Whitepaper
September 2022

The State of Zero Trust Security 2022

Analyse des Reifegrades des Identity- und Access-Managements in weltweit tätigen Unternehmen

Okta Inc.
Oskar-von-Miller-Ring 20
80333 München, Germany
info_germany@okta.com
+49 (89) 26203329

okta

Inhalt

Zero Trust ist heute unverzichtbar

Die Philosophie der Zero Trust Security – „Nie vertrauen, immer prüfen“ – hat den richtigen Nerv getroffen. Es dauerte mehrere Jahrzehnte, bis Unternehmen das bislang übliche „Burggraben“-Modell hinter sich ließen – und akzeptierten, dass es in einer Cloud-basierten Welt keinen zu schützenden Perimeter gibt und die Eindringlinge sich stets in unseren Netzwerken befinden. Mittlerweile setzen Vorstände und Entscheider weltweit auf das Zero-Trust-Framework, das sich von einem beliebten Buzzword schnell zu einem strategischen Unterscheidungsmerkmal und einer zentralen Business-Anforderung entwickelt hat. Die Definition von Forrester lautet 2022: „Zero Trust ist ein IT-Security-Modell, das den Zugriff auf Anwendungen und Daten standardmäßig verweigert. […] Zero Trust basiert auf drei Kernprinzipien: Alle Elemente gelten standardmäßig als nicht vertrauenswürdig; Least Privilege Access wird durchgesetzt; und die gesamte Security wird durchgehend überwacht.“ [1]

Heute ist Zero Trust kein theoretisches Konzept mehr, sondern ein aktives Framework für nahezu alle digitalen Unternehmen – auch wenn viele von ihnen noch viel Arbeit vor sich haben, bevor sie von den Vorteilen einer modernen Zero-Trust-Architektur profitieren können.

> Seit der Veröffentlichung des „State of Zero Trust Security 2021“-Berichts von Okta im letzten Jahr hat sich der Anteil der Unternehmen mit einer bereits laufenden definierten Zero-Trust-Initiative mehr als verdoppelt – von 24 % auf 55 %.

Okta gibt den Report „The State of Zero Trust“ seit 2019 heraus – und viele der Herausforderungen, die die Implementierung von Zero Trust schon damals beflügelt haben, sind nach wie vor sehr relevant. Office-Arbeiter, die hybrid oder remote arbeiten, verbringen 65 % weniger Zeit im Büro als noch vor der COVID-19-Pandemie und treffen ihre Teams nur an zwei Tagen in der Woche persönlich.[2] Offenbar wird der Homeoffice-Boom keine kurzfristige Episode während der Pandemie bleiben, sondern markiert einen fundamentalen Wechsel bei der Art und Weise, wie Menschen weltweit arbeiten. Analog dazu gilt auch: Der unzureichende Schutz der Identities, der durch das hohe Tempo der Cloud-Einführung und der Digitalisierung verschärft wird, stellt für Unternehmen jeder Größe eine enorme Herausforderung dar. Denn Angreifer nutzen den sich auflösenden Netzwerk-Perimeter und die dynamischen Ökosysteme immer öfter skrupellos aus. Im Kern dieses Problems steht die Identität. Mehr als 80 % aller Kompromittierungen von Web-Anwendungen im letzten Jahr gingen auf den Missbrauch von Zugangsdaten zurück – und gestohlene Zugangsdaten waren auch die häufigste Taktik bei Ransomware-Angriffen.[3]

Um ihre Systeme, Daten, Mitarbeiter und Kunden in einer dynamischen Welt zu schützen, mussten Unternehmen ihre Cyber-Security-Ansätze schnell und nachhaltig umstellen. Dazu gehörte es auch, bestehende Legacy-Lösungen abzulösen, die noch aus einfacheren Zeiten stammten. Heute bedeutet dies fast immer die Einführung von Zero Trust. Die Implementierung eines Zero-Trust-Frameworks ermöglicht es Unternehmen, ihr Security-Standing und den relativen Reifegrad ihres Modells kontinuierlich zu bewerten. So können sie auch die richtigen Sicherheitslösungen auswählen, um ihre Architektur konsequent weiterzuentwickeln.

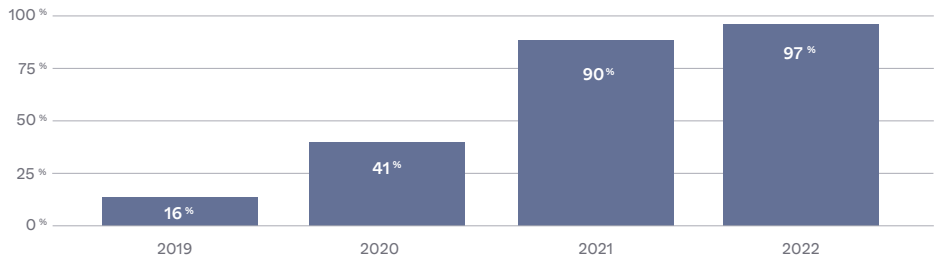
[1] Forrester: „**The Definition of Modern Zero Trust**“, Forrester Research, Inc., 24. Januar 2022.

[2] Gartner®: „**Strengthen Connection to Culture To Alleviate CEO Concerns About Hybrid Work**“, Graham Waller, Alexia Cambon, Rob O'Donohue, Gabriela Vogel, Christie Struckman, Chris Audet, 9. Juni 2022.

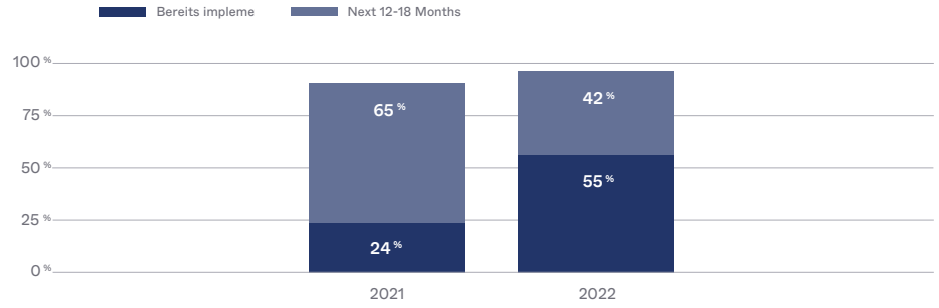
[3] Verizon: „**Data Breach Investigations Report 2022**“.

Vor vier Jahren hatten nur 16 % der befragten Unternehmen eine aktive Zero-Trust-Initiative oder wollten sie in den kommenden 12–18 Monaten starten. Heute liegt diese Zahl bei 97 %.

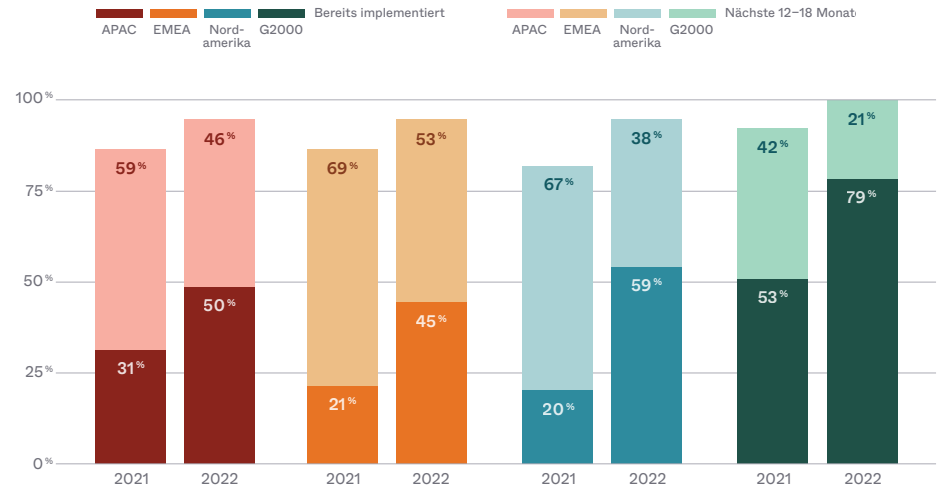
Jahresvergleich aller befragten Unternehmen Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten Monaten eines starten?



Jahresvergleich aller befragten Unternehmen Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten 12–18 Monaten eines starten?



Regionaler Jahresvergleich Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten 12–18 Monaten eines starten?

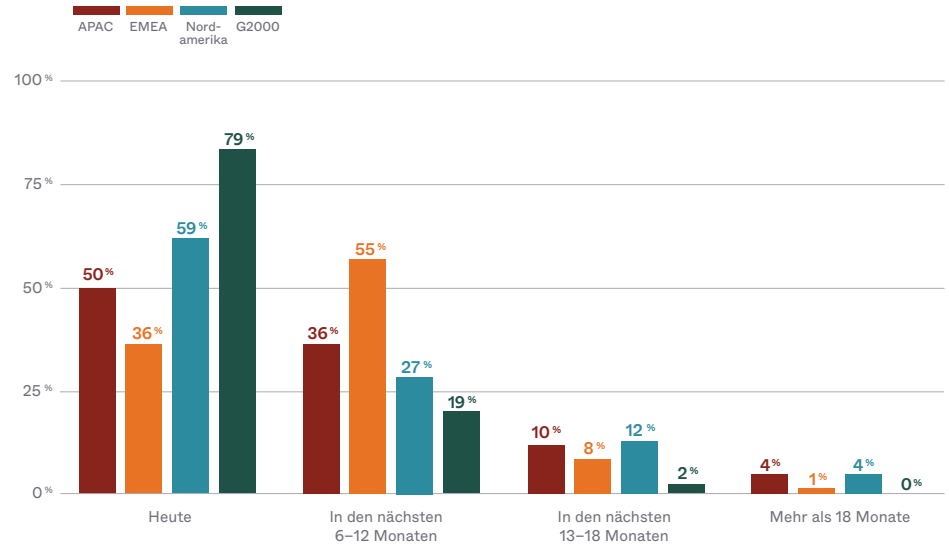


Der aktuelle Report belegt, dass dieses Konzept inzwischen praktisch flächendeckend umgesetzt wird: Fast alle befragten Unternehmen haben bereits ein Zero-Trust-Programm aufgelegt oder wollen dieses in den kommenden Monaten starten. Zudem wächst der Druck, hier schnell Fortschritte zu machen. Beispielsweise schreibt eine **Executive Order** der US-Regierung aus dem Jahr 2021 die Entwicklung einer Zero-Trust-Architektur für Behörden vor.

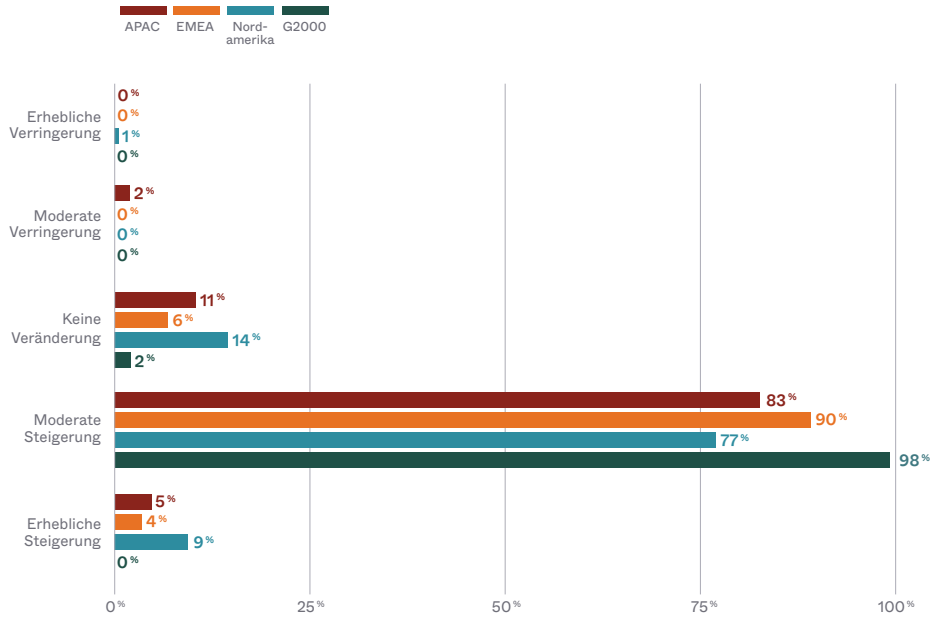
Und es bleibt nicht nur bei Plänen: Die Geschwindigkeit, mit der Unternehmen die Zero-Trust-Philosophie umsetzen, ist atemberaubend. Im Jahr 2021 berichteten 24 % der befragten Unternehmen, dass sie bereits eine Zero-Trust-Initiative implementiert haben. In diesem Jahr hat sich diese Zahl mit 55 % mehr als verdoppelt. In jeder untersuchten Region – Europa, Naher Osten und Afrika (EMEA), Asien-Pazifik-Raum (APAC) und Nordamerika – sowie bei den Global 2000-Unternehmen (G2000) erklärten mehr als 85 % der Umfrageteilnehmer, dass ihr Unternehmen im Vergleich zum Vorjahr einen moderaten oder in manchen Fällen sogar erheblichen Teil des Budgets für Zero-Trust-Initiativen abgestellt hat.

Unsere weltweite Umfrage zeigt außerdem deutlich, dass sich Zero-Trust-Initiativen nicht auf bestimmte Unternehmensgrößen, geografischen Standorte oder Branchen beschränken. Stattdessen erklärten alle Teilnehmer, dass sie auf dem kürzesten Weg Zero Trust ansteuern. In diesem Bericht untersuchen wir, wo die Unternehmen mit Blick auf den Schutz der Identities stehen, der zu den Kernprinzipien von Zero Trust gehört. Überdies analysieren wir ihren allgemeinen Fortschritt bei der Umsetzung von Zero-Trust-Initiativen in den nächsten Monaten und Jahren.

Regionaler Vergleich Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten Monaten eines starten?

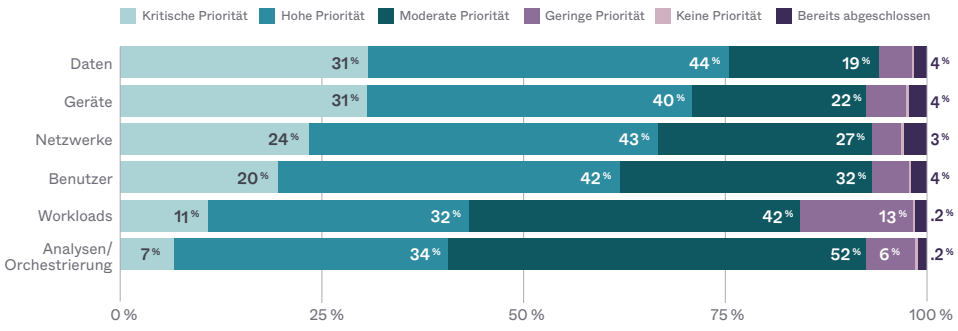


Regionaler Vergleich Wie hat sich Ihr Budget für Zero Trust in den vergangenen zwölf Monaten verändert (sofern zutreffend)?



Für den vierten jährlichen „State of Zero Trust"-Bericht befragte Okta 700 Security-Verantwortliche weltweit, was unsere bislang größte Umfrage dieser Art ist. Ziel war es, den aktuellen Stand bei der unternehmensweiten Einführung von Zero Trust Security zu ermitteln. Wir wollten wissen, welche konkreten Initiativen bereits umgesetzt wurden und wie diese kurz- und mittelfristig priorisiert werden sollen. Anhand des Zero Trust Frameworks, das von Forrester und CISA (Cybersecurity and Infrastructure Security Agency) veröffentlicht wurde, untersuchten wir die Prioritäten, die bei Zero-Trust-Initiativen heute am wichtigsten sind. Wenig überraschend zeigte sich, dass die Kategorien Daten, Netzwerk und Devices bei den befragten Unternehmen auch weiterhin die höchste Priorität haben. Wir gehen jedoch davon aus, dass sich das im Laufe der Zeit ändern könnte: Die Kategorie Benutzer gewinnt allmählich an Bedeutung, da die Unternehmen erkennen, dass sie es mit einem erweiterten Security-Perimeter zu tun haben, der weniger das Netzwerk und dafür stärker die Benutzer im Fokus hat. Identity ist ein wichtiger Bestandteil jedes Zero-Trust-Programms, wie wir in diesem Bericht ausführlich darlegen werden.

Alle Unternehmen weltweit Was sind die wichtigsten Anforderungen (nach Priorität) an Zero Trust in Ihrem Unternehmen?



Jedes Unternehmen muss seinen eigenen Weg hin zu Zero Trust finden – einen Weg, der die Best Practices der Branche, die Business-Vorgaben, die Budgets, die bestehenden Investitionen und andere Faktoren berücksichtigt. Auch wenn jeder Weg anders ist, das Ziel ist stets gleich: Unternehmen auf der ganzen Welt haben erkannt, dass die Implementierung einer zuverlässigen Zero-Trust-Infrastruktur für einen sicheren und skalierbaren zukünftigen Betrieb unverzichtbar ist.

Wichtige Erkenntnisse

Zero Trust ist kein Buzzword mehr
Die Implementierung eines Zero-Trust-Ansatzes ist für Unternehmen weltweit zum Standard-Security-Paradigma geworden. Die allermeisten haben bereits entsprechende Initiativen umgesetzt und suchen aktiv nach konkreten Lösungen, um ihren Weg zu Zero Trust zu beschleunigen. Eine starke Motivation sind dabei Sicherheitsbedenken: Unternehmen haben seit Langem Schwierigkeiten, die richtige Balance zwischen Security und Benutzerkomfort zu finden. Während der Benutzerkomfort in den letzten Jahren an erster Stelle stand, hat sich das Gleichgewicht in diesem Jahr verschoben, sodass die Security-Projekte für die Befragten eine etwas höhere Priorität erhalten haben.

Enterprise-Security kennt keine Patentrezepte.
Zero Trust ist ein robustes Leitprinzip, doch die Umsetzung ist ein komplexes Projekt, bei dem multiple Best-of-Breed-Lösungen nahtlos zusammenarbeiten müssen. Jedes Unternehmen verfügt über eine andere Ausgangssituation, unterschiedliche Ressourcen und Prioritäten, sodass sie auf unterschiedlichen Wegen das gleiche Ziel erreichen: echte Zero Trust Security.

Identities sind für die Umsetzung von Zero Trust entscheidend
Trotz aller Unterschiede haben Unternehmen auf der ganzen Welt erkannt, dass starke Identities für eine erfolgreiche Security- und Zero-Trust-Strategie entscheidend ist. Im Rahmen ihrer Zero-Trust-Initiativen treiben Unternehmen bei der Absicherung des neuen Perimeters – der Identity – enormen Aufwand. Und die konkreten Strategien für das Identity- und Access-Management (IAM), mit denen sie diese Initiativen unterstützen, lassen sich in fünf Phasen unterteilen, die wir im Folgenden genauer vorstellen.

