E-Book

Mit zuverlässigem Identity-Management lässt sich alles schützen

Die drei Prinzipien einer modernen Identity-Strategie für Mitarbeitende, Maschinen und KI

okta

Woran denkt man in Ihrem Unternehmen bei Identity-Management zuerst?

Für viele ist die erste Antwort: Sicherheit. Dafür gibt es gute Gründe. In einer Bedrohungslandschaft, die wesentlich von Anmeldedatendiebstahl, Phishing, Session Hijacking und der rapiden Zunahme autonomer Systeme geprägt wird, ist die Identität zur primären Angriffsfläche geworden. Damit verschaffen sich Angreifende Zugriff auf sensible Systeme, erweitern ihre Berechtigungen und bewegen sich lateral durch Umgebungen.

Heute bezieht sich Identität nicht mehr allein auf Mitarbeitende und Kund:innen, sondern umfasst nicht-menschliche Identitäten, Service-Accounts, Workloads, APIs und KI-Agenten, die im Namen von Benutzenden handeln. Da Unternehmen im großen Umfang KI-gestützte Systeme und Automatisierungen einführen, wächst die Anzahl der Identitäten, die Governance und Kontrolle erfordern, sehr schnell.

Viele Unternehmen hinken jedoch immer noch hinterher und bleiben an veraltete Perimeter-basierte Sicherheitsmodelle gefesselt, die sich auf Netzwerk- und Gerätekontrollen beschränken, aber keinen adäquaten Schutz vor Identity-zentrierten Bedrohungen bieten. Aufgrund der fragmentierten Übersicht über menschliche, nicht-menschliche und KI-basierte Identitäten können Security-Teams nur reagieren, anstatt Richtlinien proaktiv durchzusetzen.

KI beschleunigt die Herausforderungen für das Identity-Management

Da Unternehmen autonome KI-Agenten und automatisierte Workflows einsetzen, agieren Systeme zunehmend im Namen der Benutzenden. Diese Agenten rufen Daten ab, führen Aufgaben aus und interagieren in Maschinengeschwindigkeit mit mehreren Anwendungen. Ohne eine einheitliche Identity-Ebene zur Steuerung dieser Aktionen riskieren Unternehmen, eine neue Klasse von nicht verwalteten Identitäten zu schaffen, die außerhalb der traditionellen Sicherheitskontrollen agieren.

Definition einer modernen Identity-Strategie

Eine moderne Identity-Strategie etabliert die Identität als zentrale Kontrollebene in Ihrem gesamten Technologie-Ökosystem. Sie bietet einen einheitlichen Überblick über menschliche, nicht-menschliche und KI-gesteuerte Aktivitäten, identifiziert Schwachstellen, bevor sie ausgenutzt werden, und ermöglicht Echtzeit-Reaktionen auf neue Risiken.

Damit können auch Unternehmen sicher skalieren. Angesichts von KI-Agenten, -Services und -Anwendungen, die immer autonomer agieren, muss Identity-Management das Least-Privilege-Prinzip und richtlinienbasierte Zugriffe kontinuierlich durchsetzen.

Dieses E-Book erklärt, warum das Identity-Management im KI-Zeitalter das Fundament für Unternehmenssicherheit bildet, und geht auf folgende Themen ein:

- Wie Identity-zentrierte Bedrohungen sich entwickeln und beschleunigen
- Warum klassische Identity-Management-Ansätze Unternehmen gefährden
- Die drei Prinzipien einer modernen Identity-Strategie

Die Fragmentierung der Sicherheitstechnologien in Unternehmen

Der Tech-Stack von Unternehmen hat sich in den letzten 10 Jahren grundlegend verändert. Cloud-Services, SaaS-Anwendungen, APIs und Remote-Arbeit haben die Entwicklung und Prozesse in Unternehmen transformiert. Heute beschleunigen KI-Agenten und automatisierte Systeme diese Veränderungen noch weiter. Anwendungen vernetzen sich nicht nur, sie agieren auch. Services speichern nicht nur Daten, sie führen auch Aufgaben aus. KI-Systeme rufen Informationen ab, lösen Workflows aus und treffen systemübergreifende Entscheidungen.

