www.security-insider.de

SECURITY INSIDER

Identitätssicherheit 360°

Ganzheitlicher Schutz für moderne Unternehmen

Powered by:

okta

Liebe Leserinnen und Leser,

in der heutigen, schnelllebigen Welt ist die digitale Transformation nicht mehr nur eine Möglichkeit – sie ist eine Notwendigkeit. Unternehmen, Organisationen und Anwender müssen zunehmend auf Cloud-Technologien setzen, um wettbewerbsfähig zu bleiben und den Anforderungen der modernen Arbeitswelt gerecht zu werden. Die Cloud bietet nicht nur enorme Flexibilität und Effizienz, sondern auch die Chance, Innovationen schneller voranzutreiben und neue Geschäftsmodelle zu realisieren.

Doch mit der zunehmenden Digitalisierung und der Verlagerung von Daten und Prozessen in die Cloud steigen auch die Herausforderungen in Bezug auf Sicherheit. Datenschutz, Datensouveränität und der Schutz vor Cyberangriffen sind Themen, die heutzutage nicht nur auf der Agenda von IT-Abteilungen,

sondern auch auf strategischer Ebene in den Führungsetagen von Unternehmen ganz oben stehen müssen.

Eine der größten Hürden im digitalen Zeitalter ist dabei die Frage der Authentifizierung. Wie stellen wir sicher, dass nur berechtigte Nutzer auf kritische Systeme zugreifen können – und das auf einfache und zugleich sichere Weise? Klassische Authentifizierungsmechanismen stoßen schnell an ihre Grenzen, wenn es darum geht, den Anforderungen einer zunehmend mobilen und verteilten Arbeitswelt gerecht zu werden.

Deshalb sind innovative Lösungen wie die von Okta unerlässlich. Sie bieten Unternehmen die Möglichkeit, eine sichere und skalierbare Identitäts- und Zugriffsverwaltung zu implementieren, die den Schutz sensibler Daten gewährleistet und gleichzeitig die Nutzerfreundlichkeit und Flexibilität fördert. In diesem eBook werfen wir einen Blick auf die entscheidende Rolle von modernen Authentifizierungslösungen in der digitalen Transformation und zeigen auf, warum es für Unternehmen unerlässlich ist, auf fortschrittliche Sicherheitslösungen zu setzen.

Ich lade Sie ein, die folgenden Seiten zu entdecken und mehr darüber zu erfahren, wie Sie die digitale Zukunft Ihres Unternehmens mit der richtigen Authentifizierungsstrategie sicher und erfolgreich gestalten können.

Mit besten Grüßen

Arkadiusz Krowczynski
Senior Solution Engineer, Okta

Inhalt

Powered by:

okta

Okta Inc.
Salvatorplatz 3
80333 München
Telefon +49 (89) 2620-3329
E-Mail support@okta.com
Web www.okta.de

Vogel IT-Medien GmbH
Max-Josef-Metzger-Str. 21, 86157 Augsburg
Telefon +49 (0) 821/2177-0
E-Mail redaktion@security-insider.de
Web www.Security-Insider.de
Geschäftsführer: Tobias Teske, Günter Schürger
Chefredakteur: Peter Schmitz, V.i.S.d.P., peter.schmitz@vogel.de
Erscheinungstermin: Dezember 2024
Titel: XXX/stock.adobe.com – KI-generiert

Haftung: Für den Fall, dass Beiträge oder Informationen unzutreffend oder fehlerhaft sind, haftet der Verlag nur beim Nachweis grober Fahrlässigkeit. Für Beiträge, die namentlich gekennzeichnet sind, ist der jeweilige Autor verantwortlich.
Copyright: Vogel IT-Medien GmbH. Alle Rechte vorbehalten. Nachdruck, digitale Verwendung jeder Art, Vervielfältigung nur mit schriftlicher Genehmigung der Redaktion.

VOGEL IT MEDIEN

Worauf sich das Identitätsmanagement jetzt einstellen muss

Die digitale Identität steht im Zentrum der Digitalisierung, denn sie repräsentiert die Beschäftigten, die Kunden, die Administratoren, aber auch die Geräte, die Clouds, die Applikationen und die KI-Agenten. Cyberkriminelle sind sich dieser Bedeutung von Identity sehr bewusst, die meisten Cyberattacken starten mit dem Versuch des Identitätsdiebstahls. Eine erfolgreiche und sichere Digitalisierung ist deshalb nur möglich, wenn das Identity Management für diese Bedrohungen gerüstet ist.