Die Rolle von Identity bei Zero Trust

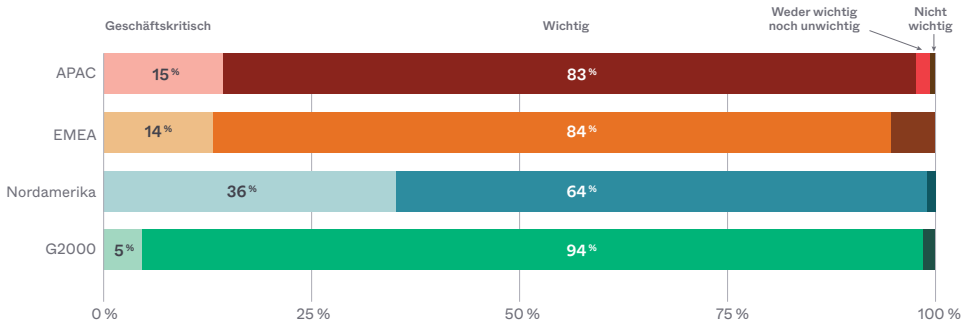
Identity: Der Kern aller Zero-Trust-Lösungen

Identity ist nicht die einzige Komponente eines umfassenden Zero-Trust-Frameworks, sie ist jedoch für jede Zero-Trust-Strategie von entscheidender Bedeutung. Sicherzustellen, dass jeder Anwender stets zur richtigen Zeit den richtigen Zugriff auf die richtigen Ressourcen hat, ist mit Blick auf die Security, das Management, die Compliance und viele weitere Business-Faktoren wichtiger denn je. Die Zero Trust Journey jedes Unternehmens ist einzigartig – und hängt ganz von den geschäftlichen Rahmenbedingungen, dem Tech-Stack und den strategischen Prioritäten ab. Heute herrscht unter Unternehmen auf der ganzen Welt weitgehend Konsens darüber, dass ein identitätsbasierter Zero-Trust-Ansatz die optimale Nutzung von IAM ermöglicht. Dabei wird IAM mit anderen wichtigen Security-Lösungen integriert und wird zu einer leistungsstarken zentrale Kontrollinstanz, die den Zugriff für Benutzer, Devices, Daten und Netzwerke intelligent steuert.

> “
> Die Zeit des „Burggraben“-Modells bei Netzwerken und Perimetern ist vorbei. Der neue Perimeter ist die Identity.
>
> John McLeod, CISO, NOV Inc.

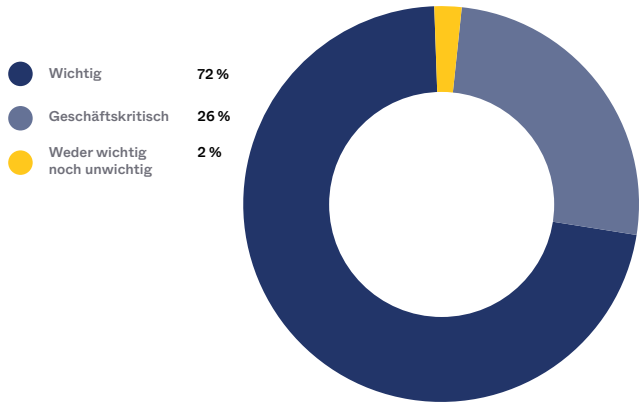
Wie wichtig ist Identity? In der diesjährigen Umfrage erklärten 80 % aller Unternehmen, dass Identität für ihre allgemeine Zero-Trust-Strategie wichtig ist, und weitere 19 % bezeichnen Identität sogar als geschäftskritisch. Damit ist Identity für 99 % der befragten Unternehmen ein wichtiges Element der Zero-Trust-Strategie. Unter den CISOs (Chief Information Security Officers) und anderen Führungskräften betrachten 26 % die Identität als geschäftskritisch (Anteil unter den 98 %, für die Identität wichtig ist). Daher überrascht es nicht, dass Gartner® den „Schutz der Identity-Systeme“ vor Kurzem im Artikel „7 Top Trends in Cybersecurity for 2022“ aufgeführt hat. Dabei weisen die Analysten darauf hin, dass der Missbrauch von Anmeldedaten für Angreifer eine der wichtigsten Methoden ist, um Zugriff auf Systeme zu erlangen und ihre Ziele zu erreichen.[4] Dies ist zwar schon seit mehreren Jahren der Fall, doch es gibt aktuell eine überraschende Zunahme bei der Erkennung und Offenlegung von Daten, sodass dieses Thema in vielen Vorständen Priorität erhalten hat.

Regionaler Vergleich Wie wichtig ist Identity für Ihre Zero-Trust-Gesamtstrategie?



[4] Gartner®: „7 Top Trends in Cybersecurity for 2022“, Susan Moore, 13. April 2022.

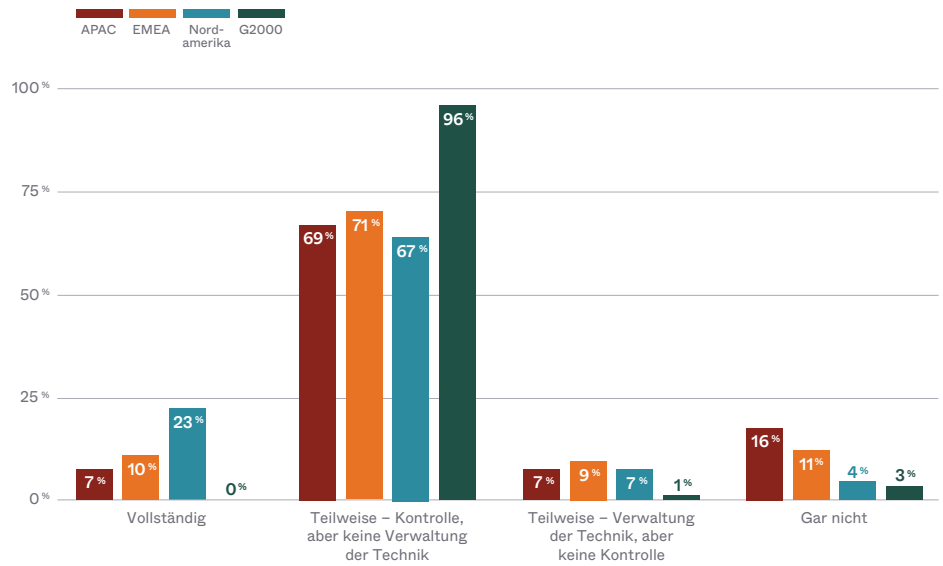
Befragte Vorstände Wie wichtig ist Identity für Ihre Zero-Trust-Gesamtstrategie?



Unternehmen arbeiten daran, Identities in ihre Zero-Trust-Initiativen und ihre Security-Strategien zu integrieren. Dazu sind enge Partnerschaften zwischen den IT- und Sicherheitsteams erforderlich. Sicherheit war schon immer eine Teamaufgabe. Doch angesichts zunehmend raffinierter Angriffe ist es heute wichtiger denn je, abteilungsübergreifend zu denken und die Silo-Ansätze der Vergangenheit zu überwinden. Das kann zum Beispiel zu neuen Schwierigkeiten führen, da immer mehr Verantwortlichen in Fragen rund um die Identity eingebunden werden müssen. Auf diese und andere neuen Probleme gehen wir im Folgenden ein.

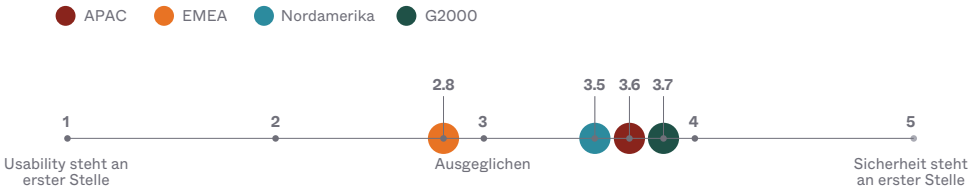
Die diesjährige Umfrage hat gezeigt, dass Sicherheitsteams von Forbes Global 2000-Unternehmen eher in großem Maßstab IAM-Technologien für ihre Sicherheitsprojekte einsetzen als Teams bei kleineren Unternehmen. Allerdings setzen immer mehr Sicherheitsteams zumindest zu einem gewissen Teil auf die Überwachung mit IAM. Im EMEA-Raum setzen 71 % der Sicherheitsteams diese Technologie zumindest teilweise ein – ein leichter Rückgang gegenüber den Ergebnissen aus dem letztjährigen Bericht. Demgegenüber sind die Zahlen im APAC-Raum und in Nordamerika praktisch unverändert geblieben.

Regionaler Vergleich In welchem Maße wird IAM (Identity and Access Management) in Ihrem Unternehmen eingesetzt?



Um wettbewerbsfähig zu bleiben und die Security nicht zu vernachlässigen, müssen Unternehmen ihre Assets für autorisierte Benutzer zugänglich machen und sie gleichzeitig vor Angreifern schützen. Die Suche nach der richtigen Balance zwischen Usability und Sicherheit ist eine ständige Herausforderung. Zu Beginn der COVID-19-Pandemie stand für viele Unternehmen die Usability im Vordergrund. Sie hatten keine andere Wahl – mussten sie doch sicherstellen, dass ihre seit Neuestem remote arbeitenden Mitarbeiter einfachen Zugriff auf alle für die Arbeit erforderlichen Tools und Assets haben. Im Jahr 2022 begannen die Unternehmen jedoch damit, sich umzuorientieren: Eine Mehrheit wies der Security nun eine etwas höhere Priorität als der Usability zu. Der neue Security-Fokus ist im APAC-Raum und Nordamerika stärker ausgeprägt, während Unternehmen im EMEA-Raum eine ausgeglichenere Balance zwischen Usability und Security anstreben. Warum neigt sich die Balance in Richtung Security? Unternehmen, die jetzt fest auf Remote- und Hybrid-Arbeit setzen, profitieren bereits von den während der Pandemie angestoßenen Investitionen in die Usability – und holen nun versäumte Security-Investitionen nach. Immer häufiger erkennen sie jedoch auch, dass stärkere Sicherheit und bessere Usability nicht im Widerspruch zueinander stehen müssen (wie zum Beispiel bei passwortloser Authentisierung). Durch die Priorisierung stärkerer Sicherheitsmaßnahmen lässt sich möglicherweise auch die Usability verbessern.

Regionaler Vergleich Wie finden Sie die richtige Balance zwischen Security und Usability in Ihrem Unternehmen?



Nutzung von Identity für Zero-Trust-Initiativen

Die fünf Phasen des Zero-Trust-Reifegrads

Unternehmen haben das allgemeine Konzept von Zero Trust und die Rolle der Identity in diesem Frameworks grundlegend implementiert. Aber wie steht es um konkrete Maßnahmen? Wir stellen einige konkrete Identity-Projekte vor, die Unternehmen jetzt vorantreiben und zur Unterstützung ihrer Zero-Trust-Initiativen für die Zukunft planen. Dabei nutzen wir das Okta Identity Adoption Model zur Unterstützung von Zero-Trust-Strategien. Dieses Modell unterteilt den Weg zu Zero Trust in fünf Phasen und zeigt Unternehmen, welche Priorität die Identity-Projekte in anderen Unternehmen genießen. Dazu gehört, was sie bereits erreicht und gerade erst begonnen haben, sowie welche Identity-Initiativen sie in den nächsten Monaten priorisieren und in Angriff nehmen wollen.

> Das Access Management ist für Identity-zentrierte Security die Source-of-Truth geworden.[5]
>
> Gartner®, *Magic Quadrant™ for Access Management*

Bei Unternehmen, die an der Implementierung einer nutzbaren Zero-Trust-Architektur arbeiten, die auf identitätsbasierten Security-Ansätzen basiert, beobachten wir fünf Phasen des Reifegrades:

Phase 1: Traditionell
Unternehmen, die am Anfang ihrer Cloud-Transformation stehen, versuchen die Herausforderungen der Cloud-Implementierung vorherzusehen oder spüren sie bereits. Dazu gehören isolierte Verzeichnisse, eine rasant wachsende Angriffsfläche sowie eine Zunahmen identitätsbasierter Attacken. In Phase 1 geht es um die ersten Schritte zu echter Zero Trust Security.

Folgende Identitätsprojekte fallen in diese Phase:

- Verbindung von Mitarbeiter-Directories mit geschäftskritischen Cloud-Anwendungen, um Transparenz darüber zu erhalten, wer worauf zugreift – unabhängig vom Standort
- Implementierung von Multi-Faktor-Authentifizierung (MFA) für Mitarbeiter, um unverzichtbaren Schutz vor Anmeldedatendiebstahl zu gewährleisten

Phase 2: Emerging
In dieser Phase treiben Unternehmen in der Regel den Ausbau ihrer Cloud-Umgebung sowie die Cloud-Nutzung voran. Dabei versuchen sie, von der Effizienz und Skalierbarkeit der Cloud zu profitieren – gleichzeitig aber die Benutzerzugriffe zu schützen und zu vereinfachen. Dadurch bleiben die remote oder hybrid arbeitenden Belegschaften sicher und produktiv.

Folgende Identity-Projekte fallen in diese Phase:

- Einführung von MFA für externe Benutzer wie Geschäftspartner und Lieferanten
- Implementierung von Single Sign-On (SSO) für Mitarbeiter für unterstützte Anwendungen
- Implementierung von Funktionen für die Self-Service-Reset von Faktoren zur Senkung der Helpdesk-Kosten
- Automatisierte Provisionierung und Deprovisionierung für Anwendungen

Phase 3: Reifend
In dieser Phase haben Unternehmen geeignete Prozesse und Business-Ziele für dynamische und remote Arbeitsmodelle entwickelt. Nun benötigen sie die richtigen Tools, um einer komplexen, weltweit tätigen Workforce zuverlässig und rund um die Uhr den Zugriff auf benötigte Unternehmens-Assets zu ermöglichen[5], ohne die Einhaltung der Compliance-Vorgaben zu gefährden.

[5]Gartner®: *„Magic Quadrant™ for Access Management“,* Henrique Teixeira, Abhyuday Data, Michael Kelley, 1. November 2021.

Folgende Identity-Projekte fallen in diese Phase:

- Ausweitung von SSO auf alle autorisierten externen Benutzer
- Automatisierte Provisionierung und Deprovisionierung für Mitarbeiter und externe Benutzer mit einem rollenbasierten Modell
- Ausarbeitung von Policy-Anforderungen zur SSO-Unterstützung für neue und bestehende Anwendungen
- Implementierung eines Privileged Access Managements in der Cloud-Infrastruktur
- Integration von Threat-Feeds von Endpunkten und Cloud-Anwendungen in die SIEM-Tools (Security Information and Event Management)

Phase 4: Gehoben

In dieser Phase wollen Unternehmen ihre Cloud-Erfolge konsolidieren und die Digitalisierung abschließen. Hierfür konsolidieren oder ersetzen sie veraltete Legacy-Technik nach Bedarf und schützen wichtige kundenspezifische Anwendungen, die ein Sicherheitsrisiko darstellen könnten.

Folgende Identity-Projekte fallen in diese Phase:

- Verwendung unterschiedlicher Authentifizierungsfaktoren für verschiedene Benutzergruppen je nach Risiko sowie zur Senkung der Lizenzierungskosten
- Implementierung von sicherem Zugriff für APIs (Application Programming Interfaces)
- Implementierung kontextbasierter Zugriffsrichtlinien
- Bereitstellung von Tools, die als Proxy agieren, um Legacy-Technologien zu modernisieren
- Orchestrierung der Security-Lösungen, um schneller auf neue Bedrohungen reagieren zu können

Phase 5: Voll entwickelt

Unternehmen in dieser Phase haben grundlegende Zero Trust Security implementiert und können diese Echtzeittransparenz für fundierte Zugriffsentscheidungen nutzen. Außerdem können sie bestehende Entscheidungen basierend auf ständig aktualisierten Informationen anpassen. So können Sie sich auf weitere Innovationen konzentrieren und diese kontinuierlich implementieren: etwa den Schutz des Enterprise Access am Edge und die Ausweitung des benutzerfreundlichen passwortlosen Zugriffs auf alle Unternehmens-Assets.

Folgende Identity-Projekte fallen in diese Phase:

- Bereitstellung von passwortlosem Zugriff überall im Unternehmen
- Fundierte Zugriffsentscheidungen auf Datenebene anhand des Benutzer- und Gerätestatus

Identity Adoption Model für Zero-Trust-Initiativen Die fünf Phasen der Identity-Implementierung

Phase 1: Traditionell Am Anfang der Journey wird über die Rolle nachgedacht, die Identity bei Sicherheitsstrategien spielt

Phase 2: Emerging Konzentriert sich auf die Optimierung der User Experience mit dedizierten Security-Maßnahmen für cloudbasierte Anwendungen

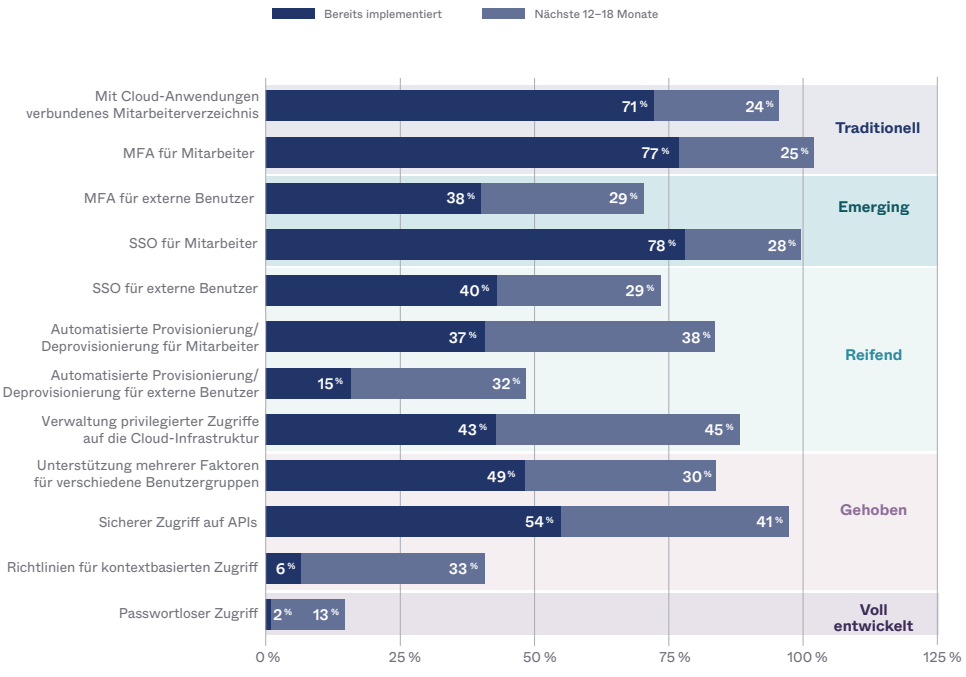
Phase 3: Reifend Betrachtet Identity als zentrale Komponente der Security-Policy und der User-Experience

Phase 4: Gehoben Erweitert den Schutz auf Legacy-Technologien und konsolidiert Identity- und Security-Strategien

Phase 5: Voll entwickelt Identity ist in ein modernes Security-Konzept integriert, das auf die Anforderungen digitalisierter Unternehmen ausgelegt ist und Least Privileged Access unterstützt

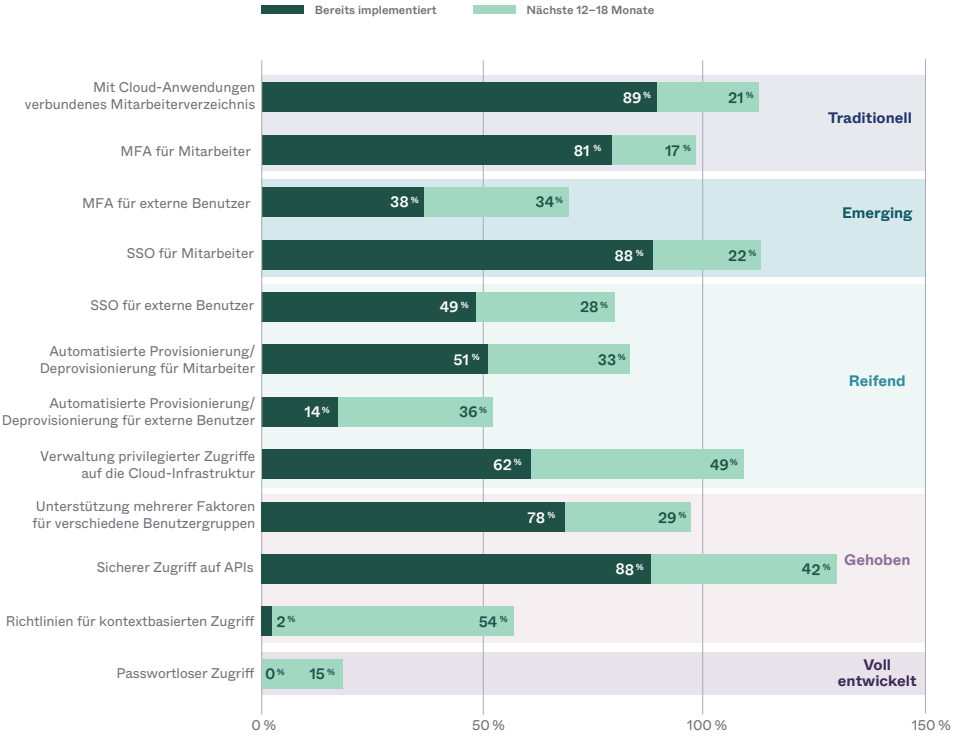
Zero Trust ist für Unternehmen kein leeres Versprechen: Die meisten Unternehmen haben die Implementierung von Zero Trust Security zumindest begonnen, angefangen bei wichtigen Identitätsinitiativen. Unsere Umfrage hat gezeigt, dass mehr als 70 % der weltweiten Teilnehmer Phase 1 (Traditionell) bereits hinter sich gelassen haben. Ganze 95 % der Umfrageteilnehmer möchten die Projekte aus Phase 1 in den nächsten 12–18 Monaten abschließen und arbeiten gerade an der Planung für Projekte der späteren Phasen. Was die Umsetzung von Phase 2 (Emerging) betrifft, hat die Mehrheit der Befragten (fast 80 %) SSO für ihre Mitarbeiter ausgerollt. Aber gerade einmal 38 % geben an, dass ihre Unternehmen MFA auf externe Benutzer ausgedehnt haben, um zu gewährleisten, dass der Zugriff auf kritische Ressourcen auf autorisierte Auftragnehmer, Lieferanten und Geschäftspartner beschränkt bleibt. Wie unten zu sehen ist, geht der Fortschritt bei Zero Trust nach Phase 2 auseinander. Fast 50 % der weltweiten Umfrageteilnehmer haben bereits die ersten Identity-Projekte aus späteren Reifephasen abgeschlossen. Ein Großteil der übrigen Teilnehmer hat die Absicht, diese Folgeprojekte in den kommenden Monaten in Angriff zu nehmen.