In dieser Umgebung ist der Ansatz mit einer einheitlichen technischen Umgebung unter einer einzigen Enterprise-Lizenz nicht mehr realistisch. Unternehmen bauen Ökosysteme mit erstklassigen Lösungen auf, um wettbewerbsfähig zu bleiben und schnell agieren zu können. Das Ergebnis ist eine leistungsstarke und flexible Infrastruktur, die aber gleichzeitig immer komplexer wird.

Moderne Tech-Stacks sind stark verteilt und umfassend vernetzt. Alle neuen Anwendungen, Services, APIs, Workloads und KI-Agenten führen neue Identitäten ein, die über Cloud- und On-Premise-Umgebungen, SaaS-Plattformen, kundenspezifische Anwendungen und Infrastrukturen hinweg aktiv sind. Ohne zentrale Kontrolle fragmentiert sich das Identity-Management zu einem verworrenen Netz aus Systemen und Umgebungen.

Isolierte Technologien führen zu blinden Flecken bei der Sicherheit

Fragmentierung führt zu schwerwiegenden Sicherheitslücken. Menschliche Identitäten, Service-Accounts, Maschinenidentitäten und KI-Agenten befinden sich oft in getrennten Systemen mit inkonsistenten Richtlinien und unvollständiger Aufsicht. Dies vergrößert die Angriffsfläche und erhöht die Wahrscheinlichkeit für unbemerkten Anmeldedatendiebstahl, Token-Missbrauch und Rechteausweitung.

Security-Teams haben Schwierigkeiten, einen einheitlichen Überblick über diese Landschaft zu erhalten, da Protokolle verteilt und Richtlinien inkonsistent sind und nicht-menschliche Identitäten sich schneller vermehren, als sie verwaltet werden können. Hinzu kommt, dass KI-Systeme immer autonomer agieren, sodass Unternehmen nun auch Kontrollen mit Maschinengeschwindigkeit durchsetzen müssen.

Viele KI-Agenten und automatisierte Services arbeiten mit dauerhaften Anmeldedaten und umfassendem Zugriff auf mehrere Systeme. Wenn diese Identitäten nicht richtig erkannt und verwaltet werden, können sie auch lange nach dem Ende ihres eigentlichen Zwecks noch über privilegierte Berechtigungen verfügen. Dadurch entsteht ein wachsender Pool von Identitäten, die über umfangreiche Berechtigungen verfügen und systemübergreifend mit geringer Aufsicht agieren. Gleichzeitig nehmen sowohl die Angriffsfläche als auch die potenziellen Auswirkungen einer Sicherheitsverletzung zu.

Angreifenden ist dieser Wandel bewusst. Identitäten sind zum primären Angriffsvektor geworden, da sie der am wenigsten vereinheitlichte Kontrollpunkt sind. Laut dem Verizon Data Breach Report 2024, an dem Okta teilgenommen hat, sind bei 80 % aller Kompromittierungen in irgendeiner Form kompromittierte Identitäten beteiligt. Die durchschnittliche Zeit bis zur Erkennung und Eindämmung einer Sicherheitsverletzung beträgt weiterhin fast 290 Tage.

Ein neuer Ansatz für Identity-Management ist erforderlich

Jedes Unternehmen ist sich der großen Bedeutung von Identity-Management für die Sicherheit bewusst. Allerdings nutzen sie es meist nur für Authentifizierung und Zugriffskontrollen und nur selten für einen ebenso wichtigen Bereich: als zentrale Kontrollebene für unternehmensweite Transparenz, Governance und zur Richtliniendurchsetzung für menschliche und nicht-menschliche Identitäten.