Hohe Anforderungen an digitale Identitäten

Wenn man von dem Management digitaler Identitäten spricht, sind eine Vielzahl von Aufgaben damit gemeint: Identitätslösungen umfassen Technologien zur Bestätigung und Verifizierung einer Identität, zur Bestimmung der Zugriffsberechtigung und des Handlungsrahmens einer Identität sowie zur Definition der Richtlinien und Prozesse, die zur Verwaltung von Identitäten innerhalb der Netzwerke und Systeme eines Unternehmens angewandt werden. Dabei müssen zahlreiche gesetzliche und technische Anforderungen erfüllt werden, zum Beispiel an die Sicherheit, aber auch an die Unterstützung der genutzten Clouds und Apps.

Den meisten Unternehmen ist es durchaus bewusst, dass sie ihre digitalen Identitäten zuverlässig verwalten müssen, doch die dafür eingesetzten Lösungen entsprechen nicht mehr den neuen Anforderungen. Das zeigen zum Beispiel die Entwicklungen bei Modern Work.

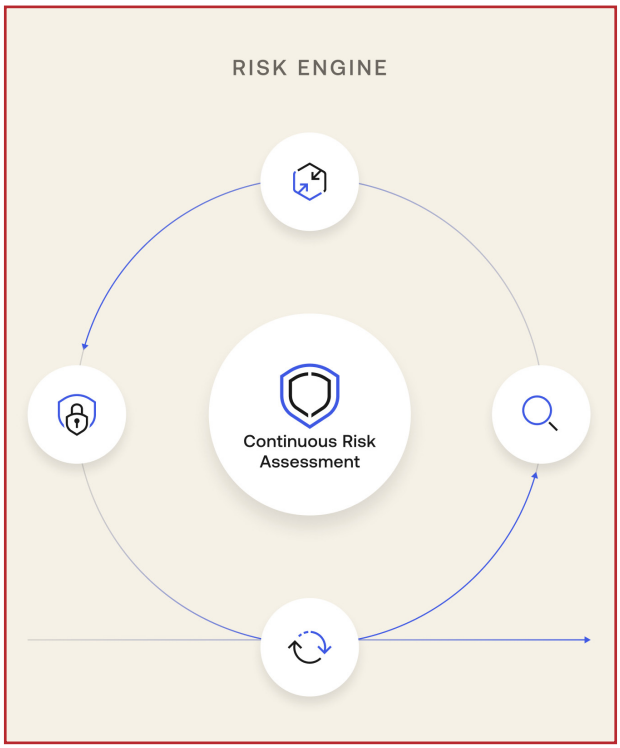
Beispiel: Das erfordert Modern Work im Identity Management

Die moderne Form des Arbeitens, oft auch Modern Work oder New Work genannt, ist standortunabhängig und flexibel. Die Beschäftigten des digitalen Zeitalters arbeiten zunehmend an mobilen Endgeräten und nutzen vermehrt Cloud-Applikationen. Alle notwendigen Funktionen des Identitätsmanagements müssen deshalb dezentral und auf allen Arten von Endgeräten verfügbar sein. Ebenso müssen neben den mobilen Apps auch die Cloud-Anwendungen unterstützt werden, also in das Identitätsmanagement integriert werden können. Identitäten und deren Überprüfung sowie die Bereitstellung und Kontrolle von Berechtigungen dürfen nicht auf die zentralen Anwendungen im Firmennetzwerk beschränkt sein, sie müssen übergreifend bei allen relevanten Applikationen angeboten werden können.

Neben der Offenheit und Integrationsfähigkeit benötigt die Identitätslösung aber auch eine hohe Sicherheit, denn die Beschäftigten sind >>

fortlaufend dem Risiko durch Cyberangriffe wie Phishing ausgesetzt. Die meisten Attacken der Internetkriminellen zielen auf digitale Identitäten ab und dienen dem Diebstahl und Missbrauch von Zugangsdaten und Berechtigungen. Tatsächlich sind 80 Prozent aller Cyberangriffe heutzutage auf irgendeine Art von Missbrauch von Anmeldedaten zurückzuführen.

Um die Beschäftigten und deren Identitäten (Workforce Identity) besser zu schützen, reichen die klassischen Verfahren wie VPN (Virtual Private Network) und MFA (Mehr-Faktor-Authentifizierung) nicht aus. Digitale Identitäten brauchen eine neue, intelligente und durchgehende Sicherheit.



