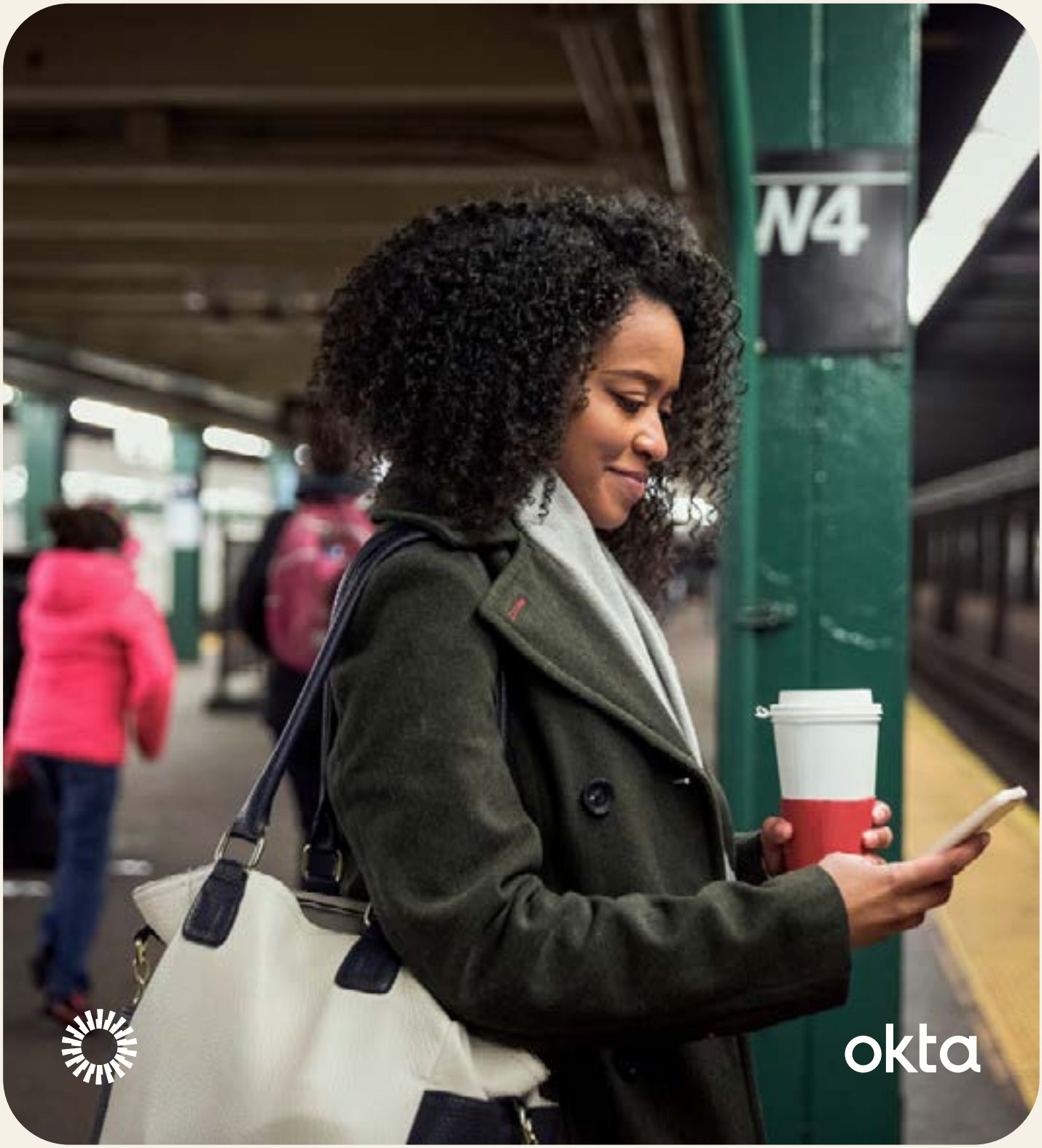
Whitepaper

Mehr Sicherheit mit Workforce Identity



Inhalt

Die wachsende Rolle von Identitäts-management in der Cyber-sicherheit

Identität spielte bei effektiven Cybersecurity-Programmen schon immer eine zentrale Rolle. Das gilt heute mehr als je zuvor, da Angreifer mit Phishing und anderen Methoden versuchen, Ihre Anmeldedaten zu stehlen und sich bei Ihren Accounts einzuloggen. Bei 45 Prozent der Data Breaches im Jahr 2022 nutzten Angreifer gestohlene Anmeldedaten, während es im Jahr zuvor noch 42 Prozent waren.[1]