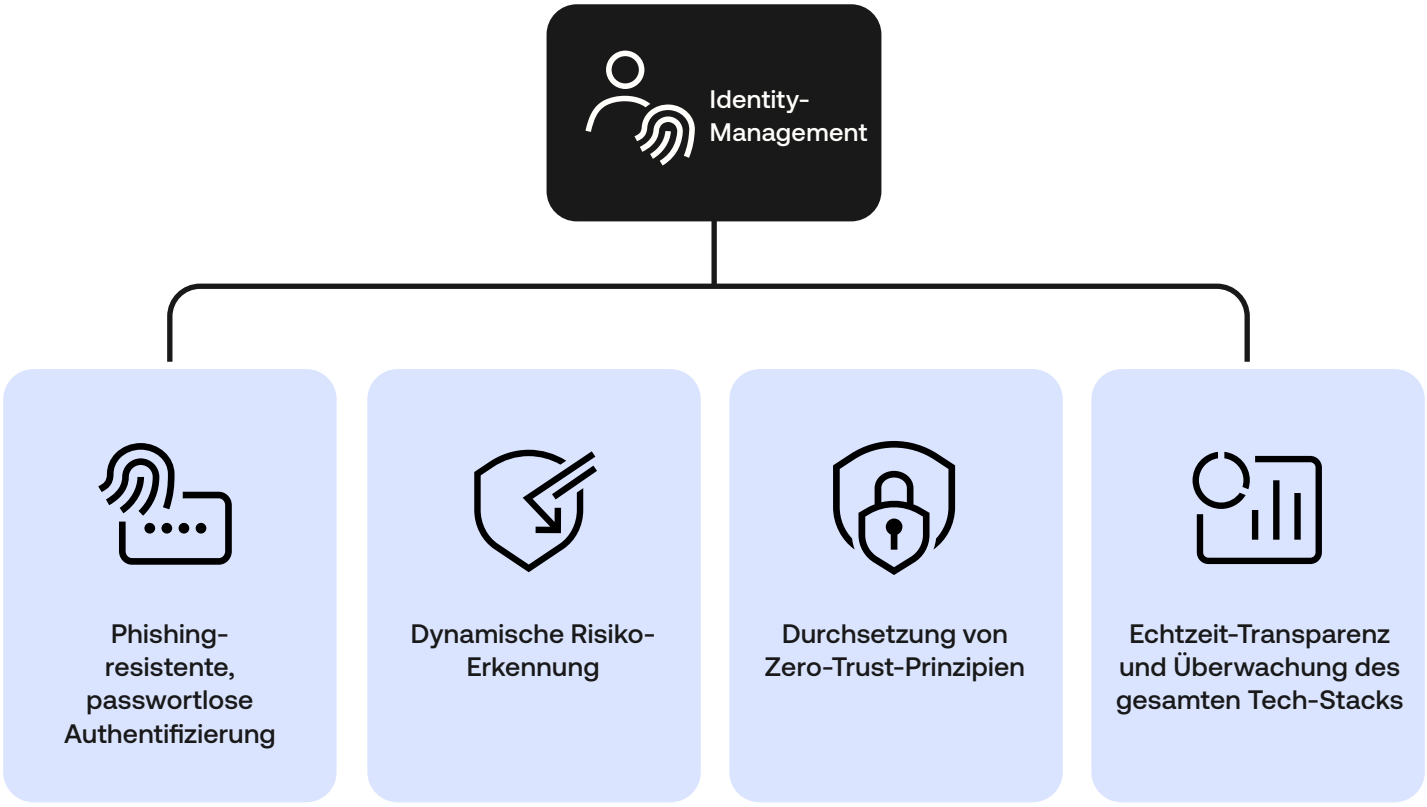
Die meisten Unternehmen nutzen Identity-Management beispielsweise für die Authentifizierung sicherer Zugriffe. Doch wenn die Identity-Management-Funktionen tiefer in die Technologie- und Sicherheitsökosysteme integriert sind, können sie auch nach der Anmeldung kontinuierliche Risikobewertung, Echtzeit-Richtliniendurchsetzung sowie automatisierte Behebungen ermöglichen. In Umgebungen, in denen KI-Agenten und automatisierte Systeme im Namen von Benutzenden agieren, muss das Identity-Management nicht nur überprüfen, wer auf ein System zugreift, sondern auch, was als Nächstes geschehen darf.

Zentralisiertes Identity-Management für das gesamte Sicherheitsökosystem

Wer dieses Potenzial ignoriert, übersieht das Offensichtliche: Identität hat sich zur primären Angriffsfläche im Bereich der Enterprise-Cybersicherheit entwickelt. Angreifende erlangen darüber Erstzugriff, eskalieren Berechtigungen und bewegen sich durch verschiedene Umgebungen. Und mithilfe von Identitäten können Unternehmen verantwortliche Benutzende festlegen, das Least-Privilege-Prinzip durchsetzen und Kontrolle im großen Maßstab gewährleisten.

Eine moderne Identity-Strategie dient als Verbindungsebene in Ihrem gesamten Sicherheits- und Technologie-Ökosystem und vereinheitlicht Transparenz, Governance und Durchsetzung. Sie stärkt die Sicherheit nicht nur bei der Anmeldung, sondern bei jeder Interaktion – unabhängig davon, ob sie von einer Person, einem Service oder einem KI-Agenten initiiert wurde.