Alle Unternehmen weltweit Nutzung von Identity für Zero-Trust-Initiativen



Betrachtet man die Unternehmen der Forbes Global 2000 als Gruppe, planen sämtliche dieser Umfrageteilnehmer den Abschluss aller Identity-Projekte aus Phase 1 innerhalb der nächsten 18 Monate (sofern nicht bereits geschehen). Und mindestens die Hälfte der Befragten aus diesen Unternehmen haben in der gleichen Zeit alle Projekte der Phasen 1–4 abgeschlossen und mit Arbeiten an Phase-5-Projekten begonnen.

Global 2000-Unternehmen Welche Projekte hat Ihr Unternehmen aktuell implementiert und welche haben in den nächsten 12–18 Monaten für Sie Priorität?



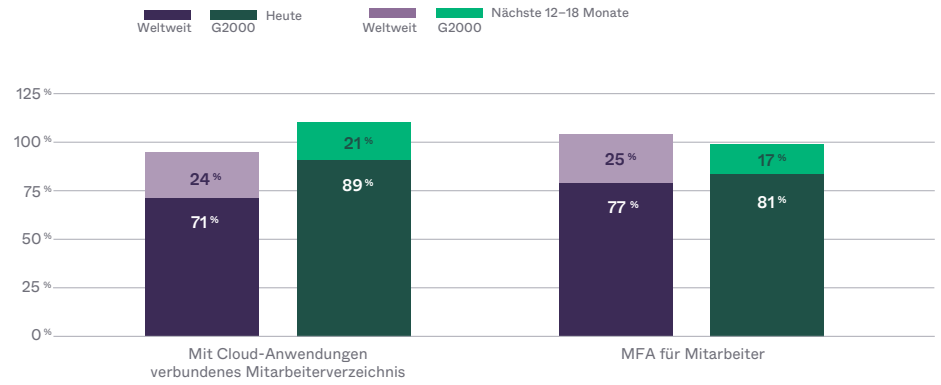
Phase 1: Traditionell

Am Anfang der Zero Trust Journey haben Unternehmen im Bereich Identity mit grundlegenden Problemen wie isolierten Verzeichnissen, einer wachsenden Angriffsfläche sowie einer steigenden Zahl identitätsbasierter Angriffe zu kämpfen. Um den Fortschritt in dieser Reifephase zu ermitteln, wollten wir von den Unternehmen wissen, ob ihre Mitarbeiter-Directories mit ihren Cloud-Anwendungen verbunden sind und ob sie MFA für ihre Mitarbeiter implementiert haben. Wir stellten fest, dass selbst Unternehmen in Phase 1 über effektive Möglichkeiten verfügen, den richtigen Mitarbeitern Zugriff auf die richtigen Ressourcen zu gewähren, indem sie mehrere Sicherheitsebenen zu ihrem Authentifizierungsprozess hinzufügen.

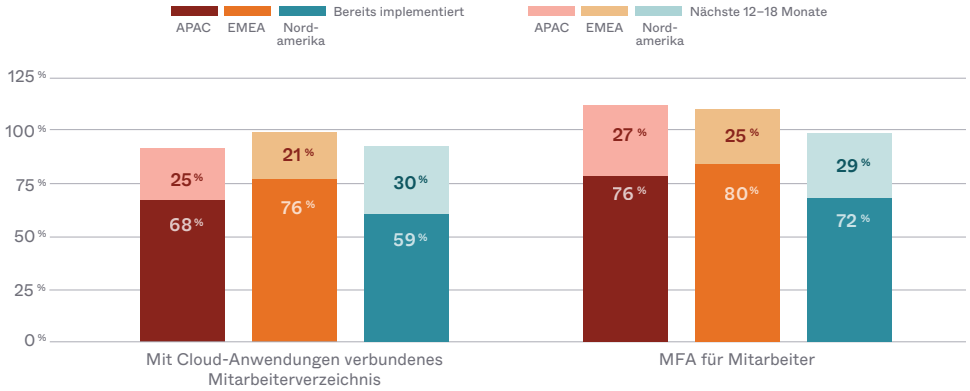
Wie der Report zeigt, wollen in den nächsten 18 Monaten fast 100 % aller Umfrageteilnehmer in weltweit tätigen oder in der Global 2000 gelisteten Unternehmen die Identity-Projekte aus Phase 1 abschließen. Die Bereitstellung von MFA für Mitarbeiter ist das insgesamt am häufigsten implementierte Identity-Projekt. Und in den nächsten 18 Monaten wollen 100 % der Umfrageteilnehmer

aus allen Regionen im Rahmen ihrer allgemeinen Identity-Strategie MFA für Mitarbeiter integrieren. Weniger Umfrageteilnehmer haben erklärt, dass das Directory ihres Unternehmens bereits mit den Cloud-Anwendungen verbunden ist. Viele arbeiten jedoch noch an ihrer Cloud-Migration und planen, dieses Identity-Projekt in den nächsten 18 Monaten abzuschließen.

Phase 1 bei allen Unternehmen weltweit und Global 2000-Unternehmen Welche Projekte hat Ihr Unternehmen aktuell implementiert und welche haben in den nächsten 12–18 Monaten für Sie Priorität?



Regionaler Vergleich für Phase 1 Welche Projekte hat Ihr Unternehmen aktuell implementiert und welche haben in den nächsten 12–18 Monaten für Sie Priorität?

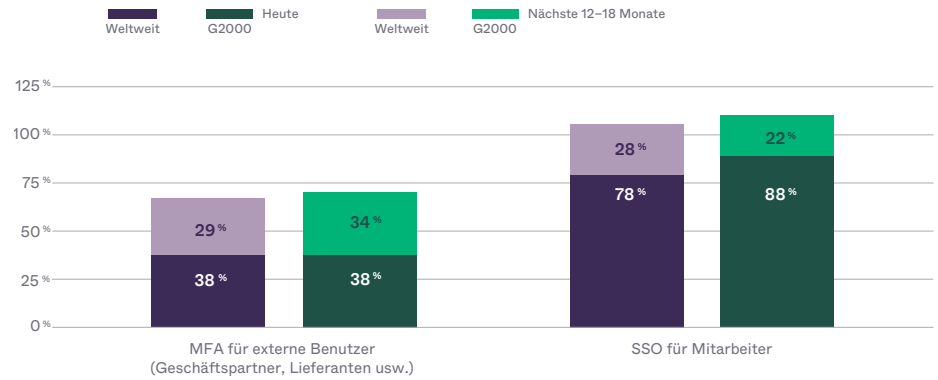


Phase 2: Emerging

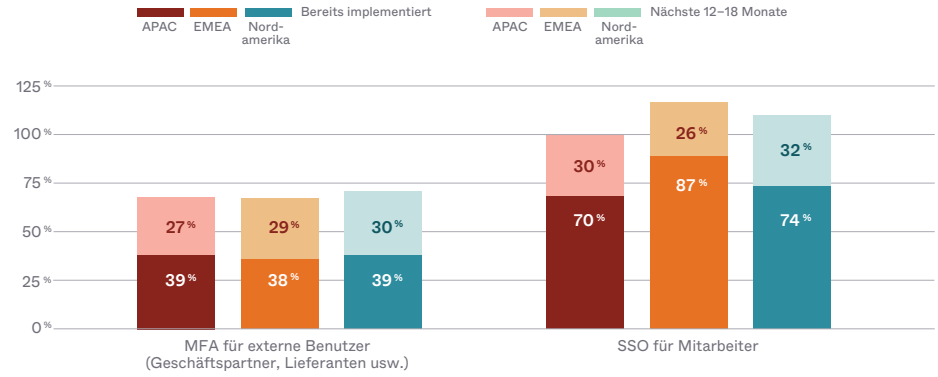
In dieser Phase versuchen Unternehmen meist, die Aktivitäten zwischen isolierten Systemen zu korrelieren, die etwa im Zuge der Cloud-Einführung oder im Zuge von M&A-Prozessen entstanden sind – und die mit einem höheren Bedarf an komfortablen Benutzerzugriffen einhergehen. Um den Fortschritt in Phase 2 bewerten zu können, wollten wir von den Umfrageteilnehmern wissen, ob ihr Unternehmen bereits MFA für externe Benutzer (einschließlich Geschäftspartner und Lieferanten) implementiert hat und ob sie SSO für Mitarbeiter bereitstellen, damit diese einfacher auf ihre Business-Tools zugreifen können.

Laut unseren Daten will mehr als die Hälfte der Umfrageteilnehmer aus jeder Region die Projekte aus Phase 2 innerhalb der nächsten 12–18 Monaten abschließen (sofern nicht bereits geschehen). Immer mehr Unternehmen beschäftigen nicht nur remote arbeitende Angestellte, sondern arbeiten auch mit externen Auftragnehmern, Freiwilligen, Lieferanten und Teilzeit-Mitarbeitern zusammen. Diese Personen stellen ein wachsendes Sicherheitsrisiko dar. Ihre Einbindung in das MFA-Konzept hat für die Unternehmen in allen Regionen Priorität, da sie auf diese Weise ihre Ressourcen sicher bereitstellen können. Die Zahlen bei MFA für externe Benutzer sind bei Unternehmen aller Größen praktisch identisch, während SSO für Mitarbeiter bei Global 2000-Unternehmen häufiger anzutreffen ist als bei kleineren Firmen (88 % bzw. 78 %).

Phase 2 bei allen Unternehmen weltweit und Global 2000-Unternehmen Welche Projekte hat Ihr Unternehmen aktuell implementiert und welche haben in den nächsten 12–18 Monaten für Sie Priorität?



Regionaler Vergleich für Phase 2 Welche Projekte hat Ihr Unternehmen aktuell implementiert und welche haben in den nächsten 12–18 Monaten für Sie Priorität?



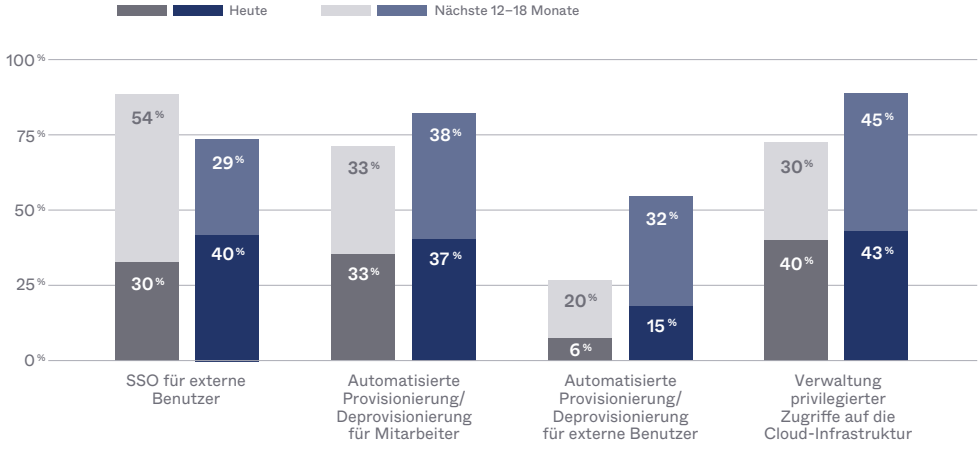
Phase 3: Reifend

Unternehmen in Phase 3 stehen vor komplexen Herausforderungen wie strengeren Compliance-Vorgaben, hybriden Infrastrukturen sowie der Anforderung, eine große, aktive, dynamische und mindestens teilweise remote arbeitende Belegschaft unterstützen zu müssen. Um diese Herausforderungen zu meistern, müssen sie ihre IAM-Funktionalitäten über die Workforce und das Legacy-Netzwerk hinaus ausdehnen. Nur so können sie der steigenden Zahl externer Benutzer sowie den wachsenden Cloud- oder Multi-Cloud-Infrastrukturen Rechnung

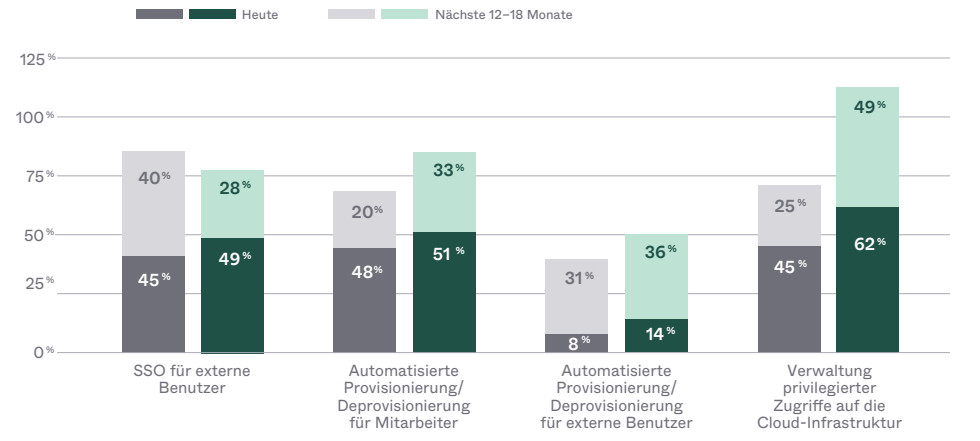
tragen. Um den Fortschritt in Phase 3 bewerten zu können, wollten wir von den Umfrageteilnehmern wissen, ob sie ihre Provisionierung und Deprovisionierung für Mitarbeiter und externe Benutzer bereits automatisiert haben. Außerdem fragten wir, ob sie ein Privileged Access Management (PAM) für ihre Cloud-Infrastruktur implementiert haben.

Diese Phase wurde von weniger Unternehmen erreicht, doch fast die Hälfte der Unternehmen weltweit und der Global 2000 wollen die Initiativen aus Phase 3 bis Ende 2023 abschließen. Unternehmen in der APAC-Region legen besonders hohen Wert auf die Automatisierung der Provisionierung und Deprovisionierung von Mitarbeitern (von 22 % auf 76 %). Zudem arbeiten mehr von ihnen daran, innerhalb der nächsten 18 Monate PAM für die Cloud zu integrierten (von 44 % auf 88 %). Alle Umfrageteilnehmer aus Nordamerika wollen in den nächsten 12–18 Monaten sowohl PAM in der Cloud als auch SSO für externe Benutzer bereitstellen. Auch die Befragten aus EMEA-Unternehmen haben vor, die Implementierung von PAM in ihrer Cloud-Infrastruktur mehr als zu verdoppeln. Innerhalb der nächsten 18 Monate soll die Implementierung 100 % erreichen.

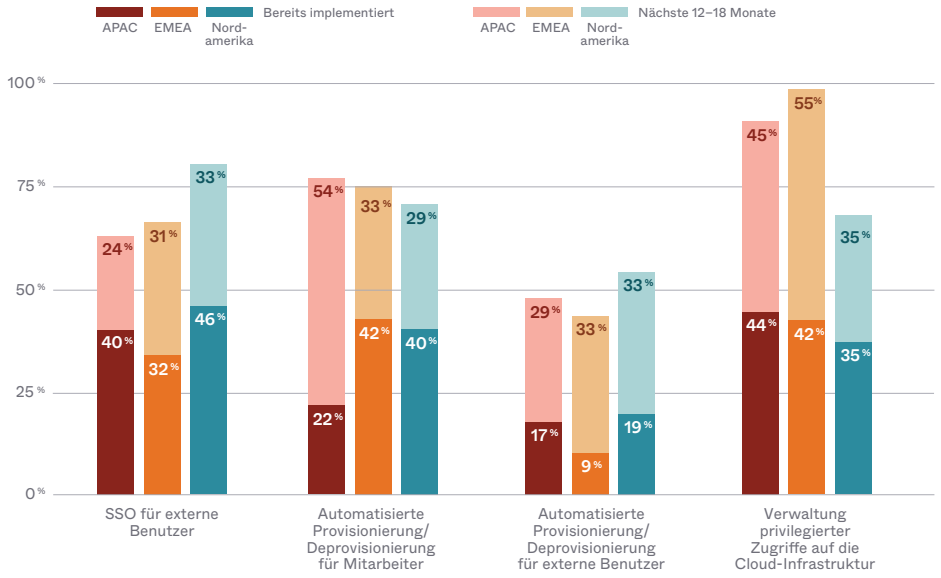
Phase 3 bei allen Unternehmen weltweit im Jahresvergleich Welche Projekte hat Ihr Unternehmen aktuell implementiert und welche haben in den nächsten 12–18 Monaten für Sie Priorität?



Global 2000-Unternehmen im Jahresvergleich für Phase 3 Welche Projekte hat Ihr Unternehmen aktuell implementiert und welche haben in den nächsten 12–18 Monaten für Sie Priorität?