Digitale Identitäten müssen zuverlässig vor Angriffen auch nach dem Login geschützt werden, etwa vor Session-Hijacking-Attacken. Die Risiko-Engine von Okta bewertet dynamisch User-, Device- und Kontext-Änderungen und ermöglicht so eine agile Neubewertung von Risiken in Echtzeit. (Bild: Okta)

Ende-zu-Ende-Sicherheit, auch und gerade für Identitäten

Genau wie die Verschlüsselung muss auch die Sicherheit digitaler Identitäten einen Ende-zu-Ende-Schutz haben. Es reicht also nicht, zum Beispiel bei der Anmeldung bei einem Cloud-Dienst oder einer Applikation die Identität zu Beginn zu prüfen. Vielmehr muss die Identitätsprüfung durchgehend stattfinden, also auch während der Dauer der Sitzung bis zur Abmeldung. Identitätssicherheit bedarf also der Kontrolle und Überprüfung vor, während und nach einer Authentifizierung.

Okta bietet dazu Identity Threat Protection mit Okta AI an, ein neues Produkt für die Okta Workforce Identity, das Echtzeiterkennung und -reaktion auf identitätsbasierte Bedrohungen bietet (siehe auch das nächste Kapitel). Es erweitert die Sicherheit über die anfängliche Authentifizierung hinaus auf jeden Zeitpunkt, an dem ein Benutzer angemeldet ist. Auf diese Weise können Administratoren und Sicherheitsteams das Benutzerrisiko während aktiver Sitzungen kontinuierlich bewerten und automatisch auf Identitätsbedrohungen in ihrer gesamten, an Okta angebundenen IT-Infrastruktur reagieren.

Klassisches MFA reicht nicht aus

Viele Unternehmen vertrauen auf einen (scheinbar) starken Identitäts- und Zugangsschutz mit MFA (Multi-Faktor-Authentifizierung), doch leider können klassische MFA-Verfahren inzwischen ausgetrickst werden. Multi-Faktor-Authentifizierung ist eine wichtige Säule im Kampf gegen identitätsbasierte Angriffe, doch ihre Wirksamkeit ist bei klassischen Verfahren oft auf den Anmeldepunkt beschränkt. Das wachsende Risiko von Bedrohungen während der Authentifizierung >>

– wie Session Hijacking, Adversary-in-the-Middle (AiTM) und MFA-Bypass-Angriffe durch Phishing – zwingt Unternehmen dazu, ihre identitätsbasierten Sicherheitsfunktionen über den Authentifizierungspunkt hinaus auszuweiten.

Eine moderne, zukunftssichere Identitätsmanagement-Lösung muss deshalb sogenanntes phishing-resistentes MFA bieten können: FastPass von Okta ist eine phishing-resistente, passwortlose Authentisierungstechnologie, die das Risiko von Phishing-Angriffen, Session-Diebstählen und unautorisierten lokalen Aktivitäten minimiert. Jedes Mal, wenn ein Anwender auf eine geschützte Ressource zugreift, überprüft FastPass den Kontext des Gerätes und bietet dabei über alle wichtigen Plattformen und Endgeräte hinweg – ob gemanagt oder nicht – durchgehend eine hochwertige Experience. FastPass erreicht durch die Kombination der biometrischen Features des Endgeräts mit den Faktoren Besitz und Inhärenz eine hohe Sicherheit. Anwender, deren Geräte keine biometrischen Daten unterstützen oder die andere Methoden bevorzugen, können sich alternativ für FastPass mit Passcodes entscheiden und so ebenfalls einen starken, phishing-resistenten MFA-Schutz gewährleisten.

Podcast-Tipp: Insider Research im Gespräch: Episode 221 „Wie Ihr Identity Management zukunftssicher wird“, mit Arkadiusz Krowczynski von Okta

Identity Management für alle Identitäten, auch die der Kunden

Das moderne Identitätsmanagement beschränkt sich aber nicht mehr auf die Beschäftigten und die Administratoren im Unternehmen, sondern es bezieht auch die digitalen Identitäten der Kunden mit ein, die Customer Identity.

Beim Customer Identity & Access Management (CIAM) geht es darum, dass Unternehmen ihren Kunden sicher und komfortabel den Zugang zu digitalen Ressourcen erschließen. Gleichzeitig müssen die Kundendaten zuverlässig geschützt werden.