Unternehmen können heutigen Anforderungen nur mit einem umfassenden und strategischen Blick auf die Identität und ihre Berechtigungen gerecht werden.



Ein genauerer Blick auf die Bedrohung

Angreifer setzen darauf, dass Unternehmen veraltete Identity-Ansätze nutzen. Bei fragmentierten IT- und Sicherheitsumgebungen sind wichtige Ressourcen, Anwendungen und Identitäten über verschiedene Systeme und Infrastrukturen verteilt, sodass Angriffe auf menschliche und nicht-menschliche Identitäten leicht übersehen werden können. Da KI-Agenten und automatisierte Systeme auf immer mehr Daten zugreifen und mehr Aktionen ausführen, werden die Folgen schwacher Identitätskontrollen immer gravierender.

Manuelle Prozesse

Umständliche, zeitaufwändige Berechtigungsverfahren machen Zugriffsentscheidungen anfällig für menschliche Fehler und führen zu inkonsistenter Richtliniendurchsetzung.

Blinde Flecken

Die Einblicke in die Echtzeit-Sicherheitslage, das Identity-Verhalten und die Berechtigungen von Benutzenden, Services, Workloads und KI-Agenten sind begrenzt.

Lange Reaktionszeiten

Angreifende oder nicht autorisierte automatisierte Prozesse nutzen verzögerte Erkennung und Behebung aus, um Identity-bezogene Schwachstellen auszunutzen, bevor Kontrollen eingreifen können.

Dieses Problem wird nicht von selbst verschwinden, sondern im Gegenteil immer schneller wachsen. KI-gestützte Anwendungen, Services, nicht-menschliche Identitäten und KI-Agenten erweitern die Identity-Angriffsfläche und erhöhen die Geschwindigkeit, mit der Aktionen ausgeführt werden. Identity-bezogene Angriffe beschränken sich nicht mehr auf gestohlene Anmeldedaten: Bedrohungen nach der Authentifizierung (z. B. gestohlene Session-Cookies, Token-Replay und Rechteausweitung) stellen Security-Teams, die verteilte Umgebungen überwachen, vor neue Herausforderungen.

Hinzu kommen Risiken durch kapitalkräftige staatlich unterstützte Angreifergruppen, Insider-Bedrohungen und nicht verwaltete autonome Systeme, sodass sich eine sich schnell entwickelnde Bedrohungslandschaft ergibt, in deren Mittelpunkt die Identität steht.

91 %

91 % aller Unternehmen setzen KI-Agenten ein, aber nur 10 % verfügen über eine Strategie für deren Verwaltung.

(Okta)

80 %

Über 80 % aller Data Breaches werden von Identity-basierten Angriffen verursacht.

(Verizon)

180 %

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

(Verizon)

1,9 Mrd.

1,9 Milliarden Session-Cookies wurden 2023 bei Mitarbeitenden von Fortune 1000-Unternehmen gestohlen.

(Fortune)

Identity-Management bedeutet Sicherheit

Die Risikolandschaft besteht aus unzähligen Bedrohungen, die Identitäten ausnutzen. Da Unternehmen die Nutzung von Cloud-Services, nicht-menschlichen Identitäten und KI-Agenten ausweiten, wird die Identität sowohl zur primären Angriffsfläche als auch zum primären Kontrollpunkt.

Die Identität ist jedoch nicht nur ein Risikofaktor, sondern auch eine hervorragende Möglichkeit zur Durchsetzung von Kontrollen. Wenn Unternehmen die Identität in den Mittelpunkt ihrer Sicherheitsstrategie stellen, können sie von der reaktiven Abwehr zur kontinuierlichen Durchsetzung übergehen und Zugriffe sowie automatisierte Aktionen überprüfen, bevor Risiken zu Schäden führen.

Durch einheitliches Identity-Management für Mitarbeitende, Services und KI-Agenten können Sie Sicherheitsverletzungen verhindern und den Wert Ihrer Sicherheits- und Technologie-Investitionen maximieren.

Die drei Prinzipien einer modernen Identity-Strategie

Nachdem wir aufgezeigt haben, warum ein Identity-zentrierter Sicherheitsansatz wichtig ist, sehen wir uns nun die praktische Seite an: Wie können Sie das aktuelle Identity-Management Ihres Unternehmens so umgestalten, dass es der KI-zentrierten Welt gerecht wird?

