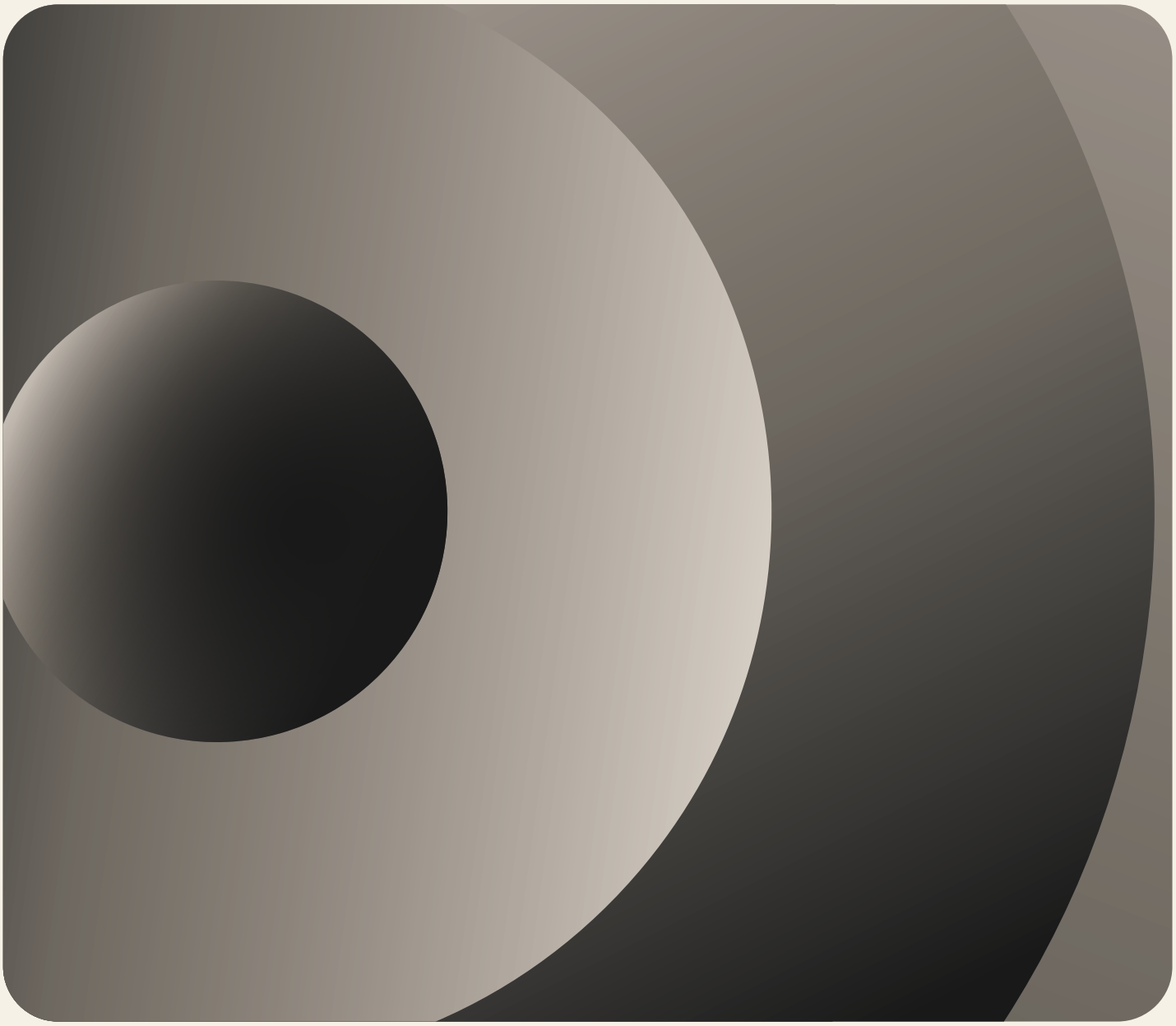
2023

Bewertung des Identity- und Access-Managements in weltweit tätigen Unternehmen

The State of Zero Trust Security 2023



okta

Inhalt

Methodologie

Methodologie der Umfrage

In Zusammenarbeit mit Qualtrics befragte Okta im April 2023 weltweit Entscheidungsträger im Bereich Informationssicherheit aus unterschiedlichsten Branchen. Als Entscheidungsträger wurden leitende Angestellte (oder höher) definiert, die für Entscheidungen über den Kauf von Technologie verantwortlich sind. Die Umfrage wurde in Englisch und Japanisch über Qualtrics-Panels in 13 Ländern durchgeführt. In diesem Report bezeichnen wir diese Umfrage als „unsere Umfrage“ und die im Namen ihres Unternehmens teilnehmenden Personen als „Umfrageteilnehmer“ oder „Befragte“.

Die Befragten

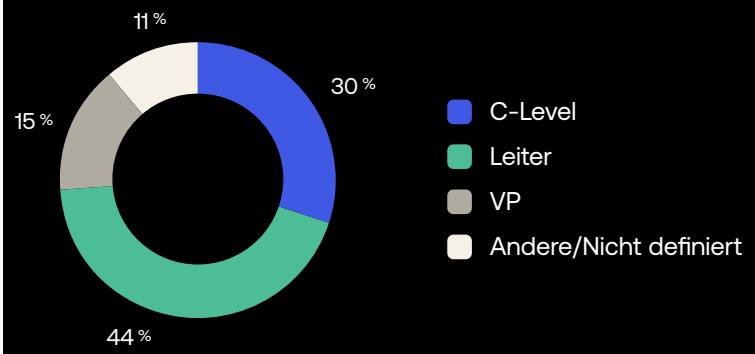
Befragt wurden insgesamt 860 Entscheidungsträger für Informationssicherheit aus Nordamerika (Vereinigte Staaten, Kanada), EMEA (Dänemark, Finnland, Frankreich, Deutschland, Irland, Niederlande, Norwegen, Schweden, Vereinigtes Königreich) und APJ (Japan, Australien). Dieser Bericht konzentriert sich auf die Segmente Gesundheitswesen, öffentlicher Sektor, Finanzdienstleistungen und Software, aber auch andere Branchen sind vertreten. (Regionen und Branchen wurden von den Befragten selbst angegeben.) Der öffentliche Sektor umfasst Organisationen aus allen drei Weltregionen, jedoch keine staatlichen/lokalen Organisationen. Zu den befragten Gruppen gehörten C-Level-Verantwortliche, Vice Presidents und Leitungspersonal. Die Umfrage richtete sich nicht an Mitarbeiter oder Kunden von Okta.

Die Methodologie im Detail

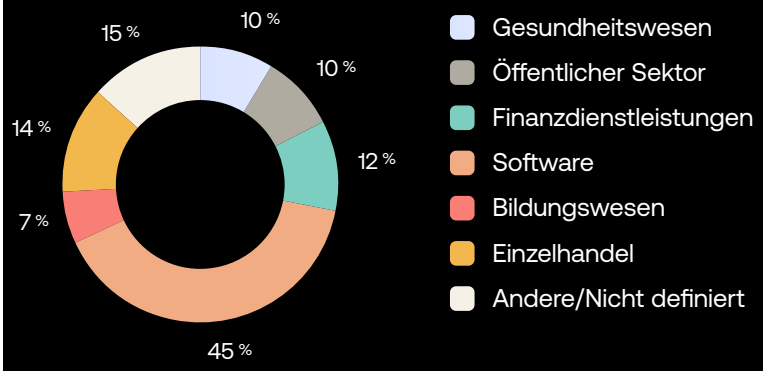
In den Diagrammen umfassen die Antworten „Global“ oder „Alle“ die Befragten in allen Sektoren (nicht nur in unseren vier Schwerpunkt-Segmenten) und allen Regionen (unabhängig davon, ob sie sich selbst als in NAM, EMEA oder APJ ansässig identifizierten). Der Einfachheit halber runden wir alle Daten in den Diagrammen auf die nächste ganze Zahl auf, einschließlich der Abrundung auf Null, wenn die Zahlen unter 0,5 liegen. Aus diesem Grund summieren sich die Summen in einigen Diagrammen nicht genau auf 100 %. Die Diagramme können in der Summe auch mehr als 100 % ergeben, wenn die Befragten mehrere zusammenhängende Fragen mit „Ja“ beantwortet haben (z. B., wenn sie angegeben haben, dass sie eine bestimmte Initiative ergriffen haben, und dass sie dies auch in Zukunft tun wollen. ■

Demografie der Befragten

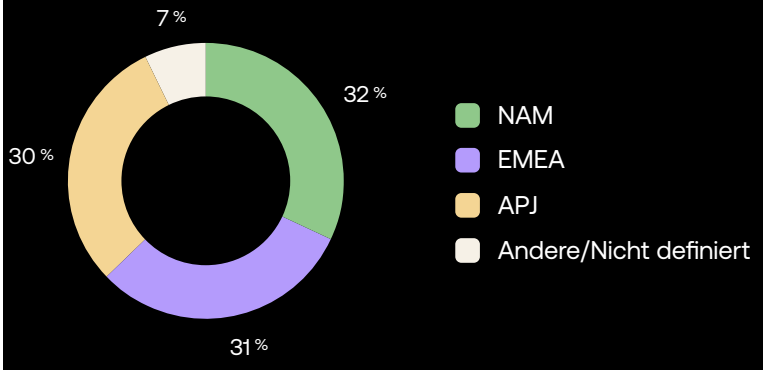
Funktion der Teilnehmer



Branche des Unternehmens



Region des Unternehmens



Zero Trust – vom Ziel zum Plan

Unternehmen treiben die Umsetzung von Zero Trust immer weiter voran, um ihre Mitarbeiter, ihre Assets und ihre Infrastrukturen zu schützen.

Vor zehn Jahren war Zero Trust nur ein Silberstreif am Horizont. Der Forrester-Forscher John Kindervag prägte den Begriff 2010, um die Schlüsselrolle des Security-Prinzips „Never trust, always verify“ zu betonen. In den zehn Jahren, die seither vergangen sind, hat sich Zero Trust rasant weiterentwickelt: von einer coolen Philosophie erst zu einem ehrgeizigen Ziel – und dann zur gelebten Realität vieler Unternehmen. Unsere jährliche Umfrage zum Stand von Zero Trust belegt, dass sich heute mehr Unternehmen als je zuvor diesem strategischen Ideal verschrieben haben – und konkrete Schritte einleiteten, um Zero Trust Security in den kommenden Monaten nahtlos umzusetzen.

Tatsächlich übersteigt die Zahl der Unternehmen, die bereits eine konkrete Zero-Trust-Strategie haben, zum ersten Mal, seit Okta 2019 den State of Zero Trust Report herausgibt, deutlich die Zahl der Unternehmen, die sich in der Planungsphase befinden (oder die das Thema nicht für wichtig genug halten, um sich damit zu beschäftigen). Ganz klar: Das Blatt hat sich gewendet.

Mit Blick auf den rasanten Anstieg der Cyberattacken und Datendiebstähle und zunehmend strenge Vorgaben wie NIST und CISA sollte dies keine große Überraschung sein. So berichtet das Identity Theft Resource Center im 2022 Annual Data Breach Report, es habe im vergangenen Jahr in den USA 1.802 Daten-Breaches gegeben, von denen insgesamt 422 Millionen Menschen betroffen waren. Im Mittelpunkt dieser Attacken stehen die Identitäten. Die Javelin-Studie Identity Fraud 2022 bewertet die Schäden durch Identitätsdiebstähle in den USA allein im Jahr 2022 mit 43 Milliarden USD — ein kleiner und hart erkämpfter Sieg im Vergleich zu den 52 Milliarden USD, die sich Identitätsdiebe 2021 geholt hatten. Ein 2023 veröffentlichter Report des U.S. Department of Justice kommt zu dem Schluss, „Identitätsbetrug ist eine Komponente nahezu aller cyberkriminellen Aktivitäten – und überall auf der Welt zu spüren. Wir haben es hier mit einer nationalen und globalen Bedrohung für die Sicherheit der Staaten und ihrer Bürger zu tun."

Im Kampf gegen moderne Bedrohungen und zunehmend raffinierte Bedrohungsakteure ist es unserer Meinung nach die beste Strategie für die Security-Teams der Unternehmen, sich an das Grundprinzip von Zero Trust zu halten: „Never trust, always verify". Mit einer Zero-Trust-Strategie legen die Unternehmen das Fundament dafür, über klassische, nicht für die Cloud-orientierte Welt von heute entwickelte Security-Ansätze hinauszugehen – und die Identitäten in den Fokus ihrer Sicherheitsmaßnahmen zu stellen. In vielen Unternehmen war die Verifizierung der Identität früher ausschließlich eine Aufgabe des IT-Teams. Unsere Daten zeigen aber, dass sich dies inzwischen maßgeblich verändert hat: Heute obliegt die Kontrolle der Identitäten weitgehend – und oft ausschließlich – dem Security-Team. Aber die SecOps-Teams sind nicht die einzigen, die von Zero Trust profitieren: Unternehmen, die dieses Prinzip umgesetzt haben, tun sich erfahrungsgemäß leichter damit, das Management der Identitäten ganzheitlich anzugehen, ihre Produktivität zu steigern und die User-Experience für Mitarbeiter und Kunden zu verbessern.

Makroökonomische Trends und die Potenziale der Cloud haben viele Unternehmen dazu veranlasst, auf zunehmend komplexe Hybrid-/Multi-Cloud-Ökosysteme zu setzen, in denen verteilte Teams jederzeit auf ebenso verteilte Ressourcen und IT-Umgebungen zugreifen können – einschließlich der Partner, Lieferanten und externer Anbieter. Identität ist der rote Faden, der all dies zusammenhält. Ein starkes Identitätsmanagement ist heute daher eine Schlüsselkomponente jeder Infrastruktur – denn nur so können die komplexen, global verteilten Mitarbeiterteams sicher und produktiv zusammenarbeiten. Die diesjährigen Daten dokumentieren, dass die Unternehmen nach wie vor damit beschäftigt sind, das Management ihrer mobilen Geräte zu optimieren, Single Sign-On (SSO) und Multi-Faktor-Authentifizierung (MFA) für externe Mitarbeiter einzuführen, die Provisioning/Deprovisioning-Workflows zu automatisieren und generell strengere Zero-Trust-Richtlinien einzuführen, um ihre Unternehmensressourcen und Mitarbeiter zu schützen.

Der Weg zu Zero Trust ist lang: Sich von jahrzehntelangen Praktiken und Prozessen zu verabschieden, den Security-Stack neu zu ordnen und schwierige Investitionsentscheidungen zu treffen, ist selbst unter optimalen Bedingungen nicht leicht. Und wie ein flüchtiger Blick in die Finanzpresse zeigt, sind die Bedingungen alles andere als optimal. Doch mit den richtigen Technologien und den richtigen Partnern konnten die Unternehmen, mit denen wir für unsere jährliche Umfrage gesprochen haben, bereits viele Herausforderungen meistern und schnelle Fortschritte erzielen. Dieser Bericht soll Unternehmen dabei helfen, besser zu verstehen, wie und wo erfolgreiche Unternehmen heute auf Zero-Trust-Modelle setzen, – und so die Weichen für die Umsetzung der entsprechenden Programme zu stellen.

Zero-Trust-Programme sind rasant auf dem Vormarsch

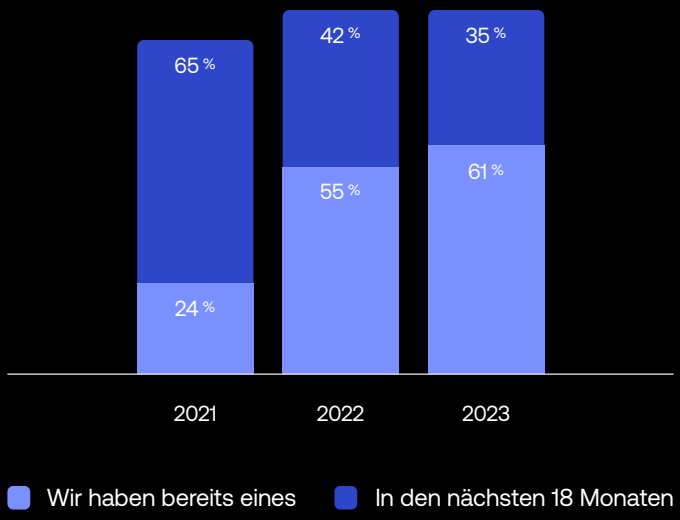
Die Zahl der Unternehmen, die bereits ein klar definiertes Zero-Trust-Modell eingeführt haben, steigt rasant. Im Jahr 2021 verfügte noch weniger als jedes vierte der von uns befragten Unternehmen über ein solches Programm. 2022 hatte bereits mehr als die Hälfte der befragten Unternehmen ein entsprechendes Modell umgesetzt – und in diesem Jahr stieg die Zahl noch einmal auf 61 %. Dementsprechend ist der Anteil der Unternehmen, die noch in der Planungsphase stehen und vorhaben, in den nächsten 12 bis 18 Monaten eine Zero-Trust-Initiative zu implementieren, im Vergleich zum Vorjahr gesunken – einfach, weil immer mehr Unternehmen die Pläne in die Tat umsetzen. Mehr als sechs von zehn befragten Unternehmen sind heute bereits auf dem Weg zu Zero Trust. Der Rest steht noch in der Planungsphase.

Sieht man sich die Daten nach Unternehmensgröße näher an, zeigt sich, dass kleinere Organisationen (mit 500 bis 999 Mitarbeitern) seltener über eine klar definierte Zero-Trust-Strategie verfügen als größere Unternehmen. Der „Sweet Spot“ sind Unternehmen mit 5.000 bis 9.999 Mitarbeitern: In diesem Segment geben drei von vier Befragten an, ein definiertes Zero-Trust-Programm implementiert zu haben. Über alle Unternehmensgrößen hinweg hat nur noch eine kleine Minderheit von Unternehmen (in allen Fällen weniger als 10 %) weder ein Zero-Trust-Programm umgesetzt, noch planen sie, in den nächsten 18 Monaten ein solches zu entwickeln.

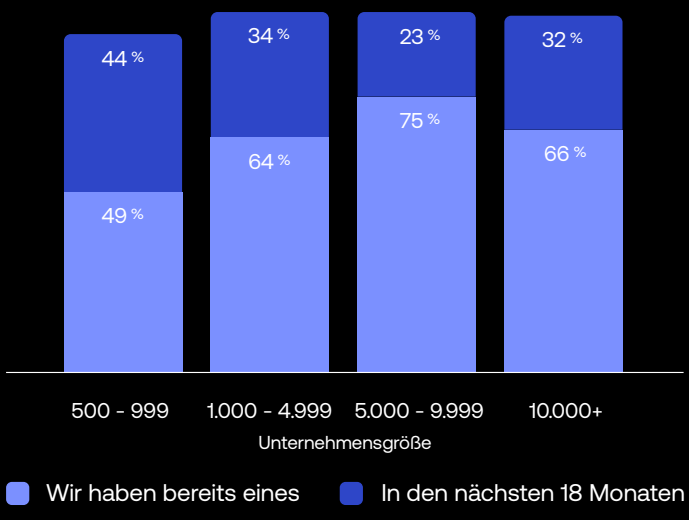
Weltweit wird Zero Trust immer mehr Teil des Business-Alltags

61 % aller Unternehmen haben weltweit bereits ein definiertes Zero-Trust-Programm eingeführt. Weitere 28 % planen die Umsetzung einer solchen Initiative innerhalb der nächsten 6-12 Monate, und weitere 7 % innerhalb der nächsten 13-18 Monate. Dieser Trend ist über alle Regionen hinweg zu beobachten. Die nordamerikanische Region hat – was die bereits umgesetzten Programme betrifft – nach wie vor einen soliden Vorsprung. Aber die in EMEA und APJ ansässigen Unternehmen machen schnell Boden gut, und fast alle Nachzügler in beiden Regionen wollen in den nächsten 6-12 oder 13-18 Monaten ein Zero-Trust-Programm auf den Weg bringen.

