E-Book

Die Leistung und das Potenzial von einheitlichem Identity-Management ausschöpfen

Fünf wichtige Vorteile für Ihr Unternehmen

okta

Die kritische Rolle von Identity-Management

Identity-Management ist für Sicherheit heute unverzichtbar. In der heutigen Cloud-basierten Welt, in der Systeme und Anwendungen stark vernetzt sind, entscheidet das Identity-Management darüber, ob vertrauliche Unternehmensdaten geschützt oder gefährdet sind.

Kriminelle Akteure haben die Identity bereits als wichtiges Ziel erkannt, doch Unternehmen aller Branchen stellen allzu oft fest, dass sie nicht auf Identity-basierte Attacken vorbereitet sind. Die Zahl dieser Angriffe steigt pro Jahr um 180 %. Dennoch dauert es weiterhin durchschnittlich 290 Tage, bis eine Sicherheitsverletzung eingedämmt ist (Verizon 2024 Data Breach Report).

Das grundlegende Problem ist die Identity-Fragmentierung über zahlreiche Technologie- und Sicherheitssysteme hinweg. Ohne einen einheitlichen Identity-Sicherheitsansatz schwächen Unternehmen ihre Risikominimierungsmaßnahmen und überlasten ihre IT- und Security-Teams, da ineffiziente Tools nicht mit den heutigen komplexen Bedrohungen Schritt halten können.

Um die Kontrolle zurückzugewinnen, müssen Unternehmen eine integrierte Identity-basierte Sicherheitsstrategie entwickeln, die Risiken in IT- und Sicherheitssystemen erkennt, in Echtzeit reagiert und zukünftige Angriffe mit zentraler Identity Governance und Sicherheitsorchestrierung verhindert.

Ein Leitfaden für zukunftsfähiges Identity-Management

In diesem E-Book erfahren Sie, wie Unternehmen eine einheitliche Identity-orientierte Sicherheitsstrategie aufbauen können. Wichtige Themen:

- Warum fragmentiertes Identity-Management die Behebung von Risiken erschwert
- Warum moderne Unternehmen einen Identity-zentrierten Sicherheitsansatz benötigen
- Die fünf wichtigen Vorteile einer einheitlichen Sicherheitsstrategie

Zuverlässige Sicherheit beginnt mit einem Identity-orientierten Sicherheitsansatz

Die Abläufe in heutigen Unternehmen unterscheiden sich enorm von denen vor fünf Jahren. Hybride Arbeit bedeutet, dass die Produktivität jetzt von nahtlosen Verbindungen mit dezentralen Netzwerken mit Vollzeitmitarbeitern, Auftragnehmern, Kunden und externen Partnern abhängt, die auf wichtige Ressourcen und Netzwerke auf der ganzen Welt zugreifen. Der zügige Umstieg auf Cloud-Services und SaaS-Anwendungen vereinfacht diese Verbindungen, sodass es leichter ist, sich immer flexibler zu vernetzen, remote zusammenzuarbeiten und abgesicherte Customer Experiences bereitzustellen.

Dieser starke Wandel bei der Arbeitsweise führt jedoch auch zu fundamentalen Veränderungen beim Schutz von Unternehmen und Kunden. Veraltete Sicherheitsparadigmen, die sich meist auf den Netzwerkperimeter und On-Premise-Umgebungen konzentrieren, sind einfach nicht für Cloud-native Anwendungen und Remote-Zusammenarbeit ausgelegt. Das herkömmliche Konzept eines Sicherheitsperimeters ist nicht mehr relevant. Sicherheitsexperten weisen seit Jahren darauf hin.

Zuverlässiges Identity-Management – mit hoher Transparenz dazu, wer von wo und unter welchen Bedingungen worauf zugreift – ist für die Sicherheit und die Bereitstellung nahtloser User Experiences unverzichtbar. Das moderne Verständnis des Zero-Trust-Prinzips sieht vor, dass die Konzepte von vertrauenswürdigen Geräten und Netzwerken nicht mehr anwendbar sind. Unternehmen müssen ihren dezentralen, hybriden Belegschaften die Möglichkeit bieten, sich von jedem Gerät und Standort zu verbinden. Gleichzeitig müssen sie sicherstellen, dass Kunden einfachen, nahtlosen und sicheren Zugriff erhalten.

