Transparenz zu allen Identity-bezogenen Bedrohungen sowie Echtzeit-Behebung

mit einer modernen Identity-zentrierten Sicherheitsstrategie

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

Zur Förderung der Flexibilität und der Remote-Zusammenarbeit setzen Unternehmen wie Ihres auf verschiedene Best-of-Breed-Lösungen. Diese sorgfältig zusammengestellten Tech-Stacks bieten in allen Bereichen bessere Ergebnisse – führen jedoch auch zu neuen Risiken.

Wenn Unternehmen wachsen und sich weiterentwickeln, fällt es ihren IT- und Security-Teams häufig schwer, die Systeme anzupassen und mit den Veränderungen Schritt zu halten. In vielen Fällen führt dies zu **fragmentierten IT-Umgebungen**, deren Kernsysteme und Identities über mehrere Systeme und Infrastrukturen verteilt sind.

Dadurch haben Sie nur einen unzureichenden Überblick über die aktuelle Sicherheitslage Ihres Unternehmens – und das Risiko für eine kostenintensive Sicherheitsverletzung steigt.

Identity ist heute der Angriffsvektor Nr. 1

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

Die Zahl Identity-basierter Angriffe steigt **im Jahresvergleich um 180 %.**

Verizon Data Breach Investigations Report 2024

Eine einheitliche Identity-Sicherheitslösung verbessert die Transparenz

Fragmentierte Sicherheits- und Tech-Stacks generieren riesige Datenmengen zu Risiken und potenziellen Bedrohungen. Ihr Team muss dabei die Informationen aus mehreren Protokollen durchsuchen und korrelieren, um zu verstehen, welche Meldungen oder Ereignisse wirklich Aufmerksamkeit erfordern. Dadurch ist es praktisch unmöglich, Risiken und Zwischenfälle in Echtzeit zu beheben.

Mit anderen Worten: Identity-Fragmentierung behindert die Transparenz und macht es unmöglich, die größten Schwachstellen in Ihrem Unternehmen zu identifizieren. Die Erkennung und Abwehr von Bedrohungen wird ausgebremst, sodass Angreifer zahlreiche Möglichkeiten haben, mit gestohlenen Anmeldedaten großen Schaden zu verursachen. Ihr Unternehmen und Ihre Kunden werden also einem unkontrollierbaren Risiko ausgesetzt – während die Bedrohungslandschaft jeden Tag raffinierter wird.

Um dieses Risiko effektiv in den Griff zu bekommen, müssen Identity-Systeme und -Prozesse in einer einheitlichen Plattform zusammengeführt werden, sodass die Effizienz gesteigert und die Kontrolle verbessert wird. Moderne Identity-Plattformen ermöglichen die Umsetzung dieses einheitlichen Sicherheitsansatzes.

Wichtige Vorteile dank Okta

Okta Platfworm unterstützt einen zuverlässigen und stark vereinfachten Ansatz für Identity-zentrierte Sicherheit. Durch eine vielschichtige Produkt-Suite und zahlreiche Funktionen bietet Okta durchgängigen Echtzeit-Schutz vor raffinierten Bedrohungen, ohne die Workflows und die Customer Experiences durch unnötige Reibungspunkte zu beeinträchtigen.

So erreichen Sie Transparenz zu allen Identity-bezogenen Bedrohungen (und ermöglichen Echtzeit-Behebung)

Effektive Risikobehebung beginnt mit einem zentralen Überblick über Ihr Risikoprofil, für den alle Signale aus Sicherheitstools in Echtzeit analysiert werden. Im Bereich Customer Identity-Management ermöglicht dies die schnelle Erkennung und Behebung von Account-Hacking, Betrug und kompromittierten Zugangsdaten, sodass vertrauliche Daten zuverlässig geschützt werden.

Außerdem darf die Risikobehebung nicht auf langsamen, manuellen Abläufen basieren. Ihre Identity-Lösung muss Echtzeit-Erkenntnisse mit automatisierten Workflows für Behebungsmaßnahmen verknüpfen, die zu den spezifischen Anforderungen Ihres Unternehmens passen.

