So kontrollieren Sie KI-Agenten und andere nicht-menschliche Identities

mit einer modernen Identity-zentrierten Sicherheitsstrategie

Nicht-menschliche Identities ermöglichen bessere Geschäftsergebnisse. Ihr Einsatz ist jedoch auch mit höheren Risiken verbunden.

Die Zahl der verwendeten nicht-menschlichen Identities (Non-Human Identities, NHIs) für die Kommunikation von Maschinen, Services und KI-Agenten hat in etlichen Branchen rasant zugenommen. Der Grund: Sie beschleunigen grundlegende Unternehmensprozesse für Zusammenarbeit, Innovation und Produktivität.

Daher sind NHIs für den zukunftssicheren Einsatz von KI in Unternehmen unverzichtbar. Allerdings schaffen sie auch neue Ansatzpunkte für Angreifer. Insbesondere KI-Agenten stellen eine Schwachstelle in Unternehmen dar, weil sie sich anders verhalten als Benutzer sowie klassische Software und häufig Zugriff auf äußerst vertrauliche Daten benötigen. Dies macht sie für Angreifer besonders attraktiv. Gleichzeitig fällt es Unternehmen schwer, sie zuverlässig abzusichern.

Ohne einen einheitlichen Identity-zentrierten Sicherheitsansatz zur Absicherung der schnell wachsenden Angriffsfläche wächst das Risiko durch NHIs erheblich.

Wichtige Fakten

Die Zahl nicht-menschlicher Identities übersteigt die Zahl menschlicher Identities um das **Fünfzigfache.**

Forbes

46 % aller Unternehmen haben im letzten Jahr eine Kompromittierung von NHI-Accounts verzeichnet (und weitere **26 %** haben den Verdacht, dass es bei ihnen dazu gekommen ist).

TechTarget ESG

Eine neue Risiko-Generation

Parallel zum wachsenden Einsatz von Cloud-Diensten und Cloud-Plattformen wie AWS hat auch die Nutzung von NHIs zugenommen, um GenAI-Tools, KI und Automatisierung sowie digitale Workflows zu ermöglichen. Unternehmenssysteme müssen sicher und effizient funktionieren, ohne ständige Überwachung durch Menschen zu erfordern. Hier kommen nicht-menschliche Identities wie Service-Accounts ins Spiel, die von KI-Agenten genutzt werden. Sie ermöglichen Anwendungen und Services die gegenseitige Authentifizierung für automatisierte Aufgaben, Datenaustausch sowie komplexe Prozesse, die andernfalls unmöglich wären oder die zeitaufwändige Verwaltung durch Menschen erfordern würden.

Da nicht verwaltete NHIs leicht angreifbar sind, müssen Unternehmen Strategien zur Minimierung dieses neuen Risikos implementieren. Wenn die von nicht-menschlichen Identities für die Authentifizierung verwendeten Secrets, Schlüssel bzw. Token in die falschen Hände gelangen, können die Angreifer umfassenden und weitreichenden Zugriff auf vertrauliche Anwendungen und Daten erhalten.

Insbesondere wenn nicht-menschliche Identities mit GenAI-Tools (generative KI) wie Chatbots und digitalen Assistenten genutzt werden, können verschiedenste neue Bedrohungen auftreten, da diese Tools keinen Benutzerkontext liefern können:

Prompt Injection und Data Poisoning

Angreifer können Prompts manipulieren oder schädliche Inhalte injizieren, sodass GenAI-Tools aus ihren Datenquellen unzulässige oder falsche Informationen generieren.

Schatten-Zugriff und laterale Bewegungen

Angreifer können GenAI-Tools missbrauchen, um an vertrauliche Inhalte in verbundenen Systemen (z. B. Salesforce, Jira, interne Wikis) zu gelangen, auf die das GenAI-Tool Zugriff hat.

Übermäßiger Datenzugriff

GenAI-Tools haben häufig Zugriff auf riesige Datenbestände. Wenn bei der Nutzung der zugrunde liegenden Datenquellen der Benutzerkontext nicht angemessen berücksichtigt wird, kann es dazu kommen, dass Benutzer an nicht für ihre Rolle geeignete Daten gelangen.

51 % aller Unternehmen setzen KI-Agenten ein.

PagerDuty

Nur **15 %** aller Security-Teams sind der Meinung, dass sie NHI-bezogene Sicherheitsverletzungen zuverlässig abwehren können.

Cloud Security Alliance

Die besonderen Risiken von KI-Agenten

Am stärksten zeigen sich die potenziellen Vorteile und Risiken nicht-menschlicher Identities bei KI-Agenten. Da sie autonom im Auftrag von Benutzern und Unternehmen arbeiten, ermöglichen sie bislang unerreichte operative Effizienz sowie die Personalisierung und Automatisierung des Kundendienstes in einem Maße, das zuvor nicht vorstellbar war.

Diese Möglichkeiten sind jedoch ein zweischneidiges Schwert. Damit KI-Agenten sich kontinuierlich verbessern können, sind sie auf Daten, Ressourcen und Feedback angewiesen – wofür wiederum autorisierter und authentifizierter Zugriff notwendig ist. Dieser umfassende Zugriff ist ein Glücksfall für Angreifer, die Identity-basierte Attacken auf die dahinter liegenden nicht-menschlichen Identities durchführen wollen.