Kriminelle Akteure wissen, dass Identity-bezogene Angriffe heute die primäre Methode für nicht autorisierte Zugriffe auf vertrauliche Daten sind. Im Jahr 2024 begann die überwältigende Mehrzahl (80 %) der Sicherheitsverletzungen mit gestohlenen Anmeldedaten bzw. einem Phishing-Angriff (Verizon 2024 Data Breach Report).

Dadurch spielen Identities für die Sicherheit eine zentrale Rolle. Unternehmen können Zero Trust beim Bedrohungsschutz – und die angestrebte nahtlose Zusammenarbeit, sichere Customer Experience und Produktivität – nur erreichen, wenn sie ganz auf einen vollständig integrierten Identity-Ansatz setzen.

Identity-Management in einen Wettbewerbsvorteil umwandeln

Identities sind das größte Sicherheitsrisiko von Unternehmen, aber auch die größte Chance. Wenn Sie die zentrale Rolle anerkennen und die Identity-gestützten Funktionen (inkl. Kundenidentitäten) modernisieren, können Sie die Risiken minimieren, Angreifern einen Schritt voraus bleiben und wichtige Vorteile erzielen. Eine starke Identity-Strategie ermöglicht schnelle Anmeldungen, flexible Zusammenarbeit, nahtlose Compliance und starke Sicherheit.

Fragmentierte Sicherheit führt zu gefährlichen blinden Flecken

Die starke Veränderung unserer Arbeitsweise – mit stärker verteilter Produktivität und Zusammenarbeit mit besonderem Fokus auf Geschwindigkeit und Flexibilität – hat auch dazu geführt, dass die Sicherheits- und Tech-Stacks heute in praktisch allen Branchen anders zusammengesetzt und strukturiert sind. Die Tage, in denen der gesamte Stack des Unternehmens mit einem einzigen ELA (Enterprise License Agreement) gekauft wurde, sind vorbei. Erfolgreiche Unternehmen hängen jetzt von einem ganzen Ökosystem aus Best-of-Breed-Lösungen ab, die auf ihr Business und ihre Sicherheits- und Customer Experience-Anforderungen abgestimmt sind. Sie müssen diese Lösungen *verknüpfen* und deren *Mehrwert maximieren, um das Wachstum zu fördern, das Unternehmen zu schützen und nahtlose sichere Interaktionen für Kunden bereitzustellen.*

Gleichzeitig erweitern die Best-of-Breed-Anwendungen den Tech-Stack immer mehr, sodass es IT- und Security-Teams schwer fällt, die Umgebung anzupassen und Schritt zu halten. In vielen Fällen führt dies zu fragmentierten IT-Umgebungen, deren Kernsysteme und Identities über mehrere Systeme und Infrastrukturen verteilt sind.

Die Folgen eines fragmentierten Identity-Systems

- Unzureichender Überblick über die aktuelle Sicherheitslage des Unternehmens sowie über die Berechtigungen der einzelnen Benutzer für die verschiedenen Systeme und Anwendungen
- Verzögerte Reaktionen erleichtern Angreifern teure, verheerende Sicherheitsverletzungen, die Identity-bezogene Schwachstellen ausnutzen
- Umständliche, zeitaufwändige und fehleranfällige Prozesse zur Berechtigungsverwaltung

Argumente für einheitliche Identity-Sicherheit

Einfach ausgedrückt, untergräbt Identity-Fragmentierung Ihre Sicherheitsmaßnahmen schon an der Wurzel. Sie 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. In einer Cloud-nativen Welt ist **Identity für Sicherheit entscheidend** – und sollte auch so behandelt werden. Sie muss im Mittelpunkt Ihrer Sicherheitsstrategie stehen und darf nicht nachträglich als Fragment hinzugefügt werden. Mit einer einheitlichen Identity-Ebene können Ihre IT- und Security-Teams Bedrohungen bewerten, Zugriffsrichtlinien durchsetzen und automatisch auf verdächtige Aktivitäten reagieren.