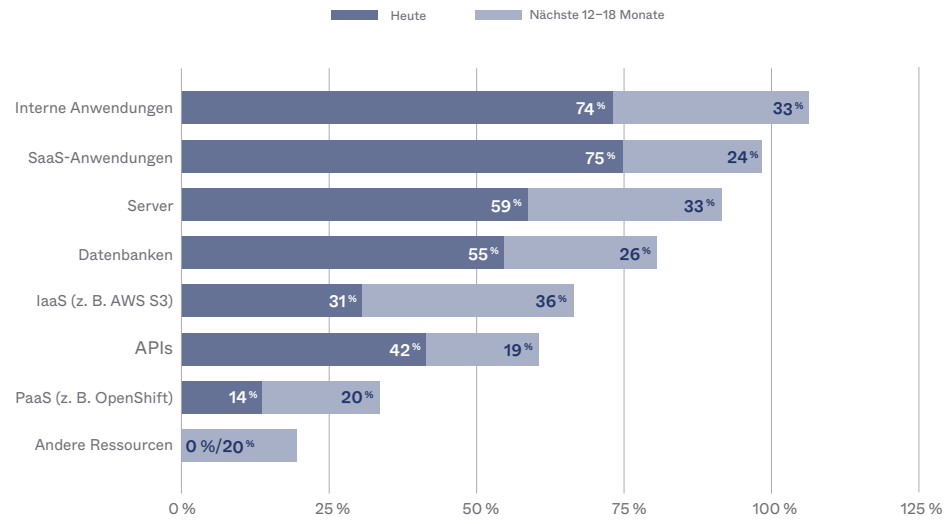


Regionaler Vergleich für Phase 3 Welche Projekte hat Ihr Unternehmen aktuell implementiert und welche haben in den nächsten 12–18 Monaten für Sie Priorität?



Die Bereitstellung von MFA und SSO – zwei Stützpfeilern moderner Security- und Usability-Konzepte – auf die Unternehmensressourcen setzt sich allmählich auf breiter Front durch: Fast 75 % aller weltweiten Umfrageteilnehmer erklärten, dass sie MFA, SSO oder beides auf interne und SaaS-Anwendungen (Software-as-a-Service) ausgeweitet haben. Mindestens 99 % wollen das in den nächsten 12–18 Monaten erreichen (sofern nicht bereits erfolgt). Die Integration von SSO, MFA oder beidem in IaaS-Umgebungen (Infrastructure-as-a-Service) soll in den nächsten 12–18 Monaten ebenfalls einen enormen Sprung tun, da Unternehmen auf der ganzen Welt den Zugriff auf diese wichtigen Ressourcen absichern wollen. Die Implementierung soll sich bis 2023 mehr als verdoppeln – von 31 % auf 67 %.

Alle Unternehmen weltweit Auf welche Arten von Ressourcen haben Sie SSO bzw. MFA bereits ausgeweitet? (Mehrfachnennungen möglich)

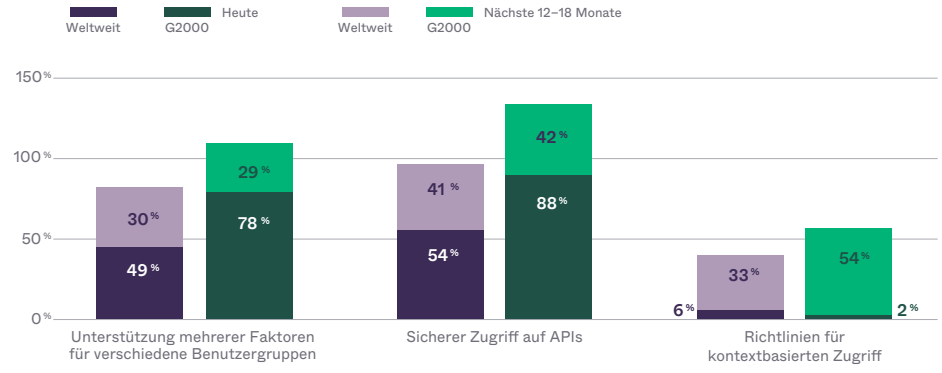


Phase 4: Gehoben

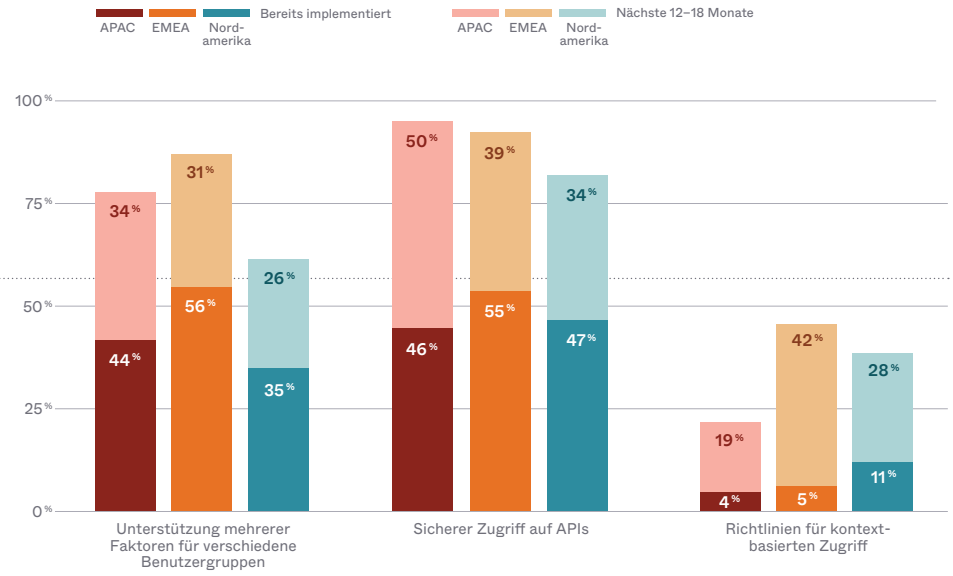
Unternehmen im oberen Segment der Reifegradkurve haben die Grundlagen von Identity-basiertem Zero Trust im Griff und verfügen über geeignete Tools und Prozesse, um immer komplexere Herausforderungen im Bereich Identität zu meistern. Wir wollten wissen, welche Fortschritte die Unternehmen in Bezug auf die folgenden Initiativen aus Phase 4 gemacht haben: Sind sie bereit, mehrere Authentifizierungsfaktoren für verschiedene Benutzergruppen zu implementieren, um Reibungsverluste zu minimieren, die Remote-Produktivität zu verbessern sowie das Prinzip „Nie vertrauen, immer prüfen“ durchzusetzen? Haben sie sichere Zugriffe auf APIs integriert? Haben sie kontextbasierte Zugriffsrichtlinien implementiert?

Alle befragten Global 2000-Unternehmen wollen ihre Identity-Projekte – einschließlich der Implementierung von MFA für verschiedene Benutzergruppen und der Absicherung der API-Zugriffe – in den nächsten 12–18 Monaten abschließen. Mindestens die Hälfte dieser Unternehmen haben vor, alle Identity-Projekte aus Phase 4 in einem vergleichbaren Zeitrahmen abzuschließen. Besonderer Schwerpunkt liegt dabei auf kontextbasierten Zugriffsrichtlinien, zum Beispiel anhand der Vertrauenswürdigkeit des für den Zugriffsversuch genutzten Endgerätes, anhand des Gerätestandort, des Benutzer bzw. der Ressource selbst sowie anhand weiterer wichtiger Eigenschaften. Umfrageteilnehmer aus Unternehmen in Nordamerika liegen mit der Absichtserklärung, mehrere Faktoren für verschiedene Benutzer zu implementieren und den Zugriff auf APIs abzusichern, aktuell hinter ihren Kollegen aus den APAC- und EMEA-Regionen. Auch sie planen aber, in den nächsten Monaten erhebliche Fortschritte zu machen.

Alle Unternehmen weltweit und Global 2000-Unternehmen: Welche Projekte hat Ihr Unternehmen aktuell implementiert und welche haben in den nächsten 12–18 Monaten für Sie Priorität?

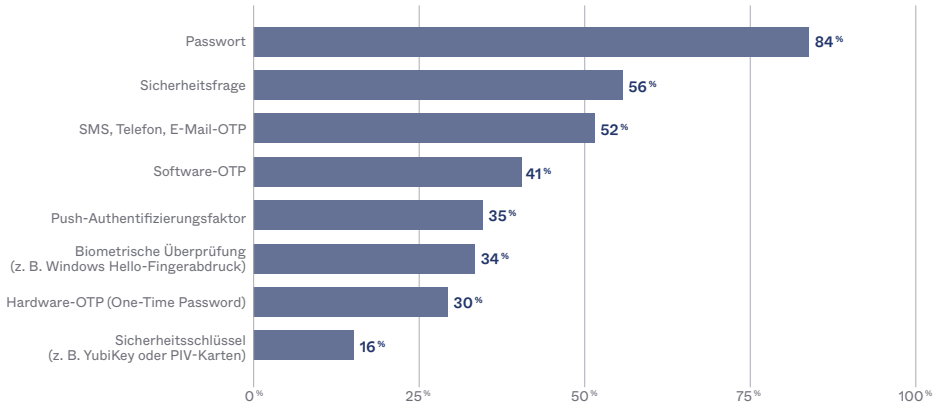


Regionaler Vergleich für Phase 4 Welche Projekte hat Ihr Unternehmen aktuell implementiert und welche haben in den nächsten 12–18 Monaten für Sie Priorität?



Wenig überraschend sind Passwörter auch weiterhin der am häufigsten eingesetzte Sicherheitsfaktor, was ein Problem darstellt: Wie bereits erwähnt hält sich „123456“ hartnäckig auf Platz 1 der am häufigsten genutzten Passwörter.[6] Auf eine positive Nachricht weist der jährliche erscheinende Okta-Bericht **Businesses at Work** von Anfang dieses Jahres hin: Unternehmen bauen die MFA-Nutzung aus und ersetzen Faktoren mit geringerer Sicherheit (z. B. Passwörter) durch sicherere Faktoren. Der Anteil der Unternehmen, die bei der Verifizierung interner sowie externer Benutzer noch auf Passwörter setzen, ist in diesem Jahr um 10 Prozentpunkte auf 84 % gesunken. Im gleichen Zeitraum ist die Nutzung der sichereren Push-Authentifizierung um mehr als 20 Prozentpunkte gestiegen.

Alle Unternehmen weltweit Wählen Sie die Authentifizierungsfaktoren aus, mit denen Ihr Unternehmen interne und externe Benutzer verifiziert. (Mehrfachnennungen möglich)

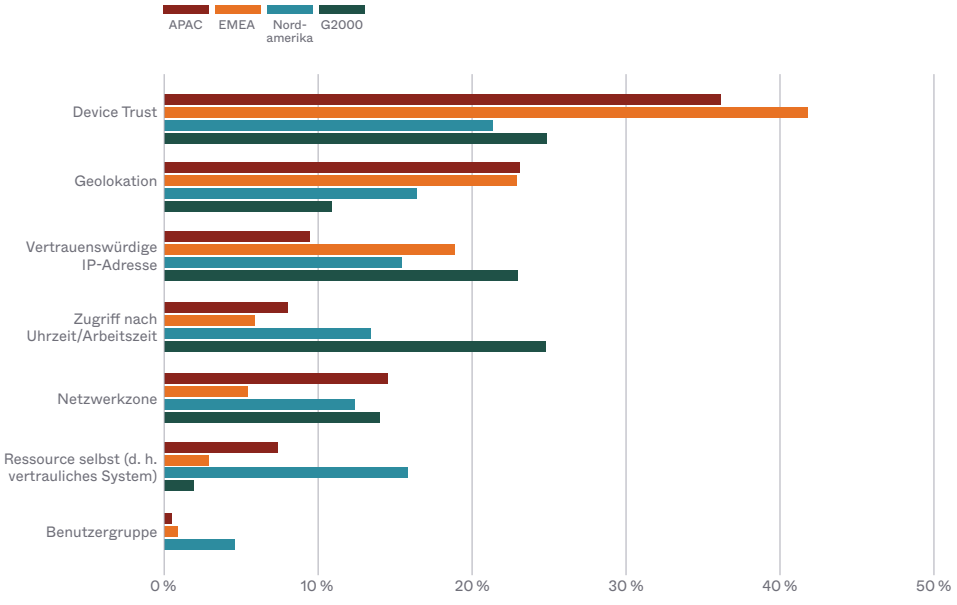


[6] Okta: „**Businesses at Work, 2022**“.

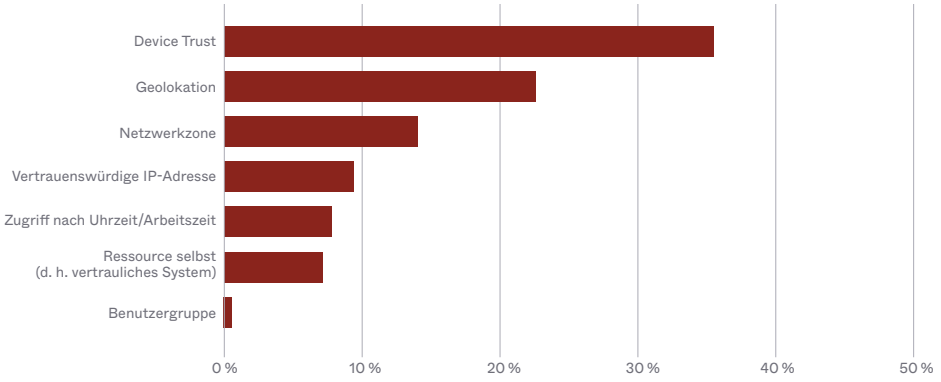
> Kompromittierte Passwörter sind meist der erste Schritt in der Data Breach Kill Chain. Auf diese Weise erlangen Angreifer Zugang zum Netzwerk, wo sie sich lateral bewegen, um weiterführende Rechte zu erlangen. Passwörter allein sind nicht mehr ausreichend sicher oder ausreichend, um Identitäten zu authentifizieren und unsere digitalen Assets zu schützen.
>
> Trey Ray, Manager of Cybersecurity, FedEx

Weltweit betrachtet, bewerten die Umfrageteilnehmer folgende Attribute als besonders wichtig, um den Zugriff auf interne Ressourcen zu bewerten und zu genehmigen: Device Trust, geografischer Standort, Vertrauenswürdigkeit der IP-Adresse. Device Trust – einschließlich Informationen darüber, ob das Gerät verwaltet wird, ob es bekannt ist und ob es verifiziert und sicher ist – war in jeder Region das wichtigste Attribut. Regional gab es jedoch Unterschiede: Für Umfrageteilnehmer aus dem APAC-Raum ist die Netzwerkzone ein wichtigeres Attribut als eine vertrauenswürdige IP-Adresse. Demgegenüber ist für Unternehmen in Nordamerika die Ressource selbst (z. B. eine vertrauliche Datenbank) im Wesentlichen gleichauf mit Geolokation und vertrauenswürdiger IP-Adresse. Die Global 2000-Unternehmen bewerten die Geolokation als weitaus weniger wichtig: Tageszeit und Netzwerkzone wurden als etwas wichtiger als vertrauenswürdige IP-Adressen eingeschätzt, während Geolokation nur den fünften Platz einnahm.

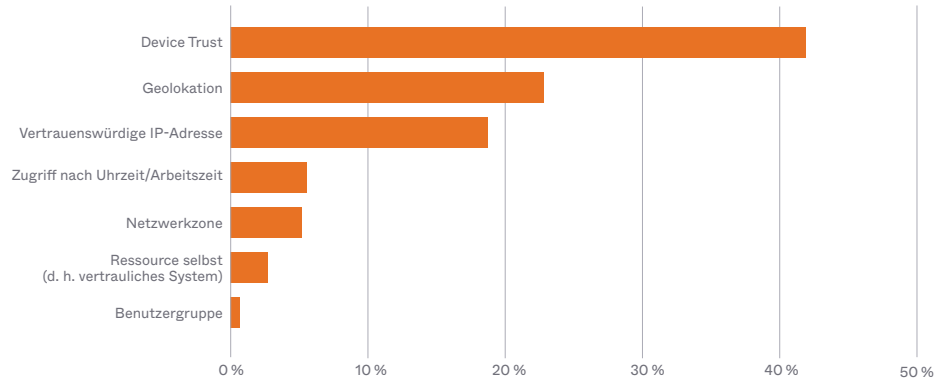
Regionaler Vergleich Was sind aus Ihrer Sicht die drei wichtigsten Faktoren bei der Steuerung und Gewährung von Zugriffen auf Ihre internen Ressourcen?



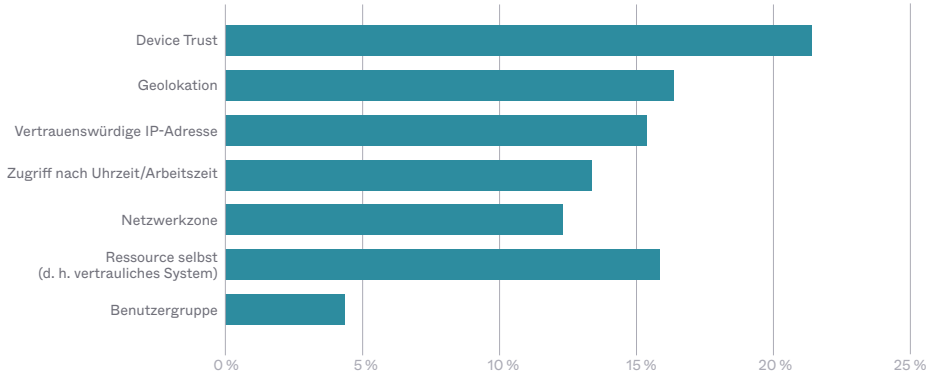
APAC-Region Was sind aus Ihrer Sicht die wichtigsten Faktoren bei der Steuerung und Gewährung von Zugriffen auf Ihre internen Ressourcen?



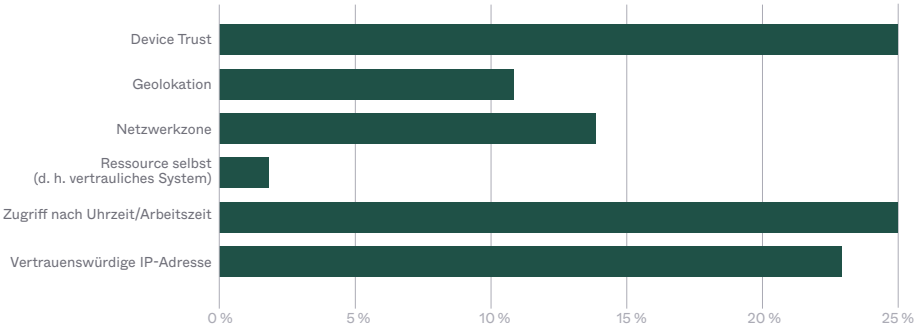
EMEA-Region Was sind aus Ihrer Sicht die wichtigsten Faktoren bei der Steuerung und Gewährung von Zugriffen auf Ihre internen Ressourcen?



Nordamerika Was sind aus Ihrer Sicht die wichtigsten Faktoren bei der Steuerung und Gewährung von Zugriffen auf Ihre internen Ressourcen?



Global 2000-Unternehmen Was sind aus Ihrer Sicht die wichtigsten Faktoren bei der Steuerung und Gewährung von Zugriffen auf Ihre internen Ressourcen?

