okta | CROWDSTRIKE | zscaler™

Gemeinsam stellen Okta, CrowdStrike und Zscaler eine integrierte branchenführende Zero-Trust-Lösung bereit, die domänenübergreifende und kontextbasierte Sicherheit gewährleistet.

Herausforderungen

Die Sicherung Ihrer User, Endgeräte und Anwendungen im Rahmen digitaler Transformationsinitiativen und dezentraler Arbeitskonzepte ist eine Herausforderung. Diese Herausforderung wird durch eine unberechenbare Bedrohungslage noch verschärft.

User-Identitäten, Endgeräte, Anwendungen und Netzwerke sind primäre Angriffsvektoren, die Ihre Angriffsfläche vergrößern und das Risiko erhöhen. Einzellösungen, die einen Bereich abdecken, sich aber nicht gut mit anderen Lösungen integrieren lassen, vermitteln Ihnen ein falsches Sicherheitsgefühl. Ein solcher Ansatz verursacht Sicherheitslücken, die kostspielige Behebungsmaßnahmen erforderlich machen, und setzt Organisationen Cyberrisiken aus. Deswegen nimmt die Zahl der Cyberangriffe trotz zusätzlicher Investitionen in Cybersicherheitslösungen zu.

Anforderungen

Seit Jahren versuchen Organisationen, potenzielle Angriffe zu vereiteln, indem sie Lücken in ihrer Sicherheitsarchitektur durch Anschaffung zusätzlicher Einzellösungen schließen. Wir sind jedoch an einem Punkt angekommen, an dem das Hinzufügen zusätzlicher Produkte lediglich die Komplexität erhöht, die Reaktionszeiten verlängert und letztlich unsere Sicherheit verringert. Daher ist es an der Zeit, bisherige Sicherheitsansätze zu überdenken und uns die Leistungsfähigkeit der KI in puncto Geschwindigkeit und Skalierbarkeit zunutze zu machen. Durch das nahtlose Zusammenspiel mehrerer zukunftsfähiger Sicherheitslösungen kann ein dringend benötigter mehrschichtiger Sicherheitsansatz geschaffen, die Betriebseffizienz gesteigert und die Komplexität reduziert werden.

Lösung

Durch Umstellung auf einen Zero-Trust-Ansatz – also einen Ansatz, der auf einer kontinuierlichen Echtzeit-Verifizierung der User-Identität, des Endgerätekontexts und der Unternehmensrichtlinien basiert – verbessern Organisationen ihre Sicherheit. Dieser Ansatz bietet im Vergleich zu herkömmlichen Einzellösungen mehr Einfachheit, bessere Sicherheit und verbesserte Geschäftsflexibilität und ermöglicht so eine erfolgreiche digitale Transformation.

Integrierte Sicherheit ist leistungsstarke Sicherheit

Zero-Trust-Architekturen basieren auf drei Grundpfeilern:

Identitäten **Endgeräte** **Applikationen**

Für Organisationen, die mit der Umstellung auf Zero Trust beginnen oder eine Zero-Trust-Lösung entwickeln, die ihre aktuellen Investitionen maximiert, bieten die starken Partnerschaften und vorab getesteten Integrationen der Marktführer Okta, CrowdStrike und Zscaler eine Blaupause für eine End-to-End-Zero-Trust-Lösung, die User, Endgeräte und Anwendungen zuverlässig schützt.

Diese Integrationen stellen sicher, dass Administratoren einen Echtzeitüberblick über die aktuelle Bedrohungslage und den Sicherheitsstatus aller Endgeräte und Anwendungen erhalten.

okta | CROWDSTRIKE | zscaler

Der Zugriff auf kritische Anwendungen kann basierend auf Kontextdaten zum User und Endgerät sowie der Zugriffsrichtlinien dynamisch geändert werden. Im Angriffsfall werden plattformübergreifend sofortige Behebungsmaßnahmen eingeleitet. Die Abwehrmaßnahmen werden durch Präventionsrichtlinien für alle Integrationen weiter gestärkt, um ähnliche Angriffe in Zukunft zu verhindern.

Das Ergebnis ist eine branchenführende cloudnative, kontextbasierte Zero-Trust-Lösung, die die Bereitstellung vereinfacht, indem sie die Komplexität von Do-it-yourself-Sicherheitslösungen eliminiert und gleichzeitig das Risiko reduziert.

Zentrale Geschäftsergebnisse

Prävention

Durch Austausch von Bedrohungsinformationen und domänenübergreifenden Telemetriedaten werden Zero-Trust-basierte Zugriffskontrollentscheidungen und kontinuierliche Überprüfung ermöglicht. Dadurch minimieren Sie die Angriffsfläche und verhindern Kompromittierungen.