Identitätsmanagement ist die einzige Technologie, die in alle Ihre IT- und Sicherheitstechnologien integriert ist – von Geräten und lokalen Anwendungen bis hin zu Cloud-Anwendungen und Workloads. Sie verbindet Ihre Benutzer mit den Ressourcen, die sie für ihre Arbeit benötigen. Außerdem ist Identitäts-management eine zentrale Komponente des Zero Trust-Sicherheitsansatzes, bei dem es darum geht, Benutzern und Services nach dem Least-Privilege-Prinzip Zugriff zu gewähren.

Identitätsmanagement verbindet Arbeitnehmer, Geräte, Anwendungen sowie Ressourcen, kann die Gefahren für Ihr Unternehmen minimieren und Bedrohungen schneller erkennen und abwehren. In diesem Dokument erfahren Sie, wie Sie mit einem Identity-basierten Ansatz Ihre Mitarbeiter, Ressourcen sowie Ihre Innovation und Produktivität schützen können.

[1] Verizon 2023 Data Breach Investigations Report

Herausforderungen bei der Absicherung von Identitäten

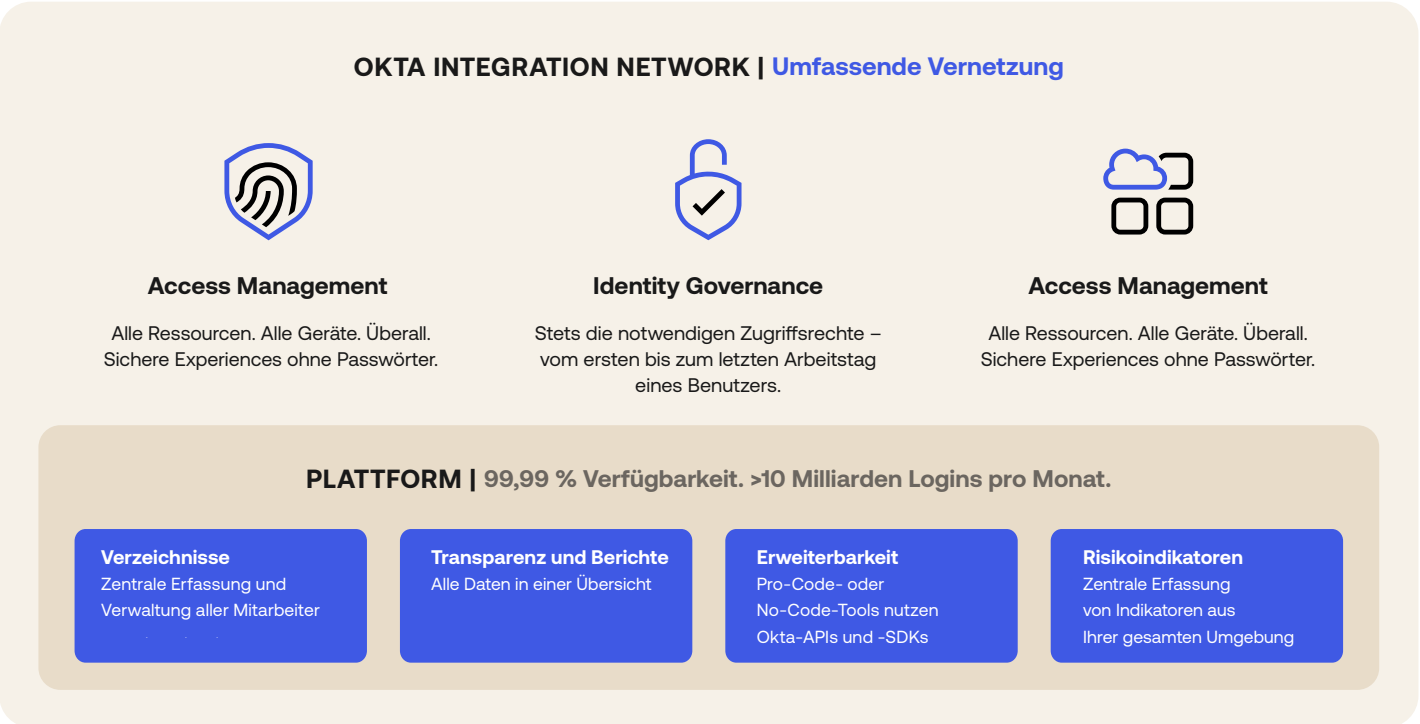
Die Bedingungen, die für den Einsatz von Zero Trust sprechen, erschweren gleichzeitig die Absicherung von Mitarbeiteridentitäten. Dabei treten diese typischen Probleme auf:

- **Fehlender Einblick in Identitätsdaten** aufgrund mehrerer Identity-Speicher, was die Erkennung, Abwehr und Behebung potenzieller aktiver Bedrohungen erschwert.
- **Manuelle, ressourcenintensive Identity-Prozesse** eröffnen Sicherheitslücken, die von Angreifern ausgenutzt werden können, z. B. inaktive Accounts, die noch nicht deprovisioniert sind.
- **Begrenzte Integration zwischen Identitätsmanagement- und anderen Technologien**, wodurch Risiken für das Unternehmen verschärft werden und die Erkennung sowie Abwehr von Bedrohung erschwert wird, z. B. dadurch, dass legitime Benutzer mit unsicheren oder kompromittierten Geräten auf SaaS-Anwendungen zugreifen.
- **Schwache User Experiences** aufgrund umständlicher Logins oder weil Mitarbeiter sich mehrere Passwörter merken müssen, was sie zur Umgehung von IAM-Kontrollen (Identity and Access Management) verleiten und damit Einfallstore für Angreifer eröffnen kann.
- **Schwache oder uneinheitliche Identity-Sicherheitskontrollen**, z. B. keine starke Authentifizierung für bestimmte Anwendungen oder Benutzer, die umfangreiche Zugriffsrechte für Ressourcen haben, vergrößern das Risiko von Sicherheitsvorfällen.

Okta Identity für zuverlässige Sicherheit

In einer Welt, in der IT-Fragmentierung und Hybrid-Arbeit der Normalzustand sind, ist Identitätsmanagement die wichtigste Verteidigungslinie. Okta Workforce Identity Cloud ist eine einheitliche Plattform, die verschiedenste Identity-basierte Use Cases abdeckt und sich nahtlos in Ihr vorhandenes Technologie-Ökosystem integriert. Dank einer zentralen Übersicht über Benutzeridentitäten erhält Ihr Unternehmen wertvolle Einblicke, die zur Erkennung und Abwehr Identity-basierter Bedrohungen beitragen – von Phishing und anderen Formen von Zugangsdaten-Missbrauch bis hin zu Session Hijacking nach erfolgter Authentifizierung. Okta bietet bewährte Integrationen in Ihr Technologie-Ökosystem und kann dadurch die Indikatoren aus anderen Tools verstärken, was schnelle und konsistente Sicherheitsreaktionen ermöglicht. Sie profitieren von Tools zur Verwaltung von User Account Lifecycles, Identity Governance, Privileged Access sowie No-Code Workflows, mit denen Sie Identity-Prozesse und Reaktionen auf potenzielle Bedrohungen automatisieren können.

Mithilfe der verschiedenen Komponenten von Okta Workforce Identity Cloud können Unternehmen den richtigen Personen zum richtigen Zeitpunkt Zugriff auf die richtigen Ressourcen gewähren. Dadurch wird die Sicherheit gestärkt und die Komplexität minimiert.