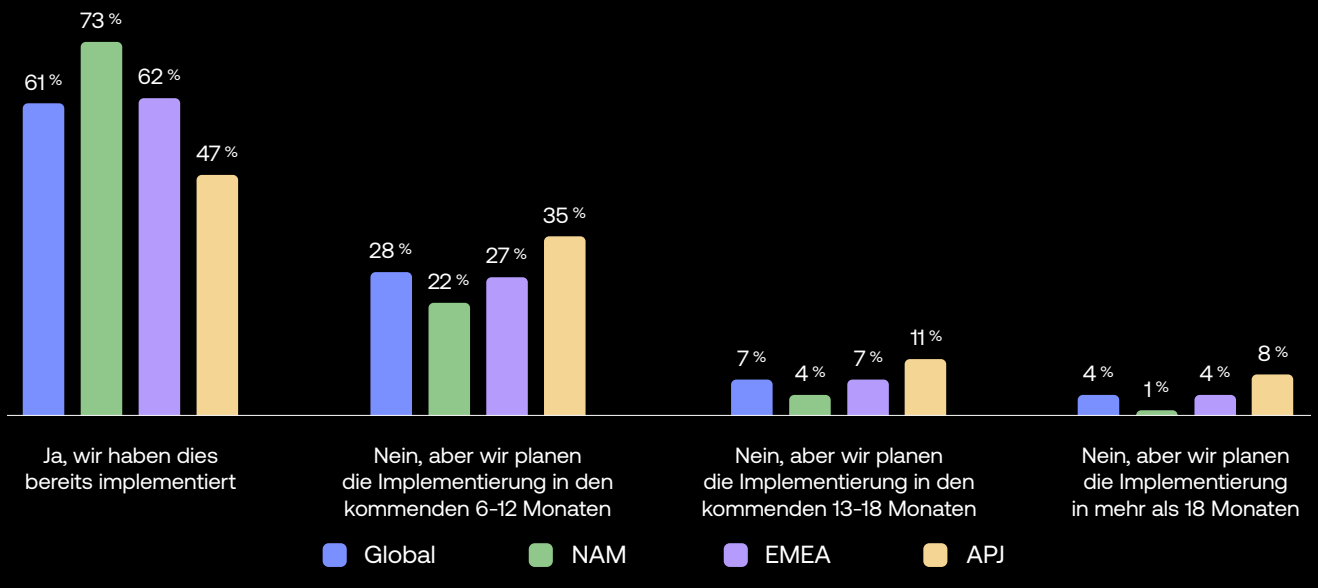
Hat Ihr Unternehmen bereits ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den kommenden 18 Monaten eine entsprechende Lösung implementieren?
Alle Befragten



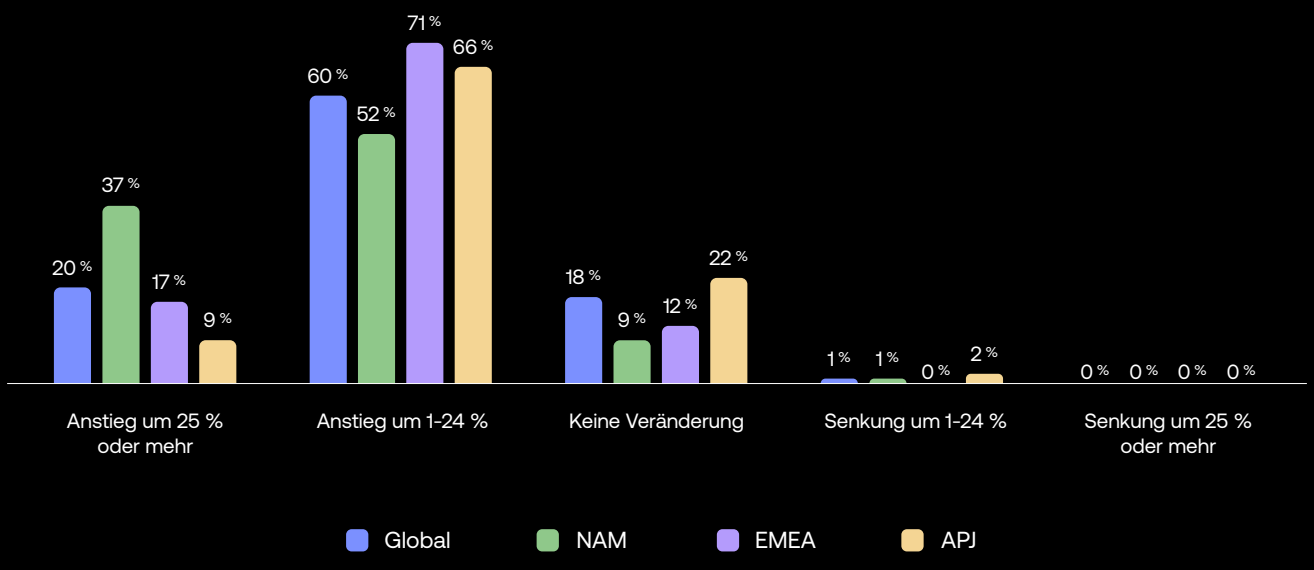
Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten 18 Monaten eines starten?
Vergleich nach Unternehmensgröße



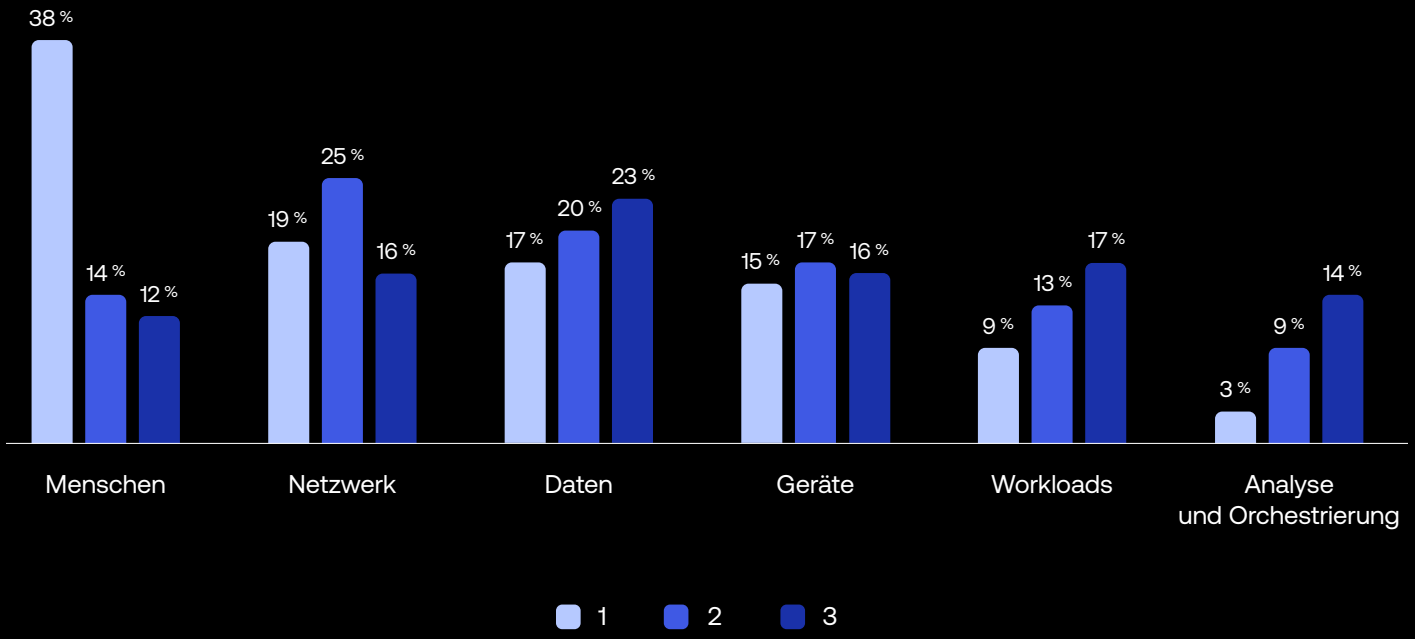
Hat Ihr Unternehmen bereits ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den kommenden 18 Monaten ein entsprechendes Projekt starten?
Vergleich der Regionen



Wie hat sich Ihr Budget für Zero Trust in den vergangenen 12–18 Monaten verändert (wenn überhaupt)?
Vergleich der Regionen



Priorisieren Sie den Stellenwert der folgenden Bereiche mit Blick auf die Security-Projekte Ihres Unternehmens (1 = am höchsten, 3 = am niedrigsten)
Alle Teilnehmer



Zero-Trust-Budgets weiterhin auf einem gesunden Niveau

In einer Zeit, in der makroökonomische Faktoren über alle Regionen und Branchen hinweg zu Personal- und Kosteneinsparungen führen, scheinen die Budgets für Zero-Trust-Sicherheitsinitiativen ziemlich unantastbar zu sein. Bei der überwältigenden Mehrheit der befragten Unternehmen sind diese Budgets nicht nur konstant geblieben, sondern in den letzten 12-18 Monaten sogar gestiegen. Weltweit haben 60 % der Unternehmen diese Budgets seit dem vergangenen Jahr um 1–24 % erhöht. Ein weiteres Fünftel hat sogar noch mehr zugelegt. Weniger als 3 % der befragten Organisationen mussten Budgetkürzungen hinnehmen – und das gilt für alle Regionen.

Die Mitarbeiter bleiben im Fokus der meisten Security-Projekte

Als wir die Befragten baten, die drei wichtigsten Sicherheitsbedenken ihrer Unternehmen zu benennen, war „Menschen“ in diesem Jahr die beliebteste Antwort. „Netzwerk“ und „Daten“ folgten mit großem Abstand auf den Plätzen zwei und drei. „Menschen“ standen bei der Security schon immer im Fokus. Aber in diesem Jahr ist die Kategorie ein regelrechter Ausreißer – ein deutlicher Hinweis darauf, dass das Verständnis für den hohen Stellenwert der Identitäten in Zero-Trust-Modellen zunimmt.

Zero Trust ist kein theoretisches Konzept mehr, sondern hält im Alltag der Unternehmen Einzug

Wichtige Erkenntnisse

Zero Trust hat sich schnell vom Maßnahmenplan zum alltäglichen Vorgang entwickelt.

Viele Unternehmen, die Zero Trust lange als theoretisches Konstrukt betrachteten, haben dieses Framework inzwischen weitgehend in die Tat umgesetzt oder sind auf dem besten Weg dorthin. Die Entwicklung ist dramatisch: Gaben 2021 nur 24 % der Befragten an, über ein strategisches Zero-Trust-Programm zu verfügen, stieg die Zahl im letzten Jahr auf 55 % und in diesem Jahr auf 61 %. Das ist ein Trend, den wir in allen Regionen und bei allen Unternehmensgrößen beobachten. Unter unseren vier Schwerpunktbranchen liegen die Finanzdienstleistungen mit einem Anteil von 71 % der Unternehmen, die eine Zero-Trust-Initiative eingeführt haben, knapp vor der Softwarebranche mit 69 %. Schlüsselt man die Zahlen nach Region auf, liegt Nordamerika mit 73 % der Unternehmen, die eine definierte Zero-Trust-Initiative eingeführt haben, an der Spitze. In APJ ist der Anteil der Unternehmen mit einem solchen Programm mit 47 % am geringsten – aber dafür ist die Wahrscheinlichkeit, dass eine solche Initiative in den nächsten 6-12 Monaten umgesetzt werden soll, mit 35 % am höchsten.

Die Identität wird inzwischen allgemein als Schlüssel für die Zero-Trust-Umsetzung angesehen.

Was sich in einem Jahr alles ändern kann: Letztes Jahr bewerteten 71 % der Befragten die Identität als zentralen Bestandteil der Zero-Trust-Strategie, aber nur 27 % der Befragten hielten sie für geschäftskritisch. In diesem Jahr hat sich das Blatt gewendet: 51 % der Befragten bewerten Identität als „sehr wichtig“, und 40 % halten sie für „relativ wichtig“. Der Sinneswandel ist alles andere als überraschend: Immer mehr Unternehmen erkennen, dass ein starkes Identity & Access Management (IAM) eine Schlüsselstrategie ist, wenn es gilt, Menschen und Assets in einer Hybrid-/Multi-Cloud-Welt zu schützen.

Die Zero-Trust-Budgets steigen weiter – ungeachtet aller Markt-Trends.

Unterschiedlichste makroökonomische Trends zwingen Unternehmen weltweit, ihre Budgets zurückzufahren. Doch die Ausgaben für Zero Trust steigen unbeeindruckt weiter. Ganze 80 % der Umfrageteilnehmer gaben in diesem Jahr an, dass ihre Budgets für Zero-Trust-Security im Vergleich zum Vorjahr gestiegen sind: 60 % vermelden Budgetzunahmen zwischen 1 % und 24 %. Weitere 20 % verzeichneten einen noch deutlicheren Anstieg (um 25 % oder mehr). Bedenken wegen höherer Kosten spielen in diesem Report seit inzwischen drei Jahren eine wichtige Rolle. Aber mit Blick auf die steigende Zahl von Betrugsfällen und Insider-Bedrohungen sowie die zunehmende Nachfrage nach hybriden Arbeitsmodellen und uneingeschränktem Cloud-Zugriff kommen Unternehmen aller Größen und Branchen nicht umhin, ihren Fokus – und ihre Budgets – auf identitätsbasierte Security zu verlagern.

Die Einführung von Zero Trust ist nach wie vor kein Selbstläufer.

Die Befragten nannten in diesem Jahr Bedenken hinsichtlich der Kosten sowie technologische Lücken als die größten Herausforderungen bei der Einführung von Zero Trust. Dahinter folgten Datenschutzbestimmungen/Datensicherheit und ein Mangel an qualifizierten Mitarbeitern. Aber die Landschaft hat sich verändert: In den vergangenen Jahren hat ein Aspekt die anderen Anliegen stets bei weitem überragt. Dieses Jahr sind die Herausforderungen ausgewogener verteilt – und reichen von der einfachen Integration und dem Bekanntheitsgrad der Lösung über die die Einhaltung von Audits bis hin zur Akzeptanz auf Seiten der Stakeholder. In diesem Zusammenhang wollen wir auch noch einmal betonen, dass sich die Zuständigkeit für das IAM in den Unternehmen zunehmend von der IT-Abteilung auf eine gemeinsame Verantwortung verlagert hat, die allerdings hauptsächlich von den Security-Teams gemanagt wird. ■

Identität: Das Herzstück von Zero Trust

Unternehmen weltweit erkennen die Schlüsselrolle, die Identitäten in modernen Security-Konzepten zukommt.

In einer Welt, in der der traditionelle Netzwerk-Perimeter nahezu verschwunden ist, hat sich die Identität als der neue Perimeter etabliert – als erste Verteidigungslinie der Unternehmen. Die große Herausforderung unserer Zeit ist es, die Identität jedes Menschen und jeder Maschine bei jedem einzelnen Zugriffsversuch auf Ihre Ressourcen zu verifizieren – von jedem Ort der Welt aus und mit einer breiten Palette genehmigter und nicht genehmigter Geräte.

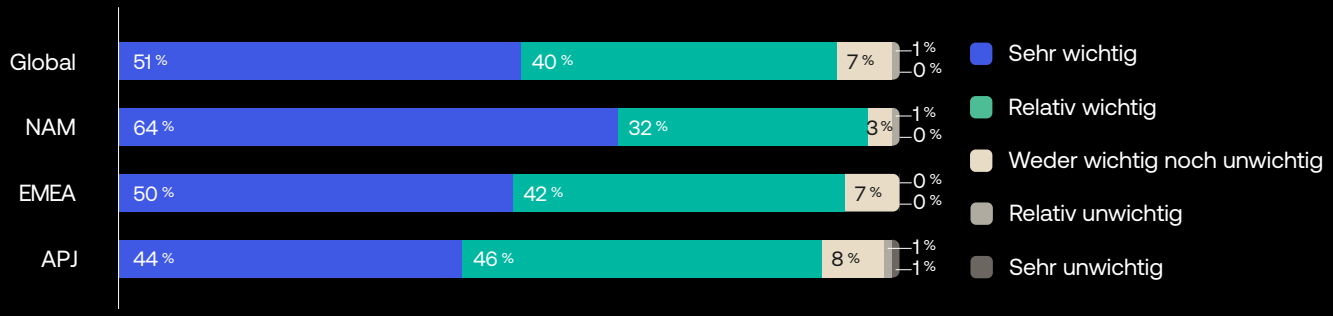
Der Lohn der Mühe ist ein erfolgreiches Business. Wie die diesjährigen Daten zeigen, erkennen Unternehmen aller Größen und Branchen zunehmend, dass Identität nicht nur ein Teilbereich der Security ist. Sie ist auch das Tor zur sicheren Skalierung des Geschäfts, und ermöglicht es ihnen, ihren Umsatz zu steigern, die Kundenbindung zu stärken, die Assets und den Ruf zu schützen und vieles mehr.

All diese Trends spiegeln sich in den Umfrageergebnissen des Jahres 2023 wider: Die Unternehmen zeigen klar, dass sie der Identität im Rahmen ihrer Zero-Trust-Initiativen deutlich höhere Bedeutung beimessen als je zuvor. Weltweit gibt mehr als die Hälfte der Befragten an, dass Identität äußerst wichtig für ihre Zero-Trust-Strategie ist – ein deutlicher Anstieg im Vergleich zum Prozentsatz, der dies im Jahr 2022 angab, und das über alle geografischen Regionen hinweg, wie im Folgenden erläutert wird.

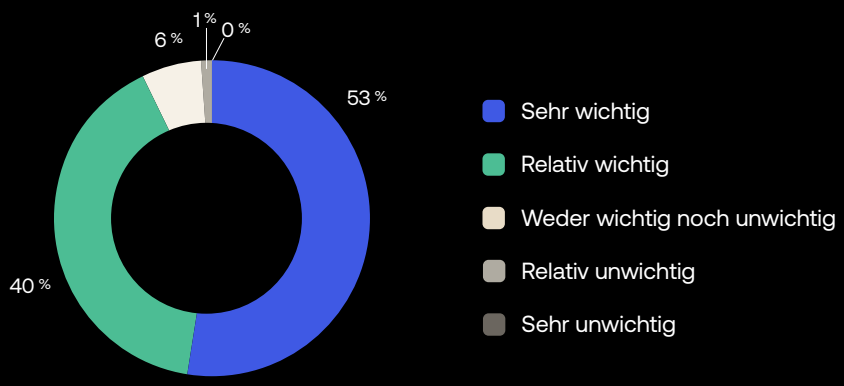
„Die IT-Verantwortlichen richten ihre IAM-Investitionen sowohl nach den Security- als auch nach den Business-Zielen aus. Wirkungsvoll umgesetzt, stellt IAM sichere Prozesse für Autorisierung, Policy Enforcement, das Provisioning und das Deprovisioning sicher, minimiert Reibungsverluste und unterstützt einen effizienten Geschäftsbetrieb ... So kann es zur Verbesserung der Sicherheit und der Produktivität beitragen."