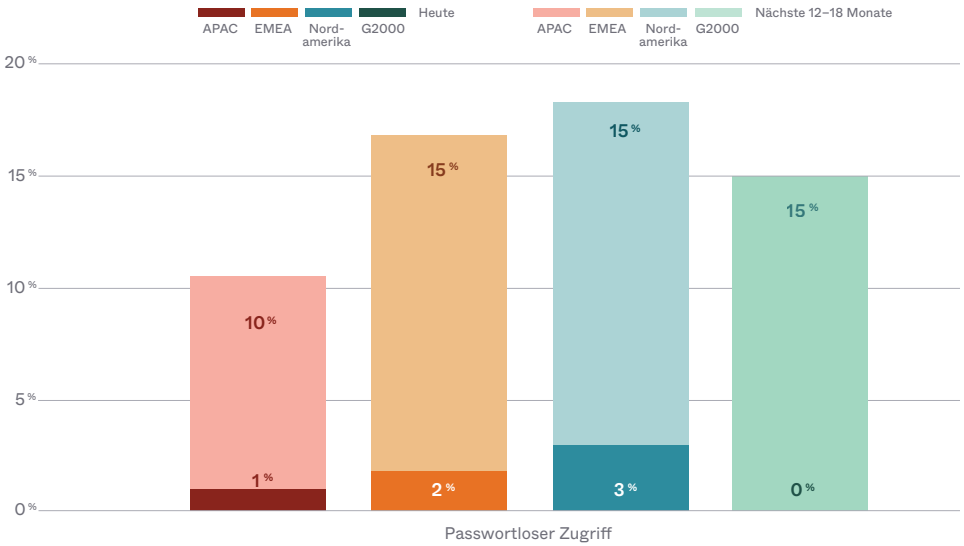


Phase 5: Voll entwickelt

Unternehmen in dieser Phase haben ihren Betrieb bereits auf Cloud-basierte Plattformen wie Amazon Web Services (AWS), Google Cloud (GCP) oder Microsoft Azure verlagert und konzentrieren sich auf die Einführung und Automatisierung der Edge Security. Hier verlagert sich der Fokus von der Implementierung der grundlegenden Zero-Trust-Projekte aus früheren Phasen auf die Optimierung des User-Lifecycle-Managements. Dabei werden sichere Zugriffskontrollen für Server integriert und passwortlose Zugriffe auf der Basis hochsicherer Faktoren wie Faktorsequenzierung, biometrische Anmeldung per Web-Authentifizierung (WebAuthn) sowie U2F-Sicherheitsschlüssel (Universal 2nd Factor) ermöglicht.

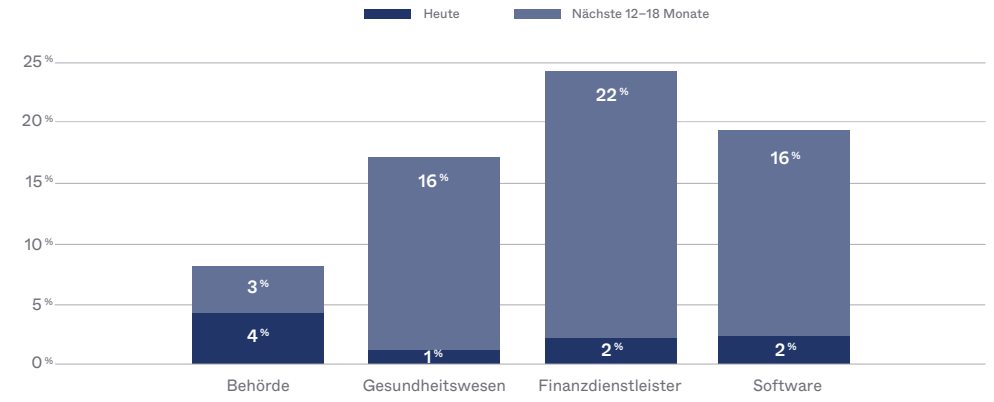
Zuversichtlich stimmt uns, dass Umfrageteilnehmer aus allen Regionen die Implementierung von passwortlosem Zugriff in den nächsten 12–18 Monaten vorantreiben wollen. Das ist insbesondere deshalb erfreulich, weil heute bei mehr als der Hälfte aller Datensicherheitsverstöße schwache oder gestohlene Anmeldedaten eine Rolle spielen – und der Missbrauch von Anmeldedaten für die Zunahme von Ransomware-Angriffen und weiteren Identity-basierten Attacken verantwortlich ist.[3] Unternehmen in Nordamerika liegen bei der Implementierung passwortloser Zugriffsoptionen an der Spitze – und viele weitere nordamerikanische Umfrageteilnehmer wollen in den nächsten Monaten nachziehen.

Regionaler Vergleich Haben Sie bereits passwortlose Zugriffsoptionen implementiert oder planen das in den nächsten 12–18 Monaten?



Nach Branche betrachtet wollen fast 22 % der befragten Finanzdienstleister in den kommenden 12–18 Monaten passwortlose Zugriffsoptionen integrieren. Im Gesundheitswesen und im Software-Sektor wollen das 16 % der Unternehmen. Nachzügler sind Behörden, von denen nur etwa 7 % passwortlose Zugriffe bieten oder die Implementierung in den nächsten Monaten planen.

Branchenvergleich Haben Sie bereits passwortlose Zugriffsoptionen implementiert oder planen das in den nächsten 12–18 Monaten?



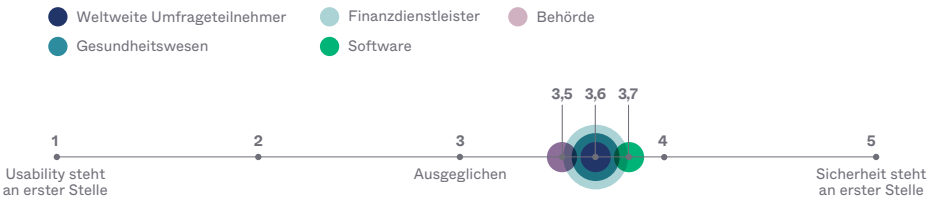
Branchen

Zero-Trust-Fortschritt nach Branche

Jede Branche (und letztendlich jedes Unternehmen) verfügt über eigene Vorgaben, Prioritäten und Bestimmungen und folgt einem jeweils eigenen Weg zu Zero Trust. Bei der diesjährigen Untersuchung sahen wir uns vier wichtige Branchen genauer an: Gesundheitswesen, Finanzdienstleister, Software-Unternehmen und – zum ersten Mal – Behörden. Dadurch wollten wir besser verstehen, wie sich die individuellen Anforderungen der Unternehmen in diesen Sektoren auf die Einführung von Zero Trust auswirken. Insbesondere wollten wir wissen, wie diese vier Branchen die richtige Balance zwischen Security und Usability finden.

Unternehmen suchen natürlich nach Möglichkeiten, um beides zu erreichen. Interessant ist, dass die Umfrageteilnehmer in diesem Jahr der Security im Durchschnitt einen höheren Stellenwert einräumen als der Usability – anders als noch 2021, als Benutzerkomfort leicht vor der Sicherheit lag. Ein Beispiel für einen stärkeren Fokus auf Sicherheit: Branchen wie das Gesundheitswesen reduzieren die Abhängigkeit von unsicheren Faktoren wie Passwörtern, die anfällig für Angriffe mithilfe von Anmeldedaten sind. In allen Zielmärkten waren die vier größten Herausforderungen bei der Implementierung einer Zero-Trust-Sicherheitsstrategie bemerkenswert gleich: Die größte Hürde ist in diesem Jahr der Fachkräftemangel, gefolgt von der Unterstützung der Stakeholder, Kostenbedenken und fehlende Informationen zu Security-Lösungen, die Zero Trust unterstützen.

Wie finden Sie die richtige Balance zwischen Security und Usability in Ihrem Unternehmen?

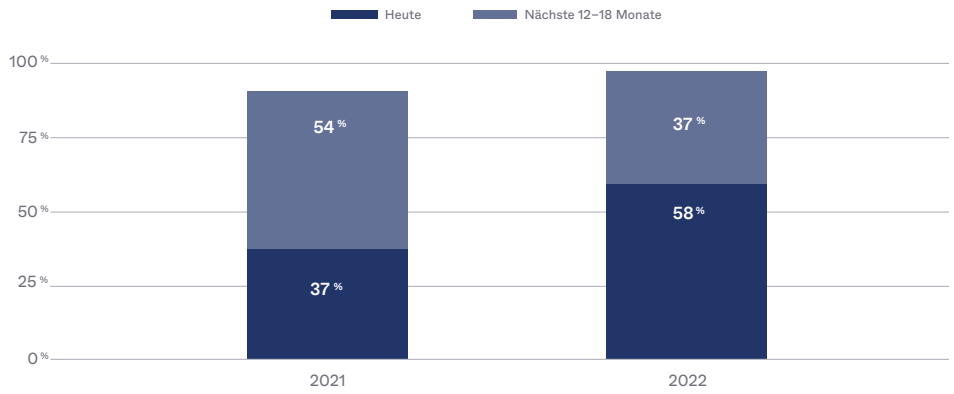


Wichtigste Sektoren

Gesundheitswesen

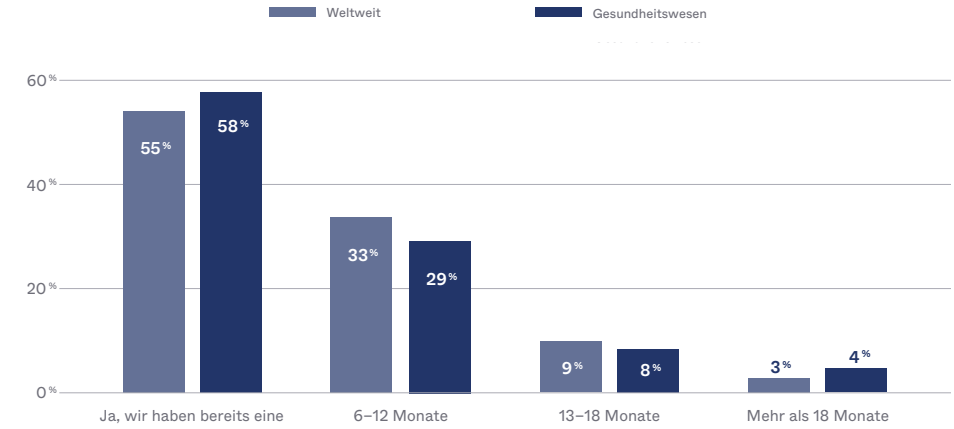
Die letzten Zauderer im Gesundheitswesen finalisieren derzeit ihre Pläne für die Zero-Trust-Implementierung: Die Zahl der Umfrageteilnehmer aus dem Gesundheitswesen, die eine Zero-Trust-Initiative vorantreiben oder sie in den nächsten 12–18 Monaten angehen wollen, ist von 91 % (2021) auf 96 % (2022) gestiegen. Beeindruckende 58 % der Befragten im Gesundheitswesen haben bereits mit der Implementierung ihrer Zero-Trust-Initiativen begonnen, was eine beinahe 21-prozentige Zunahme gegenüber den 37 % bedeutet, die im Bericht des vergangenen Jahres damit begonnen hatten. Die Mehrheit der Umfrageteilnehmer aus Gesundheitsunternehmen, die noch keine Zero-Trust-Initiative implementiert haben, wollen das innerhalb der nächsten 6–12 Monate nachholen.

Gesundheitswesen im Jahresvergleich Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten 12–18 Monaten eines starten?

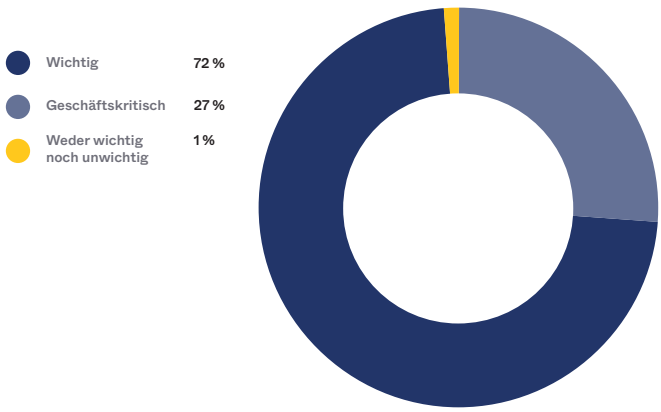


Für ganze 98 % der Befragten in diesem Sektor spielt Identity bei ihren allgemeinen Zero-Trust-Sicherheitsstrategien eine wichtige Rolle. Für 72 % ist Identity wichtig und für 27 % sogar geschäftskritisch. Und sie setzen diese Strategien in die Tat um: Die Mehrheit der Umfrageteilnehmer aus dem Gesundheitswesen haben bereits ein Zero-Trust-Programm ins Leben gerufen – und die meisten übrigen wollen entsprechende Initiativen innerhalb der nächsten 6–12 Monate starten. Zu den wichtigsten Identity-Projekten, die sie in dieser Zeit abschließen wollen, gehört die Ausdehnung von SSO auf die Mitarbeiter sowie die Absicherung des Zugriff auf APIs.

Alle Unternehmen weltweit und Einrichtungen des Gesundheitswesens im Vergleich
Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten Monaten eines starten?

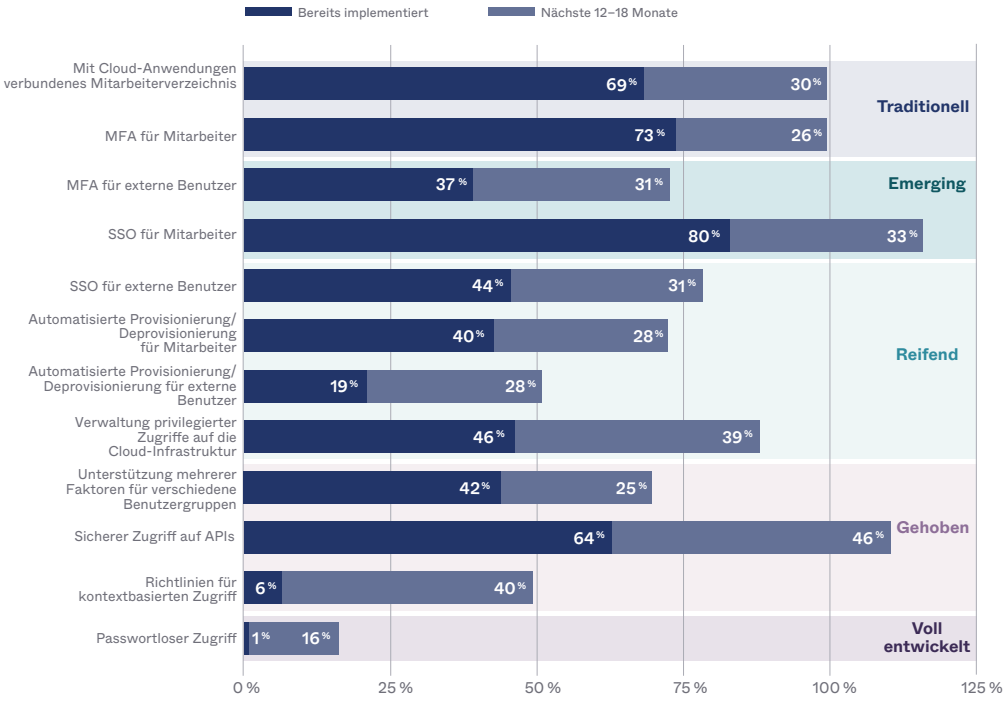


Gesundheitswesen Wie wichtig ist Identity für Ihre Zero-Trust-Strategie?

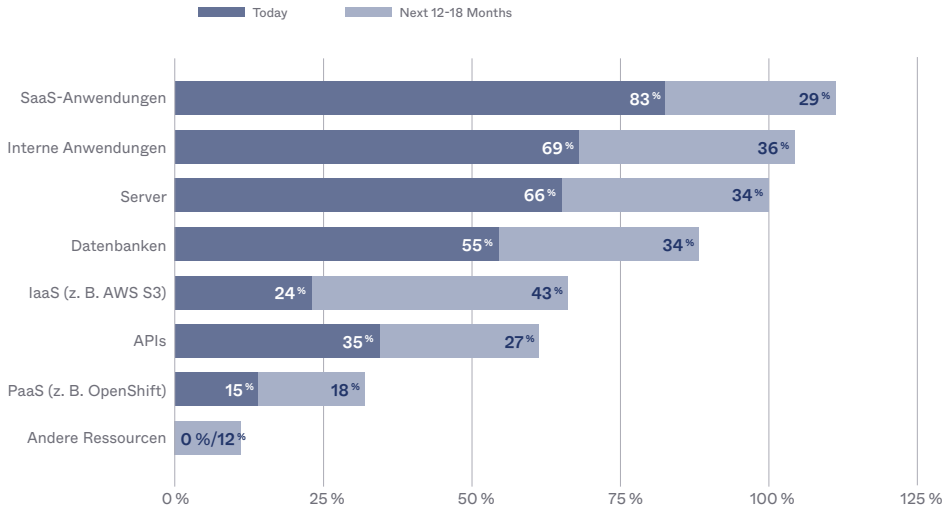


In den nächsten Monaten werden in diesem Sektor verstärkt kontextbasierte Zugriffsrichtlinien implementiert: Nur 6 % der Unternehmen nutzen bislang entsprechende Policies, doch weitere 40 % wollen sie in den nächsten 12–18 Monaten einführen. Alle Umfrageteilnehmer haben in den kommenden 12–18 Monaten vor, SSO, MFA oder beides in SaaS-Anwendungen, interne Anwendungen und Server zu integrieren. Gesundheitsunternehmen konzentrieren sich auch auf IaaS. Die Zahl der Befragten, die SSO, MFA oder beides auf diese Ressourcenkategorie ausdehnen möchten, wird sich in den nächsten Monaten fast verdreifachen.

Gesundheitswesen Welche der folgenden Initiativen hat Ihr Unternehmen aktuell implementiert und welche sollen in den nächsten 12–18 Monaten implementiert werden?

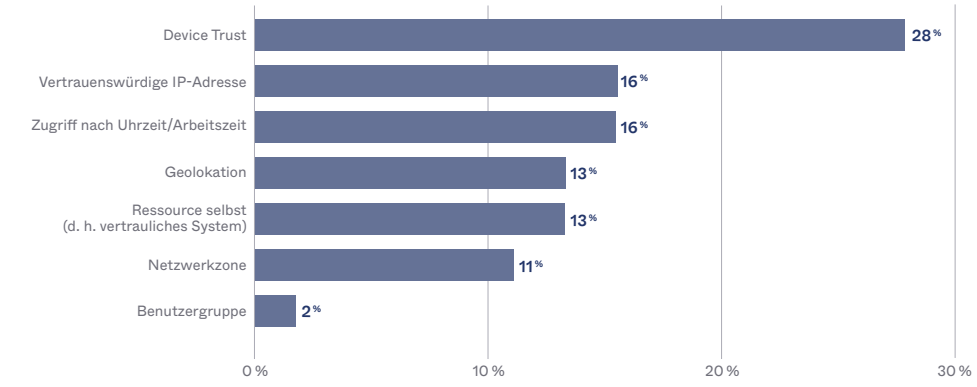


Gesundheitswesen Auf welche Arten von Ressourcen haben Sie SSO bzw. MFA bereits ausgeweitet?