Okta Workforce Identity Cloud

Eine Identity-Plattform für Transparenz und Kontrolle

Unternehmen nutzen häufig mehrere IAM-Einzellösungen für On-Premise- und Cloud-Anwendungen. Gründe für diesen Identity-Wildwuchs sind Merger & Akquisitionen, verschiedene Zugriffsmöglichkeiten für Auftragnehmer und Geschäftspartner sowie die Implementierung neuer Anwendungen für neue Geschäftszwecke. IT- und Security-Teams fällt die Definition der Ressourcenzugriffe angesichts dieser Situation schwer und implementieren manuelle Prozesse zum Hinzufügen bzw. Entfernen von Benutzern und Ändern der Berechtigungen. Diese manuellen Prozesse können jedoch auch zu Fehlern führen. Der Identity-Wildwuchs erschwert auch die Durchsetzung einheitlicher Sicherheits- und Compliance-Richtlinien. Wenn Benutzer sich mehrere Passwörter für mehrere Anwendungen merken und eingeben müssen, stört das ihre Arbeitsprozesse und erhöht das Risiko, dass sie das gleiche Passwort für mehrere Services verwenden. Die Konsolidierung von IAM in ein einziges Benutzerverzeichnis und einen Technologie-Stack schafft eine übersichtliche und zentrale Single Source of Truth, die einen einheitlichen Identity-Sicherheitsansatz für On-Premise- und Cloud-Ressourcen gewährleistet. Für Benutzer verringert die Implementierung von Single Sign-On (SSO) die Wahrscheinlichkeit von Password Fatigue (Passwortmüdigkeit) und die Mehrfachnutzung von Passwörtern für mehrere unsichere Anwendungen.

Mit einem modernen Cloud-Verzeichnis und standardmäßig verfügbaren Integrationen in alle Informationsquellen des Unternehmens beseitigt Okta Identity-Silos und ermöglicht einen zentralen Überblick über alle Benutzergruppen. Diese Informationsquellen können AD- und LDAP-Verzeichnisse, HR-Systeme wie Workday, SaaS-Anwendungen wie Google Workspace, CSV-Dateien und Identity-Lösungen von Drittanbietern sein. Mit Okta können Sie das User Management zentralisieren, indem Sie Benutzerprofile und -attribute aus mehreren Identity-Quellen zusammenführen, Benutzerattribute über verschiedene Quellen hinweg ändern und den User Lifecycle-Status in einer zentralen Konsole verwalten. Alle Änderungen werden automatisch synchronisiert, sodass Sie nicht aufwendig mehrere Verzeichnisse auf dem neuesten Stand halten müssen. Echtzeitdaten und vordefinierte Berichte liefern ein umfassenderes Bild potenzieller Sicherheitsrisiken.

Das Cloud-basierte SSO von Okta vernetzt alle Bereiche von der Cloud bis zur lokalen Umgebung, sodass alle Ihre Anwendungen ganz einfach eingebunden werden. Die Zugriffsverwaltung für Mitarbeiter, Auftragnehmer und Partner erfolgt zentral, wobei einheitliche Richtlinien schnell angewendet und durchgesetzt werden können. Das verbessert die Sicherheitslage erheblich. Über die Single Source of Truth können Sie mühelos Zugriffsberechtigungen für Benutzer, Gruppen und Anwendungen anzeigen, hinzufügen oder ändern. Dadurch ist sichergestellt, dass die richtigen Personen die richtigen Berechtigungen für genau die Ressourcen erhalten, die sie zu einem konkreten Zeitpunkt benötigen. Wenn Ihre Endbenutzer nur einen Satz Anmeldeinformationen benötigen, können sie schnell auf alle notwendigen Ressourcen zugreifen und bleiben produktiv.

Arrow Global Group PLC konnte Okta innerhalb von nur 6 Stunden in 13 separaten Active Directory-Instanzen implementieren.

Überblick über privilegierte Ressourcen und Identity Governance

In der Vergangenheit wurden vorrangig IGA-Lösungen (Identity Governance and Administration) zum Organisieren von Audits und Nachweisen der Compliance eingesetzt. Ebenso nutzten Unternehmen PAM-Tools (Privileged Access Management) zum Zuweisen, Überwachen und Absichern von privilegierten Zugriffen auf vertrauliche lokale Unternehmenssysteme. Seit jedoch immer mehr Workloads in die Cloud verlagert werden, sollen diese Anwendungen immer mehr Probleme lösen. Unternehmen müssen heute sicherstellen und nachweisen, dass Benutzer lediglich über die für ihre Arbeit notwendigen Zugriffsrechte verfügen – und dass die Zugriffsberechtigungen angepasst werden, sobald sich die Arbeitsanforderungen ändern.