— The Identity-Defined Security Alliance's
2022 Trends in Securing Digital Identities Report

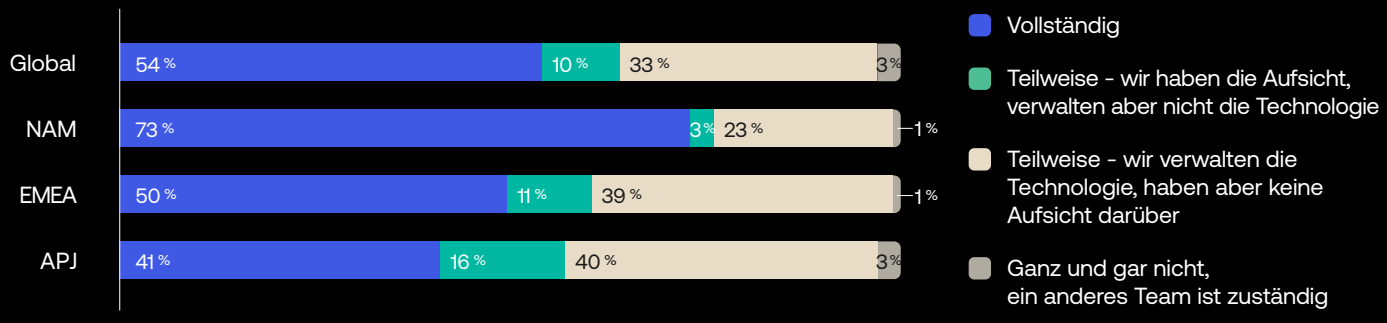
Wie wichtig ist Identität für ihre Zero-Trust-Strategie?
Vergleich der Regionen



Wie wichtig ist Identität für ihre Zero-Trust-Strategie?
Teilnehmer auf C-Level



In welchem Maß zeichnet in Ihrem Unternehmen die Security für das Thema IAM verantwortlich?
Vergleich der Regionen



Bitte beachten Sie, dass die Werte in einer Spalte aufgrund der Rundung auf ganze Zahlen aufsummiert nicht genau 100 % ergeben müssen.

Der Stellenwert der Identitäten ist klar

Es zeichnet sich immer mehr ab, dass der Identität eine Schlüsselrolle bei der Umsetzung von Zero-Trust-Programmen zukommt. Im vergangenen Jahr gaben nur 27 % der weltweit Befragten an, dass Identität für ihre Zero-Trust-Sicherheitsstrategie äußerst wichtig ist; dieses Jahr ist die Zahl auf 51 % gestiegen. Aufgeschlüsselt nach Regionen steht Nordamerika an der Spitze: Fast zwei Drittel der Befragten stufen Identität als äußerst wichtig ein, während fast ein Drittel sie als relativ wichtig erachtet. In den Regionen EMEA und APJ müssen möglicherweise noch einige Awareness-Hürden genommen werden: 7 % bzw. 8 % der Befragten erklärten, Identität sei weder wichtig noch unwichtig; in der Region APJ bezeichneten einige wenige (2 %) Identität sogar als relativ unwichtig oder äußerst unwichtig.

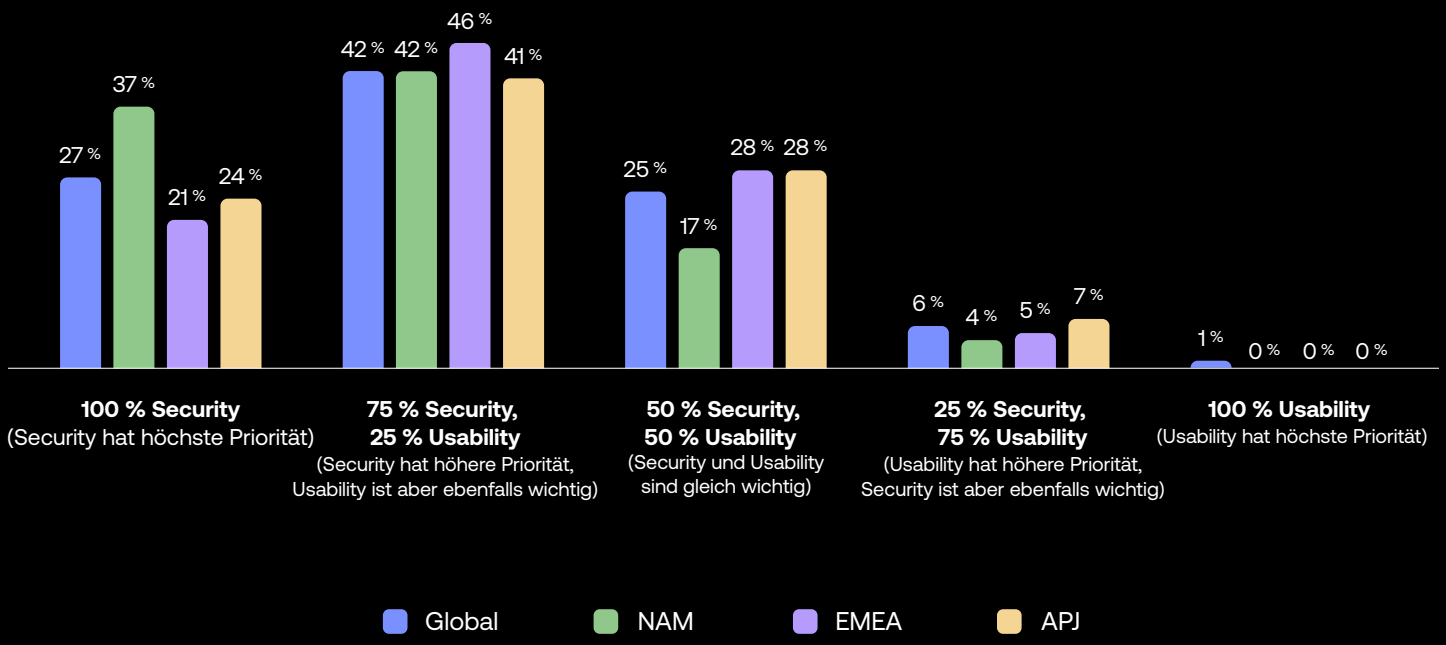
Die C-Suite meldet sich zu Wort

Die überwiegende Mehrheit der befragten C-Level räumt der Identität wie im Vorjahr hohe Priorität ein. Mehr als die Hälfte der von uns befragten Verantwortlichen gibt in diesem Jahr an, dass Identität für die Zero-Trust-Strategie äußerst wichtig ist. Weitere 40 % erklärten, dass sie relativ wichtig ist. (Letztes Jahr erklärten nur 26 % der befragten C-Level, dass Identität ein wichtiges Thema ist). Was wir daraus mitnehmen: Weltweit hat sich die Erkenntnis durchgesetzt, dass der Identität in modernen Security-Konzepten eine Schlüsselrolle zukommt.

Die Verantwortung für IAM verlagert sich

Ein Weg, um die dynamische Entwicklung der Security-Modelle moderner Unternehmen zu verstehen, ist es, zu untersuchen, wer in der Organisation die Verantwortung für das Thema IAM trägt. Identität war lange Zeit vor allem Sache der IT-Abteilung. In den letzten Jahren hat sich die Zuständigkeit zunehmend auf das Security-Team verlagert, da identitätsbasierte Bedrohungen wie Phishing nach wie vor zu den dominanten Threats gehören. (Bei 74 % aller Angriffe des vergangenen Jahres spielte die Komponente Mensch eine Rolle, so der Verizon 2023 Data Breach Investigations Report.) In der Hälfte der Unternehmen in der EMEA-Region liegt IAM inzwischen in den Händen der Security-Teams; in Nordamerika sind es sogar 73 %. In der APJ-Region ist die Zuständigkeit etwas weiter gefächert: 41 % der Unternehmen haben das Management der Identitäten vollständig der Security übertragen; in weiteren 56 % der Unternehmen zeichnet die Security entweder für das Monitoring oder für das Management der Identitäten verantwortlich – aber nicht für beides.

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



Security hat heute höhere Priorität als Usability

Die Angriffsfläche der hybriden Multi-Cloud-Netzwerke von heute hat sich dramatisch vergrößert, was die Unternehmen zunehmend anfällig für identitätsbasierte Angriffe macht. Aus diesem Grund haben viele Unternehmen ihre Prioritäten – mitunter drastisch - verlagert: weg von der Usability, hin zur Security. Weltweit geben mehr als zwei von drei Unternehmen entweder an, dass die Security unangefochten an erster Stelle steht, oder dass ihre Prioritäten aktuell zu drei Vierteln auf die Security und zu einem Viertel auf die Usability gewichtet sind. Dies ist ein großer Unterschied zum Jahr 2021, als die Unternehmen während der Pandemie unter Hochdruck auf Teleworking-Modelle wechselten und Usability das Gebot der Stunde war. Am seltensten gaben die Befragten aus der EMEA-Region an, dass Security oberste Priorität genießt (21 %). Unter den nordamerikanischen Befragten waren es 37 %. ■

Der Reifegrad der Workforce Identity

Die Unternehmen wissen um den Mehrwert eines starken Identity-Managements. Jetzt gilt es, diesen in der Praxis zu erschließen.

Zero Trust lässt sich nicht über Nacht einführen. Komplexe Projekte, dynamische Prioritäten und steigende Anforderungen nehmen die Zeit und die Ressourcen der Unternehmen in Anspruch – und machen es ihnen schwer, ohne klare Frameworks eigene Schwächen zu identifizieren und Fortschritte zu dokumentieren. Das unten beschriebene Workforce Identity Reifegradmodell von Okta kann Unternehmen dabei helfen, den Aspekt Identität bei der Zero-Trust-Einführung durchgehend im Blick zu behalten und erreichte Fortschritte zu dokumentieren. Bis alle Phasen abgeschlossen sind, wird es einige Zeit dauern. Aber wenn ein Unternehmen seine Security nach den Identitäten ausrichtet, kann es seinen Schutz nachhaltig stärken: Es reduziert die Angriffsfläche, verkürzt die Reaktionszeiten auf Angriffe, senkt die IT-Kosten und den Verwaltungsaufwand – und wird auch sonst sicherer, effizienter und flexibler. Auf den folgenden Seiten werden wir Ihnen die vier Phasen vorstellen.

Der Reifegrad der Workforce Identity

Die vier Phasen

Phase 1: Grundlegend Konsolidierung und Vereinfachung	• Reduzierung des manuellen Verwaltungsaufwands • Verkleinerung der Angriffsfläche • Konsolidierung der Verzeichnisse
Phase 2: Skalierend Mehrstufige Security-Mechanismen	• Automatisierung des On- und Offboardings • Optimierung der IT-Produktivität • Entlastung der Administratoren
Phase 3: Fortschrittlich Automatisierung und Optimierung der Experience	• Vernetzung aller Identity-Lösungen • Automatisierung aller administrativen Abläufe • Ablösung von Legacy-Systemen
Phase 4: Strategisch Verbesserung und Weiterentwicklung der Identität	• Modernisierung der Access-Experience • Eliminierung der Risiken von Passwörtern • Optimierung des digitalen Reifegrads

Phase 1: Grundlegend

Konsolidierung und Vereinfachung

Zu den vorrangigen Zielen von Unternehmen in Phase 1 gehört in der Regel die Reduzierung des manuellen Verwaltungsaufwands und die Verbesserung des Schutzes vor identitätsbasierten Angriffen. In dieser Phase versuchen die Unternehmen, die manuelle Verwaltung von Benutzern und Diensten zu automatisieren und ihre Sicherheitsmaßnahmen zu stärken. Erschwert wird dies oft durch die Vielzahl ad-hoc gestarteter, nicht aufeinander abgestimmter Initiativen, die ungewollt die Angriffsfläche vergrößern und zu einem Wildwuchs an Verzeichnissen führen.

Zu den wertvollsten Identity-Projekten, die Unternehmen in Phase 1 erwägen sollten, gehören: die Konsolidierung der Identity-Lösungen, die Implementierung grundlegender SSO- und MFA-Funktionalitäten mit rollenbasierten Zugriffsrichtlinien, die Implementierung einer hoch verfügbaren Architektur, das Einführen von SLA-Standards und die umfassende Inventarisierung der On-Premises- und Cloud-Anwendungen.

Phase 2: Skalierend

Mehrstufige Security-Mechanismen

In Phase 2 fokussieren die Unternehmen meist auf die Steigerung der IT-Produktivität und die Reduzierung des Verwaltungsaufwands und der zugehörigen Kosten. In dieser Phase verlassen sich viele Unternehmen noch zu sehr auf Passwörter und setzen auf manuelle Prozesse beim On- und Offboarding der Benutzer. Zu ihren Zielen gehört die Steigerung der Produktivität, die Entlastung der IT-Administratoren, die Verbesserung des Security-Standings und die Vereinfachung der Benutzerzugriffe auf Anwendungen.

Zu den Projekten, die in Phase 2 in Betracht gezogen werden sollten, gehört die Ausdehnung der MFA auf weitere Anwendungen, Lieferanten und Geschäftspartner, die Konsolidierung der Security- und Zugriffskontrollsysteme für Cloud- und On-Premises-Anwendungen, die Implementierung rollenbasierter Zugriffskontrollen und dynamischer Access Policies sowie die Einführung dedizierter Tools für Security- und Compliance-Audits sowie für das Monitoring.

Phase 3: Fortschrittlich

Automatisierung und Optimierung der Experience

In Phase 3 treiben die Unternehmen die Automatisierung der verbleibenden manuellen Prozesse voran und integrieren alle Identity-Lösungen mit einer einzigen, durchgängigen Management-Plattform. Auf diese Weise tragen sie maßgeblich zur Produktivität ihrer hybriden Workforce bei, stellen die Weichen für die Konsolidierung und Ablösung vorhandener Legacy-Technologien und ermöglichen die nahtlose Integration und Kommunikation aller Systeme.

Zu den Projekten, die in dieser Phase in Betracht gezogen werden sollten, gehört etwa die Implementierung einer attributbasierten und richtlinienbasierten Zugriffskontrolle sowie die Durchsetzung von Least Privilege Access für APIs, kritische Infrastrukturen und Anwendungen. Darüber hinaus sollten Organisationen eine regelmäßige Neuzertifizierung der Benutzerzugriffe gewährleisten und einen sicheren, passwortlosen Zugang zu kritischen Infrastrukturen umsetzen.

Phase 4: Strategisch

Verbesserung und Weiterentwicklung der Identität

In dieser Phase sind die Unternehmen durch leistungsfähige, nahtlos vernetzte Identity-Lösungen geschützt, die ihnen ein Höchstmaß an Sicherheit und Effizienz garantieren. So können sie ihre Next-Level-Ziele in Angriff nehmen, wie die Bereitstellung einer modernen Access-Experience und die Reduzierung Passwort-bezogener Risiken.

In Phase 4 sollten die Unternehmen die passwortlose Authentisierung in allen Bereichen einführen und umsetzen; die Incident-Prävention, -Erkennung und -Response vollständig automatisieren; einen Risiko-basierten Just-in-Time-Zugang einrichten; und sicherstellen, dass Zero Standing Privileges gelten.

Der Reifegrad der Workforce Identity

Umsetzung von Zero-Trust-Projekten

Die Philosophie von Zero Trust „Never trust, always verify“ hat sich in Windeseile von einem theoretischen Ansatz zum alltäglichen Prinzip weiterentwickelt. Heute ist es ganz normal, dass zukunftsorientierte Unternehmen Identity-Initiativen zur obersten Priorität machen. Auf diese Weise stärken sie auch ihr Security-Standing – beginnend mit der Skalierung von MFA und SSO auf ihre Workforce und externe Benutzer sowie auf Anwendungen, APIs und andere wichtige Bereiche ihrer Netzwerkstruktur. In allen Regionen nimmt die Zahl der Unternehmen, die immer komplexere identitätsbasierte Zero-Trust-Projekte angehen, zu – und ihre Fortschritte sind vielversprechend.

Unternehmen weltweit verfolgen verstärkt einen identitätsbasierten Zero-Trust-Ansatz, um jederzeit einen zuverlässigen Zugang für eine zunehmend komplexe Workforce aus Vollzeitbeschäftigten, Lieferanten, Partnern und Anbietern sicherzustellen. Dazu gehört auch, dass immer mehr Unternehmen MFA für externe Benutzer (34 % der diesjährigen Befragten haben diese Security-Maßnahme bereits eingeführt) und Mitarbeiter (33 %) implementieren.