Moderne Identity-Plattformen ermöglichen die Umsetzung dieses einheitlichen Sicherheitsansatzes.

Vorteile einer einheitlichen, Identity-zentrierten Sicherheitsstrategie

Nur wenige bezweifeln den Bedarf nach einheitlichen und konsolidierten Identity-Systemen und -Prozessen. Die Herausforderung für die meisten Unternehmen liegt darin, dieses Konzept in eine praktikable Strategie zu verwandeln.

Eine einheitliche Identity-zentrierte Sicherheitsstrategie bietet mehrere spürbare Vorteile, die sich in der Summe darauf auswirken, wie Ihr Unternehmen kritische Assets schützen, Kundeninteraktionen absichern, alltägliche Workflows vereinfachen und die Leistung in allen Geschäftsbereichen steigern kann.

Vorteil 1: Transparenz zu allen Identity-bezogenen Bedrohungen sowie Echtzeit-Behebung

Vorteil 2: Vollständige Umsetzung zuverlässiger Zero-Standing/Least-Standing-Privilegien

Vorteil 3: Bewährte Zero-Trust-Strategie

Vorteil 4: Bessere Kontrolle über nicht-menschliche und Maschinen-Identities

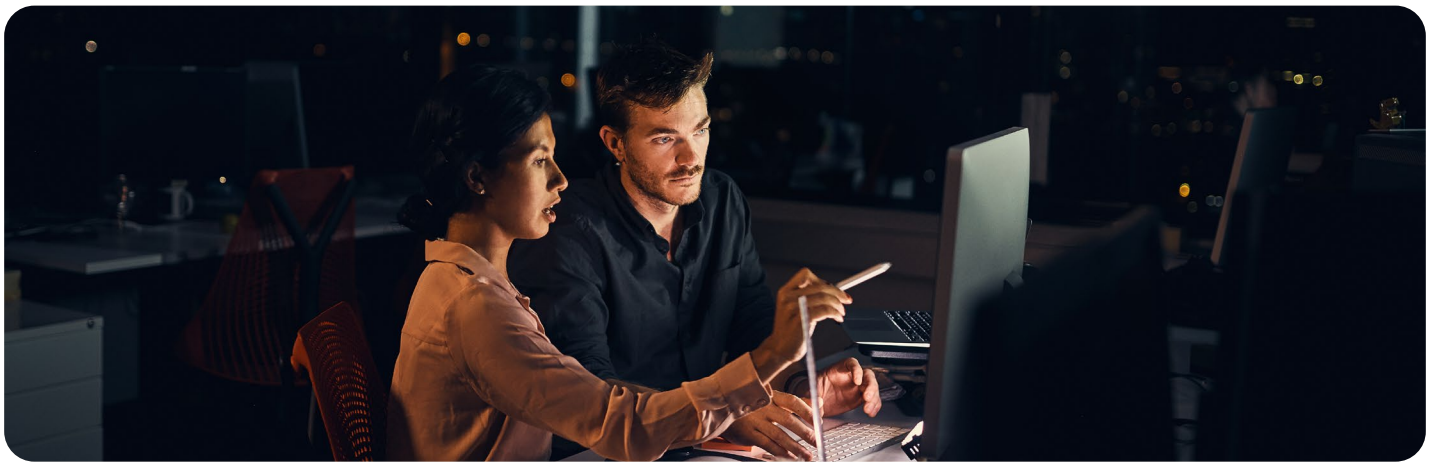
Vorteil 5: Bestmögliche Nutzung Ihrer Technologie- und Sicherheitsinvestitionen

Wichtige Vorteile dank Okta

Okta unterstützt einen zuverlässigen und stark vereinfachten Ansatz für Identity-zentrierte Sicherheit. Durch eine vielschichtige Produkt-Suite und zahlreiche Funktionen bietet Okta End-to-End-Schutz vor raffinierten Bedrohungen, ohne die Workflows und die Customer Experiences durch unnötige Reibungspunkte zu beeinträchtigen. Und durch die einheitliche Identity-Orchestrierung ermöglicht Okta einen neuen Grad der Transparenz zu Signalen und Richtlinien in Ihren IT-, Sicherheits- und Kundenumgebungen. Dadurch stehen Ihren Teams leistungsstarke Möglichkeiten zur Echtzeit-Abwehr potenzieller Risiken zur Verfügung.