Moderne, Cloud-native Identity-Plattformen stellen eine Möglichkeit dar, die Fragmentierung zu reduzieren und die Kontrolle zu zentralisieren. Sie bieten einheitliche Echtzeit-Transparenz zu menschlichen und nicht-menschlichen Identitäten, Services und KI-Agenten, wodurch IT- und Security-Teams in die Lage versetzt werden, blinde Flecken zu beseitigen, Risiken aufzudecken und schneller zu reagieren.

Dieser Vorteil lässt sich in drei Kernprinzipien unterteilen:

Vollständige Transparenz

Stellt sicher, dass Schwachstellen bei Benutzenden, nicht-menschlichen Identitäten oder KI-Agenten nicht unbemerkt oder unbeachtet bleiben.

Leistungsstarke Orchestrierung

Erzwingt Echtzeit-Korrekturen und einheitliche richtlinienbasierte Kontrollen für Systeme, Services und automatisierte Workflows.

Umfassende und starke Integrationen

Verbindet das Identity-Management in Ihrem gesamten Sicherheits- und Technologie-Ökosystem, um einheitliche Governance und Durchsetzung zu ermöglichen.

Wenn Unternehmen die Marktangebote evaluieren, sollten sie sich für eine Plattform entscheiden, die alle drei Prinzipien erfüllt.

Prinzip 1

Vollständige Transparenz

Die individuelle Verwaltung von Zugriffsberechtigungen für Anwendungen, Services und Systeme schafft ausnutzbare Sicherheitslücken und führt zur inkonsistenten Durchsetzung von Richtlinien. Da die Zahl der nicht-menschlichen Identitäten und KI-Agenten wächst, weiten sich diese Lücken über Benutzer-Accounts hinaus auf APIs, Workloads und automatisierte Prozesse aus.

Eine moderne Identity-Plattform muss das Management des Zugriffslebenszyklus zentralisieren und vereinfachen und gleichzeitig eine umfassende Echtzeitansicht der Identity-Aktivitäten in Ihrer Umgebung bereitstellen. Sie sollte eine einheitliche Übersicht über menschliche Identitäten, Service-Accounts, Workloads und KI-Agenten bieten, damit Teams Schwachstellen frühzeitig erkennen und Richtlinien im großen Maßstab konsistent durchsetzen können.

Grundlegende Funktionen

Zugriffskontrolle und Lebenszyklusverwaltung

Zentrale Provisionierung und Deprovisionierung für mehrere verschiedene Systeme, Automatisierung von Joiner-Mover-Leaver-Prozessen und kontinuierliche Zertifizierung der Zugriffe für Benutzende und nicht-menschliche Identitäten

Sicherheits- und Bedrohungsübersicht

Überwachung der Identity-Konfigurationen, Erkennung von Konfigurationsfehlern und Bereitstellung von Echtzeit-Einblicken in Identity-bezogene Risiken bei Anwendungen, Infrastruktur und KI-gestützten Systemen

Kontrollen für privilegierte und sensible Zugriffe

Schutzmaßnahmen für Identitäten mit umfangreichen Berechtigungen, einschließlich Administratorkonten, Service-Accounts und KI-Agenten

Kontinuierliche Risikobewertung

Echtzeitüberwachung und Signalaggregation, damit verdächtige Aktivitäten von Benutzenden und automatisierten Systemen schnell erkannt und abgewehrt werden können

Checkliste der erforderlichen Funktionen

- ☐ Einblick in Bedrohungen durch Benutzende, nicht-menschliche Identitäten, KI-Agenten und Kunden-Accounts
- ☐ Einbeziehung von Drittanbieter-Signalen aus dem gesamten Tech-Stack für umfassenden Echtzeitüberblick über Bedrohungen
- ☐ Kontinuierliche Bewertung des Identity-Standings anhand der Zero-Trust-Prinzipien
- ☐ Identifizierung von Konfigurationsfehlern, z. B. uneinheitliche MFA-Durchsetzung, Account-Wildwuchs und übermäßig privilegierte Service-Accounts
- ☐ Automatische Provisionierung und Deprovisionierung, wenn Mitarbeitende die Rolle ändern oder nicht-menschliche Identitäten nicht mehr benötigt werden
- ☐ Durchsetzung granularer Zugriffskontrollen für privilegierte Benutzende, Services und KI-Agenten
- ☐ Erkennung nicht-menschlicher Identitäten und Überwachung ihrer Berechtigungen und ihres Verhaltens
- ☐ Integration mit HR-Systemen und Verzeichnissen für eine zentrale Identity-Lebenszyklusverwaltung
- ☐ Verwaltung und Absicherung von Kundenidentitäten im großen Maßstab