Ein Blick auf die Branchen der befragten Unternehmen zeigt, das folgende Sicherheitsmaßnahmen zu den wichtigsten des Jahres zählen:

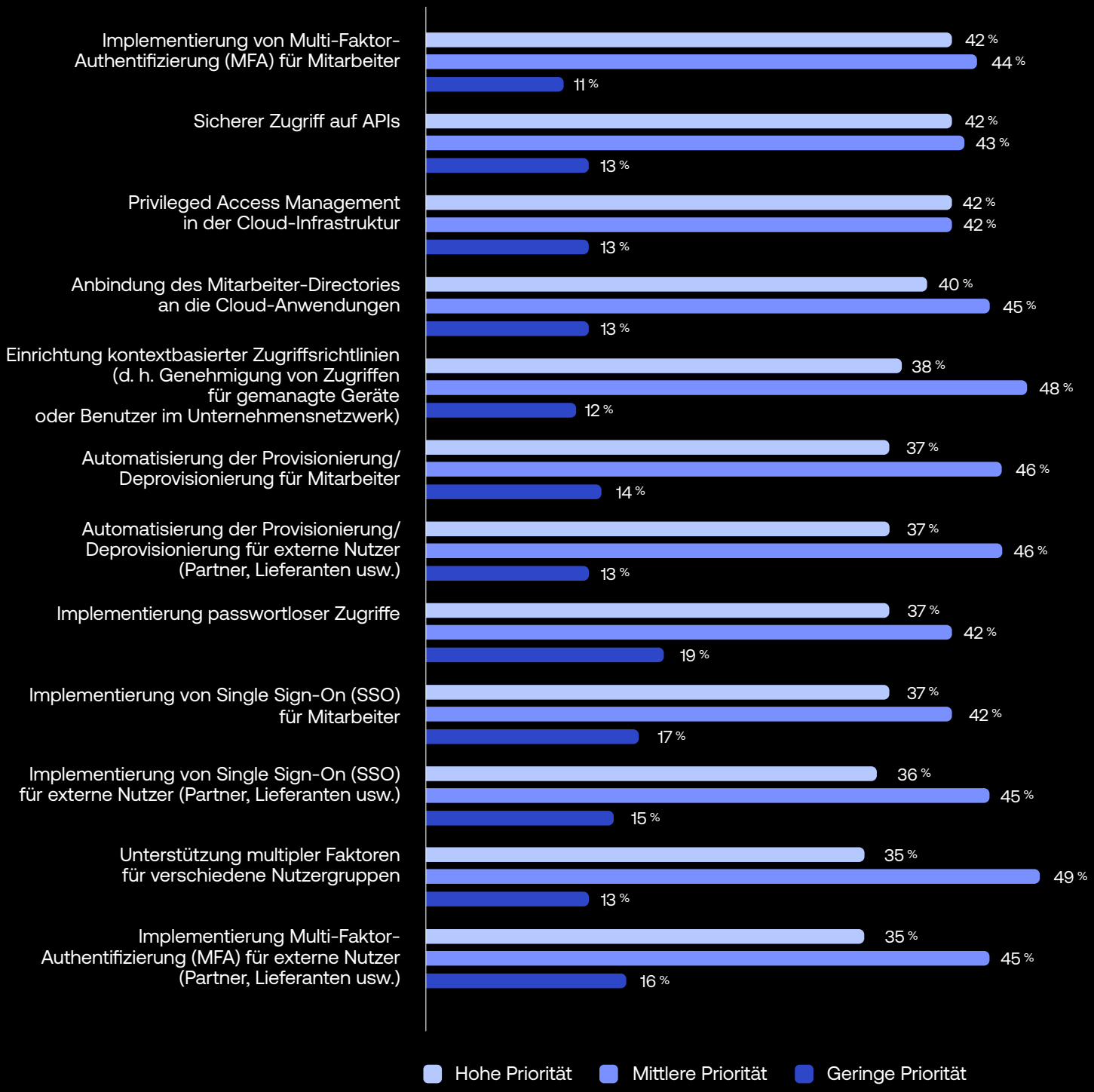
- **Im Gesundheitswesen:** MFA für externe Benutzer, MFA für Mitarbeiter und die Anbindung von Directories an Cloud-Anwendungen
- **Im öffentlichen Sektor:** MFA für externe Benutzer, sicherer API-Zugriff und MFA für Mitarbeiter
- **Im Finanzsektor:** MFA für Mitarbeiter, MFA für externe Benutzer und Privileged Access Management für die Cloud
- **In der Software-Branche:** MFA für Mitarbeiter, sicherer API-Zugriff und MFA für externe Benutzer

Und auch die geplanten Security-Initiativen der diesjährigen Befragten zeigen einen deutlichen Trend, wobei das Privileged Access Management in der Cloud, sicherer API-Zugriff und MFA für Mitarbeiter zu den Top-3-Implementierungen gehören.

Sowohl 2021 als auch 2022 standen MFA und SSO für Mitarbeiter bei der Befragung an der Spitze der umgesetzten Maßnahmen, dicht gefolgt von der Anbindung der Mitarbeiter-Directories an Cloud-Anwendungen. Im Jahr 2021 galt die SSO-Einführung für externe Benutzer als oberste Priorität für die nächsten 12-18 Monate, während im Jahr 2022 ein Privileged Access Management für die Cloud diesen Platz einnahm.

Welche dieser Security-Maßnahmen haben Sie bereits implementiert?
Alle Befragten

Bewerten Sie, welche dieser Security-Maßnahmen für Ihr Unternehmen in den nächsten 12-18 Monaten die höchste Priorität hat.
Alle Befragten



Bitte beachten Sie, dass die Werte in einer Spalte aufgrund der Rundung auf ganze Zahlen aufsummiert nicht genau 100 % ergeben müssen.

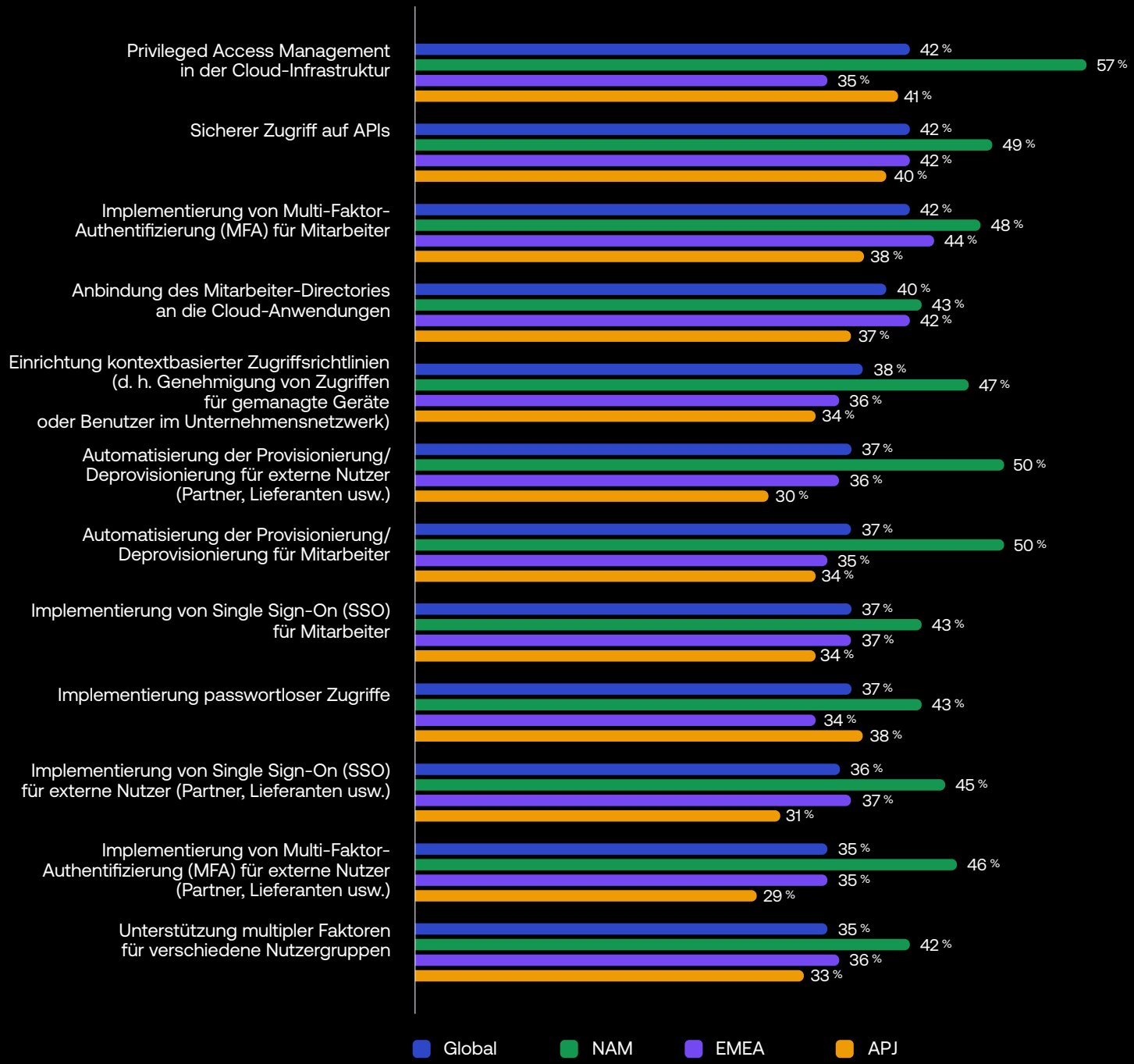
Der Reifegrad der Workforce Identity

Planung von Implementierungen

2021	#1	Single Sign-On für externe Benutzer (57 %)
	#2	Kontextbasierte Zugriffsrichtlinien (43 %)
	#3	MFA-Implementierung (Multi-Faktor-Authentisierung) für externe Benutzer wie Partner und Lieferanten (42 %)
2022	#1	Privileged Access Management für die Cloud (45 %)
	#2	Sicherer Zugriff auf APIs (41 %)
	#3	Automatisierung der Provisionierung/Deprovisionierung für Mitarbeiter (38 %)
2023	#1	Privileged Access Management für die Cloud (42 %)
	#2	Sicherer Zugriff auf APIs (42 %)
	#3	Implementierung von Multi-Faktor-Authentifizierung (MFA) für Mitarbeiter (42 %)

Jedes Jahr bitten wir die Befragten, die Zero-Trust-Lösungen anzugeben, deren Einführung sie in den nächsten ein bis anderthalb Jahren planen. Ein Vergleich der Top-3-Antworten weltweit von Jahr zu Jahr lässt einige interessante Trends erkennen. Im Jahr 2021 war der größte Pain Point der Unternehmen die Integration externer Benutzer in SSO und MFA sowie die Einführung strengerer Zugriffsrichtlinien. Mit Implementierung dieser Maßnahmen in zahlreichen Unternehmen verschob sich der Schwerpunkt auf einen sicheren Privileged Access für die Cloud, den API-Zugriff und auf ein automatisiertes Provisioning/Deprovisioning für Mitarbeiter (2022) und auf die MFA-Einführung für Mitarbeiter (2023).

Welche dieser Security-Maßnahmen hat für Ihr Unternehmen in den nächsten 12-18 Monaten oberste Priorität?
(Die Übersicht umfasst nur Antworten mit Wertung „hoher Priorität“.)
Vergleich der Regionen



Nordamerikanische Unternehmen räumen Security einen höheren Stellenwert ein

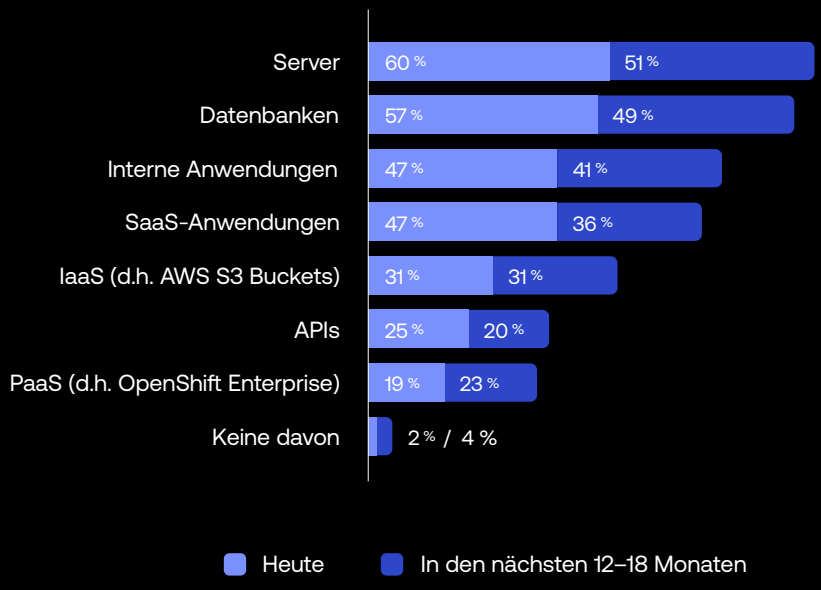
Betrachten wir die diesjährigen Ergebnisse genauer, zeichnen sich regional gesehen deutliche Unterschiede ab. Die Befragten aus Nordamerika bewerteten Security-Maßnahmen aller Art als hohe Priorität, allen voran Privileged Access Management für die Cloud und automatisiertes Provisioning/Deprovisioning.

In EMEA führen die MFA-Implementierung für Mitarbeiter, ein sicherer API-Zugriff und die Integration von Mitarbeiterverzeichnissen in Cloud-Anwendungen die Liste an. Bei den Unternehmen der APJ-Region zeigte sich weniger die Tendenz zu hohen Prioritäten als eine ausgewogene Planung zukünftiger Maßnahmen, mit Privileged Access Management für die Cloud und sicheren API-Zugriffen an erster Stelle, gefolgt von MFA-Implementierung für Mitarbeiter, Einführung eines passwortlosen Access und der Integration von Mitarbeiterverzeichnissen in Cloud-Apps.

Der Reifegrad der Workforce Identity

Sichere Authentisierung

Für welche Arten von Ressourcen haben Sie bereits MFA/SSO eingeführt – und für welche Ressourcen planen Sie es in den nächsten 12-18 Monaten?
Alle Befragten



Hinweis: Die Gesamtsumme der Spalten kann 100 % übersteigen, da die Befragten beide Antwortmöglichkeiten gewählt haben.

MFA /SSO soll vor allem auf Server und Datenbanken ausgedehnt werden

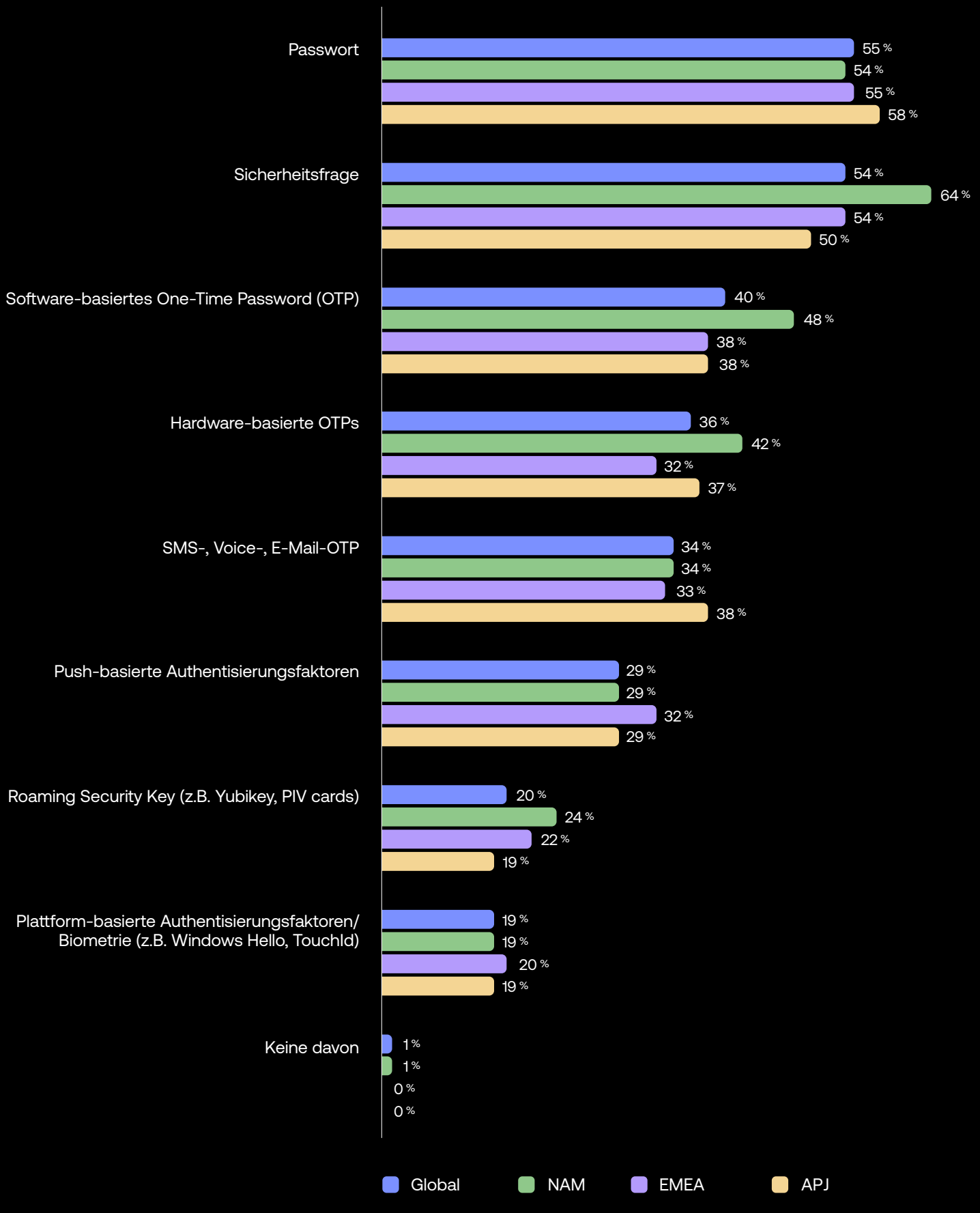
Wie der Report 2022 zeigte, legten die Unternehmen ihren Schwerpunkt vorrangig auf die Skalierung von MFA und SSO auf interne und SaaS-Anwendungen (Software-as-a-Service). Dieses Jahr verlagerte sich der Fokus jedoch auf grundlegende Netzwerkkomponenten: Drei von fünf Befragten (60 %) gaben an, bereits mit MFA und/oder SSO ihre Server zu schützen, während auch im Bereich Datenbanken 57 % der Befragten auf MFA und/oder SSO als identitätsbasierte Security-Maßnahme setzen. Aus regionaler Sicht gab es keine relevanten Unterschiede: Die befragten Unternehmen aus Nordamerika, EMEA und APJ nannten allen voran Server, Datenbanken und (interne und SaaS-)Anwendungen sowohl bei der Frage, wo Sie MFA/SSO einsetzen als auch planen, den Schutz zu erweitern.

Stärkere Sicherheitsfaktoren gewinnen an Beliebtheit

Passwörter sind noch immer der Go-To-Standard bei mehr als der Hälfte der Befragten aller Regionen und stehen damit weiterhin trotz ihres geringen Sicherheitsgrades ungeschlagen an der Spitze der Authentifikatoren. Sicherheitsfragen (ein ähnlich geringer Sicherheitsfaktor) belegen weltweit, in EMEA und APJ den zweiten Platz, während sie in Nordamerika sogar den ersten Platz einnehmen. Im Großen und Ganzen setzen Unternehmen noch immer vermehrt auf Faktoren mit geringem Sicherheitsgrad (dazu gehören auch Hardware-OTPs und SMS-/Telefon-/E-Mail-OTPs), obwohl diese äußerst anfällig für Cyberangriffe sind.

Faktoren mit einem mittleren Sicherheitsgrad, wie physische OTP-Token und Push-Authentifizierungsfaktoren, verzeichnen geringere Einsatzzahlen (36 % bzw. 29 %) – und nur 19 % der Unternehmen nutzen Faktoren mit einem hohen Sicherheitsgrad wie Plattform-basierte Authentifikatoren oder biometrische Verfahren. Wir gehen davon aus, dass die Tendenz zu MFA auch in Zukunft anhält, während eine wachsende Anzahl an Richtlinien im Finanz- und öffentlichen Sektor die Weichen für passwortlose und andere Phishing-resistente Authentifikatoren mit hohem Sicherheitsgrad stellen.