Vorteil 1

Transparenz zu allen Identity-bezogenen Bedrohungen sowie Echtzeit-Behebung



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.

Für die schnellere und effektivere Risikobehebung benötigen Sie zunächst einen zentralen, umfassenden Überblick über Ihr Identity-Risikoprofil. Dabei müssen Sie in der Lage sein, alle Signale aus allen Sicherheitstools in Echtzeit zu analysieren und zu priorisieren, um entscheidungsrelevante Erkenntnisse zu gewinnen. Unternehmen, die Kundenidentitäten verwalten, müssen in der Lage sein, Account-Hacking, betrügerische Aktivitäten und kompromittierte Anmeldedaten in Echtzeit zu erkennen und zu beheben, um das Vertrauen ihrer Kunden sowie ihre vertraulichen Daten zu schützen.

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. Wenn Sie Ihren Sicherheits-Stack zu einer modernen Identity-Lösung zusammenführen, können Sie Ihre Phishing-Schutzmaßnahmen in eine zentrale Identity-zentrierte Risk Engine integrieren. Dadurch erhalten Sie einen umfassenden Echtzeit-Überblick über Identity-Bedrohungen, sobald diese auftreten. Ganz gleich, ob Sie Ihre Mitarbeiter oder Ihre Kunden schützen möchten, erhalten Sie die Transparenz, die Sie angesichts der aktuellen Bedrohungslandschaft benötigen und mit einheitlichem Identity-Management erhalten können.

Die Vorteile von Okta

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 nicht autorisierte Zugriffe zu vermeiden
- Verbesserung der Login-Sicherheit, um ungewöhnliche Aktivitäten schnell zu erkennen und darauf reagieren zu können
- Blockierung nicht vertrauenswürdiger Anwendungen, bevor sie Authentifizierungs-prozesse ausnutzen können

Vorteil 2

Vollständige Umsetzung zuverlässiger Zero-Standing/Least-Standing-Privilegien

Die Etablierung und Durchsetzung von Zugriffen nach dem Least-Privilege-Prinzip im gesamten Unternehmen kann sich wie eine endlose, niemals zu bewältigende Herausforderung anfühlen. Das gilt ganz besonders dann, wenn ein fragmentierter Tech-Stack stark von manuellen Integrationen abhängt.

Bei modernen Identity-Lösungen stehen Ihnen Tools und Funktionen zur Verfügung, die jederzeit genau die Zugriffe ermöglichen, die zum jeweiligen Zeitpunkt angemessen sind. Durch die Vereinheitlichung von Identity Governance und Privileged Access Management erhalten Unternehmen zentrale Transparenz dazu, wer worauf zugreifen kann. Außerdem können sie diese Zugriffe stark granular kontrollieren.

Eine einheitliche Identity-Sicherheitslösung vereinfacht außerdem das Identity-Management, da Governance, Privileged Access Management und andere Identity-bezogene Funktionen in einer einzigen Plattform konsolidiert werden. Durch die Zentralisierung können die Zugriffsrichtlinien vereinheitlicht und der Schutz der wichtigsten Daten Ihres Unternehmens verbessert werden.