Prinzip 2

Leistungsstarke Orchestrierung

Fragmentierte Sicherheitstechnologien generieren enorme Mengen an Risikodaten. Ohne eine einheitliche, Identity-orientierte Kontrollebene zur Analyse und Reaktion auf diese Daten müssen die Teams Protokolle systemübergreifend korrelieren und können erst reagieren, nachdem der Schaden bereits entstanden ist. Das Ergebnis ist eine langsame Sicherheitsstruktur, die mit automatisierten Workflows, nicht-menschlichen Identitäten und KI-Agenten, die mit Maschinengeschwindigkeit arbeiten, nicht Schritt halten kann.

Eine moderne Identity-Plattform muss Unternehmen die Möglichkeit bieten, Bedrohungen in Echtzeit zu verhindern, zu erkennen und zu beheben. Neben einer Übersicht muss sie Risikoindikatoren in automatisierte Durchsetzungsmaßnahmen umwandeln und gewährleisten, dass verdächtiges Verhalten von Benutzenden, Service-Accounts oder KI-Agenten sofort bewertet und kontrolliert wird.

Checkliste der erforderlichen Funktionen

- ☐ Vereinfachung der Konfiguration automatisierter Maßnahmen zur Behebung und Richtliniendurchsetzung
- ☐ Anpassung der Reaktionen auf Risikosignale, Kontextdaten und dynamische Richtlinien
- ☐ Auslösung von Schutzmaßnahmen wie Step-up-Authentifizierung, Session-Sperrungen oder Universal Logout
- ☐ Integration Phishing-resistenter Authentifizierungsmethoden, um den kontinuierlichen Schutz zu stärken
- ☐ Bewertung des Gerätestatus und des kontextbezogenen Risikos während aktiver Sessions
- ☐ Blockierung gefährlicher IP-Adressen oder ungewöhnlicher Aktivitäten in Echtzeit
- ☐ Implementierung sicherer Self-Service-Wiederherstellung von Authentifizierungsfaktoren, ohne die Sicherheitskontrollen zu schwächen
- ☐ Kontinuierliche Bewertung der Identitätsaktivitäten nach der Authentifizierung, einschließlich automatisierter und KI-gesteuerter Aktionen

Prinzip 3

Umfassende und starke Integrationen

Ihr Technologie-Ökosystem ist nur so stark wie die Verbindungen zwischen seinen Komponenten. Ohne die nahtlose Integration von Anwendungen, Infrastruktur, Sicherheitstools, APIs und KI-Systemen haben Unternehmen Schwierigkeiten, konsistente Identity-Kontrollen durchzusetzen und den vollen Mehrwert ihrer Investitionen zu realisieren.

Eine moderne Identity-Plattform muss jeden Teil der Umgebung verbinden, um konsistente Governance, Risikoüberwachung und Durchsetzung zu ermöglichen. Anbieterneutrale Identity-Plattformen ermöglichen die Vereinheitlichung von menschlichen und nicht-menschlichen Identitäten über SaaS, Cloud, benutzerdefinierte Anwendungen und KI-gesteuerte Systeme hinweg, ohne IT- und Entwicklungsteams mit unnötigem Integrationsaufwand zu belasten.

Checkliste der erforderlichen Funktionen

- ☐ Integration mit zentralen Enterprise-SaaS-Anwendungen für CRM, Produktivität, Zusammenarbeit, ERP, IT-Ablaufverwaltung usw.
- ☐ Erweiterung des Identity-Schutzes über Provisionierung und Single Sign-On hinaus, um Kontrollen vor, während und nach der Authentifizierung durchzusetzen
- ☐ Integration mit Sicherheitstools in Ihren gesamten Stack, um Bedrohungserkennung, Risikobewertung und automatisierte Behebung zu verbessern
- ☐ Unterstützung von APIs, Services und KI-Agenten mit konsistenter Identity Governance und Richtliniendurchsetzung
- ☐ No-Code- oder Low-Code-Automatisierungsfunktionen, um systemübergreifend sichere Workflows auszulösen
- ☐ Erweiterbarkeit zur Unterstützung neuer Anwendungen, Services und KI-Funktionen, wenn sich Ihre Umgebung weiterentwickelt