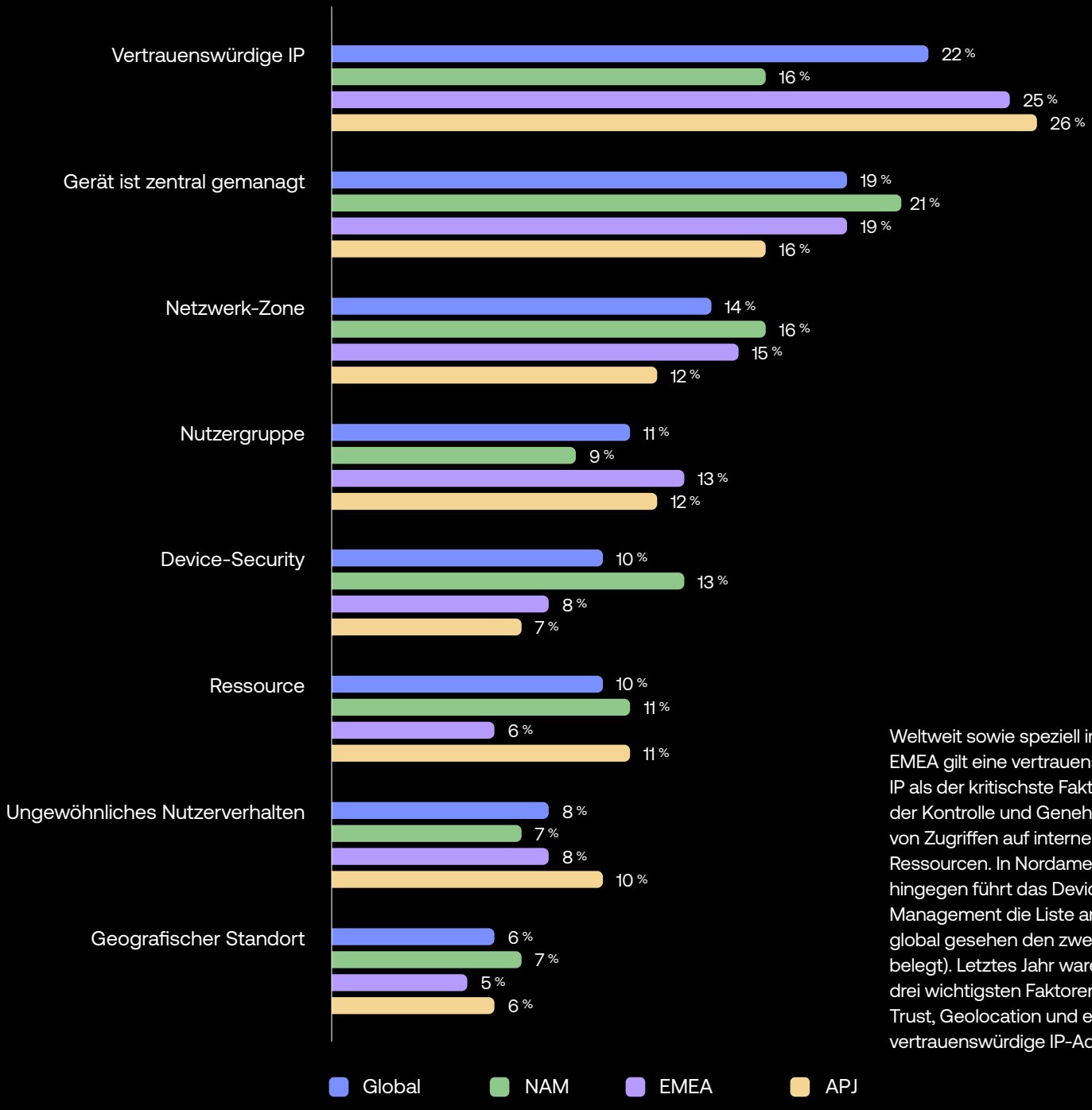
Welche Sicherheitsfaktoren nutzen Sie zur Verifikation interner und externer Nutzer?
Vergleich der Regionen



Der Reifegrad der Workforce Identity

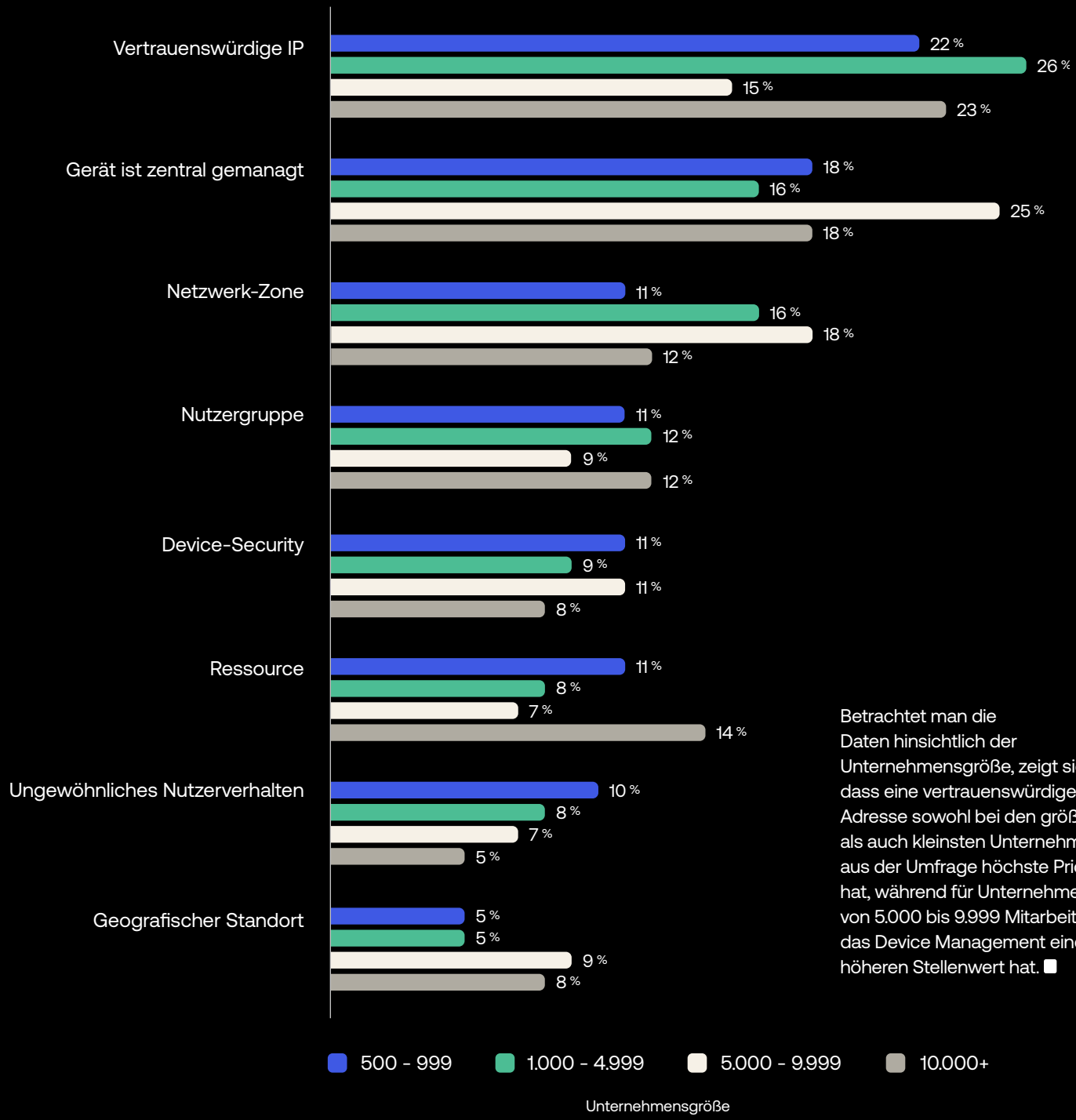
Genehmigung von Zugriffen auf interne Ressourcen

Geben Sie an, welcher Faktor für Sie bei Kontrolle und Genehmigung des Zugriffs auf interne Ressourcen ausschlaggebend ist?
Vergleich der Regionen



Weltweit sowie speziell in APJ und EMEA gilt eine vertrauenswürdige IP als der kritischste Faktor bei der Kontrolle und Genehmigung von Zugriffen auf interne Ressourcen. In Nordamerika hingegen führt das Device Management die Liste an (das global gesehen den zweiten Platz belegt). Letztes Jahr waren die drei wichtigsten Faktoren Device Trust, Geolocation und eine vertrauenswürdige IP-Adresse.

Geben Sie an, welcher Faktor für Sie bei Kontrolle und Genehmigung des Zugriffs auf interne Ressourcen ausschlaggebend ist?
Nach Unternehmensgröße



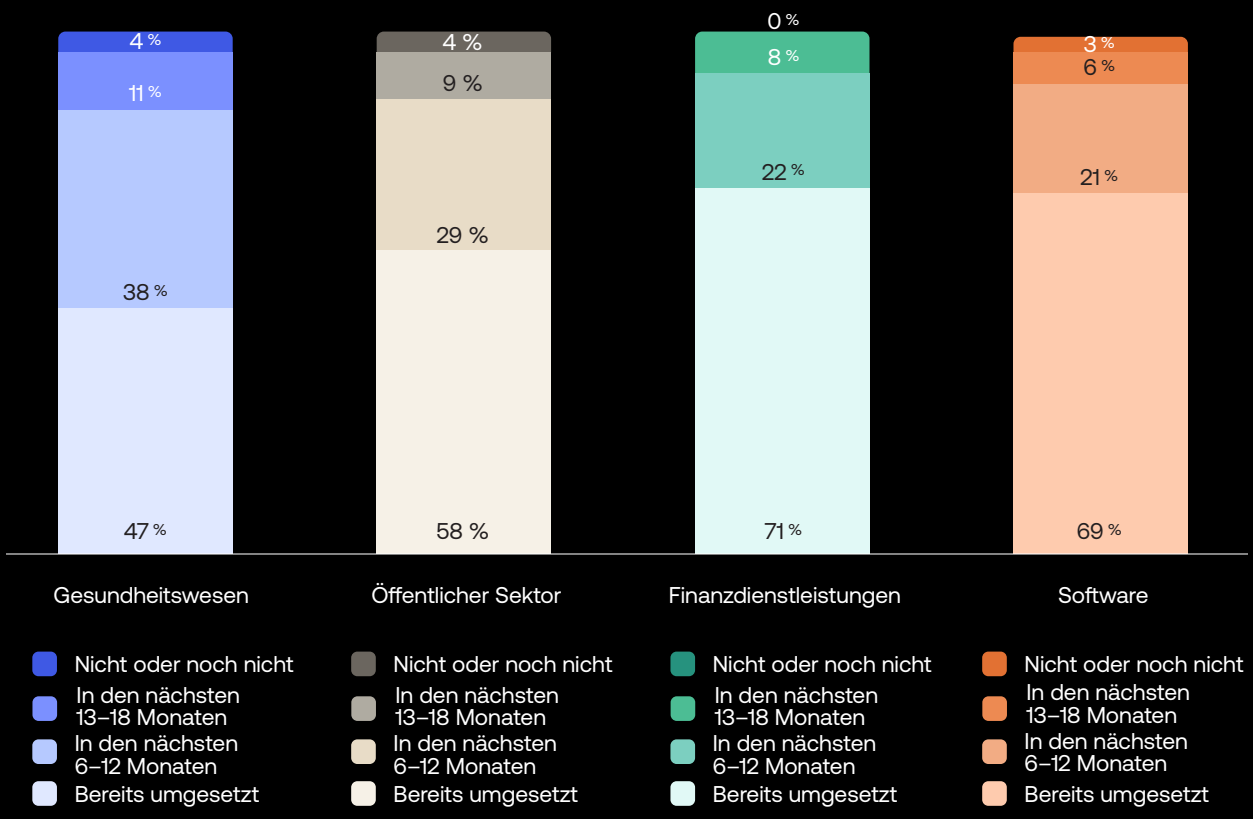
Betrachtet man die Daten hinsichtlich der Unternehmensgröße, zeigt sich, dass eine vertrauenswürdige IP-Adresse sowohl bei den größten als auch kleinsten Unternehmen aus der Umfrage höchste Priorität hat, während für Unternehmen von 5.000 bis 9.999 Mitarbeiter das Device Management einen höheren Stellenwert hat. ■

Zero Trust: Entwicklung nach Branche

Die einzelnen vertikalen Branchen im Detail

Jede Zero Trust Journey variiert von Branche zu Branche, genauso wie die Prioritäten und Praktiken einzelner Unternehmen. Bei der diesjährigen Umfrage stellten wir wieder vier wichtige Branchen in den Fokus: Gesundheitswesen, Behörden, Finanzdienstleister und Software-Unternehmen. Besonders die ersten drei unterliegen strengen Regularien und legen deshalb großen Wert darauf, ihre Ökosystem mithilfe von Zero Trust zu schützen und eine zuverlässige Compliance sicherzustellen. Insgesamt scheinen alle vier Branchen im Vergleich zu letztem Jahr einige Fortschritte gemacht zu haben – ihre Zero Trust Journey ist aber lange noch nicht beendet.

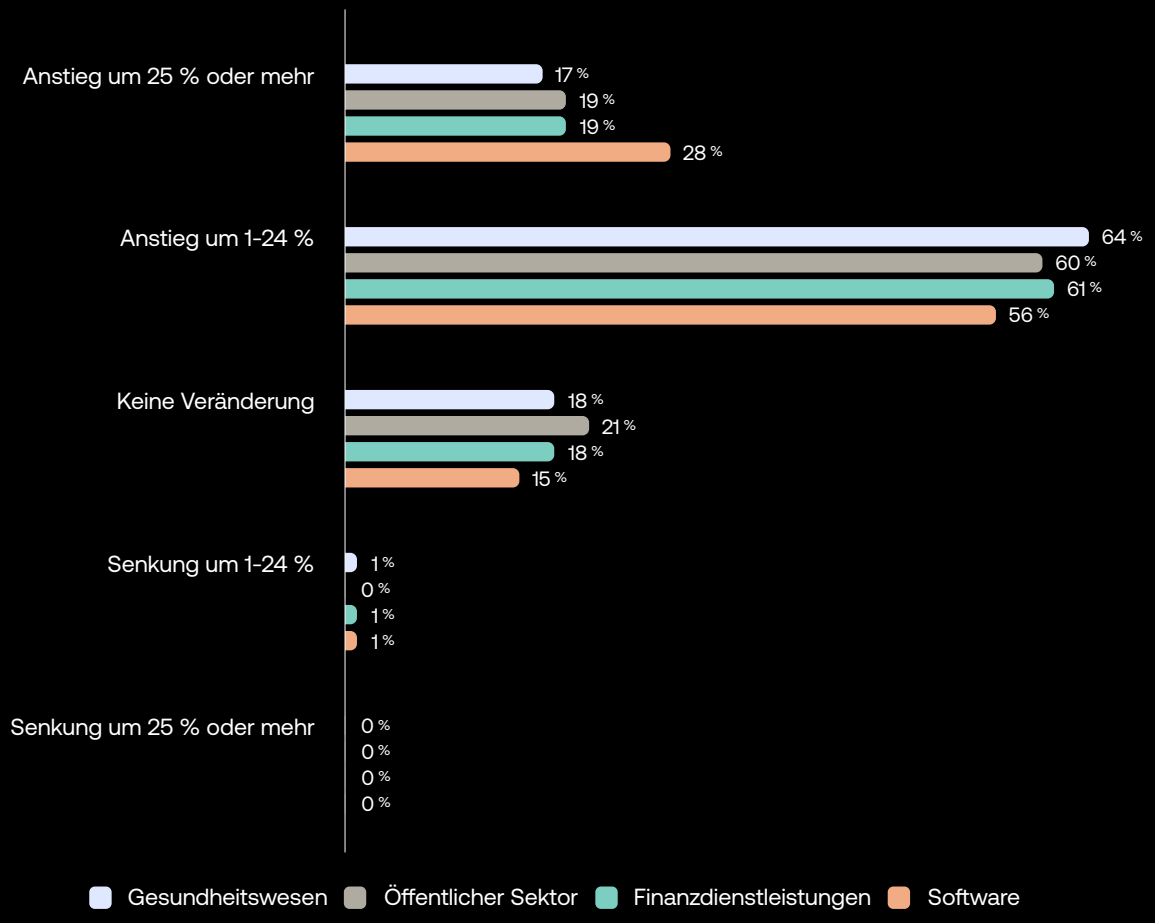
Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten 12–18 Monaten eines starten?
Vergleich nach Branche



Finanzdienstleister und Softwareunternehmen sind die Spitzenreiter bei der Einführung von Zero Trust

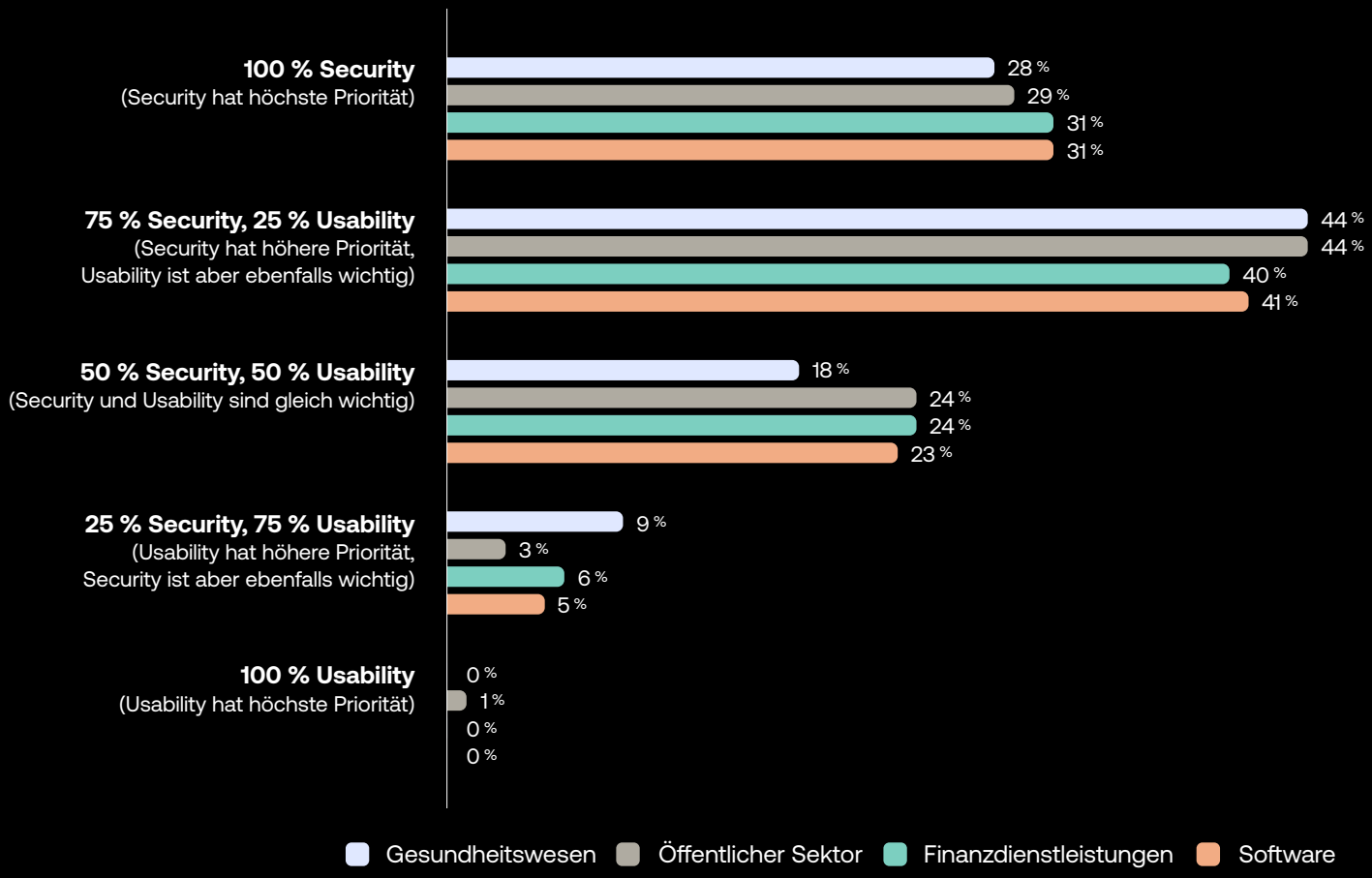
Die diesjährige Umfrage zeigt branchenübergreifend einen deutlichen Trend zu Zero Trust. Weniger als 4 % der befragten Unternehmen in jeder unserer Fokusbranchen gab als Antwort, „keine aktive Zero-Trust-Initiative oder für die kommenden 18 Monate geplant“ zu haben. Finanzdienstleister und Software-Unternehmen setzen (mit 71 bzw. 68 %) am ehesten auf eine solche Initiative, wobei das Gesundheitsweisen und Behörden, wie auf den folgenden Seiten zu sehen, nicht viel zurückstehen.