Die Okta Identity Cloud eignet sich für Consumer- und SaaS-Apps unterschiedlicher Branchen. Die Okta Customer Identity Cloud für Consumer-Apps zum Beispiel hilft Unternehmen, die Registrierung und Anmeldung über alle Geräte und Plattformen hinweg zu optimieren, um eine höhere Kundengewinnung und -bindung, ein besseres Erlebnis und eine umfassendere Sicht auf die Benutzer zu erreichen. Von der Anmeldung und Profilerstellung bis hin zu erweiterten Sicherheitsfunktionen wie der adaptiven Multi-Faktor-Authentifizierung (MFA) haben Unternehmen alles, was sie brauchen, um Kundenidentitäten sicher zu managen. >>

Sichere Identitäten sind passwortlos

Im Zeitalter der Künstlichen Intelligenz, in dem die Bedrohungen zunehmen, sind Passwörter und herkömmliche Formen der MFA ebenso unpraktisch wie schutzlos, so die FIDO Alliance. Durch die Umstellung auf phishing-resistente Passkeys können Unternehmen ihre Kunden besser schützen. Entsprechend sollten moderne Lösungen für das Identitätsmanagement Passkeys unterstützen.

Passkeys sind ein Ersatz für Passwörter, der es Benutzern schneller und einfacher ermöglicht, sich auf jedem Gerät bei Apps und Websites anzumelden. Während Passwörter nach wie vor die gängigste Authentifizierungsmethode sind, bieten Passkeys eine bequemere und sicherere Alternative. Passkeys basieren auf den offenen Standards der FIDO Alliance und des W3C und ermöglichen schnellere, einfachere und sicherere Anmeldungen bei Apps und Websites auf allen Geräten eines Benutzers.

Modernes Identity Management muss auch Compliance-Vorgaben wie NIS2 erfüllen

Nicht zuletzt muss modernes, zukunftssicheres Identity Management auch neue Compliance-Vorgaben wie NIS2 umsetzen. Die NIS2-Richtlinie der Europäischen Union verpflichtet Unternehmen, ihre Cybersicherheitsstrategie zu verbessern, regelmäßig Audits durchzuführen und sicherheitsrelevante Vorfälle frühzeitig zu melden. Das gilt vor allem für Unternehmen, die kritische Dienste bereitstellen, aber auch indirekt für alle, die diese Anbieter als Lieferanten unterstützen oder unterstützen möchten.

Dabei ist die Sicherheit der digitalen Identitäten von zentraler Bedeutung, zum einen weil Cyberattacken insbesondere mit Identitätsdiebstahl beginnen, zum anderen weil NIS2 konkret Maßnahmen für ein besseres Risikomanagement fordert, darunter explizit Konzepte für die Zugriffskontrolle und die Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung.

Fazit

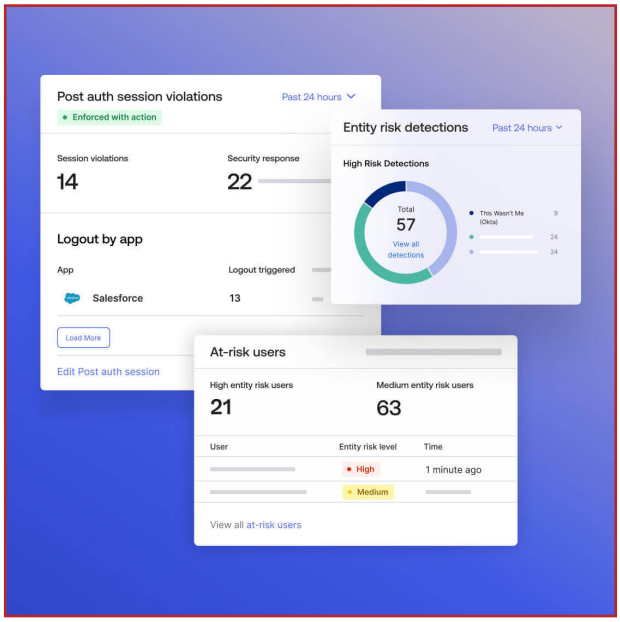
Es gibt also viele wichtige Gründe, sich mit der Modernisierung und Zukunftssicherheit des Identitätsmanagements zu befassen, darunter auch die zunehmenden Identitätsrisiken und die Möglichkeiten, die Künstliche Intelligenz (KI) für die Identitätssicherheit inzwischen bietet, wie im nächsten Kapitel näher betrachtet wird. *Oliver Schonschek*

Identitätsbasierte Bedrohungen erkennen und abwehren

Das moderne Identitätsmanagement beschränkt sich nicht nur auf die Verwaltung von Identitäten und Berechtigungen. Auch die Erkennung und Abwehr von identitätsbasierten Gefahren gehört dazu: mit Identity Threat Protection. Dabei hilft auch Künstliche Intelligenz (KI), die bei der Risikobewertung in Echtzeit eine zentrale Rolle spielt. Entscheidend ist dabei auch, welche Datenquellen der KI zur Verfügung stehen.