Die Vorteile von Okta

Okta Identity Governance

- Einheitlicher Überblick über Zugriffe auf allen Systemen und Anwendungen, sodass die Kontrolle und Überwachung verbessert wird
- Vereinfachte Gewährung rollen- und gruppenbasierter Zugriffsrechte, sodass Sie sicherstellen können, dass die richtigen Personen über die richtigen Zugriffsrechte verfügen
- Vereinfachtes Onboarding für neue Mitarbeiter, da sie vom ersten Tag über die richtigen Zugriffsrechte verfügen, wodurch die Produktivität steigt und Risiken reduziert werden
- Automatisierte Rollenänderungen und Deprovisionierungen, um die Sicherheit zu gewährleisten

Okta Privileged Access

- Schutz hochprivilegierter Informationen mit sicheren Zugriffskontrollen
- Für spezifische Benutzer und Anwendungsfälle anpassbare Zugriffsprotokolle
- Hohe Transparenz zu privilegierten Aktivitäten, sodass Auditing und Risikomanagement vereinfacht werden
- Vereinfachte Zugriffsanfragen mit benutzerfreundlichen Integrationen, die Workflows beschleunigen, ohne die Sicherheit zu kompromittieren

Okta Integration Network

Die Okta-Bibliothek mit mehr als 7.000 vorkonfigurierten Integrationen hilft Ihnen, zentrale Zugriffstransparenz zu praktisch jeder Komponente Ihres Tech-Stacks zu erhalten.

Vorteil 3

Bewährte Zero-Trust-Strategie

Obwohl sich die meisten Unternehmen bereits vor längerer Zeit die Umsetzung der Zero-Trust-Prinzipien zum Ziel gesetzt haben, arbeiten heute nur wenige mit einem Zero-Trust-Framework. Der Grund: Ebenso wie bei der Durchsetzung von Zugriffen nach dem Least-Privilege-Prinzip bedeutet die Umsetzung von Zero Trust bei einem fragmentierten Identity-Stack, dass die Überwachung manuell erfolgen muss – was von Menschen nicht in der erforderlichen Geschwindigkeit geleistet werden kann.

Ein einheitlicher Identity-zentrierter Sicherheitsansatz ist erforderlich, um (mit hoher Zuverlässigkeit) bestätigen zu können, dass Ihre Abläufe dem Zero-Trust-Prinzip gerecht werden. Wenn Sie Ihren Tech-Stack mit einer modernen Identity-Plattform vereinheitlichen, können Sie die Einhaltung der Zero-Trust-Prinzipien in Ihrem gesamten Tech-Stack ganz einfach erreichen – und nachweisen. Sie müssen nicht mehr manuell prüfen, ob die einzelnen Benutzer über die richtigen Berechtigungen für jede Anwendung und jedes System verfügen. Eine einheitliche Identity-Lösung ersetzt diese mühsame (und fehleranfällige) Aufgabe durch automatisierte Analysen und bietet dabei mit weniger Ressourcenaufwand mehr Zuverlässigkeit und besseren Schutz vor Bedrohungen.

Die Vorteile von Okta

Identity Security Posture Management

- Automatische Scans Ihrer Tools und Evaluierung Ihrer Konfiguration basierend auf aggregierten Zero-Trust-Frameworks
- Proaktive Identifizierung von Schwachstellen und Sicherheitslücken, bevor sie ausgenutzt werden können
- Kontinuierliche Aufdeckung kritischer Konfigurationsfehler und Lücken, z. B. inkonsistente MFA-Durchsetzung und Account-Ausbreitung
- Zuverlässiger Nachweis der Einhaltung von Zero-Trust-Prinzipien innerhalb von Minuten statt Tagen oder Wochen