Inwiefern hat sich Ihr Budget für Zero Trust in den vergangenen zwölf Monaten verändert (sofern zutreffend)?
Vergleich nach Branche



Trotz der schwierigen gesamtwirtschaftlichen Lage, die zu Budgetkürzungen an verschiedenen Stellen führt, investieren die Unternehmen aller vier Fokusbranchen genau im richtigen Bereich: ihrer Zero-Trust-Security. Vier von fünf befragten Unternehmen der Schwerpunkt-Branchen erhöhten im letzten Jahr ihr Budget für Security-Maßnahmen, wobei nahezu kein Unternehmen seine finanziellen Mittel für Security reduzierte.

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



Was ist also die Kernaussage dieses umfassenden, Security-zentrierten Diagramms: In einem Klima, in dem fast fünf Data Breaches täglich stattfinden (laut The Identity Theft Resource Centers 2022 Data Breach Report), hat Security einen höheren Stellenwert als Benutzerfreundlichkeit. Die meisten der befragten Unternehmen aller vier untersuchten Branchen gaben an, dass ihre Prioritäten zu 75 % auf der Security und zu 25 % auf der Benutzerfreundlichkeit liegen. Die zweithäufigste Antwort war, dass Security die oberste Priorität hat. Auch wenn eine reibungslose User-Experience für Mitarbeiter und Lieferanten ein wichtiger Punkt ist, überwiegt sie nicht das Risiko eines Data Breaches oder Compliance-Verstoßes.

Zero Trust – Entwicklung nach Branche

Gesundheits-wesen

Obwohl das Gesundheitswesen manchmal etwas langsamer agiert, machen die Einrichtungen dennoch Fortschritte bei der Planung und Einführung von Zero Trust. Ein Großteil der Befragten aus dem Gesundheitswesen setzt entweder bereits auf Zero Trust oder verfolgen eine Zero-Trust-Strategie für die nahe Zukunft. Und auch wenn etliche Einrichtungen dieses Sektors noch immer vor der Herausforderung stehen, sich von risikoreichen Faktoren mit einem geringen Sicherheitsgrad zu lösen, ist ihnen die Bedeutung für Identity im Großen und Ganzen bewusst, weshalb sie MFA und SSO für interne und externe Benutzer, ihre Datenbanken und andere Ressourcen einsetzen.

Fast 100 % schreiben Zero Trust auf ihre strategische Roadmap

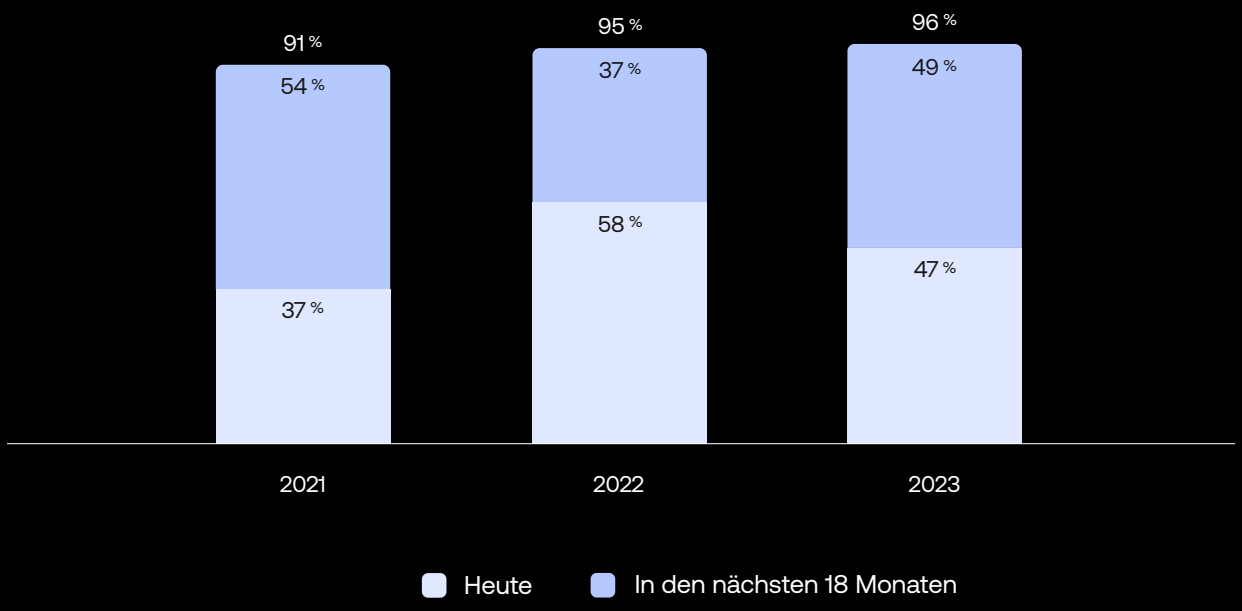
Über die letzten drei Jahre schwankte das Interesse des Gesundheitswesens für Zero Trust – doch nicht um viel. Bis auf 4 % setzen alle befragten Gesundheitseinrichtungen auf Zero Trust oder planen, es in den nächsten 18 Monaten einzuführen. Und jedes Jahr rückt die Zahl der Einrichtungen mit aktiver Zero-Trust-Initiative oder entsprechenden Plänen näher an die 100 %. (Im Vergleich zum Vorjahr gaben dieses Jahr weniger Einrichtungen an, bereits eine Zero-Trust-Strategie zu verfolgen, was laut The Wall Street Journal möglicherweise auf IT-Einsparungen im Jahr 2022 zurückzuführen ist, die nun wieder zurückgehen). Alles in allem erwarten wir einen Aufschwung der Zero-Trust-Initiativen im Gesundheitswesen, während diejenigen, die bereits darauf vertrauen, diese Kapazitäten ausbauen werden.

Das Gesundheitswesen liegt leicht hinter dem Durchschnitt mit der Absicht aufzuholen

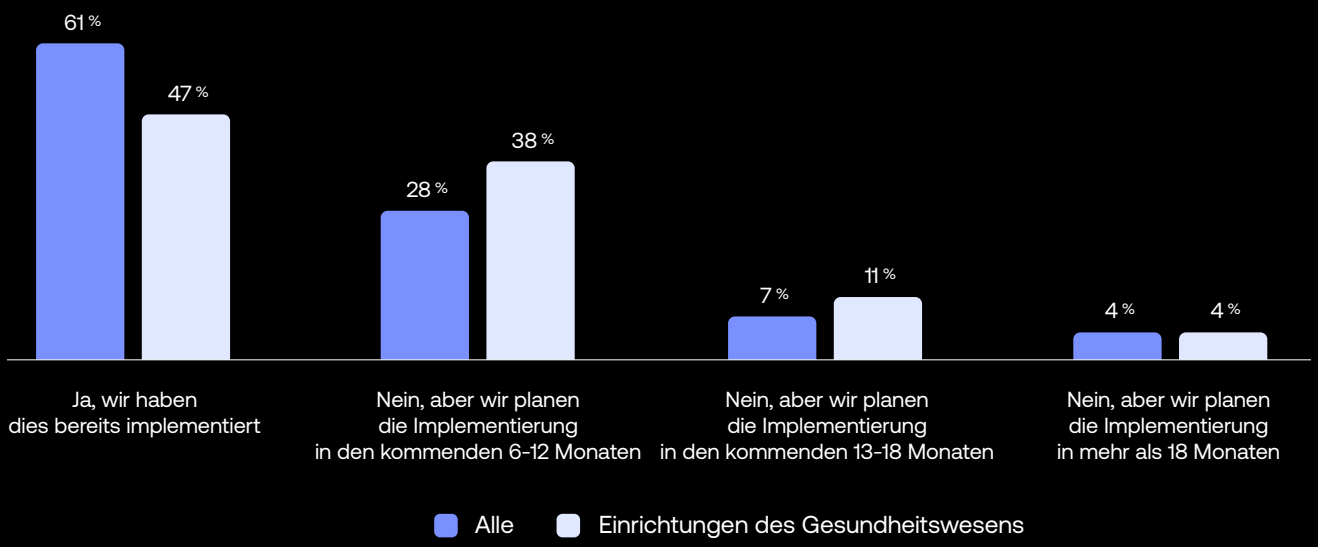
Im Vergleich zum globalen Durchschnitt zeigt sich, dass das Gesundheitswesen in Sachen Zero Trust anderen Unternehmen noch immer nachsteht. Allerdings treiben die Einrichtungen die Projekte mit Hochdruck voran, und liegen im globalen Spiegel bei einer geplanten Einführung in den nächsten 6-12 Monaten weit vorn. 38 % der Gesundheitseinrichtungen planen in diesem Zeitraum, Zero Trust zu implementieren – wohingegen nur 28 % der Unternehmen weltweit sich dieses Ziel gesetzt haben.

Bei der Frage, wie wichtig Identity für ihre Zero-Trust-Strategie sei, antworteten neun von zehn Gesundheitseinrichtungen entweder mit „sehr wichtig“ oder „relativ wichtig“. Angesichts der hochsensiblen Personendaten, deren Schutz oberste Priorität für das Gesundheitswesen hat (und auch im Fokus der Aufsichtsbehörden steht), ist das natürlich nicht überraschend.

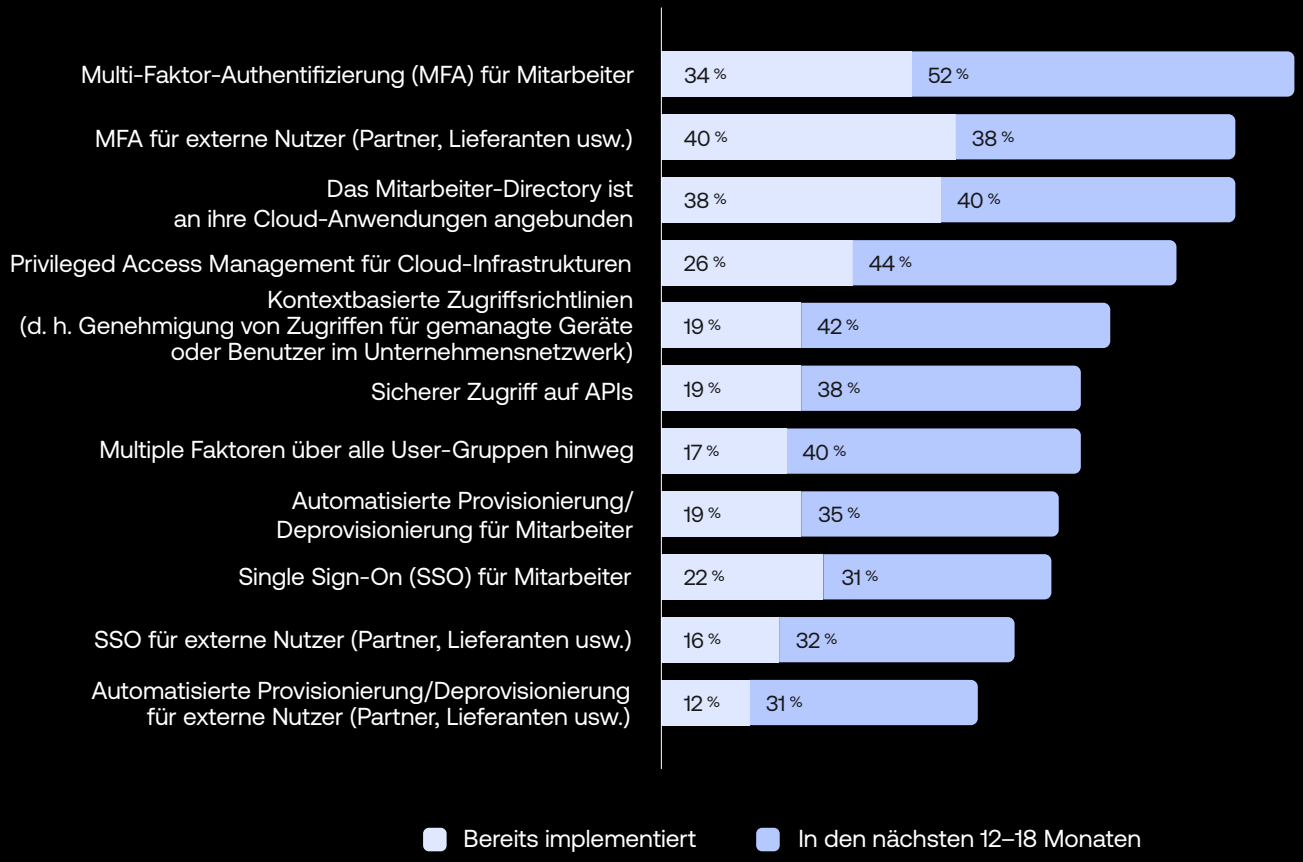
Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten 18 Monaten eines starten?
Das Gesundheitswesen im Jahresvergleich



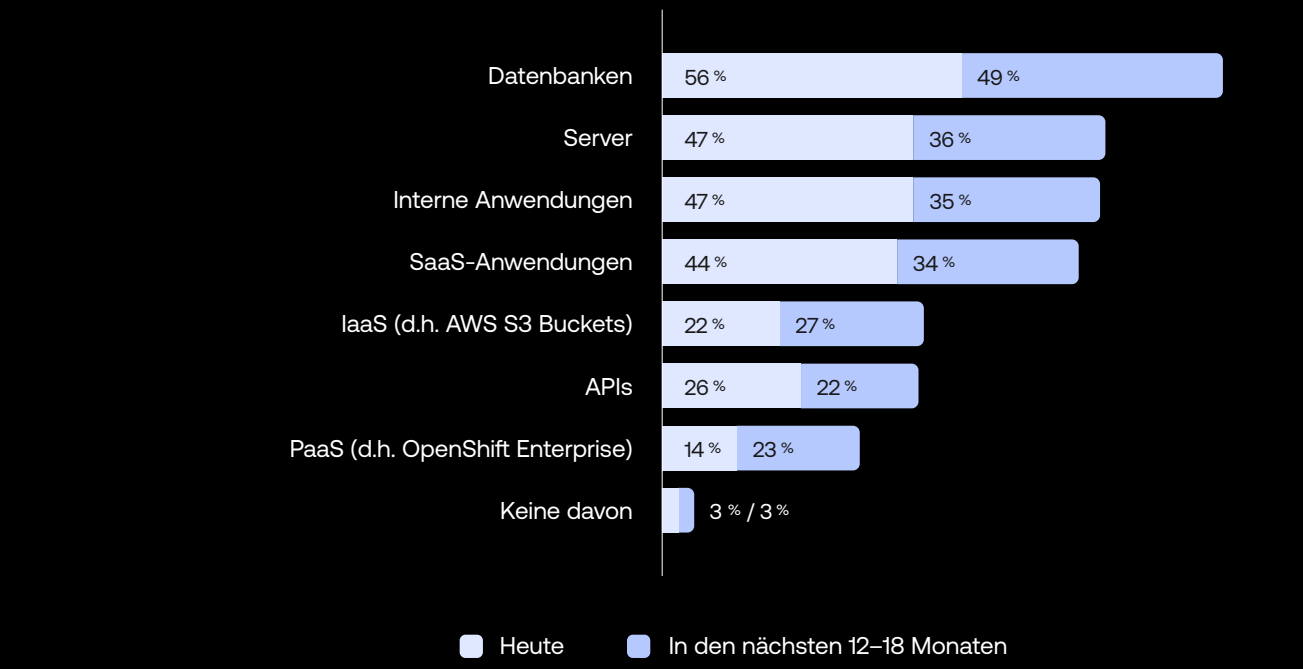
Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten Monaten eines starten?
Gesundheitswesen vs. Alle Befragten



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



Für den Zugriff auf welche Ressourcen verwenden Sie SSO und/oder MFA, und auf welche Ressourcen möchten Sie sie innerhalb der nächsten 12-18 Monate ausweiten?
Gesundheitswesen



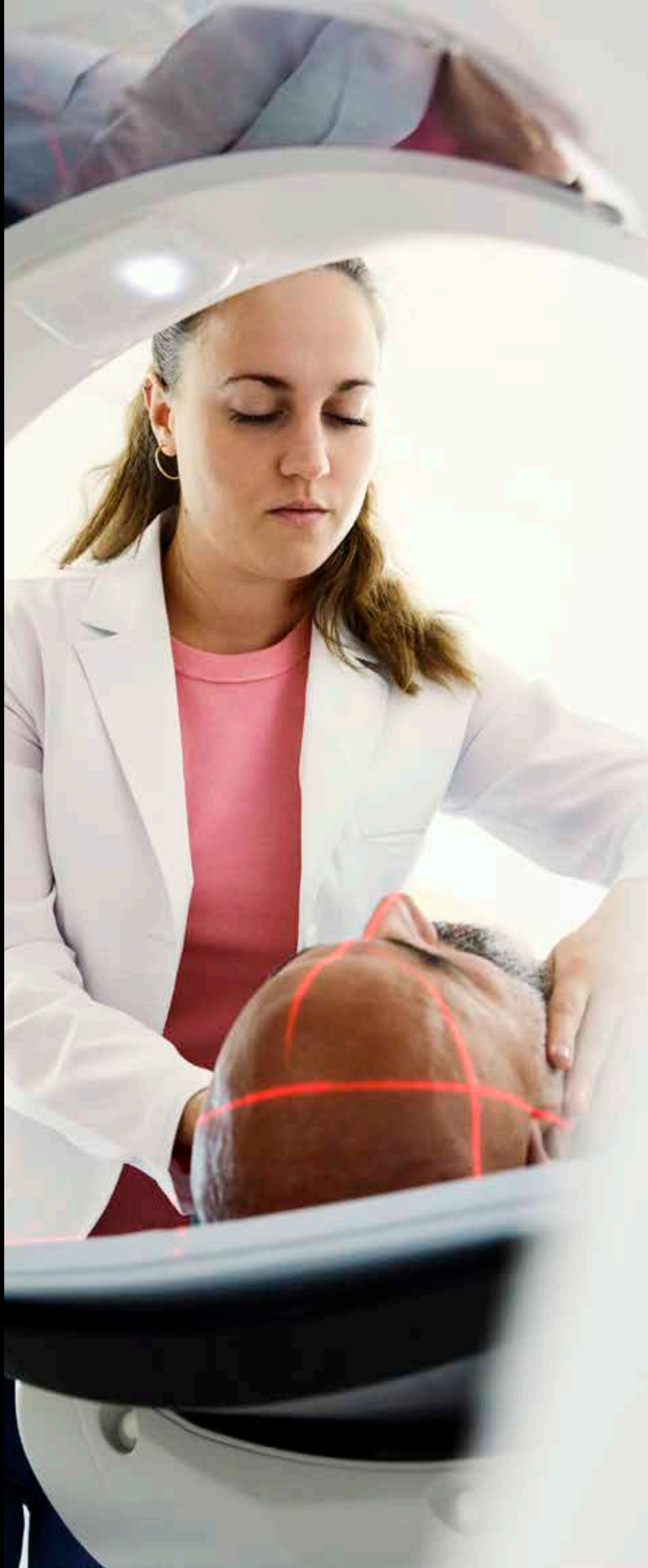
Hinweis: Die Gesamtsumme der Spalten kann 100 % übersteigen, da die Befragten beide Antwortmöglichkeiten gewählt haben.