Identitätssicherheit in Zeiten von KI

„Da KI die Grenze zwischen Mensch und Maschine verwischt, ist Identität von entscheidender Bedeutung, um sicherzustellen, dass wir Menschen sicher mit Technologie verbinden können", beschreibt Todd McKinnon, Mitbegründer und CEO von Okta, die neue Bedrohungslage und Bedeutung digitaler Identitäten.



Identity Threat Protection mit Okta AI bietet Echtzeit-Erkennung und Reaktion auf identitätsbasierte Bedrohungen. (Bild: Okta)

Okta bringt in seiner Lösung das Identitätsmanagement und KI zusammen: Okta AI ist eine Suite KI-gestützter Funktionen, die es Unternehmen ermöglicht, die Leistungsfähigkeit von KI zu nutzen, um bessere Erfahrungen bei der Nutzung von Identitäten und Berechtigungen zu schaffen und sich vor Cyberangriffen zu schützen. Okta AI ist sowohl in die Workforce Identity Cloud als auch in die Customer Identity Cloud eingebettet und ermöglicht es, Identitätsaktionen durchzuführen und in Echtzeit auf Bedrohungen zu reagieren.

Im Bereich Workforce Identity ermöglicht Okta AI IT- und Sicherheitsteams, Sicherheitsrichtlinien und -verwaltung zu optimieren, die Admin-Tätigkeiten zu vereinfachen und die Bedrohungserkennung mit dynamischer und datengesteuerter Risikobewertung sowohl beim Login als auch während der gesamten Benutzersitzung zu automatisieren. Im Bereich Customer Identity bietet Okta AI Inline-Empfehlungen und -Aktionen für Entwickler und digitale Teams, um den Anmeldefluss zu verbessern, menschliche Benutzer von automatisierten Bots zu unterscheiden und ihre Apps schneller zu erstellen.

>>

Okta hat klare Richtlinien für die KI-Nutzung festgelegt. Dazu gehören die Trennung personenbezogener Kundendaten, der Verzicht auf die Verwendung sensibler Daten und die regelmäßige Aktualisierung dieser Richtlinien, um mit neuen Technologien Schritt zu halten.

Identitätsbedrohungen mit AI in Echtzeit bewerten

Okta Identity Threat Protection mit Okta AI ist ein neues Produkt für Okta Workforce Identity Cloud, das Echtzeiterkennung und -reaktion auf identitätsbasierte Bedrohungen bietet. Es erweitert die Sicherheit über die anfängliche Authentifizierung hinaus auf jeden Zeitpunkt, an dem ein Benutzer angemeldet ist. Auf diese Weise können Administratoren und Sicherheitsteams das Benutzerrisiko während aktiver Sitzungen kontinuierlich bewerten und automatisch auf Identitätsbedrohungen in ihrem gesamten Ökosystem reagieren.

Dazu erklärte Sagnik Nandy, President und Chief Development Officer von Workforce Identity Cloud bei Okta: „Unternehmen müssen in der Lage sein, nicht nur beim Login Einblicke in Risiken zu gewinnen, sondern diese auch zu jedem Zeitpunkt der Benutzersitzung neu zu bewerten. Identity Threat Protection erweitert Oktas adaptive Risikoanalyse und bietet automatische Abhilfe und Reaktion, sodass Unternehmen potenzielle Bedrohungen in Echtzeit stoppen können."

Umfassender Kontext zu den Identitätsbedrohungen

Identity Threat Protection (ITP) umfasst Integrationen, die in Zusammenarbeit mit Partnern wie CrowdStrike, Jamf, Material Security, Netskope, Palo Alto Networks, SGNL, Trellix, Zimperium und Zscaler entwickelt wurden. Mit dem Austausch über das Shared Signals Framework (SSF) werden so Erkenntnisse aus verschiedenen Sicherheitstechnologien gewonnen.

Webinar-Tipp: „So schützen Sie ihre Kunden und Mitarbeiter in Echtzeit: Identity Threat Protection mit AI", mit Arkadiusz Krowczynski, Senior Solutions Engineer, Okta

Wenn Identity Threat Protection ein ungewöhnliches Ereignis erkennt – sei es eine Änderung der IP-Adresse oder des Gerätekontexts – können vom Administrator konfigurierte Richtlinien und Funktionen bestimmte Aktionen einleiten, wie das sofortige Beenden der aktiven Benutzersitzung. Diese schnelle, koordinierte Reaktionsfähigkeit ermöglicht es Organisationen, Identitätsbedrohungen effektiver zu neutralisieren.