Vorteil 4

Bessere Kontrolle über nicht-menschliche und Maschinen-Identities

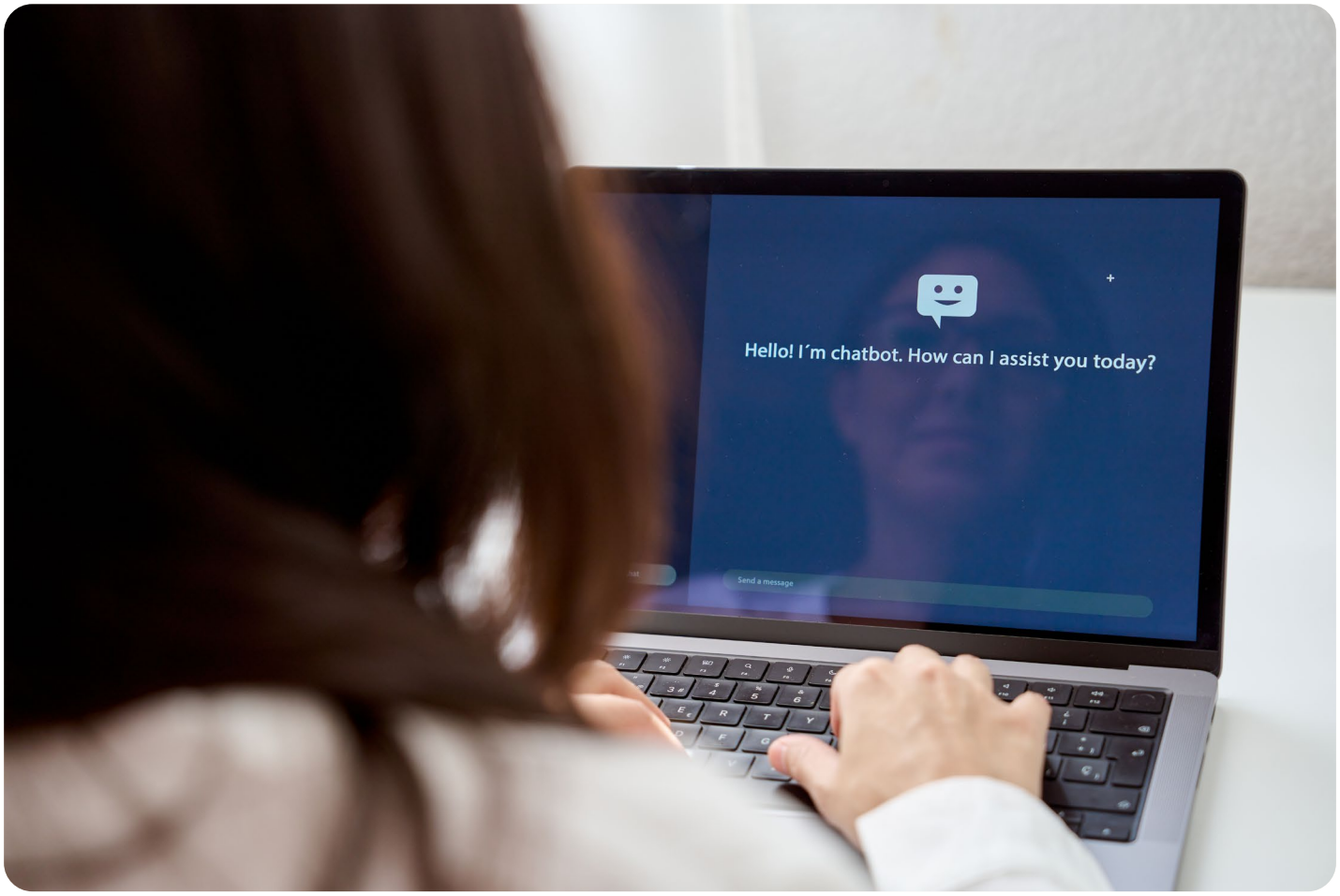
Nicht-menschliche Identities (z. B. Maschinen-, Service- und KI-Agent-Identities) beschleunigen die Möglichkeiten Ihres Unternehmens für Zusammenarbeit, Innovationen und Produktivität. Sie stellen aber auch einen schnell wachsenden und größtenteils unüberwachten Vektor dar, der zu Angriffen einlädt.

Einheitliches Identity-Management beseitigt diesen blinden Fleck, da Sie einen umfassenden Überblick über nicht-menschliche Identities in Ihrem gesamten Tech-Stack erhalten und somit wissen, wo sich diese Identities befinden und worauf sie zugreifen können. Durch diese neue Transparenz können Sie deren Autorisierungen überwachen, die Zugriffsrechte auf wichtige Ressourcen mit feingranularen Kontrollen verwalten und diese nicht-menschlichen Identities in eine wirklich umfassende Identity-Sicherheitsstrategie integrieren, die auf dem Least-Privileged-Prinzip basiert.