Vorteile einer einheitlichen Sicherheitsstrategie

Einheitliche, Identity-zentrierte Sicherheit ist nicht mehr nur ein Konzept. In der Praxis liefert sie messbare Ergebnisse, die den Schutz stärken, betriebliche Abläufe optimieren und es Unternehmen ermöglichen, in einer komplexeren Umgebung sicher zu skalieren.

Identity-Sicherheit und Kompromittierungsschutz

Stärken Sie Ihre Sicherheitslage, indem Sie jede menschliche und nicht-menschliche Identität schützen, sodass Sie Identity-zentrierte Bedrohungen erkennen, eindämmen und beheben können, bevor sie zu Sicherheitsverletzungen führen.

Operative Effizienz und Resilienz

Vereinfachen Sie Abläufe und reduzieren Sie die Komplexität, indem Sie fragmentierte Identity-Management-Systeme in einer einheitlichen Kontrollebene zusammenführen, die die Agilität verbessert, den betrieblichen Aufwand senkt und die Zeit bis zur Wertschöpfung verkürzt.

KI-Erkennung und -Kontrolle

Implementieren Sie Governance für KI-Agenten und automatisierte Systeme, indem Sie zentrale Transparenz, Richtliniendurchsetzung und sichere Zugriffskontrollen für neue KI-gesteuerte Workflows bereitstellen.

Hier erfahren Sie mehr über die Vorteile einer einheitlichen Sicherheitsstrategie.

Der Weg zu Identity-zentrierter Sicherheit

Vollständig umgesetzte Identity-zentrierte Sicherheit unterstützt ein offenes Ökosystem, das das Erstellen, Verbinden und Betreiben von Anwendungen, Services und automatisierten Systemen standardmäßig sicher und kontrollierbar macht – ohne Identity-Silos.

Das bedeutet auch, dass keine kostspieligen und zeitaufwändigen kundenspezifischen Integrationen mehr notwendig sind. Es gibt auch keine Sicherheitslücken und blinden Flecken bei Mitarbeitenden, Kund:innen und maschinengestützten Umgebungen mehr. Der einheitliche Identity-basierte Tech-Stack ermöglicht einheitliche Governance und Richtliniendurchsetzung für jede Interaktion.

Mit zuverlässigem Identity-Management lässt sich alles schützen

Es kann nicht genug betont werden, dass zuverlässiges Identity-Management gleichbedeutend ist mit Sicherheit. Damit IT- und Sicherheitsverantwortliche Bedrohungen immer einen Schritt voraus sind und robusten, langfristigen Schutz aufbauen können, müssen sie die Verwaltung, Durchsetzung und Integration von Identitäten in ihren Umgebungen modernisieren.

Mit einheitlichem Identity-Management von Personen, nicht-menschlichen Identitäten und automatisierten Systemen reduzieren Unternehmen Risiken, stärken die operative Kontrolle und ermöglichen sichere Innovationen im großen Maßstab. Eine starke Identity-Basis schützt vor immer raffinierteren Angriffen und gewährleistet gleichzeitig die Agilität, die in heutigen verteilten und KI-gestützten Umgebungen erforderlich ist.

Wenn Sie Ihre Identity-Management-Strategie voranbringen und gezielte Empfehlungen von Okta-Fachleuten erhalten möchten, können Sie hier mehr erfahren oder sich mit unserem Team in Verbindung setzen.

Über Okta
Okta ist das weltweit führende Identity-Unternehmen. Wir schützen die Identität von KI-Agenten, Maschinen und menschlichen Benutzenden, damit unsere Kundinnen und Kunden sowie Partner jede Technologie sicher nutzen können. Unsere Lösungen unterstützen Unternehmen sowie Entwicklungsteams dabei, die Sicherheit und Effizienz zu steigern und die Ziele zu erreichen. Gleichzeitig werden Benutzende, Mitarbeitende sowie Partner zuverlässig geschützt. Weltweit führende Marken vertrauen bei Authentifizierung, Autorisierung und mehr auf Okta. Weitere Informationen finden Sie unter okta.com/de.

okta

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