Okta stellt eine zentrale Management-Konsole bereit, über der Sie alle Komponenten Ihrer Identity Fabrik (Identitätsstruktur) verwalten können: IAM, IGA und PAM. Hier erstellen Sie robuste Richtlinien und implementieren sie einheitlich für alle Benutzergruppen und Anwendungen, sodass Sie nicht mehr von Legacy-Infrastrukturen abhängig sind und auf die aufwändige Zugriffsverwaltung für diese Ressourcen verzichten können. Dabei können die verschiedenen Identity-Systeme auch Sicherheitsindikatoren austauschen, sodass der Schutz Ihres Unternehmens gestärkt und effizienter umgesetzt wird.

Bessere und stärker geschützte Authentifizierungsprozesse

Phishing-Betrug steht bei Internetkriminalität in den USA auf Platz 1 und verursacht die größten finanziellen Schäden für seine Opfer.[2] Bisher galt Multi-Faktor-Authentifizierung (MFA) als erste Wahl zur Verhinderung von Anmeldedaten-Diebstahl. Einige viel beachtete Cyberangriffe haben jedoch gezeigt, dass MFA keine hundertprozentige Sicherheit mehr bietet. Phishing-resistente MFA verzichtet auf Shared Secrets wie Sicherheitsfragen und kann so verhindern, dass Angreifer die Authentifizierung unterlaufen können. Zudem bietet sie Schutz vor gefälschten Domänen, die von Angreifern eingerichtet wurden, um Benutzer hereinzulegen.

Okta unterstützt nicht nur alle verbreiteten Phishing-resistenten Authentifizierungsverfahren, sondern bietet mit FastPass zudem eine hochsichere und unkomplizierte Anwendung für Benutzer an. Diese Phishing-resistente und passwortlose Authentifizierungslösung für verwaltete und unverwaltete Geräte verzichtet auf umständliche externe Faktoren wie Einmal-Passwörter und Push-Benachrichtigungen und integriert stattdessen biometrische Funktionen auf vielen Systemen. FastPass bietet plattform- und geräteübergreifend einheitliche User Experiences, minimiert Reibungspunkte für Mitarbeiter und lässt sie produktiv arbeiten.

[2] Federal Bureau of Investigation Internet Crime Report 2022

Mit Okta FastPass können Sie auch Anforderungen für die Geräte festlegen und durchsetzen, die auf Ihre Ressourcen zugreifen. Beispielsweise lässt sich einstellen, dass der Zugriff nur für vertrauenswürdige Geräte gewährt wird oder die Geräte über aktuelle Betriebssysteme oder Sicherheits-Patches verfügen müssen.

Die hervorragende User Experience endet jedoch nicht mit der Benutzerauthentifizierung in FastPass. Okta Identity Governance erlaubt Benutzern die einfache Anforderung von Zugriffsrechten für neue Anwendungen und Ressourcen in ihren bevorzugten Collaboration-Tools.

Nach der internen Einführung von Okta FastPass verzeichnete das IT-Team von Okta bei Anfragen zur Passwortrücksetzung einen Rückgang von 98 Prozent.

Stärkere Sicherheit und Compliance mit Tools und Automatisierung

Zugriffsberechtigungen von Benutzern verändern sich ständig – sei es durch Neueinstellungen, durch Wechsel der beruflichen Position oder nach dem Ausscheiden aus dem Unternehmen. Sie stellen damit für IT-Teams einen erheblichen Aufwand dar. Gleichzeitig gilt: Wenn die Zugriffsberechtigungen nicht auf dem neuesten Stand gehalten werden, entstehen Risiken für das Unternehmen. Je länger die Deprovisionierung der Konten eines Angestellten dauert, der das Unternehmen verlässt, desto anfälliger ist das Unternehmen für einen Angriff.