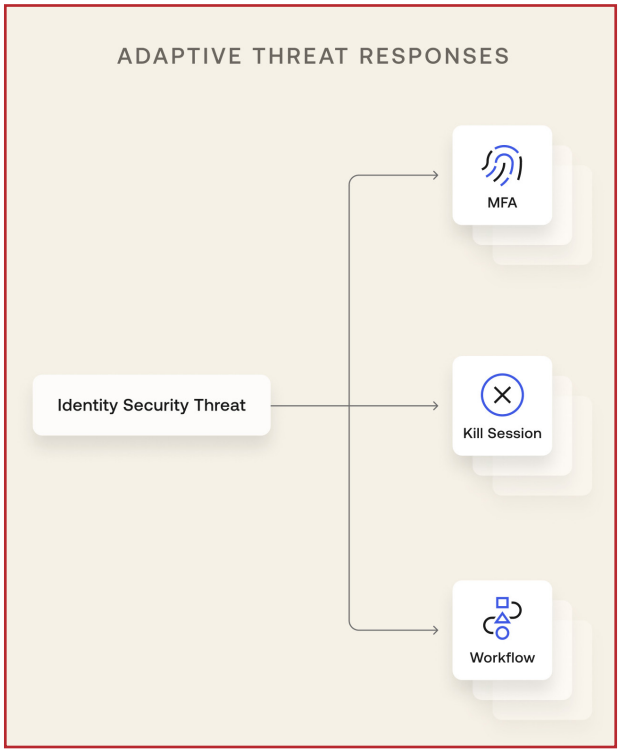
Durch die Nutzung des SSF während der aktiven Sitzung eines Benutzers ermöglicht Identity Threat Protection Unternehmen, Risiken durch umfassendere Bedrohungserkennungs- und Reaktionsfunktionen zu minimieren:

- Durch die kontinuierliche Risikobewertung werden Sicherheitsrichtlinien sowohl bei der Anmeldung als auch während einer aktiven >>

Benutzersitzung durchgesetzt, wodurch das Risiko eines unbefugten Zugriffs verringert wird.

- Das Shared Signals Framework ermöglicht es Sicherheitsteams, neu auftretende Bedrohungen zwischen verschiedenen Sicherheitstechnologien, darunter Mobile Device Management (MDM), Cloud Access Security Broker (CASB) und Endpoint Detection & Response (EDR)-Lösungen, zu erkennen und darauf zu reagieren.
- Adaptive Actions reagiert auf Bedrohungen in Echtzeit mit gezielten Aktionen, wie der universellen Abmeldung von unterstützten Anwendungen mit aktivierter Funktion, es fordert Benutzer zur On-Demand-Multi-Faktor-Authentifizierung auf und führt automatisierte Workflows aus, um auf neu auftretende Risiken zu reagieren.

Oliver Schonschek



Werden Identitätsbedrohungen erkannt, können Workflows gestartet werden, um zum Beispiel basierend auf Änderungen des Identitäts-, Geräte- oder Benutzerrisikos einen schreibgeschützten Zugriff zu erzwingen und Änderungen an zu schützenden Daten zu verhindern. Alternativ kann die Nutzung von MFA (Mehr-Faktor-Authentifizierung) oder die Beendigung der Sitzung erzwungen werden. (Bild: Okta)

Vorteile durch Identity Threat Protection (ITP) mit AI

- ITP bewertet kontinuierlich die Sitzungs-, Authentifizierungs- und Identitätsrisikorichtlinien, um Risiken zu identifizieren, die während einer aktiven Sitzung auftreten und nicht nur, wenn sich Benutzer anmelden. Das Shared Signals Framework (SSF) ermöglicht eine kontinuierliche Zugriffsüberwachung, auch wenn der Benutzer nicht mit Okta interagiert.
- ITP wertet Risikosignale aus, die Okta identifiziert, und Signale, die Sicherheitsanbieter identifizieren. Organisationen können Risikosignale aus mehreren Quellen analysieren, um ihren Schutz vor Identitätsbedrohungen zu erhöhen.
- ITP bewertet kontinuierlich Richtlinienkriterien, um Aktionen wie das Beenden einer Sitzung oder die Aufforderung zur MFA durch den Benutzer zu veranlassen. Es kann auch flexible Workflows initiieren, um basierend auf Änderungen der Identität, des Gerätekontexts oder des Entitätsrisikos schreibgeschützten Zugriff zu erzwingen, oder einen Vorfallmanagementprozess starten, um den Benutzer, das Gerät oder die App unter Quarantäne zu stellen.
- Man kann Sitzungen über alle unterstützten Apps und Geräte hinweg sofort beenden und so umfassende Sicherheit bei Bedrohungen oder bei der Verwaltung des Mitarbeiter-Lebenszyklus gewährleisten.

