübergreifende Sicherheitslösung bereit, die Transparenzlücken beseitigt, die Sichtbarkeit verbessert und die Reaktionszeiten für eine robuste Bedrohungsabwehr beschleunigt. Dieser kombinierte Ansatz sichert und authentifiziert Identitäten, ermöglicht dynamische, kontextabhängige Zero-Trust-Zugriffskontrollen und schützt verteilte Endgeräte, während er SIEM der nächsten Generation zur Bedrohungserkennung und -reaktion in Echtzeit nutzt.

Durch die Korrelation von Risikosignalen aus verschiedenen Identitäts-, Endgeräte-, Cloud- und Netzwerkebenen erhalten Sicherheitsteams eine einheitliche Sicht auf die Bewegungen böswilliger Akteure und können so Bedrohungen erkennen, eindämmen und neutralisieren, bevor sie Schaden anrichten. Mit KI-gestützter Automatisierung, bidirektionalem Austausch von Bedrohungsinformationen und koordinierten Reaktionsmaßnahmen erkennt die gemeinsame Lösung Bedrohungen nicht nur, sondern stoppt sie, bevor sie eskalieren können.

Sicherheitsteams können die Taktiken von Angrifern vorhersehen, Reaktionsmaßnahmen automatisieren und mit Maschinengeschwindigkeit vorgehen, um Angriffe frühzeitig einzudämmen.

Da Cyberbedrohungen immer schneller und raffinierter werden, müssen Unternehmen eine proaktive, KI-gestützte Abwehr einführen, die mit der Geschwindigkeit der Angreifer Schritt hält und sicherstellt, dass Bedrohungen neutralisiert werden, bevor sie sich auf das Unternehmen auswirken.

Ganzheitliche Sicherheit: Einheitlicher Schutz für ein neues Zeitalter

Für Unternehmen, die auf Zero Trust umstellen oder eine Zero-Trust-Lösung entwickeln wollen, die ihre aktuellen

1. CrowdStrike 2025 Global Threat Report, https://www.crowdstrike.com/en-us/global-threat-report/

Investitionen maximiert, bieten die starken Partnerschaften und bewährten Integrationen der Marktführer CrowdStrike, Okta und Zscaler eine Blaupause für eine Zero-Trust-Komplettlösung.

Diese Integrationen bieten Administratoren Echtzeit-Einblicke in die Bedrohungslandschaft und den Sicherheitsstatus von Endgeräten und Anwendungen. Der Zugriff auf kritische Anwendungen kann basierend auf User, Endgerät und Zugriffsrichtlinien geändert werden. Im Falle eines Angriffs wird schnell eine plattformübergreifende Behebung eingeleitet. Die Abwehrmaßnahmen werden durch Präventionsrichtlinien für alle Integrationen weiter gestärkt, um ähnliche Angriffe in Zukunft zu verhindern.

Das Gesamtergebnis ist eine erstklassige, Cloud-native, dynamische, kontextgesteuerte Zero-Trust-Lösung, mit der die zuständigen Fachkräfte KI-gestützten Bedrohungen mit reduziertem Risiko und vereinfachter Bereitstellung immer einen Schritt voraus sind.

Lösungshighlights

Zero Trust Adaptive Access:

Zscaler erzwingt die Vergabe minimaler Zugriffsrechte basierend auf Useridentität, Gerätestatus und kontext+ bezogenem Risiko, wobei die Zscaler Zero Trust Exchange (ZTE) Identity Threat Protection mit Okta AI (ITP) und CrowdStrike Falcon® ZTA-Scores integriert, um risikobasierte Zugriffsrichtlinien in Echtzeit bereitzustellen.

Einheitliche, domänenübergreifende Bedrohungserkennung und -reaktion:

CrowdStrike gewährleistet umfassende Transparenz und koordinierte, automatisierte Reaktionen alle Endgeräte, Identitäten und Anwendungen über Integrationen von CrowdStrike Falcon® Next-Gen SIEM und CrowdStrike Falcon® Fusion SOAR mit Okta und Zscaler. So können domänenübergreifende Bedro+ hungen schnell erkannt und gestoppt und ihre laterale Ausbreitung verhindert werden.

Erkennung von identitäts- und endgerätebezogenen Bedrohungen:

CrowdStrike erkennt und entschärft Bedrohungen, die auf User und Endpunkte abzielen, indem Zscaler-Deception-Signale an Okta ITP weitergeleitet werden, um adaptive Reaktionen zu ermöglichen, während die CrowdStrike-Telemetrie erweiterte Kontextdaten zur Optimierung der Bedrohungserkennung bereitstellt.