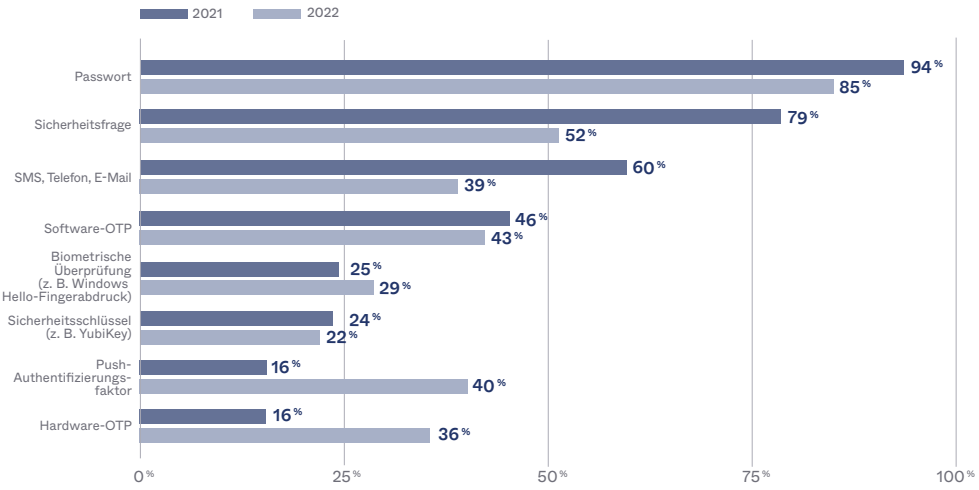
Drei Faktoren wurden 2022 von Gesundheitsunternehmen für die Kontrolle und Gewährung des Zugriffs auf interne Ressourcen als besonders wichtig genannt: Device Trust, geografischer Standort und vertrauenswürdige IP-Adresse. Während Device Trust mit einigem Abstand an der Spitze steht, sind in diesem Sektor andere Faktoren fast ebenso wichtig, zum Beispiel der Zugriff basierend auf Uhrzeit oder Arbeitszeiten und die Vertraulichkeit der Ressource.

Gesundheitswesen Was ist aus Ihrer Sicht der wichtigste Faktor bei der Steuerung und Gewährung von Zugriffen auf Ihre internen Ressourcen?



Im Jahresvergleich ist der Anteil der Gesundheitsunternehmen, die noch Passwörter einsetzen (geringere Sicherheit) zurückgegangen, während die Implementierung von Push Authentifizierung (höhere Sicherheit) von 16 % im letzten Jahr auf über 40 % in diesem Jahr gestiegen ist.

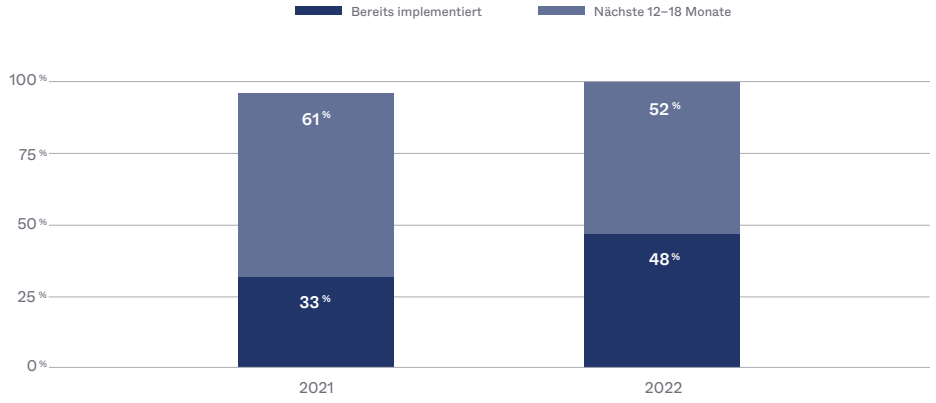
Gesundheitswesen im Jahresvergleich Wählen Sie die Authentifizierungsfaktoren aus, mit denen Ihr Unternehmen interne und externe Benutzer verifiziert. (Mehrfachnennungen möglich)



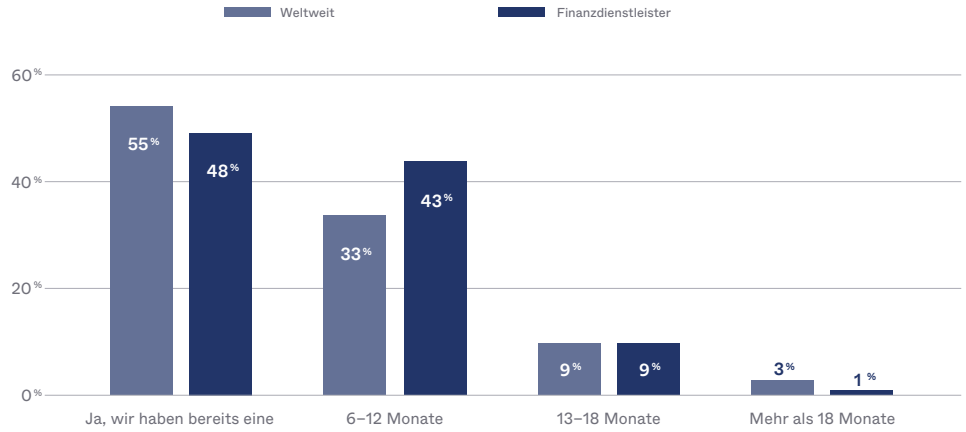
Finanzdienstleister

Zero Trust hat für Unternehmen im Finanzdienstleistungsbereich einen hohen Stellenwert: Innerhalb der kommenden 12–18 Monate wollen fast alle Befragten aus diesem Sektor eine Zero-Trust-Initiative starten. Tatsächlich hat fast die Hälfte der Umfrageteilnehmer (48 %) bereits eine solche Initiative am Laufen. Im vergangenen Jahr war es nur ein Drittel der Befragten – eine Steigerung um satte 15 Prozentpunkte.

Finanzdienstleistungen im Jahresvergleich Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten 12–18 Monaten eines starten?

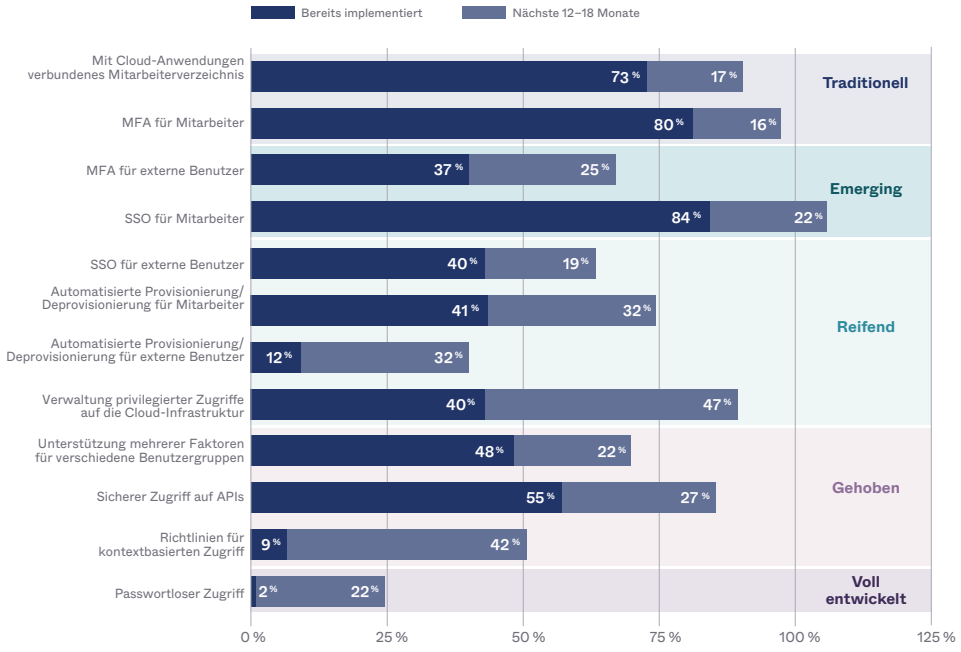


Alle Unternehmen weltweit und Finanzdienstleister im Vergleich Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten Monaten eines starten?



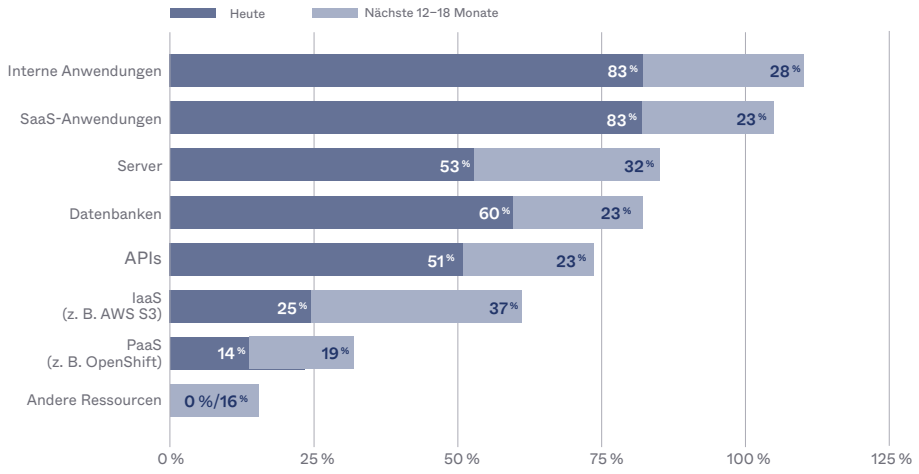
Dabei haben die meisten Finanzdienstleister bereits mit der Definition von Zero-Trust-Initiativen begonnen. Die allermeisten Unternehmen in diesem Sektor, die noch keine definierte Zero-Trust-Initiative implementiert haben, wollen das innerhalb der nächsten 6–12 Monate nachholen. Im Vergleich zu anderen Sektoren hängen Finanzdienstleister beim Zero-Trust-Reifegrad leicht hinterher, sie haben jedoch spezifische und konkrete Pläne, um kurzfristig erhebliche Fortschritte zu erzielen.

Finanzdienstleister Welche der folgenden Initiativen hat Ihr Unternehmen aktuell implementiert bzw. welche sollen in den nächsten 12–18 Monaten implementiert werden?



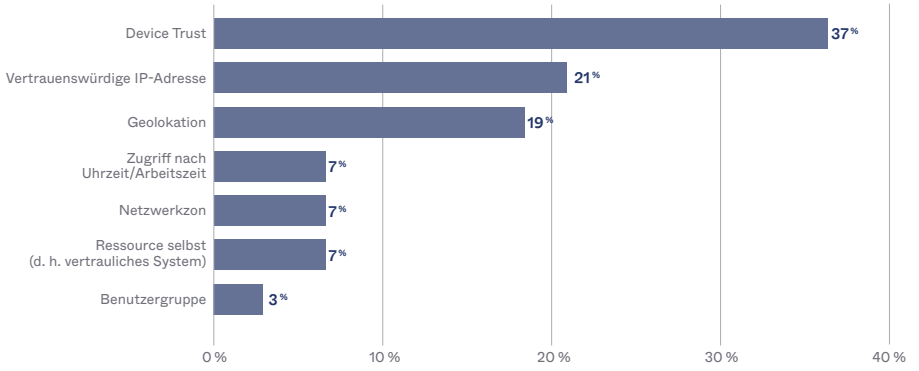
Alle Umfrageteilnehmer in diesem Sektor haben SSO, MFA oder beides bereits auf SaaS-Anwendungen und interne Anwendungen ausgedehnt oder haben das in den kommenden 12–18 Monaten vor. Ein Blick auf die Details zeigt, dass Finanzdienstleister zusätzliche Verifizierungsfaktoren für die Authentifizierung nutzen möchten. Das bedeutet die Ausdehnung von SSO auf alle Endpunkte (wo immer möglich), einschließlich SaaS- und lokaler Anwendungen, sowie die Einführung von Multi-Faktor-Authentifizierung (wo immer möglich). Dies gilt insbesondere für vertrauliche Anwendungen für Geldüberweisungen und -zahlungen sowie für alle privilegierten Zugriffe. Ein weiteres Identity-Projekt, auf das sich Finanzdienstleister in den kommenden Monaten konzentrieren werden, ist IaaS. Allein die bereits bestehenden Pläne würden die IaaS-Implementierungsrate bis Ende 2023 mehr als verdoppeln. Insgesamt wollen fast 75 % (oder mehr) der befragten Finanzdienstleister innerhalb der nächsten 18 Monate SSO, MFA oder beides auf Server, Datenbanken und APIs ausdehnen.

Finanzdienstleister Auf welche Arten von Ressourcen haben Sie SSO bzw. MFA bereits ausgedehnt oder wollen das in den nächsten 12–18 Monaten tun?

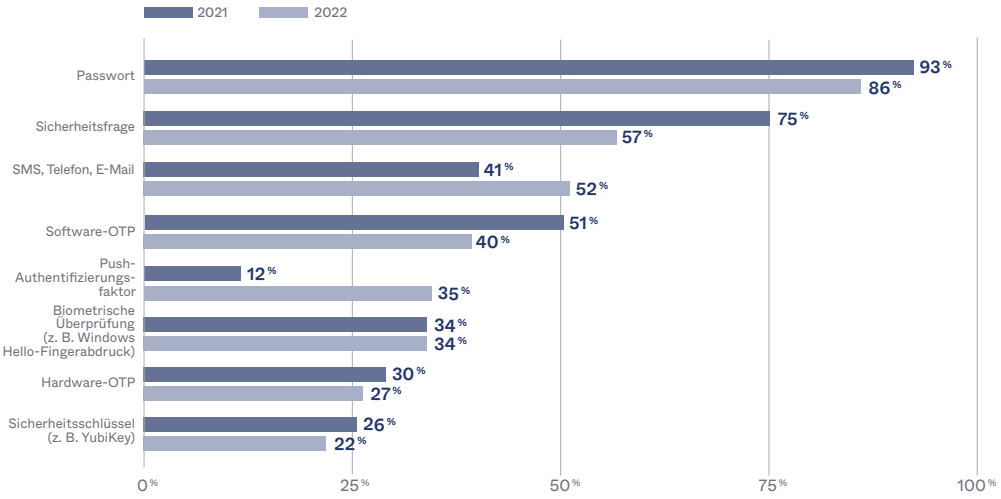


Für die befragten Beschäftigten aus dem Finanzdienstleistungssektor ist Device Trust der wichtigste Faktor bei der Kontrolle und Gewährung des Zugriffs auf interne Ressourcen. Mehr als 36 % der Umfrageteilnehmer bezeichneten das als ihren wichtigsten Authentifizierungsfaktor. Die Zahl der Befragten aus diesem Sektor, die Passwörter und Sicherheitsfragen als Authentifizierungsfaktoren nutzen, ist seit dem letzten Jahr zurückgegangen. Dagegen hat die Nutzung von Push-Authentifizierung, einem sichereren Faktor, um mehr als 20 Prozentpunkte zugenommen.

Finanzdienstleister Was sind aus Ihrer Sicht die wichtigsten Faktoren bei der Steuerung und Gewährung von Zugriffen auf Ihre internen Ressourcen?



Finanzdienstleister im Jahresvergleich Wählen Sie die Authentifizierungsfaktoren aus, mit denen Ihr Unternehmen interne und externe Benutzer verifiziert. (Mehrfachnennungen möglich)

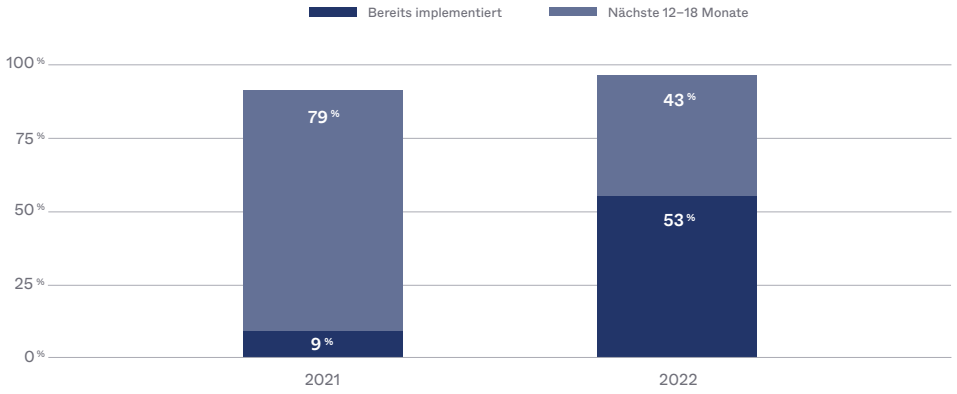


Software

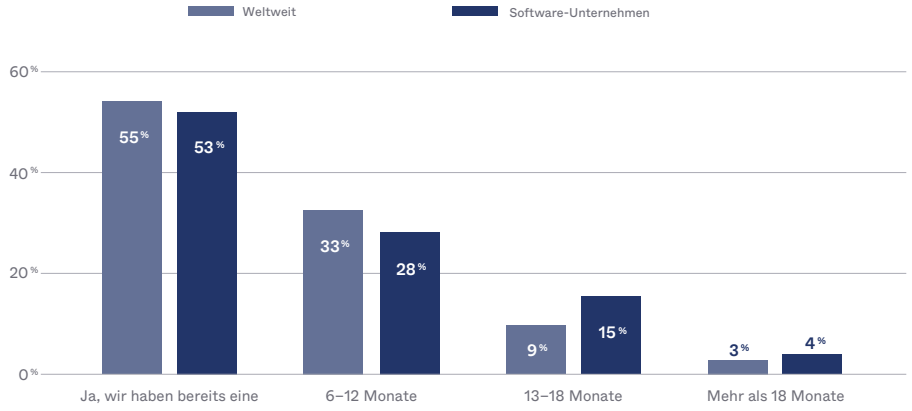
Im letztjährigen Bericht hatte die Software-Branche einen erheblichen Abstand hinter den anderen untersuchten Sektoren. Damals erklärten die Umfrageteilnehmer aus Software-Unternehmen jedoch, dass sie in den folgenden 12–18 Monaten ihre Zero-Trust-Projekte vorantreiben würden – und sie haben dieses Ziel mehr als erreicht. 2021 hatten nur 9 % der untersuchten Software-Unternehmen eine konkrete Zero-Trust-Initiative angestoßen, weitere 79 % wollten damit beginnen. In diesem Jahr stieg die Zahl der Unternehmen mit einer laufenden Initiative auf fast 53 % – und weitere rund 43 % wollen in den nächsten 12–18 Monaten eine konkrete Initiative beginnen. Insgesamt haben also ganze 96 % der Software-Unternehmen ihren Zero Trust Journey zumindest begonnen. Bei der Zero-Trust-

Implementierung haben wir die gleiche schnelle Zunahme verzeichnet, was zeigt, dass Software-Unternehmen schnell reagieren. Das Tempo, mit der sie ihre Zero-Trust-Strategien definieren, steigt, und die Unternehmen rechnen üblicherweise mit der Implementierung einer Zero-Trust-Initiative innerhalb der nächsten 6–12 Monate.

Software-Unternehmen im Jahresvergleich Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten 12–18 Monaten eines starten?

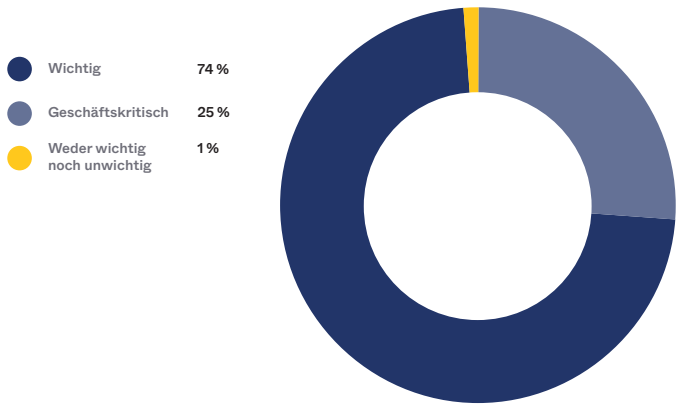


Alle Unternehmen weltweit und Software-Unternehmen im Vergleich Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten Monaten eines starten?