Die Vorteile von Okta

Identity Security Posture Management

- Erkennung nicht-menschlicher Identities und zentraler Überblick darüber, unter welchen Bedingungen bzw. wann sie auf welche Ressourcen zugreifen können
- Festlegen granularer Berechtigungen für nicht-menschliche Identities, um die Angriffsfläche zu reduzieren



Vorteil 5

Bestmögliche Nutzung Ihrer Technologie- und Sicherheitsinvestitionen

Die Interkonnektivität Ihres Tech-Stacks ist das Medium, durch das die Technologie-Investitionen Mehrwert für das Unternehmen generieren. Ohne umfassende, nahtlose Integrationen zwischen den zahlreichen Komponenten Ihres Tech-Stacks können Sie Ihre Technologie- und Sicherheitsinvestitionen nicht optimal nutzen und nicht den vollen ROI erreichen.

Das gilt ganz besonders für Ihre Sicherheitstools: Jede Lösung generiert enorme Mengen an Daten und Signalen. Doch wenn diese Signale isoliert bleiben, sind keine zuverlässigen und flexiblen Reaktionen auf Bedrohungen möglich. Zudem sind Sie auch nicht auf die aktuellen Anforderungen vorbereitet, die den Schutz der vertraulichen internen System und die Bereitstellung sicherer Customer Experiences verlangen.

Mit einer einheitlichen Identity-zentrierten Sicherheitsstrategie können Sie das volle Potenzial Ihres erweiterten Sicherheits- und Tech-Stacks nutzen, da diese Signale in einer zentralen Plattform zusammengeführt werden, die kontinuierlich Ihre Sicherheitslage evaluiert, den Zugriff für Anwendungen und Systeme verwaltet, Kundenidentitäten schützt und automatische Behebungsstrategien festlegt.

Kundenreferenzen

HubSpot
80 % der Tickets zu Zugriffsanfragen werden jetzt automatisiert bearbeitet

Delivery Hero
Durch Vermeidung von Ausfallzeiten 28.800 Stunden Produktivität gewonnen

TakedaID
Identity-Bereitstellung mit Okta fünfmal schneller als bei einer internen Lösung

Identity-gestützte Lösungen, die Ihre Anforderungen heute und auch in Zukunft erfüllen

Diese fünf Vorteile sind mehr als nur schmissig klingende Schlagwörter für das Sicherheitshandbuch Ihres Unternehmens. Sie sind wichtige Bedingungen für die Sicherheit und den Erfolg Ihres Unternehmens. Angesichts einer Risikolandschaft, die durch immer raffiniertere Bedrohungen und neue KI-gestützte Angriffsmethoden geprägt ist, führt der sicherste Weg zu einem resilienten und sicheren Unternehmen über einen einheitlichen Identity-zentrierten Sicherheitsansatz.

Warum? Weil Identity-Sicherheit *gleichbedeutend* mit Unternehmenssicherheit ist und als Grundlage für jede moderne Strategie für Unternehmensschutz dienen sollte. Um dieses Versprechen einer besseren Sicherheit einhalten zu können, müssen Sie jedoch die Identity-Fragmentierung hinter sich lassen, durch die Risiken übersehen werden können (und Geschäftswert verloren gehen kann). Ein einheitlicher Identity-zentrierter Sicherheitsansatz trägt nicht nur dazu bei, dass Unternehmen den immer schnelleren Bedrohungen einen Schritt voraus bleiben, sondern unterstützt auch die nahtlosen und reibungslosen IT-Umgebungen, die für Wettbewerbsfähigkeit unverzichtbar sind.

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

okta

Okta GmbH
Salvatorplatz 3
80333 München, Germany
info_germany@okta.com
+49 (89) 2620 3329