Bei vielen Unternehmen ist die Überwachung von nicht-menschlichen und Maschinen-Identities unzureichend oder überhaupt nicht vorhanden. Viel zu oft haben nicht-menschliche Identities übermäßige Zugriffsrechte und niemals rotierte Anmeldedaten oder sind auch lange nach ihrer Nutzung noch aktiv. Das führt zu kritischen Schwachstellen, die sich von Angreifern ausnutzen lassen. In IT- und Sicherheitsumgebungen, in denen Identity-Funktionen über unterschiedliche Systeme und Anwendungen verteilt sind, können diese Schwachstellen unbemerkt bleiben – bis es zu spät ist.

Identity ist die Schwachstelle. Die Lösung ist Identity-Sicherheit.

Der beste Schutz vor NHI-Schwachstellen beginnt mit der Vermeidung fragmentierter Identity-Systeme, die Lücken bei Transparenz und Durchsetzung möglich machen. Durch einheitliche Identity-Systeme in einer zentralen Plattform erhalten Unternehmen bessere Kontrolle über ihre nicht-menschlichen Identities und profitieren gleichzeitig von effizienterer Verwaltung. Moderne Identity-Plattformen helfen Ihnen, diesen einheitlichen Sicherheitsansatz umzusetzen.

Das ist insbesondere bei der Entwicklung von GenAI-Lösungen in Amazon Bedrock wichtig, wo der schnellen Bereitstellung sichere Zugriffskontrollen an die Seite gestellt werden müssen. Okta dient dabei als Identity-Kontrollebene für Ihre Bedrock-Umgebung und gewährleistet, dass nur autorisierte Benutzer und KI-Agenten auf sensible Modelle und Services zugreifen können.

Die Vorteile von Okta

Die Okta Platform implementiert einen zuverlässigen und vereinfachten Ansatz zur Verwaltung von nicht-menschlichen und Maschinen-Identities. Sie zentralisiert das Identity-Management Ihres Unternehmens in einem Identity-Security-Fabric, beseitigt dadurch blinde Flecken und bietet einen umfassenden Überblick darüber, wo sich Ihre nicht-menschlichen Identities befinden und welche Zugriffsrechte sie haben.

Identity Security Posture Management

- Kontinuierliche Überwachung und Risikoanalyse von NHIs
- Automatische Erkennung lokaler, nicht über den Identitätsverbund abgesicherter Service-Accounts und Kennzeichnung riskanter NHIs
- Erkennung von MFA-Lücken und Anmeldedaten-Missbrauch bei Maschinen-Identities
- Abgleich mit Compliance-Framework sowie geführte Workflows zur Behebung bei NHI-bezogenen Sicherheitsproblemen

Okta Privileged Access

- Sichere Verwaltung von Service-Account-Passwörtern und Durchsetzung von Richtlinien dazu, wer wie lange worauf zugreifen darf
- Automatische Rotation von Secrets, damit kein Gefährdung durch lange verwendete Anmeldedaten entsteht
- Auditiert und verfolgt, wer oder was den Account ausgecheckt hat

Secure Identity-Integrationen

Erweiterte Sicherheitsintegrationen mit SaaS-Anwendungen, die unnötig lange NHI-Zugriffe verhindern und nicht-menschliche Identities im gesamten Ökosystem schützen.

- **Lifecycle- und Entitlement-Management:** Automatisierte Identity-Provisionierung und Deprovisionierung für NHIs zur Gewährleistung von Just-in-Time-Zugriff
- **Einheitliches Single Sign-On (SSO) und Richtliniendurchsetzung:** Erweiterung von SSO und Sicherheitsrichtlinien auf Service-Accounts und Maschinen-Identities
- **Workflow-Automatisierung und Beendigung von Sessions:** Verhindert verwaiste NHIs durch Erzwingung von automatisiertem Offboarding und Session-Widerruf

Okta und Amazon: Der Schlüssel zur Absicherung von GenAI

Amazon Q bietet GenAI-basierte Unterstützung für alle AWS-Entwickler und führt damit gänzlich neue Möglichkeiten ein, wie Software-Entwickler, Business-Intelligence-Analysten, Kundendienst-Mitarbeiter und weitere zentrale Teams ihre Arbeit erledigen können.

Jetzt können Unternehmen die Effizienz, Produktivität und Customer Experience-Vorteile von Amazon Q mit den KI-fähigen Okta-Sicherheitstools kombinieren. Das gibt ihnen die Möglichkeit, GenAI-Funktionen in ihre Kernprozesse zu integrieren, ohne neue Risiken einzuführen.

Sichere GenAI-Implementierung

Schützen Sie die in Amazon Q gespeicherten Daten mit den Enterprise-gerechten Identity-Sicherheits-funktionen von Okta vor unbefugten Zugriffen. Und nutzen Sie die automatisierten Okta-Tools zur Lebenszyklusverwaltung, um das Identity-Management zu optimieren.