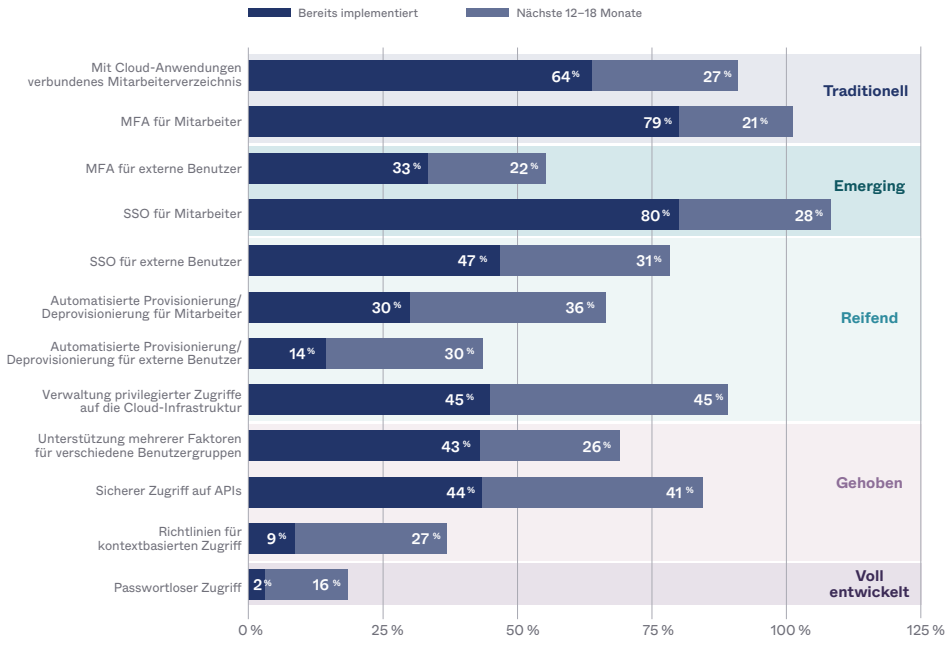
99 % der Umfrageteilnehmer aus dem Software-Sektor erklären, dass Identity für ihre allgemeine Zero-Trust-Strategie wichtig oder geschäftskritisch (25 %) ist.

Software-Unternehmen Wie wichtig ist Identity für Ihre Zero-Trust-Strategie?

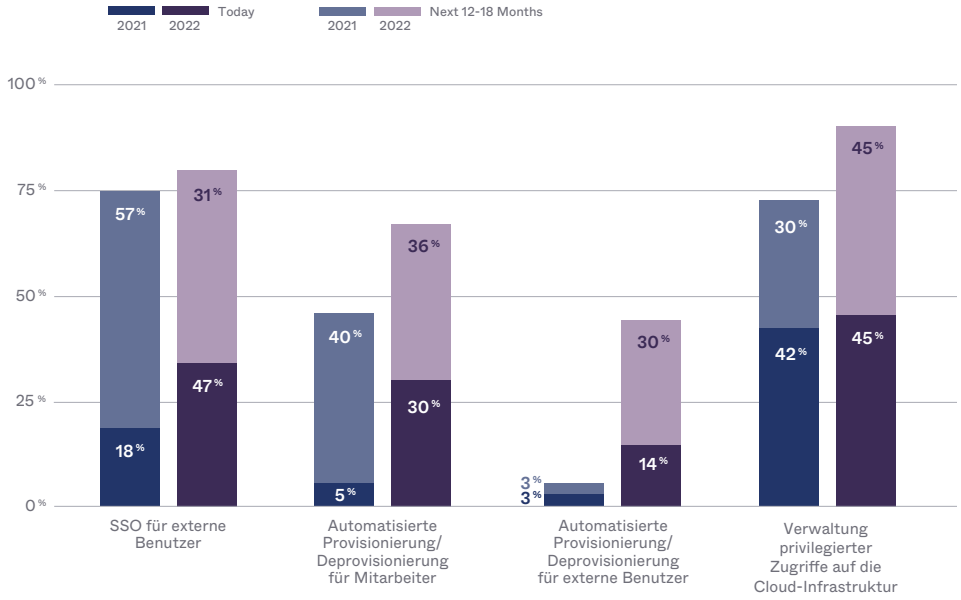


Unter allen untersuchten Branchen zeigten Software-Unternehmen bei den Initiativen von Phase 3 des Reifegrades im Jahresvergleich den größten Fortschritt. Sie alle erzielten große Erfolge bei der Einführung von Identity-Projekten und implementierten SSO für externe Benutzer sowie die Automatisierung der Provisionierung und Deprovisionierung aller Benutzer. Fast 100 % aller untersuchten Software-Unternehmen wollten bis Ende 2023 PAM in der Cloud-Infrastruktur bereitstellen.

Software-Unternehmen Welche der folgenden Initiativen hat Ihr Unternehmen aktuell implementiert bzw. welche sollen in den nächsten 12–18 Monaten implementiert werden?

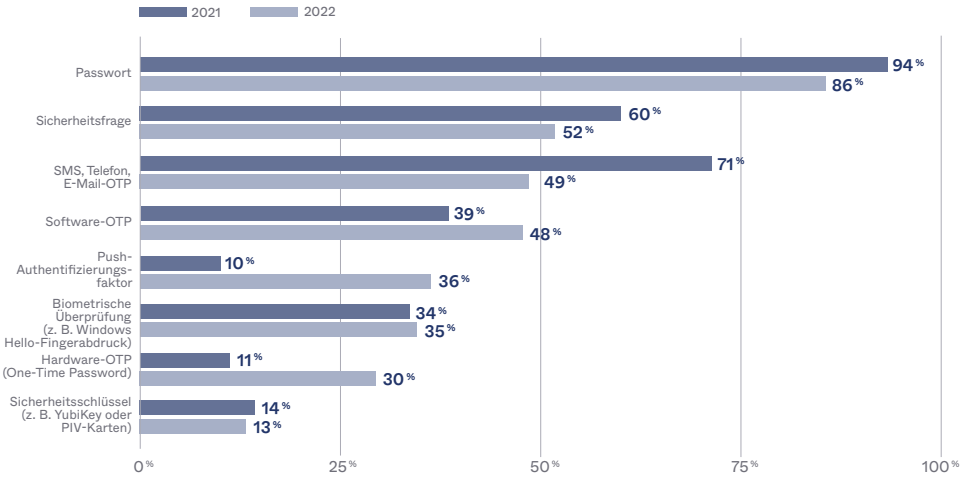


Software-Unternehmen im Jahresvergleich in Phase 3 Welche der folgenden Initiativen hat Ihr Unternehmen aktuell implementiert bzw. welche sollen in den nächsten 12–18 Monaten implementiert werden?



Im Software-Sektor beobachteten wir bei Authentifizierungsfaktoren mit geringerer Sicherheit wie Passwörtern, Sicherheitsfragen, SMS, Sprachanrufen und E-Mails einen leichten Rückgang gegenüber 2021, während Push-Authentifizierung erheblich häufiger genutzt wird.

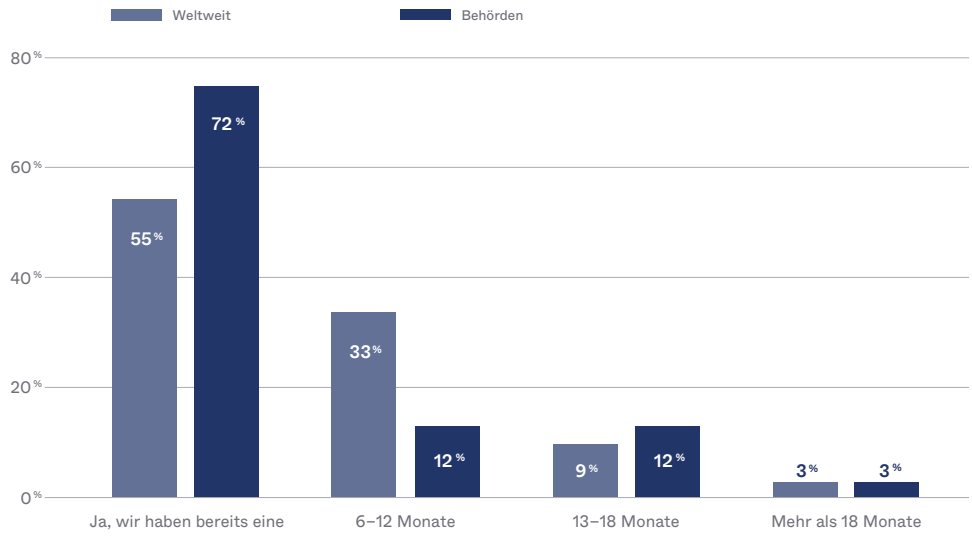
Software-Unternehmen Wählen Sie die Authentifizierungsfaktoren aus, mit denen Ihr Unternehmen interne und externe Benutzer verifiziert. (Mehrfachnennungen möglich)



Öffentlicher Dienst

Bei der Umsetzung von Zero-Trust-Programmen sind Behörden den anderen Sektoren tendenziell voraus und haben Pläne, innerhalb der nächsten Monate die Einführung konkreter Identity-Projekte zur Unterstützung einer Zero-Trust-Strategie stetig voranzutreiben. In den USA wirkten kürzlich erlassene Regierungsverordnungen, die eine schnelle und entschiedene Cyber-Modernisierung (und nicht nur inkrementelle Verbesserungen) forderten, als Beschleuniger. Bundesbehörden müssen hier in absehbarer Zeit klare Anforderungen erfüllen. Andere Behörden auf der ganzen Welt unterziehen ihren Zero-Trust-Ansatz einer ähnlichen Neubewertung. In Großbritannien gab das National Cyber Security Centre eine hilfreiche Empfehlung mit acht Designprinzipien für Zero-Trust-Architekturen. Dazu gehören auch Identity-basierte Empfehlungen wie „Vertrauen Sie keinem Netzwerk – auch nicht Ihrem eigenen."[7]

Alle Unternehmen weltweit und Behörden im Vergleich Hat Ihre Einrichtung aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten Monaten eines starten?

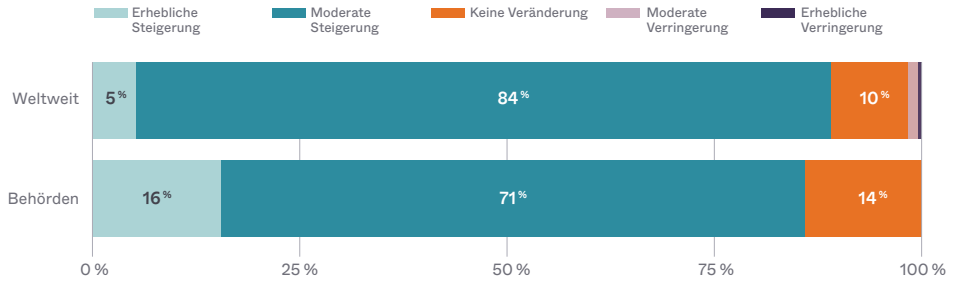


Weltweit investierte in den letzten 12 Monaten ein höherer prozentualer Anteil von Behörden erhebliche Summen in die Förderung ihrer Zero-Trust-Initiativen. Im Fall der US-Regierung wurden für die **Zero-Trust-Strategie des Weißen Hauses** keine zusätzlichen Mittel bereitgestellt, doch Behörden können für ihre Zero-Trust-Initiativen Gelder beim Technology Modernization Fund (TMF) beantragen.[8]

[7] „Zero Trust Architecture Design Principles", National Cyber Security Centre, 23. Juli 2021, Ncsc.gov.uk/collection/zero-trust-architecture/dont-trust-any-network, abgerufen am 10. August 2022.

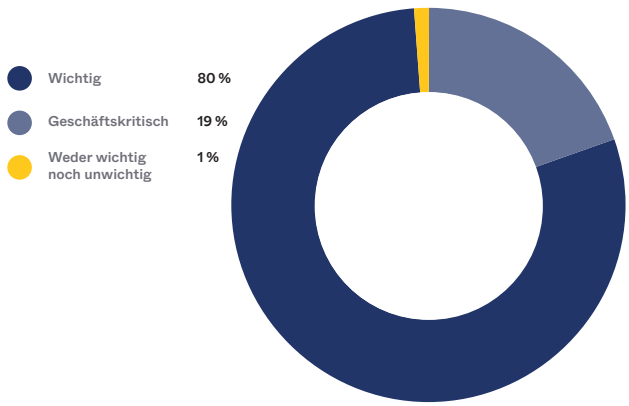
[8] FCW.com: „**How the TMF Helps Agencies Pave the Way Toward Zero Trust**", 2022.

Alle Unternehmen weltweit und Behörden im Vergleich Wie hat sich Ihr Budget für Zero-Trust-Security in den vergangenen zwölf Monaten verändert (sofern zutreffend)?



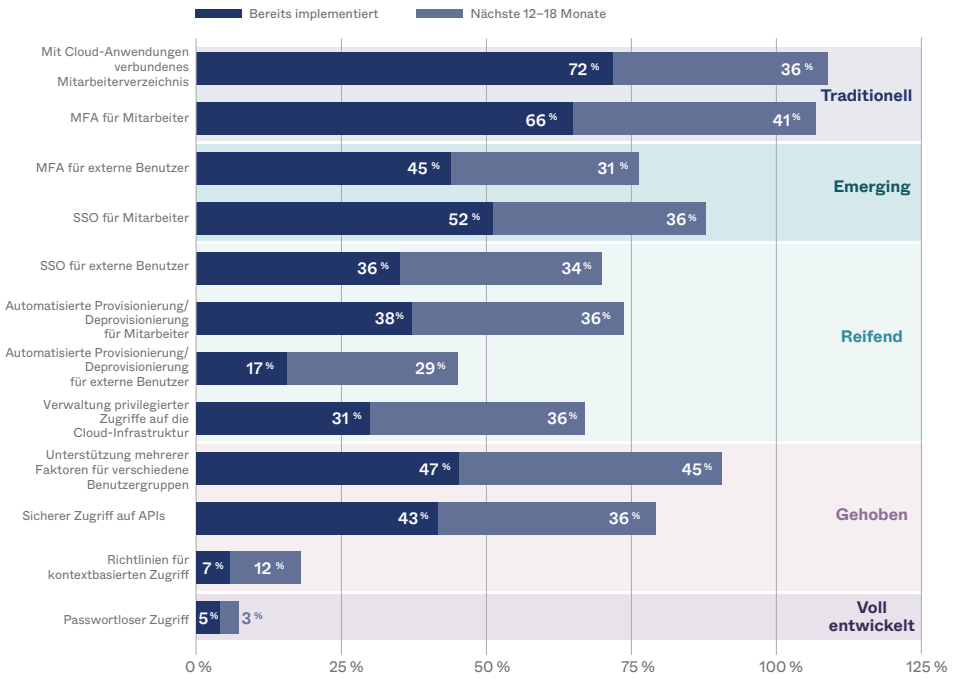
Fast alle Umfrageteilnehmer in Behörden weltweit erklärten, dass Identity ein wichtiger Teil ihrer Zero-Trust-Gesamtstrategie ist, wobei 19 % sie sogar als geschäftskritisch einstufen. (In den USA fordert eine neue bundesweite Zero-Trust-Strategie Phishing-sicheres MFA für die Workforce sowie als Option für öffentliche Kunden.) Außerdem ist Identity die erste Säule im **CISA Zero Trust Maturity Model**, vergleichbar mit der „Benutzer"-Säule in der Zero-Trust-Referenzarchitektur des US-Verteidigungsministeriums.

Behörden Wie wichtig ist Identity für Ihre Zero-Trust-Strategie?

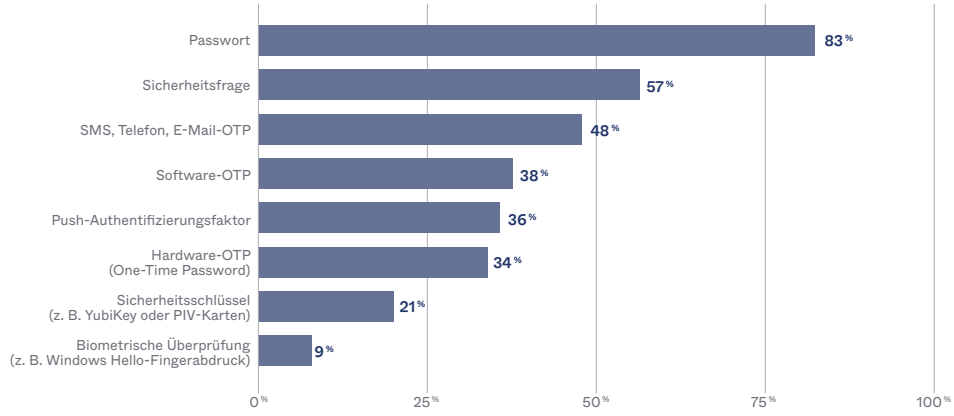


Umfrageteilnehmer aus Behörden planen, in den nächsten 12–18 Monaten erhebliche Fortschritte beim Reifegrad zu machen. Konkret sehen die Pläne vor, den Reifegrad-Fortschritt bei 6 von 12 Identity-Projekten zu verdoppeln, wobei Initiativen wie die Implementierung von MFA für Mitarbeiter und Benutzergruppen Priorität hat. Bei den Identity-Projekten aus dem Anfangsbereich der Reifegradkurve (also z. B. MFA und SSO) liegen Behörden hinter allen anderen Umfrageteilnehmern. Sie erklärten jedoch, dass sie nicht nur an der Implementierung dieser Projekte arbeiten, sondern in den nächsten Monaten zahlreiche weitere integrieren wollen.

Behörden Welche der folgenden Initiativen hat Ihre Einrichtung implementiert bzw. welche sollen in den nächsten 12–18 Monaten implementiert werden?



Behörden Wählen Sie die Authentifizierungsfaktoren aus, mit denen Ihre Einrichtung interne und externe Benutzer verifiziert. (Mehrfachnennungen möglich)



Aktuelle Situation bei Zero Trust

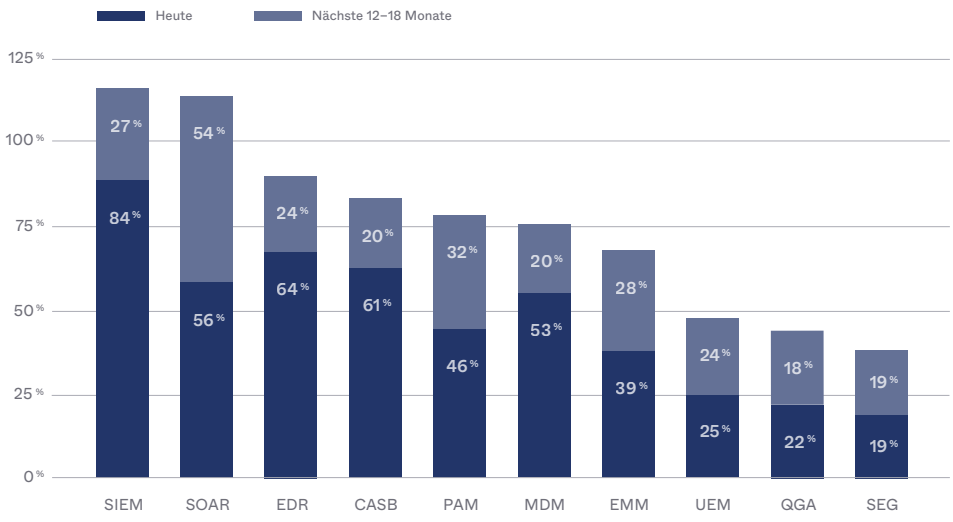
Die Identity-zentrierten Security-Ökosysteme von heute

Es gibt keine einzige Einzellösung, die jeden Aspekt der Zero-Trust-Empfehlungen von Forrester, NIST (National Institute of Standards and Technology) und anderen Organisationen abdeckt. Identity-Technologie hat sich jedoch als eine tragende Säule der Sicherheitsarchitektur etabliert, und es wird immer deutlicher, dass die Identity bei der Planung der Security eine zentrale Rolle spielen muss – und keine nachträglich angeflanschte Nebensache ist.