MFA und die Anbindung von Directories stehen für das Gesundheitswesen an erster Stelle

MFA für Mitarbeiter und externe Benutzer zählen zu den wichtigsten Initiativen für Gesundheitseinrichtungen – das ist auch dieses Jahr nicht anders. Gemeinsam mit der Anbindung von Mitarbeiter-Directories an Cloud-Anwendungen bilden sie die Top-3-Antworten für bereits umgesetzte Security-Initiativen. Mehr als ein Drittel der befragten Gesundheitseinrichtungen setzen bereits auf MFA für ihre Workforce – und bei 52 % steht die Einführung von MFA für Mitarbeiter künftig ganz oben auf der To-Do-Liste. Andere Initiativen wie SSO und eine automatisierte Provisionierung haben dieses Jahr für das Gesundheitswesen einen geringeren Stellenwert.

Datenbanken, Server und Anwendungen stehen an der Spitze beim SSO-/MFA-Schutz

Gesundheitseinrichtungen legen den Schwerpunkt bei der SSO- bzw. MFA-Erweiterung vor allem auf den Schutz von Datenbanken, deren sensible, private Patientendaten ein attraktives Ziel für Cyberkriminelle darstellen. Aber auch die SSO-/MFA-Skalierung auf die Server und SaaS-Anwendungen rangiert weit oben – sowohl bei bereits umgesetzten als auch zukünftigen Initiativen in diesem Sektor.



Vertrauenswürdige IP-Adressen und ein starkes Device Management sind entscheidend für die Zugriffskontrolle

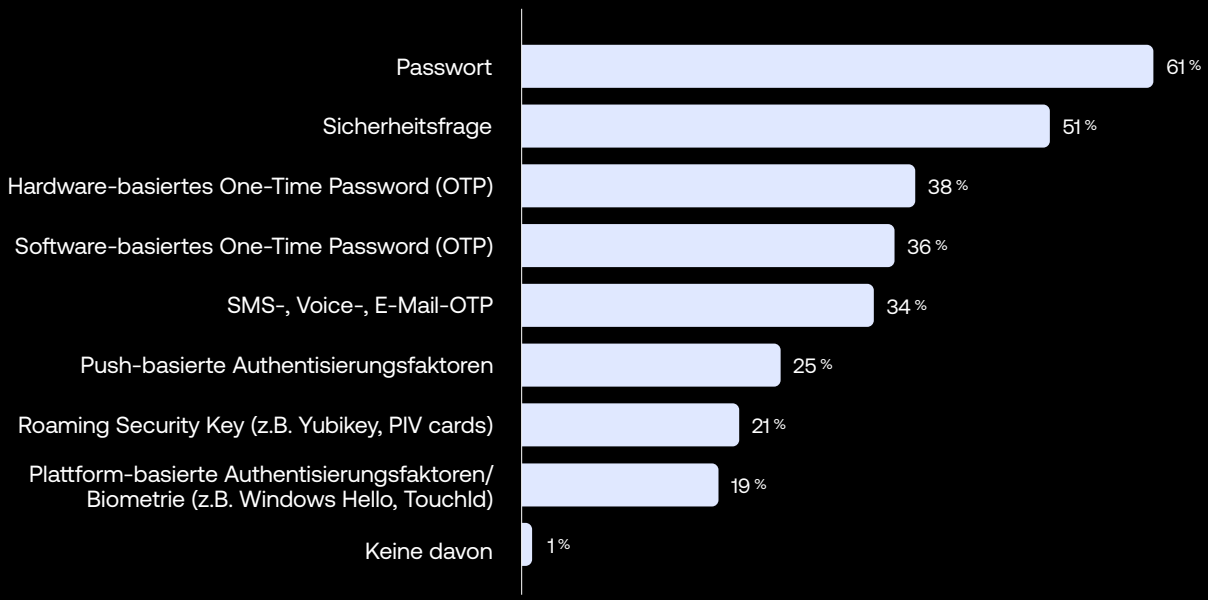
Mehr als die Hälfte der befragten Gesundheitseinrichtungen erachten eine vertrauenswürdige IP-Adresse oder das Device Management als wichtigsten Faktor für die Zugriffskontrolle und -genehmigungen interner Ressourcen – was sich auch bei den Befragten weltweit widerspiegelt. Kurz dahinter rangieren die Benutzergruppe und die Ressource selbst.

Das Gesundheitswesen setzt bei der Authentisierung auf Passwörter und Sicherheitsfragen

Mit 61 % sind Passwörter auch im Gesundheitswesen immer noch der Spitzenreiter unter den Authentifikatoren. Eine passwortlose Zukunft ist also noch in weiter Ferne. Sicherheitsfragen stehen jedoch um nicht viel nach und werden von mehr als der Hälfte der befragten Gesundheitseinrichtungen eingesetzt. One-Time-Passwörter (OTP) – via Hardware, Software, SMS, Telefon und E-Mail – teilen sich den dritten Platz, während Plattform-basierte Authentifikatoren und biometrischen Verfahren die Schlusslichter für diesen Sektor bilden.

Was sind aus Ihrer Sicht die wichtigsten Faktoren bei der Kontrolle und Genehmigung von Zugriffen auf Ihre internen Ressourcen?
Gesundheitswesen

Welche Sicherheitsfaktoren nutzen Sie aktuell zur Verifikation interner und externer Nutzer?
Gesundheitswesen



Zero Trust – Entwicklung nach Branche

Öffentlicher Sektor

Keine andere Branche steht so unter Druck, ihre Security mit Zero Trust zu stärken, wie der öffentliche Sektor. In Nordamerika zum Beispiel fordert die U.S. Federal Zero Trust Strategy seit kurzem, dass allen Bundesbehörden bis September 2024 spezifische Cybersecurity-Standards und -ziele erfüllen – und versucht damit die Regierung vor der steigenden Anzahl komplexer und langwieriger Bedrohungskampagnen zu schützen. Die US-Regierung setzte zuvor bereits andere Guidelines in Kraft: z. B. die National Cybersecurity Strategy und die Zero Trust Strategy and Roadmap des Department of Defense.

Dieses Jahr wurden Behörden aus Nordamerika, EMEA und den APJ-Regionen befragt. (In diesem Report schließt der öffentliche Sektor keine staatlichen oder kommunalen Einrichtungen mit ein.) Unsere Befragung zeigte, dass 58 % der öffentlichen Einrichtungen bereits Zero-Trust-Initiativen implementiert haben und 38 % die Einführung von Zero Trust planen. Diese Behörden setzen beim Schutz ihrer kritischsten Ressourcen auf SSO bzw. MFA und stellen mit strengen Richtlinien, die Sicherheit ihrer Infrastrukturen und Assets sicher.

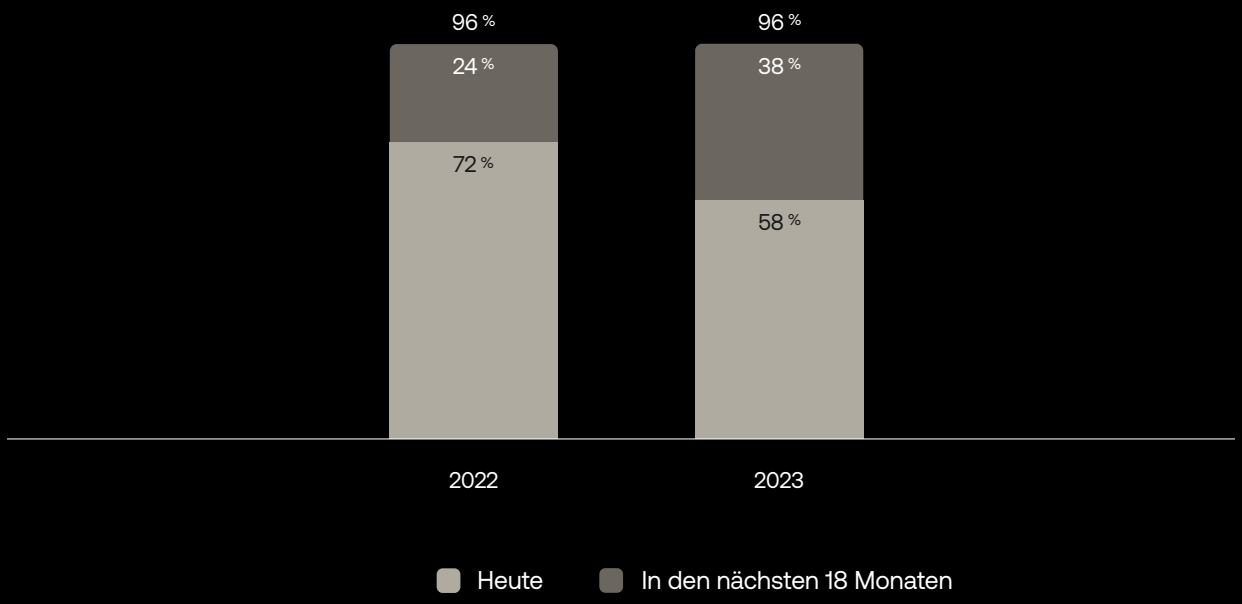
Beinahe alle Einrichtungen des öffentlichen Sektors verfolgen eine Zero-Trust-Strategie

Der öffentliche Sektor bleibt seiner Entscheidung für Zero Trust treu. Von 2022 bis 2023 blieb die Gesamtzahl der öffentlichen Einrichtungen mit aktiven Zero-Trust-Initiativen oder entsprechenden Zukunftsplänen relativ konstant bei 96 %. Letztes Jahr gaben 72 % der befragten Behörden an, bereits eine Zero-Trust-Initiative im Einsatz zu haben. Allerdings müssen wir anmerken, dass die letztjährigen Befragten aus dem öffentlichen Sektor zu 86 % ihren Sitz in Nordamerika hatten. Dieses Jahr haben wir den Kreis der Befragten erweitert: Nur 31 % der befragten Behörden stammen aus Nordamerika – und im Rahmen dieser breiteren Stichprobe gaben nur 58 % an, bereits Zero Trust implementiert zu haben, während 38 % in naher Zukunft konkrete Pläne in die Tat umsetzen wollen.

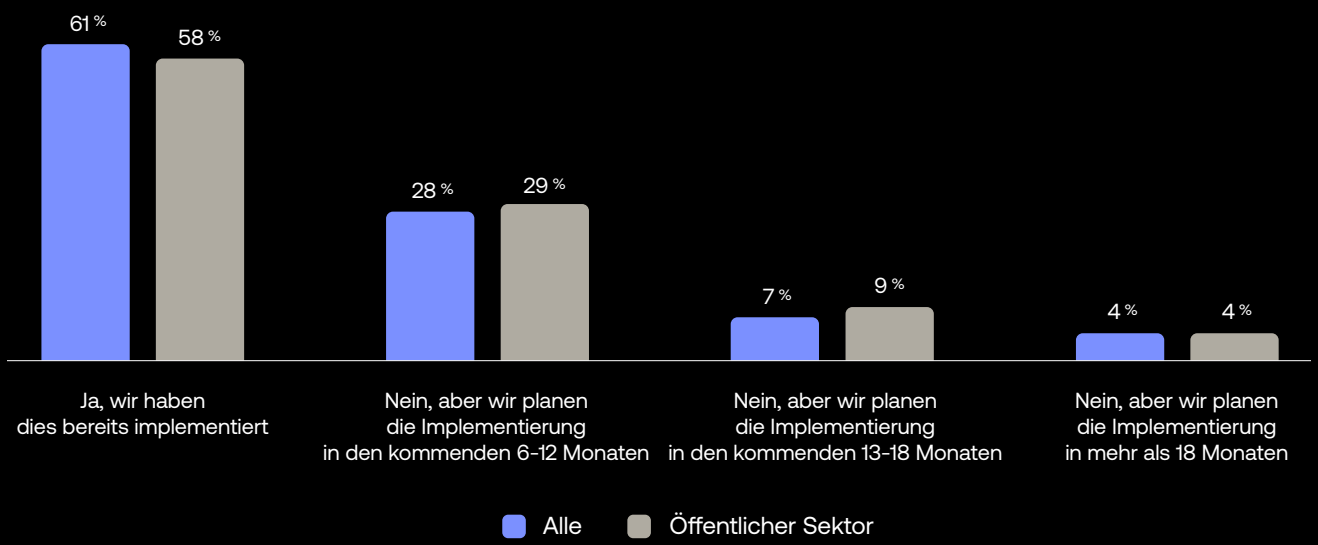
Der öffentliche Sektor liegt bei aktiven Initiativen zurück, hat bei der Zukunftsplanung jedoch die Nase vorn

Die diesjährigen befragten Behörden liegen in puncto umgesetzter Zero-Trust-Initiativen fast gleichauf mit dem globalen Durchschnitt. 61 % der befragten Einrichtungen und Unternehmen verfügen über ein solches Programm; der öffentliche Sektor liegt demgegenüber bei 58 %. Fast ein Drittel der Behörden plant allerdings die Implementierung von Zero Trust in den nächsten 6-12 Monaten – vor allem hinsichtlich staatlicher Vorgaben – und liegt damit leicht über dem weltweiten Durchschnitt.

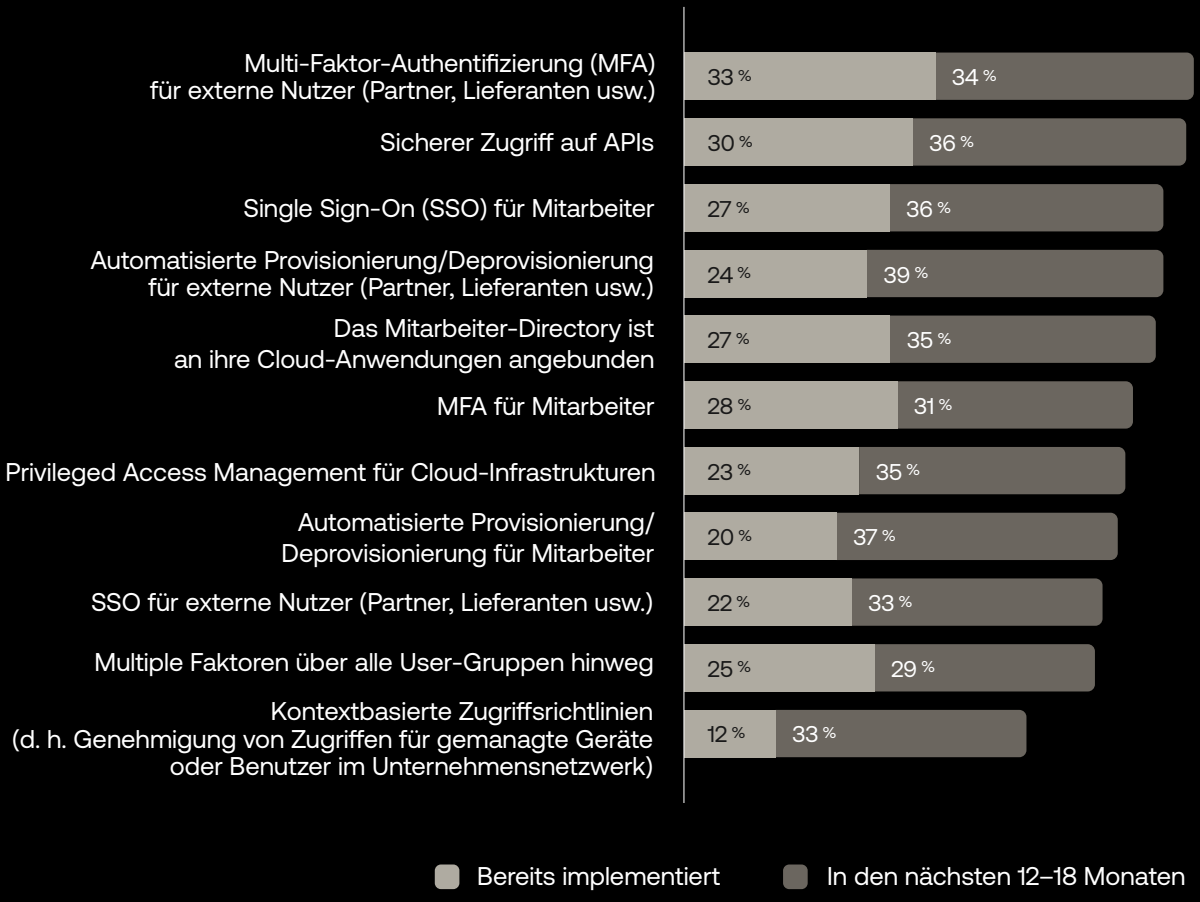
Hat Ihre Einrichtung aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten 18 Monaten eines starten?
Öffentlicher Sektor im Jahresvergleich



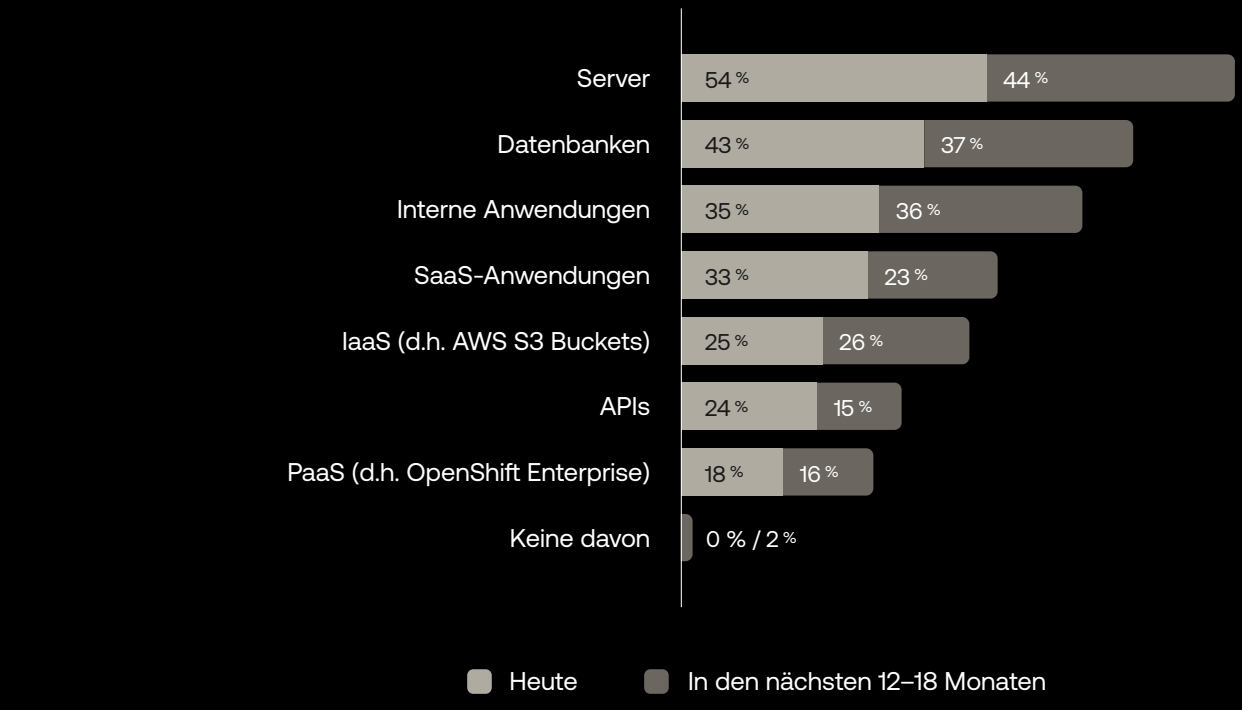
Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten Monaten eines starten?
Öffentlicher Sektor vs. Alle Befragten