Okta Workflows macht es Ihnen leicht, Ihr Identitätsmanagement zu automatisieren und zu skalieren – ohne eine einzige Codezeile zu schreiben. Gleichzeitig vereinfacht Lifecycle Management die Provisionierung und Deprovisionierung von Benutzern mithilfe automatisierter Prozesse – von der Kontoerstellung bis zur Kontolöschung. Dabei werden Trigger von HR-Systemen und anderen Verzeichnissen ausgewertet. Diese Automatisierung verbessert die Sicherheit, weil das Risiko von Angriffen per „Schatten"-Konten (d. h. noch nicht deprovisionierten Konten) minimiert wird. Die Automatisierung der Benutzerrollen- und Berechtigungsprozesse erleichtert auch die Implementierung von Zero Trust-Initiativen, da sich damit das Least-Privilege-Prinzip für Benutzerzugriffe auf Systeme und Anwendungen durchsetzen lässt. So können Sie beispielsweise bei vorübergehenden Änderungen von Benutzerrollen oder aufgrund anderer Trigger bedingten oder befristeten Zugriff auf bestimmte Anwendungen gewähren.

Okta Identity Governance vereinfacht und automatisiert mithilfe dieser Funktionen Access Requests, Access Certification-Kampagnen sowie Entitlement Management. Gleichzeitig vereinfachen die Out-of-the-Box-Reporting-Funktionen die Durchführung von Audits sowie den Nachweis von Compliance.

Proaktiver Schutz vor typischen Identity-basierten Bedrohungen

Brute-Force-Angriffe und typische Phishing-Methoden setzen zur Automatisierung und Vervielfältigung ihrer Attacken auf Bots. Dementsprechend sollten auch Unternehmen ihre Schutzmaßnahmen gegen diese alltäglichen Angriffe automatisieren.

Die in Okta Workforce Identity Cloud integrierten Sicherheitsfunktionen erkennen typische Identity-Bedrohungen, die vor und nach der Authentifizierung ansetzen, und reagieren zuverlässig darauf, bevor Schaden für Ihr Unternehmen entsteht. Dabei bietet die Lösung bietet diese Vorteile:

- Nutzung von Datenanalysen und Machine Learning zur Abwehr von Brute-Force-Angriffen. Okta aggregiert Daten über Sign-in-Aktivitäten, bewertet die Quelle von Sign-in-Anfragen vor der Authentifizierung und blockiert automatisch gefährliche IP-Adressen.
- Abwehr von Phishing-Versuchen durch Kontrolle der Quelle von Authentifizierungsanfragen und Verschärfung der Authentifizierung abhängig von Risikofaktoren.
- Verhinderung der Umgehung von MFA mit Phishing-resistenter Authentifizierung und Überprüfung sicherheitsbezogener Geräteattribute, sobald ein Benutzer eine neue Anwendung startet.
- Blockierung des Zugriffs von Malware-verseuchten Geräten auf Ihre Ressourcen, indem Okta in Ihre EDR-Lösungen (Endpoint Detection and Response) integriert wird.

Beim Identitätsmanagement ist es heute nicht damit getan, den erfolgreichen Login zu gewährleisten. Zum Schutz vor raffinierten Identity-Angriffen wie Session-Hijacking muss die Identity-Sicherheit die gesamte Dauer von User Sessions abdecken.

Kontinuierliche Analyse von Benutzerrisiken und automatische Behebung von Bedrohungen

Da die meisten Cyberangriffe auf irgendeine Weise die Identität angreifen, sollten Identity-Lösungen bei der Erkennung und Reaktion an erster Stelle stehen. Gartner schätzt, dass 90 Prozent aller Unternehmen bis zum Jahr 2026 Zugriffsmanagement-Tools mit eingebetteten ITDR-Funktionen (Identity Threat Detection and Response) als wichtigste Methode zur Abwehr von Identity-Angriffen einsetzen werden (aktuell sind es nur 20 Prozent).[3]

Identity Threat Protection mit Okta AI bietet Unternehmen die Möglichkeit, im Rahmen einer Zero Trust-Sicherheitsstrategie Identity-Bedrohungen in ihren Ökosystemen automatisch zu erkennen und darauf zu reagieren. Okta integriert Identity-bezogene Indikatoren aus Ihren vorhandenen Sicherheitslösungen und erweitert die Echtzeit-Risikoidentifizierung auf die gesamte User Session. Das beschleunigt die Behebung und ermöglicht maßgeschneiderte Reaktionen vor, während und nach der Authentifizierung. Identity Threat Protection bietet Unternehmen folgende Möglichkeiten:

- Bedrohungsindikatoren von verschiedenen führenden Sicherheitsanbietern können aggregiert, analysiert und in Maßnahmen umgesetzt werden. Dazu gehören Lösungen für EDR/XDR (Endpoint Detection & Response/ Extended Detection and Response), CASB (Cloud Access Security Broker), Netzwerksicherheit, Mobile Threat Defense, Unified Endpoint Management, E-Mail-Sicherheit und andere.
- Kontinuierliche Re-Evaluierung von Zugriffsrechten und Erkennung von Richtlinienverstößen, wenn sich das Benutzerrisiko und -verhalten während Sessions und Anwendungszugriffen verändert. Dadurch können Sie Risiken wie kompromittierte Anmeldedaten, Datenexfiltration, Session Hijacking oder nicht autorisierte Zugriffsversuche identifizieren und abwehren.
- Umfassender Überblick über Identity-basierte Bedrohungen mit Identity Threat-Analysen.
- Automatische Auslösung konkreter Reaktionsmaßnahmen auf neue Identity-Bedrohungen, z. B. Sofort-Abmeldung, MFA-Anforderung oder andere maßgeschneiderte Aktionen.

[3] 2022 Gartner® Magic Quadrant for Access Management™

Workforce Identity Cloud: Eine Plattform für Identity-zentrierte Sicherheit

Okta ist wie kein anderer Anbieter in der Lage, die Sicherheitslage Ihres Unternehmens zu verbessern. Angesichts der zahlreichen Angriffe auf Benutzer und ihre Anmeldedaten sollten Sie die Identity zentralisieren, Identity-Automatisierung implementieren und das Identitätsmanagement in Ihre Sicherheitslösungen integrieren. Das gibt Ihnen die Möglichkeit, Least-Privilege-Sicherheitsrichtlinien für alle Ihre Mitarbeiter einheitlich durchzusetzen, Identity-basierte Attacken schneller zu erkennen und abzuwehren sowie die Compliance-Einhaltung effizient zu demonstrieren. Mit Okta AI können Unternehmen Identity-Prozesse automatisieren, die Effizienz des IT- und Security-Teams optimieren und Risiken durch manuelle Prozesse minimieren.

Buyer's Guide für Workforce Identity

Okta Workforce Identity Cloud bietet Ihren Mitarbeitern den einfachen und sicheren Zugang zu Ressourcen, die sie benötigen. Dadurch können Sie sich auf andere strategische Prioritäten konzentrieren, zum Beispiel darauf, Kosten zu senken und mehr für Ihre Kunden zu tun.

Erfahren Sie mehr darüber, wie Sie mit einer Identity-Security-Plattform Ihre Daten schützen, Ihre Unternehmensprozesse beschleunigen und flexibler machen und Ihren Mitarbeitern neue Möglichkeiten eröffnen. Der Buyer's Guide für Workforce Identity baut auf dem Okta Workforce Identity-Reifegradmodell auf und untersucht die Elemente, mit denen Workforce Identity in jeder Phase der Implementierung umgesetzt wird – von den Grundlagen bis hin zu strategischen Entscheidungen.

Über Okta

Okta ist das weltweit führende Identity-Unternehmen. Als der führende unabhängige Identity-Partner ermöglichen wir es jedermann, jede Technologie sicher zu nutzen – überall, mit jedem Device und jeder App. Die weltweit renommiertesten Marken vertrauen beim Schutz von Zugriff, Authentisierung und Automatisierung auf Okta. Im Mittelpunkt unserer Okta Workforce Identity und Customer Identity Clouds stehen Flexibilität und Neutralität. Mit unseren individualisierbaren Lösungen und unseren über 7.000 schlüsselfertigen Integrationen können sich Business-Verantwortliche und Entwickler ganz auf neue Innovationen und eine rasche Digitalisierung konzentrieren. Wir entwickeln eine Welt, in denen Ihre Identity ganz Ihnen gehört. Mehr unter okta.com/de.