Schutz durch alle Phasen der Authentifizierung

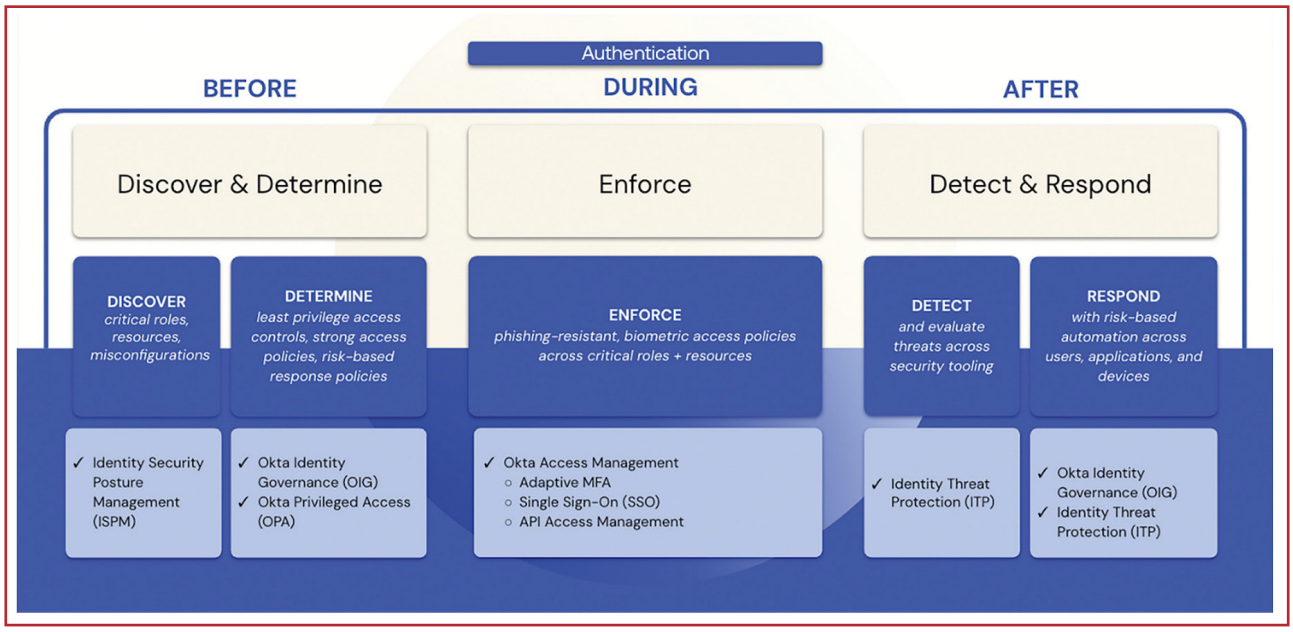
Die Okta-Identitätslösung bietet Unternehmen eine umfassende Sicherheitsstrategie, die nahtlos auf alle Phasen des Authentifizierungsprozesses abgestimmt ist. Diese ganzheitliche Lösung integriert sich in die zentrale Sicherheitsarchitektur eines Unternehmens und hilft dabei, Identitäten und Zugriffsrechte effizient und sicher zu verwalten.

1. Before: Discover & Determine

In der Vorbereitungsphase identifiziert Okta kritische Rollen, Ressourcen und potenzielle Fehlkonfigurationen innerhalb der IT-Landschaft. Die Lösung unterstützt Unternehmen dabei, Prinzipien des minimalen Zugriffs (Least Privilege Access) durchzusetzen und robuste, risikobasierte Richtlinien zu entwickeln.

- **Discover**: Identifikation von Schwachstellen und sensiblen Ressourcen durch **Identity Security Posture Management (ISPM)**.
- **Determine**: Umsetzung von Zugriffsrichtlinien mit **Okta Identity Governance (OIG)** und **Okta Privileged Access (OPA)**.

>>



Die Sicherheitslösung von Okta umfasst drei zentrale Phasen: Vor der Authentifizierung (Before), während der Authentifizierung (During) und nach der Authentifizierung (After), wie im Schaubild dargestellt. (Bild: Okta)

2. During: Enforce

Während der Authentifizierung sorgt Okta für eine reibungslose und sichere Zugriffskontrolle. Durch den Einsatz von phishing-resistenten Mechanismen und biometrischen Technologien wird ein sicherer Zugriff auf kritische Rollen und Ressourcen gewährleistet.