Mit einer einheitlichen Identity-Sicherheitslösung wird dies ermöglicht. Durch die Integration Phishing-resistenter Maßnahmen mit einer modernen, Identity-zentrierten Risk Engine erhalten Sie einen Echtzeit-Überblick über neue Bedrohungen. Ganz gleich, ob Sie Ihre Mitarbeiter oder Ihre Kunden schützen möchten, erhalten Sie den umfassenden Schutz, den Sie angesichts der aktuellen Bedrohungslandschaft benötigen – und nur mit einem einheitlichen Identity-Ansatz erreichen können.

Die Vorteile von Okta

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

Identity Threat Protection mit Okta AI

- Echtzeit-Transparenz zu Bedrohungen für alle Systeme, Geräte und Benutzertypen, wodurch eine proaktive Sicherheitslage ermöglicht wird
- Nutzung von Drittanbieter-Signalen zusätzlich zu Daten aus dem Okta-Ökosystem, sodass Sie detailliertere Erkenntnisse erhalten und Bedrohungen schneller erkennen können
- Schnelle Behebung von Bedrohungen mit anpassbaren, automatisierten Aktionen, z. B. Auslösung von MFA oder Abmeldung kompromittierter Benutzer

Okta FastPass

- Unterstützung passwortloser Phishing-resistenter 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

Sicheres Onboarding für Anwendungen

- Gewährleistung, dass neue Benutzer (Mitarbeiter ebenso wie Kunden) ab dem ersten Tag über die richtigen Zugriffsrechte auf wichtige Anwendungen und Ressourcen verfügen
- Anpassung der Zugriffsrechte von Endbenutzern über eine zentrale Plattform
- Integration mit HR-Software und Directories zur konsolidierten Verwaltung von Mitarbeiterinformationen und -berechtigungen und Verknüpfung mit Customer Identity-Systemen zur Verwaltung und Absicherung von Kundenkonten im benötigten Umfang
- Automatische Entfernung von Zugriffsrechten, wenn Mitarbeiter das Unternehmen verlassen – verbessert die Sicherheit und senkt die Kosten
- Nahtlose Verwaltung von Kundenkonten für sichere Zugriffe basierend auf ihrem aktuellen Status, ihren Aktivitäten und Präferenzen

Identity Security Posture Management

- Aufdeckung und Priorisierung verborgener Identity-Risiken bei allen Ihren Identity-Anbietern, SaaS-Umgebungen und Cloud-Infrastrukturen dank kontinuierlicher Überwachung und KI-gestützter Analysen
- Proaktive Reduzierung der Angriffsfläche, indem kritische Schwachstellen wie MFA-Umgehung, Wildwuchs bei Administratorkonten, unvollständiges Benutzer-Offboarding und Risiken durch nicht-menschliche Identities erkannt werden, bevor sie ausgenutzt werden können
- Vereinfachte Validierung der Compliance mit Frameworks wie NIST, CIS, ISO und PCI-DSS durch kontinuierliche, automatisierte Überwachungs- und Reporting-Kontrollen
- Steigerung der Produktivität Ihres Security-Teams dank konsolidiertem Identity-Kontext zu allen Systemen sowie grafischer Darstellung komplexer Identity-Beziehungen, sodass Teams die Sicherheitslage mit minimalem Zeitaufwand verstehen und verwalten können

Transparenz entscheidet

Angesichts einer Risikolandschaft, die durch immer raffiniertere Bedrohungen geprägt ist, führt der sicherste Weg zu einem resilienten und sicheren Unternehmen über einen einheitlichen Identity-zentrierten Sicherheitsansatz.

Um dieses Versprechen einer besseren Sicherheit halten zu können, müssen Sie jedoch die Identity-Fragmentierung beseitigen, da sie Ihre Sicherheitsumgebung schwächt und zu Sicherheitslücken führt.

Möchten Sie mehr darüber erfahren, wie Sie Ihre Sicherheits-strategie mit modernen Identity-Lösungen vereinheitlichen können? Kontaktieren Sie uns und vereinbaren Sie eine Demo, um die Okta Platform in Aktion zu erleben.