Automatisiertes Identity Lifecycle Management:

Okta optimiert die Bereitstellung und Aufhebung von Bereitstellungen für User durch die Okta SCIM-Integration, ermöglicht rollenbasierte Updates in Echtzeit und reduziert den manuellen Arbeitsaufwand.

Einheitliche Risikotransparenz:

Zscaler Risk360 und Data Fabric erfassen Identitätspro+ tokolle von Okta und Endgerätesignale von CrowdStrike.

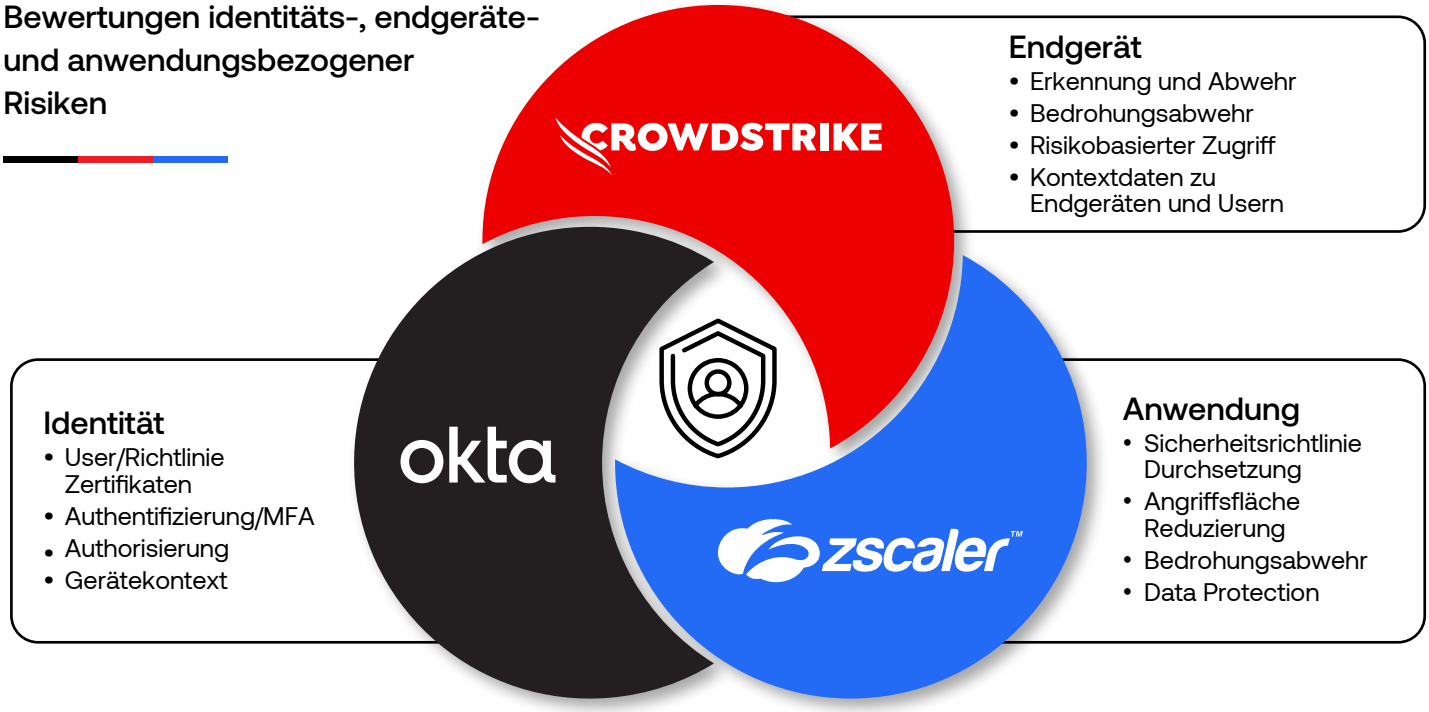
Kontinuierliche Authentifizierung und risikobasierter Zugriff:

Zscaler erzwingt dynamische Zugriffsrichtlinien, wobei Okta eine verstärkte Authentifizierung auslöst, wenn von Zscaler oder CrowdStrike ein anomales Verhalten erkannt wird.

Plattformübergreifender Austausch von Bedrohungsinformationen:

Zscaler stellt einheitliche Telemetriedaten bereit, um die Erkennung und Reaktion zu beschleunigen, wobei CrowdStrike die benutzerdefinierten Blocklisten von Zscaler für proaktiven Schutz erweitert.