- **Lösungen in dieser Phase**: **Okta Access Management, Adaptive MFA, Single Sign-On (SSO)** und **API Access Management**.

3. After: Detect & Respond

Nach der Authentifizierung liegt der Fokus darauf, Bedrohungen frühzeitig zu erkennen und automatisierte Reaktionen zu ermöglichen. Die Kombination aus proaktiver Bedrohungsanalyse und automatisierter Reaktion auf verdächtige Aktivitäten stellt sicher, dass Risiken minimiert werden.

- **Detect**: Bedrohungserkennung mit **Identity Threat Protection (ITP)**.

- **Respond**: Automatisierte Reaktionen auf Sicherheitsvorfälle durch Integration von **OIG** und **ITP**.

Ganzheitliche Sicherheitslösung

Die Okta-Lösung deckt die gesamte Sicherheitskette von der Identifikation bis zur Reaktion ab. Sie kombiniert starke Authentifizierungsmethoden, umfassende Governance-Tools und KI-gestützte Bedrohungserkennung in einer zentralen Plattform. Durch die Integration in bestehende Systeme ermöglicht Okta eine flexible, skalierbare und hochsichere Identitätsverwaltung für moderne Unternehmen.

Diese durchgängige Sicherheitsstrategie stärkt die Sicherheitslage des Unternehmens und schützt sensible Daten vor internen und externen Bedrohungen.

Kostenlose Demo-Version

Jetzt ausprobieren – kostenlos!

Überzeugen Sie sich selbst von den Vorteilen der Identity-Lösung. Testen Sie die Okta-Demo-Version ganz unverbindlich und erleben Sie, wie einfach sichere Identitätsmanagement-Lösungen sein können.
Starten Sie noch heute!

Sie wollen sich selbst ein Bild von den Vorteilen der Okta-Lösungen machen? Dann nutzen Sie den Kontakt zu den Okta-Expertinnen und -Experten und stellen Sie Ihre Fragen:
https://www.okta.com/de/contact/

So hilft Okta bei der Modernisierung des Identitätsmanagements

Welche Vorteile ein modernes Identitätsmanagement mit sich bringt, zeigen die zahlreichen Praxisbeispiele von Okta-Kunden.

Zukunftsfähige Identitätslösungen sind bereits heute erfolgreich im Einsatz und zeigen den Weg, wie sich die neuen Herausforderungen für die Sicherheit digitaler Identitäten bewältigen lassen. Hier kommen einige der über 19.300 Kunden von Okta zu Wort.

Zentralisiertes System mit Absicherung gegen unberechtigte Zugriffe

„Wir waren auf der Suche nach einem zentralisierten System mit modernster Absicherung gegen unberechtigte Zugriffe. Das haben wir in Okta gefunden."
Niklas Lammers, IT-Projektleiter, HDI Systeme

Zeitgemäße Sicherheit mit einer hochwertigen Customer Experience

„Okta als Single Source of Truth für User Identities macht es uns leicht, jederzeit den Überblick darüber zu behalten, wer sich wo anmeldet. So vereinen wir zeitgemäße Sicherheit mit einer hochwertigen Customer Experience."
Nima Attarzadeh, Senior Manager of Identity & Digital Services, Merz

Reduzierung der Identitätsrisiken und Sicherung des Geschäftsbetriebs

„Identität ist zum Schlüssel moderner Sicherheit geworden. Die Kontrolle der Identitätsausbreitung bei gleichzeitiger Aufrechterhaltung des Geschäftsbetriebs ist eine Herausforderung, die mit herkömmlichen Lösungen nicht gelöst werden konnte. Identity Security Posture Management bietet uns auf einzigartige Weise kontinuierliche Transparenz und reduziert Identitätsrisiken mit einer schnellen Amortisierungszeit und einem datengesteuerten Ansatz."
Matthew Sharp, CISO bei Xactly

Über Okta

Okta ist das weltweit führende Identitätsunternehmen. Als führender unabhängiger Identitätspartner ermöglichen wir jedem die sichere Nutzung jeder Technologie – überall, auf jedem Gerät oder jeder App. Die größten Marken vertrauen auf Okta, um sicheren Zugriff, Authentifizierung und Automatisierung zu ermöglichen. Mit Flexibilität und Neutralität im Kern unserer Okta Workforce Identity Cloud und Customer Identity Cloud können sich Manager und Entwickler dank anpassbarer Lösungen und mehr als 7.000 vorgefertigter Integrationen auf Innovationen konzentrieren und die digitale Transformation beschleunigen.

Weitere Informationen finden Sie unter: www.okta.de