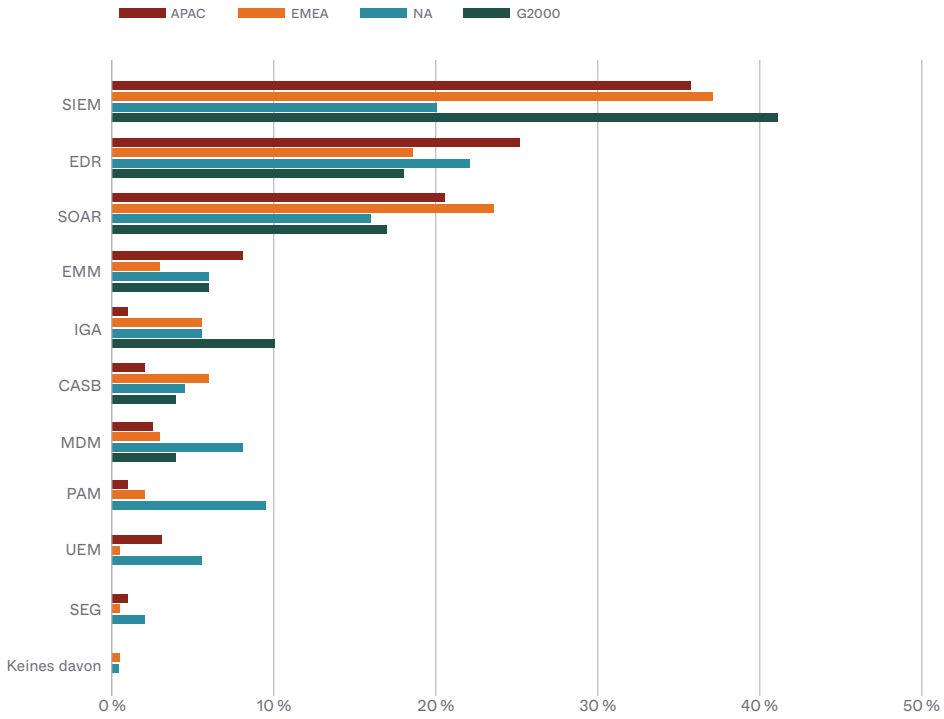
Der von Unternehmen implementierte Zero-Trust-Schutz ist effektiver und effizienter, wenn er die vorhandene IAM-Lösung in die gesamte unternehmensweite Security-Architektur integrieren kann. Dazu gehören zum Beispiel SIEM, SOAR (Security Orchestration, Automation and Response), Enterprise Mobility Management für die Endpoint Protection; Mobile Device Management; CASB (Cloud Access Security Broker) sowie PAM (Privileged Access Management). Im Zusammenspiel ermöglichen es IAM und SIEM den Unternehmen beispielsweise, sicherheitsrelevante Ereignisse fundiert zu bewerten. Eine Integration von IAM mit SOAR erlaubt die Automatisierung der Security-Response, während mit EDR integriertes IAM die Identität heranziehen kann, um unabhängige Datenpunkte zentral zu korrelieren um laufende Angriffe zuverlässig zu identifizieren.

Wir wollten von Security-Verantwortlichen wissen, bei welchen Tools die Integration mit ihren IAM-Lösungen ihrer Meinung nach am wichtigsten war, um auf diese Weise starke Zero Trust Security zu etablieren. In fast jeder Region sowie für mehr als 40 % der Global 2000-Unternehmen war SIEM das wichtigste zu integrierende Element. Die einzige Region, für die SIEM nicht das kritischste Element war, war Nordamerika. Hier hatte EDR einen knappen Vorsprung. In Bezug auf aktuelle IAM-Integrationen stehen heute SIEM, EDR und CASB an der Spitze, die schon heute in drei von fünf befragten Unternehmen integriert sind.

Alle Unternehmen weltweit Welches der folgenden Systeme haben Sie mit Ihrer IAM-Lösung integriert oder wollen Sie in den nächsten 12–18 Monaten implementieren? (Mehrfachnennungen möglich)



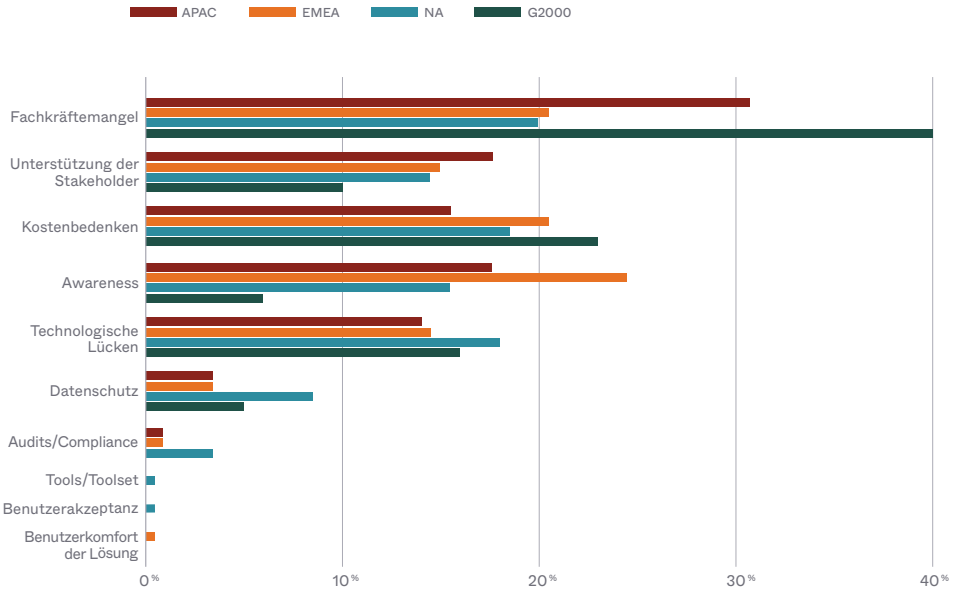
Regionaler Vergleich Welches der folgenden Systeme sollte Ihrer Meinung nach vorrangig mit einer IAM-Lösung integriert werden, um Zero Trust Security zu erreichen?



Die Verheißungen (und Herausforderungen) von Zero Trust

Weltweit haben die Unternehmen seit dem letzten Jahr erhebliche Fortschritte bei ihren Zero-Trust-Initiativen gemacht. Sie stehen jedoch immer noch vor einer Reihe großer Herausforderungen. Zum Beispiel müssen sie erhebliche Investitionen tätigen, damit ihre Teams die neuen Technologien implementieren können. Wir wollten von den Security-Verantwortlichen auch wissen, wo sie die größten Schwierigkeiten bei der Implementierung konkreter Zero-Trust-Initiativen sind. Ihre Antworten waren aufschlussreich: Fachkräftemangel wurde in Nordamerika, der APAC-Region und unter den Global 2000 am häufigsten genannt. Im EMEA-Raum galten Kostenbedenken als gleichwertiges Hindernis – und die fehlende Kenntnis (von Lösungen, die Zero Trust unterstützen) wurde noch höher eingestuft. Ein Blick auf die drei größten Herausforderungen jeder Gruppe zeigt, dass Fachkräftemangel und Kostenbedenken für jede Gruppe in den Top 3 lagen, ergänzt von Technologielücken (Nordamerika und APAC-Region) sowie Unterstützung durch die Stakeholder im EMEA-Raum und unter den Global 2000.

Regionaler Vergleich Vor welchen Herausforderungen steht Ihr Unternehmen bei der Implementierung eines Zero-Trust-Security-Modells?



Größte Hindernisse bei der Implementierung einer Zero-Trust-Initiative Bewerten Sie die drei größten Herausforderungen Ihres Unternehmens bei der Implementierung eines Zero-Trust-Security-Programms.

APAC
1. Mangel an Mitarbeitern/Expertise für Implementierung
2. Technologische Lücken
3. Kostenbedenken

EMEA
1. Mangel an Mitarbeitern/Expertise für Implementierung
2. Unterstützung der Stakeholder
3. Kostenbedenken

Nordamerika
1. Mangel an Mitarbeitern/Expertise für Implementierung
2. Technologische Lücken
3. Kostenbedenken

Global 2000
1. Mangel an Mitarbeitern/Expertise für Implementierung
2. Unterstützung der Stakeholder
3. Kostenbedenken

Alle Umfrageteilnehmer weltweit
1. Mangel an Mitarbeitern/Expertise für Implementierung
2. Unterstützung der Stakeholder
3. Kostenbedenken

Was bringt die Zukunft für Zero Trust?

Angesichts des Fachkräftemangels, der weltweit spürbar ist, müssen Unternehmen Lösungen finden, mit denen sie ihre Zero-Trust-Initiativen vorantreiben können, ohne weitere Budgets schaffen, Experten anstellen oder Mitarbeiter schulen zu müssen. Die Unternehmen benötigen Lösungen, die sich mit ihren vorhandenen Security-Ökosystemen integrieren lassen, um maximalen Mehrwert zu erzielen. Darüber hinaus müssen sich diese Lösungen schneller und einfacher bereitstellen und skalieren lassen, um mit dem Wachstum der Unternehmen Schritt zu halten und die Zero-Trust-EInführung vorantreiben zu können. Sorgen bezüglich der Unterstützung seitens der Stakeholder können in einigen Fällen daher kommen, dass die Security-Abteilungen keine vollständige Kontrolle über ihre IAM-Lösungen sowie über andere Security-Lösungen in ihren Umgebungen haben. Andere Abteilungen, die weniger in Zero-Trust-Initiativen involviert sind, haben möglicherweise Einwände gegen die Bereitstellung von Ressourcen für solche Maßnahmen.

Diese Herausforderungen bieten jedoch auch Chancen. Unternehmen müssen die Abteilungen, mit denen sie arbeiten, schulen – und ein gemeinsames Fundament schaffen, damit der Bedarf nach Zero-Trust-Initiativen allen Beteiligten klar ist. Sie sollten sich an anderen Unternehmen orientieren, um Ansatzpunkte für die Orchestrierung ihrer eigenen Aktivitäten zu erhalten. Am wichtigsten ist möglicherweise aber, dass sie für die Implementierung der Zero-Trust-Lösungen mit den richtigen Partnern zusammenarbeiten müssen. Nur so können sie die Lösungen finden, die sie für ihre jeweilige Phase in der Reifegradkurve benötigen, und diese in ihre vorhandene Security-Infrastruktur integrieren. So lassen sich alle verbliebenen Hindernisse überwinden.

Zusammenfassung der wichtigsten Erkenntnisse

Erstens ist Zero Trust nicht mehr einfach ein Buzzword, sondern hat sich innerhalb kürzester Zeit von einer interessanten Idee und Security-Theorie zu einem wichtigen geschäftlichen Prinzip entwickelt – und Unternehmen auf der ganzen Welt arbeiten an der Umsetzung entsprechender Pläne.

Zweitens gibt es nicht den einen geradlinigen Weg zum Erreichen von Zero Trust. Jedes Unternehmen hat eigene Ausgangspunkte und Prioritäten, die individuelle Lösungen erforderlich machen. Diese müssen letztendlich in einem einfacheren, effizienteren und effektiven Security-Programm integriert werden.

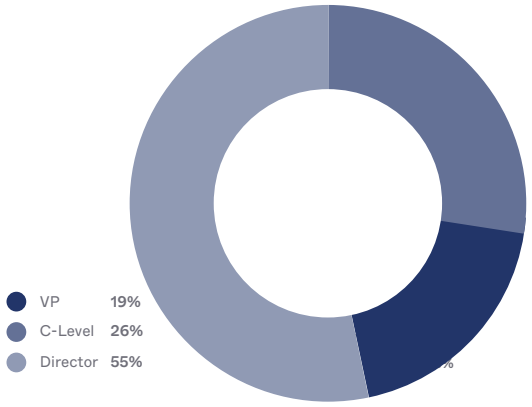
Drittens ist Identity eine zentrale Komponente von Zero Trust. Im Fokus steht dabei die Frage, wie Sie Ihre komplexe Lösung effizient vernetzen, den neuen Perimeter schützen, die richtige Balance aus Security und Usability finden sowie gewährleisten, dass Ihre moderne, remote arbeitende Workforce zuverlässig auf ihre Assets zugreifen kann.

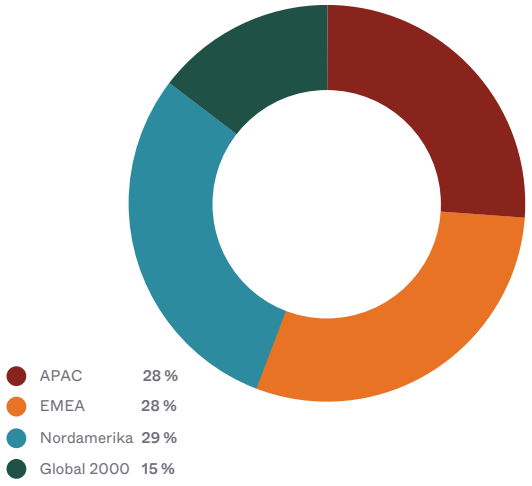
Wenn Sie bereit sind, die Position Ihres Unternehmens auf der Reifegradkurve zu ermitteln, haben wir eine nützliche Ressource für Sie. Mehr dazu **hier**.

Umfrage-Methodik

Im Auftrag von Okta hat Pulse Q&A eine weltweite Umfrage unter 700 Security-Entscheidern durchgeführt. Befragt wurden Abteilungsleiter oder höherrangige Führungskräfte aus verschiedenen Unternehmen und Branchen. Die Entscheidungsträger waren definiert als Personen, die Entscheidungen für Technologiekäufe treffen. Unter ihnen führte unser Partner Pulse Anfang 2022 eine Umfrage durch. In diesem Report bezeichnen wir diese Umfrage als „unsere Umfrage“ und die im Namen ihres Unternehmens teilnehmenden Personen als „Umfrageteilnehmer“ oder „Befragte“.

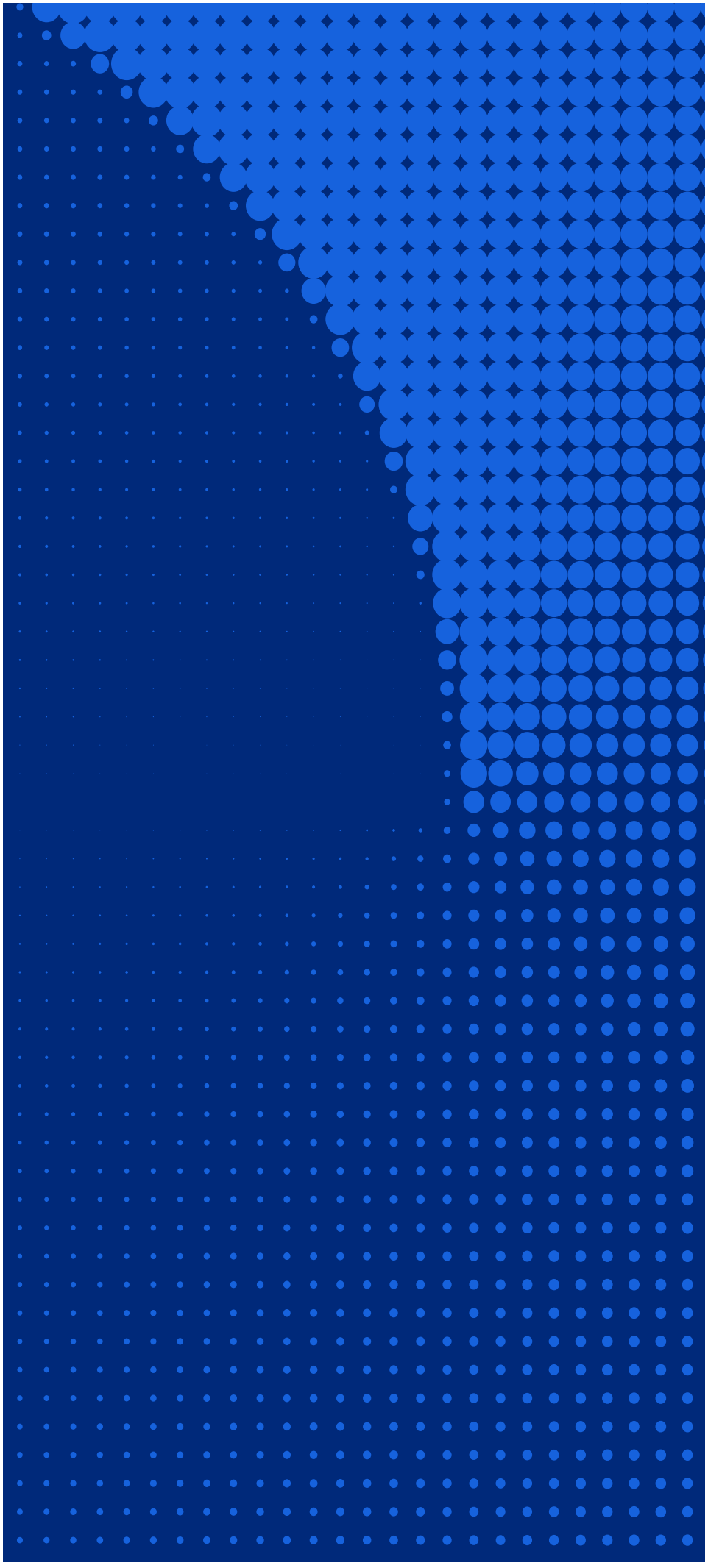
Wer hat an der Umfrage teilgenommen?
Diese Übersicht zeigt die 700 Umfrageteilnehmer sowie ihre Unternehmen. Bei den Branchen konzentrierten wir uns auf vier Sektoren und drei geografische Regionen sowie die Unternehmen der Forbes Global 2000. Die befragten Security-Verantwortlichen waren Vice Presidents, Abteilungsleiter oder Vorstände und wir nutzten Prozentanteile in jedem Segment zur Normalisierung.





Über Okta

Okta ist ein führender unabhängiger Identity-Anbieter. Die Okta Identity Cloud erlaubt es Unternehmen, die richtigen Menschen zur richtigen Zeit mit den richtigen Technologien zu verbinden. Mit über 7.000 schlüsselfertigen Integrationen ermöglicht es Okta Anwendern und Unternehmen auf der ganzen Welt, einfach und sicher auf benötigte Anwendungen und Infrastrukturdienste zuzugreifen und so ihr volles Potenzial zu erschließen. Über 15.800 Unternehmen setzen auf Okta, um die Identitäten ihrer Mitarbeiter und Kunden zu schützen – darunter JetBlue, Nordstrom, Slack, Takeda, Teach for America und Twilio. Weitere Informationen finden Sie unter Okta.com/de.



okta