okta

Transparenz entscheidet

So deckt eine moderne Identity-zentrierte Sicherheitsstrategie alle Bedrohungen auf und wehrt Angriffe in Echtzeit ab

Ihr Unternehmen wächst und verändert sich. Für Ihr Risikoprofil gilt das ebenfalls.

Wenn Unternehmen wachsen und sich weiterentwickeln, verändern sich auch ihre Tech-Stacks. Allzu oft haben IT- und Security-Teams Schwierigkeiten, mit diesen Entwicklungen Schritt zu halten.

Das führt zu fragmentierten IT-Umgebungen mit verteilten Ressourcen und Identities.

Dadurch haben Sie nur einen unzureichenden Überblick – und das Risiko für eine kostenintensive Sicherheitsverletzung steigt.

Angreifer erkennen eine Chance, wenn sie sich ihnen präsentiert. Daher ist die Identity ihr Angriffsvektor Nr. 1 geworden.

80 % aller Data Breaches begannen mit gestohlenen Anmeldedaten bzw. einem Phishing-Angriff.

(Verizon)

Viele Unternehmen sind kaum in der Lage, auf Bedrohungen zu reagieren.

180 %

Die Zahl Identity-basierter Angriffe ist im Jahresvergleich um 180 % gestiegen.

(Okta)

290 Tage

Unternehmen benötigen im Durchschnitt 290 Tage, um eine Sicherheitsverletzung einzudämmen.

(Verizon)

4,8 Mio. $

Die Kosten pro Data Breach betragen im Durchschnitt 4,88 Mio. US-Dollar.

(IBM)

Identity-Fragmentierung gefährdet Ihr Unternehmen, da es so unmöglich ist, die größten Schwachstellen zu identifizieren.

- Langsamere Erkennung und Abwehr von Bedrohungen
- Eine nicht zu bewältigende Menge unorganisierter Risikodaten
- Unkontrollierbare Risiken in einer immer raffinierteren Bedrohungslandschaft

Frage:

Wie können moderne Unternehmen die Risiken durch Identity-Fragmentierung beseitigen?

Antwort:

Mit einem einheitlichen Ansatz für Identity-zentrierte Sicherheit.

Mit Okta ist das möglich.

Dank Identity-Orchestrierung ermöglicht Okta eine völlig neue Übersicht über die Signale, Richtlinien und Benutzeraktivitäten in Ihren IT-, Sicherheits- und Kundenumgebungen. Dadurch stehen Ihren Teams mehr proaktive Möglichkeiten zur Echtzeit-Erkennung und -Behebung von Bedrohungen zur Verfügung.

Identity Threat Protection mit Okta AI

Automatisierte Reaktionen auf alle Arten von Identity-Bedrohungen

- Analyse und Priorisierung der Risikoindikatoren von allen Systemen, Geräten und Benutzertypen, wodurch eine proaktive Sicherheitslage ermöglicht wird
- Nutzung von Third-Party- und First-Party-Signalen, um verdächtige Aktivitäten und kompromittierte Anmeldedaten in Echtzeit zu erkennen und abzuwehren
- Schnelle Behebung von Bedrohungen mit anpassbaren, automatisierten Aktionen, z. B. Auslösung von MFA oder Abmeldung kompromittierter Benutzer

Okta FastPass

Passwortlose Phishing-resistente Authentifizierung für nahtlose und sichere User Experiences

- Verifizierung der Gerätesicherheit während der Authentifizierung, um Compliance zu gewährleisten
- Warnungen an Benutzer und Administratoren bei Phishing-Versuchen sowie Protokollierung von Angriffen zur Verbesserung der Transparenz
- Blockierung nicht vertrauenswürdiger Anwendungen, bevor sie Authentifizierungsprozesse ausnutzen können

Okta Identity Security Posture Management

Vollständiger Überblick über blinde Flecken im Identity-Management Ihres Unternehmens

- Vollständiger Überblick über blinde Flecken in den Identity-Sicherheitsmaßnahmen Ihres Unternehmens
- Erkennung schwerwiegender Schwachstellen wie MFA-Umgehung, Wildwuchs bei Administratorkonten sowie unvollständigem Benutzer-Offboarding
- Überwachung nicht-menschlicher Identities und Identifizierung von Risiken wie nicht rotierten API-Keys und übermäßig privilegierten Service-Accounts

Okta bietet eine sichere Methoden zum Onboarding von Anwendungen

Identity-Transparenz ist unverzichtbar für die Absicherung aller Zugriffsphasen, einschließlich des Anwendungs-Onboardings. Mit Okta erhalten Sie Echtzeit-Erkenntnisse über Benutzeraktivitäten und Risikoindikatoren, sodass Sie neue Anwendungen in fünf einfachen Schritten nahtlos integrieren können.

1. Gewährleistung, dass neue Benutzer ab dem ersten Tag über die richtigen Zugriffsrechte verfügen
2. Anpassung der Zugriffsrechte von Endbenutzern über eine zentrale Plattform
3. Integration mit HR-Software und Kundenverzeichnissen für konsolidiertes Identity-Management
4. Automatische Entfernung von Zugriffsrechten, wenn Mitarbeiter das Unternehmen verlassen
5. Verwaltung von Kundenkonten mit sicheren Zugriffen basierend auf ihren aktuellen Aktivitäten

Möchten Sie mehr darüber erfahren, wie Sie Ihre Sicherheitsstrategie mit modernen Identity-Lösungen vereinheitlichen können?

Kontaktieren Sie unser Team und vereinbaren Sie eine Demo, um die Okta Platform in Aktion zu erleben.

Kontakt

okta