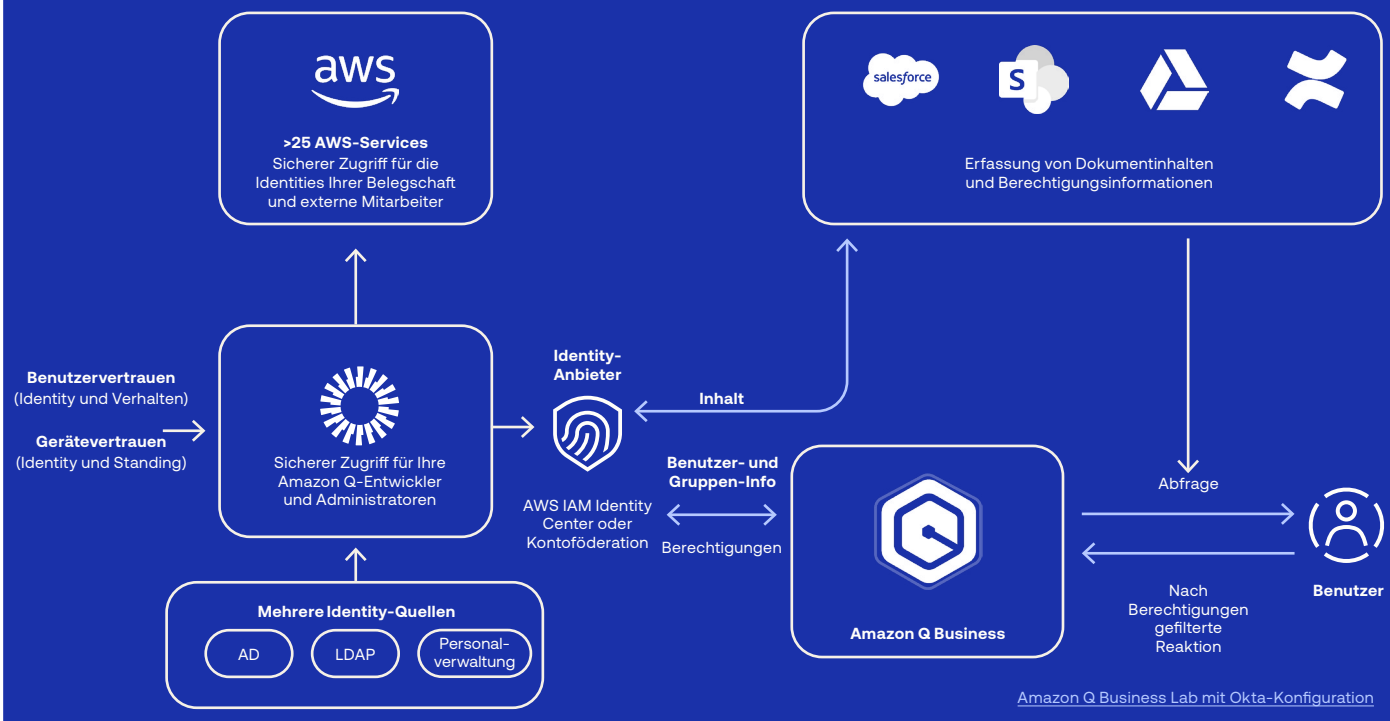
Turbo für die Produktivität

Unterstützen Sie die Kreativität und Produktivität Ihrer Teams mit Amazon Q. Sie können Meeting-Zusammenfassungen generieren, Content erstellen und Aufgaben abschließen – komplett ohne Daten neuen Risiken auszusetzen.

Bereitstellung von nahtlosem Zugriff

Der rollenbasierte Zugriff auf konkret festgelegte Datensätze gewährleistet optimierte und abgesicherte Zugriffe. Sie können Abonnements auf Anfrage oder anhand automatisierter Kriterien erlauben und profitieren dadurch von besserer Kostenkontrolle.

Amazon Q Business mit Okta nutzen



Amazon Q Business Lab mit Okta-Konfiguration

Nicht-menschliche Identities sicher nutzen

Innerhalb kürzester Zeit wurde KI von einer potenziell zukünftig nutzbaren Technologie zu einer geschäftlichen Notwendigkeit. Für wettbewerbsorientierte Unternehmen ist die Nutzung moderner Tools wie KI-Agenten unverzichtbar. Nicht-menschliche Identities können jedoch nur dann effektiv genutzt werden, wenn ihre Sicherheit gewährleistet ist.

Mit Okta können KI-unterstützte Workflows auf einer einheitlichen Identity-Plattform ausgeführt werden, die riskante Fragmentierung vermeidet und die Basis Ihres Sicherheits-Ökosystems stärkt. All das macht der Identity-Security-Fabric von Okta möglich.

Deshalb arbeiten AWS und Okta gemeinsam daran, eine sichere Grundlage für die nächste Generation intelligenter Automatisierung bereitzustellen. Unabhängig davon, ob Sie KI-Agenten in AWS bereitstellen oder Amazon Q teamübergreifend nutzen, gewährleistet die Okta Identity Platform, dass diese Identities sicher, kontrolliert und überprüfbar sind.

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