Bewertungen identitäts-, endgeräte- und anwendungsbezogener Risiken



Gemeinsame Telemetrie und Bedrohungsinformationen

Die Vorteile kombinierter Synergien für Cyber-Resilienz der neuen Generation

1. Erweiterter Zero Trust-Zugriff:
Zero Trust-Zugriff verhindert die laterale Ausbreitung von Bedrohungen durch die adaptive Durchsetzung von Zugriffsrichtlinien basierend auf Useridentität, Gerätestatus und Echtzeit-Bedrohungskontext.

2. Automatisierte Bedrohungserkennung und -behebung:
Echtzeiterkennung und Bedrohungsinformationen lösen sofortige, koordinierte Reaktionen aus, einschließlich Richtlinien+ durchsetzung und Abmeldung auf allen Geräten und aus allen Anwendungen.

3. Einheitliche Risikotransparenz:
Zscaler Risk360 lässt sich mit Protokollen von CrowdStrike und Okta integrieren, um kontextualisierte Telemetrie und umfassende Risikoeinblicke bereitzustellen und so die Untersuchung und Behebung von Sicherheitsvorfällen zu beschleunigen.

4. Schnelle Untersuchung und Reaktion:
Die beschleunigte Untersuchung und Reaktion durch die Integration mit CrowdStrike Falcon Next-Gen SIEM ermöglicht einheitliche Transparenz, KI-gestützte Erkennung und automa+ tisierte Workflows, um domänenübergreifende Bedrohungen schnell einzudämmen.

5. Effiziente Identitätsverwaltung:
Die SCIM-basierte Bereitstellung von Okta gewährleistet eine sichere, automatisierte User-Bereitstellung/Aufhebung der User-Bereitstellung und gewährleistet, dass nur autorisierte Zugriffsanforderungen genehmigt werden.

6. Verbesserte User Experience:
Nahtloser Zugriff durch Okta SSO, MFA und die adaptiven Richtlinien von Zscaler steigert die Produktivität, ohne die Sicherheit zu beeinträchtigen.

Fazit

CrowdStrike, Okta und Zscaler stellen integrierte Sicherheitslösungen bereit, die den Schutz verbessern, die Komplexität reduzieren und Skalierbarkeit für die dynamischen digitalen Ökosysteme von heute gewährleisten.

Gemeinsam statten sie Unternehmen mit einer Zero-Trust-Abwehr aus, die den identitätsbasierten Zugriff vereinfacht und die domänen+ übergreifende Bedrohungserkennung verbessert. Diese leistungsstarke Partnerschaft unterstützt Unternehmen dabei, ihren Cybersicher+ heitsstatus proaktiv zu stärken und im KI-Zeitalter Resilienz aufzubau+

Über CrowdStrike

CrowdStrike (NASDAQ: CRWD), ein weltweit führendes Unternehmen im Bereich Cybersicherheit, hat mit der weltweit fortschrittlichsten Cloud-nativen Plattform zum Schutz kritischer Unternehmensrisi+ kobereiche – Endgeräte und Cloud-Workloads, Identität und Daten – vollkommen neue Perspektiven für die Sicherheit eröffnet. Die kompakte Falcon-Plattform wurde speziell für die Cloud entwickelt und überzeugt mit einer schnellen, skalierbaren Bereitstellung, überlegenem Schutz, hoher Leistung, geringer Komplexität und unmittelbarem Nutzen.

Über Okta

Okta, Inc. ist The World's Identity Company™. Wir sichern Identitäten, um allen Menschen die sichere Nutzung aller Technologien zu ermöglichen. Mithilfe unserer Kunden- und Mitarbeiterlösungen können Unternehmen und Entwickler die Leistungsfähigkeit des identitäts+ basierten Zugriffs nutzen, um Sicher+ heit, Effizienz und Erfolg zu steigern – und gleichzeitig ihre User, Mitarbeiter und Geschäftspartner zu schützen. Erfahren Sie auf okta.com, warum die weltweit führenden Marken auf Okta vertrauen, wen es um Authentifizierung, Autorisierung usw. geht.

Über Zscaler

Zscaler (NASDAQ: ZS) unterstützt Sie bei der digitalen Transformation – für agiles, effizientes, unterbrechungs+ freies und sicheres Arbeiten. Die Zscaler Zero Trust Exchange schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwen+ dungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die in 150 Rechenzentren auf der ganzen Welt verfügbare SASE-basierte Zero Trust Exchange ist die weltweit größte Inline-Cloud-Sicherheitsplattform.

Erfahren Sie mehr über unsere Lösungen unter okta.com, crowdstrike.com, und zscaler.de |