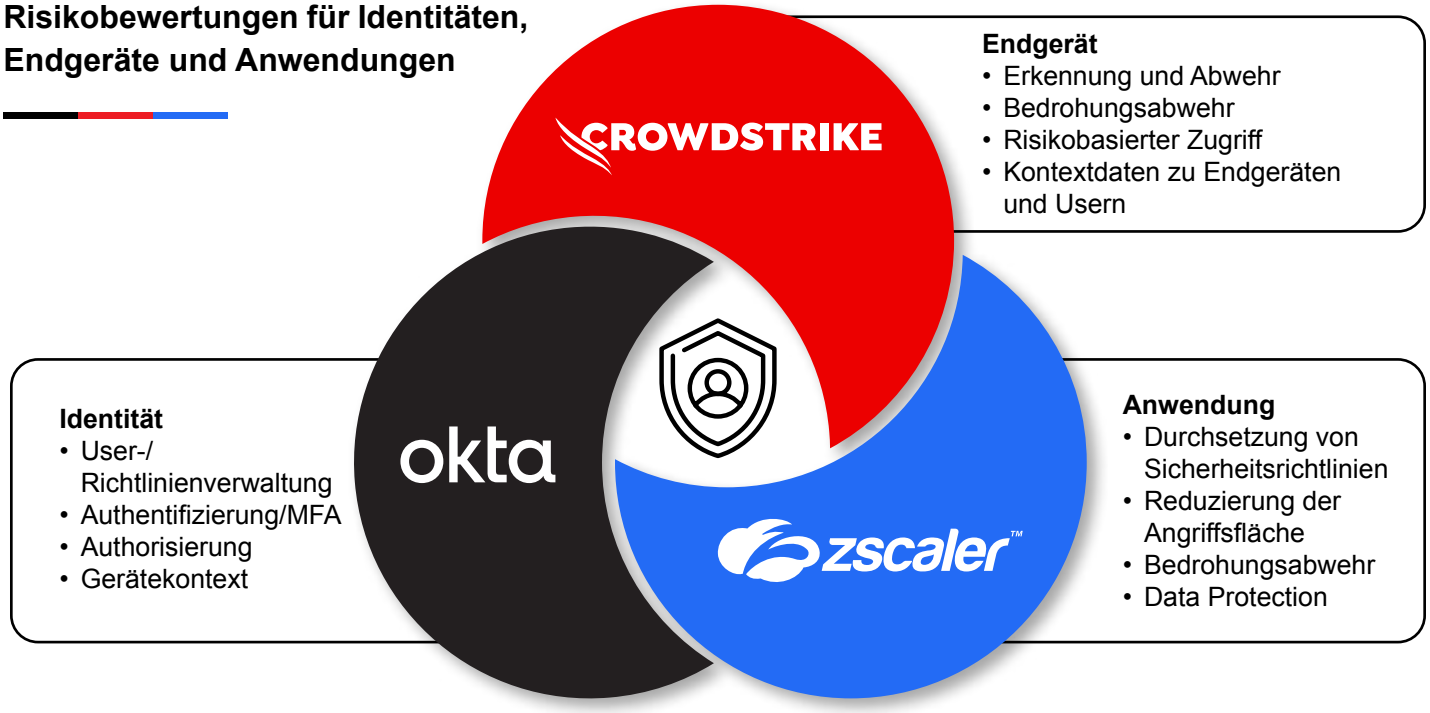
Eindämmung

Durch zuverlässige Erkennung, Verhinderung lateraler Bewegungen und domänenübergreifende Durchsetzung können neuartige Bedrohungen (Kompromittierung von Anmeldedaten, Zero-Day-Malware, Ransomware, Insider-Bedrohungen usw.) in Echtzeit eingedämmt werden.

Antwort

Beschleunigen Sie die Erkennung und Reaktion auf Bedrohungen in mehreren Domänen durch den Austausch kontextbezogener Telemetriedaten, um Vorfälle durch umgehende Erkennung, Priorisierung und Untersuchung schneller und präziser zu beheben.

Risikobewertungen für Identitäten, Endgeräte und Anwendungen



Endgerät
- Erkennung und Abwehr
- Bedrohungsabwehr
- Risikobasierter Zugriff
- Kontextdaten zu Endgeräten und Usern

Identität
- User-/ Richtlinienverwaltung
- Authentifizierung/MFA
- Authorisierung
- Gerätekontext

Anwendung
- Durchsetzung von Sicherheitsrichtlinien
- Reduzierung der Angriffsfläche
- Bedrohungsabwehr
- Data Protection

Gemeinsame Telemetrie und Bedrohungsinformationen

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