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



Für den Zugriff auf welche Ressourcen verwenden Sie SSO und/ oder MFA, und auf welche Ressourcen möchten Sie sie innerhalb der nächsten 12-18 Monate ausweiten?
Öffentlicher Sektor



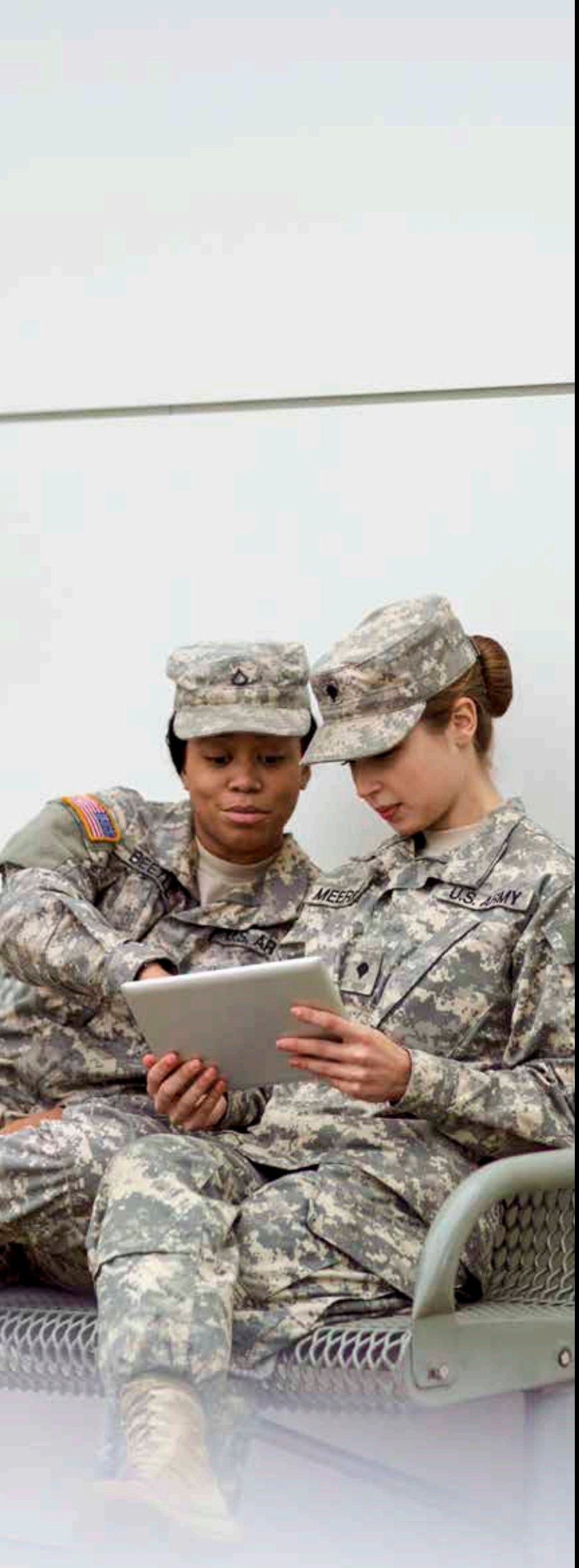
Hinweis: Die Gesamtsumme der Spalten kann 100 % übersteigen, da die Befragten beide Antwortmöglichkeiten gewählt haben.

MFA für externe Benutzer und sichere API-Zugriffe haben für den öffentlichen Sektor die höchste Priorität

Regierungsbehörden auf der ganzen Welt sind auf eine Vielzahl internationaler Lieferanten und externer Partner angewiesen. Da ist es nicht verwunderlich, dass MFA für externe Benutzer (wie Partner und Third-Party-Anbieter) mit 33 % und sichere API-Zugriffe mit 30 % an der Spitze der Sicherheitsmaßnahmen für den öffentlichen Sektor stehen. Weitere 34 % der öffentlichen Einrichtungen streben eine Implementierung von MFA für externe Benutzer in den nächsten 12-18 Monaten an. Kurz dahinter liegen die Einführung von SSO für Mitarbeiter und ein automatisiertes Provisioning/Deprovisioning externer Benutzer.

Servern und Datenbanken stehen bei MFA/SSO im Fokus

Server und Datenbanken sind für den öffentlichen Sektor das Maß aller Dinge, wenn es um SSO- und MFA-Schutz geht. Mehr als die Hälfte der befragten öffentlichen Einrichtungen gaben an, ihre Server bereits mit SSO bzw. MFA zu schützen, und 43 % haben eines oder beide für ihre Datenbanken im Einsatz. Mit einem Drittel der Behörden stehen interne und SaaS-Anwendungen nicht um viel nach, dicht gefolgt von IaaS, APIs und PaaS.



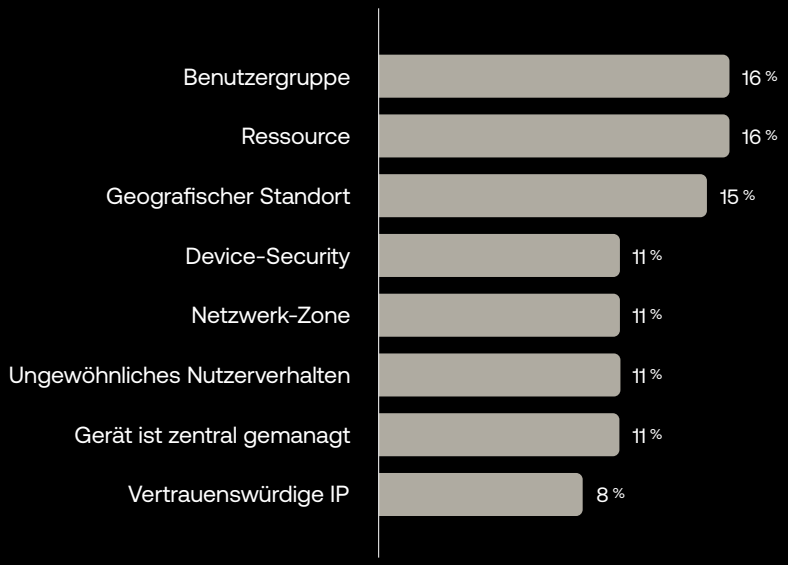
User-Gruppe und die Ressource selbst als wichtigste Faktoren für den Ressourcenzugriff

Einrichtungen des öffentlichen Sektors sind besonders darauf bedacht, dass ihre Daten vor unerwünschten Blicken geschützt sind. Bei der Kontrolle und Genehmigung des Zugriffs auf interne Ressourcen sind eine ganze Reihe von Faktoren ausschlaggebend: Ganz oben auf der Liste steht zunächst die User-Gruppe – gefolgt von der Ressource selbst, dem geografischen Standort und weiteren gleichwertigen Faktoren.

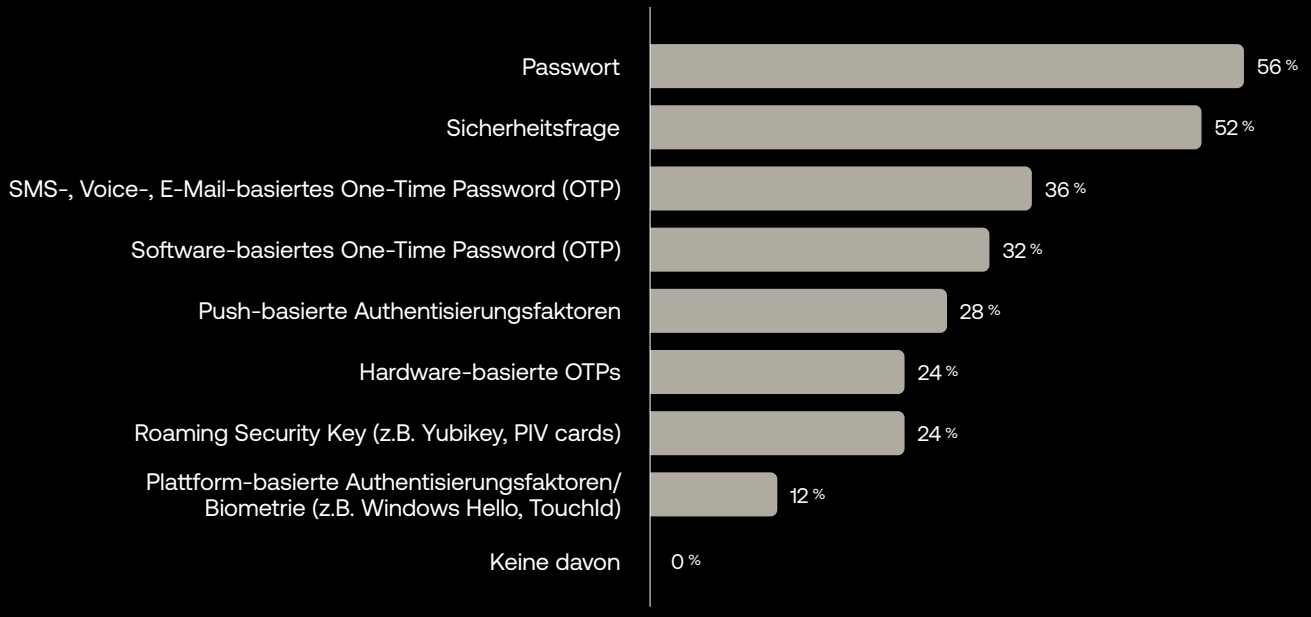
„Passwort“ und „Sicherheitsfrage“ bleiben Top-Faktoren bei der Verifizierung von Usern

Wie bereits erwähnt, verlässt sich der öffentliche Sektor nach wie vor auf Autorisierungsmethoden, die relativ geringe Sicherheit bieten. Befragte nennen hierbei am häufigsten „Passwort“ und „Sicherheitsfrage“ als Faktoren. Doch auch das dürfte sich ändern, da auch Faktoren wie Software- und Hardware-OTP sowie SMS-, Sprach- und E-Mail-OTP eine immer größere Rolle spielen. Diese Faktoren leisten ein höheres Maß an Sicherheit. (Die flüchtige Natur dieser Optionen macht sie sicherer als gespeicherte Passwörter und Sicherheitsfragen, die potenziell gehackt werden können.) ■

Geben Sie an, welcher Faktor für Sie bei Kontrolle und Genehmigung des Zugriffs auf interne Ressourcen ausschlaggebend ist.
Öffentlicher Sektor



Welche Sicherheitsfaktoren nutzen Sie aktuell zur Verifikation interner und externer Nutzer?
Öffentlicher Sektor



Zero Trust – Entwicklung nach Branche

Finanzdienst-leistungen

Finanzdienstleister stellen ein attraktives Ziel für Cyberkriminelle dar. Das zeigt sich daran, dass kaum eine andere Branche in den letzten Jahren so viele Sicherheitsvorfälle verzeichnet hat. Mindestens 79 US-Finanzdienstleister meldeten allein im Jahr 2022 Datenschutzverletzungen, bei denen jeweils mindestens 1.000 Verbraucher betroffen waren. Bei den größten Fällen von Datenschutzverletzung waren sogar Millionen von Verbrauchern betroffen. Zero Trust definiert für diese Unternehmen einen klaren Weg zur besseren Sicherung ihrer essenziellen Systeme und Kundendaten. Heutzutage verfolgen ca. zwei Drittel aller Finanzdienstleister einen Zero-Trust-Ansatz – und diejenigen, die das noch nicht tun, planen es.

Sieben von zehn Finanzdienstleistern vertrauen bereits auf Zero Trust

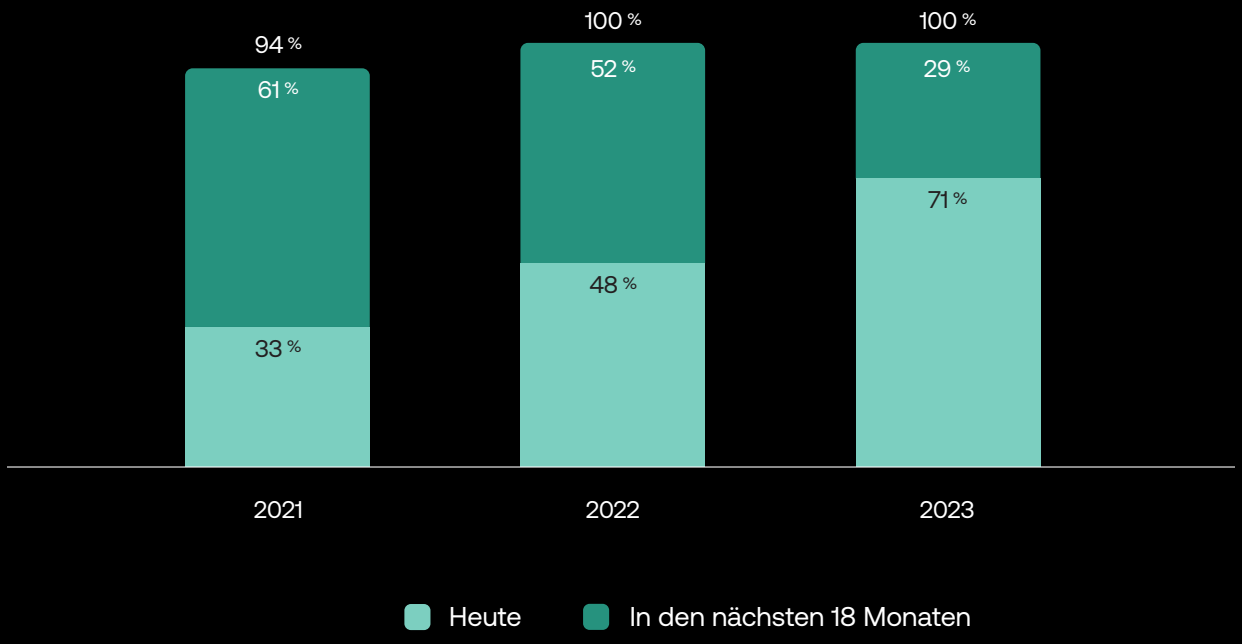
Sicherheitsvorfälle können sehr kostspielig sein, wie der IBM Report „Cost of a Data Breach 2023“ belegt. Es ist also kein Zufall, dass sich jedes Jahr mehr und mehr Finanzdienstleister für ein Zero-Trust-Modell entscheiden. Im Jahr 2021 gab nur ca. ein Drittel der Befragten im Finanzsektor an, ein klar definiertes Zero-Trust-Modell zu nutzen. Im Jahr 2022 stieg diese Zahl auf fast die Hälfte der Befragten an. In diesem Jahr gaben ganze 71 % der befragten Dienstleister an, einem Zero-Trust-Ansatz zu folgen. Eine beeindruckende Wachstumskurve für einen Zeitraum von gerade einmal drei Jahren.

Finanzdienstleister als Vorreiter bei der Umsetzung von Zero-Trust-Modellen

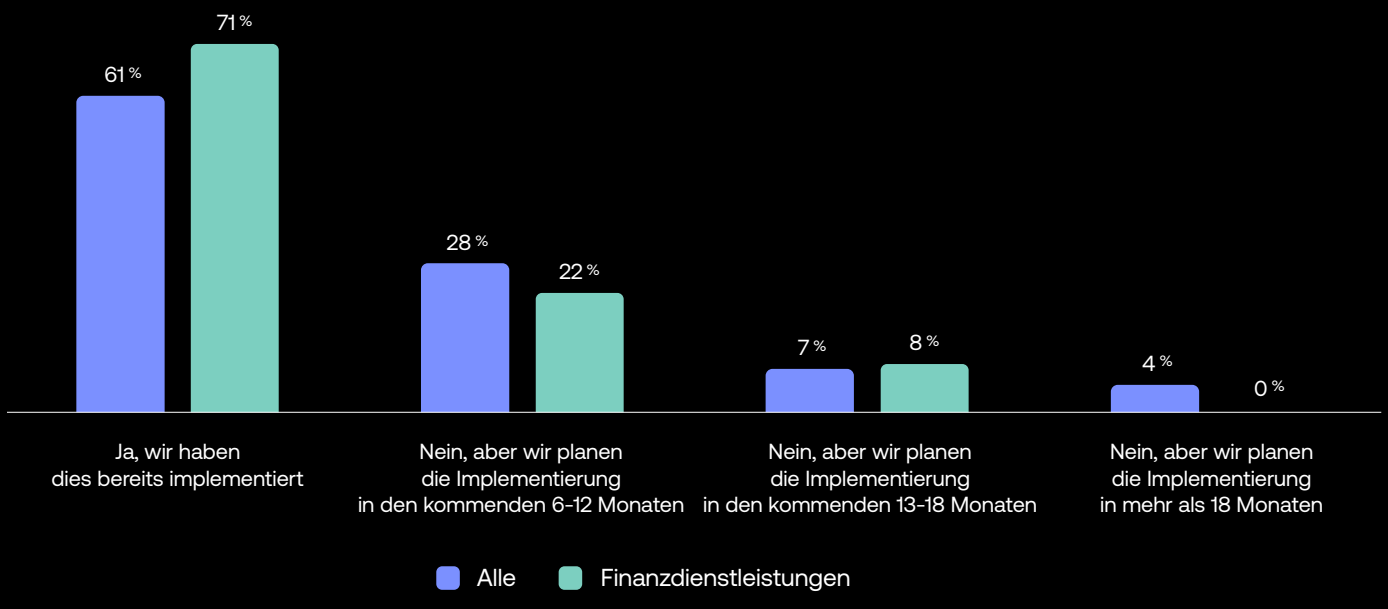
Mehr als zwei Drittel der Finanzdienstleister setzen bereits auf ein Zero-Trust-Modell. 22 % der übrigen Finanzdienstleister gaben an, dies innerhalb der nächsten 12 Monaten ebenfalls zu tun. Weitere 8 % haben es sich zum Ziel gemacht, innerhalb der nächsten 18 Monate auf Zero-Trust umzusteigen. Damit übertrifft der Finanzsektor bereits den weltweiten Durchschnitt für die Umsetzung von Zero-Trust-Modellen. Alle Befragten geben an, dass sie bereits ein Zero-Trust-Modell implementiert haben oder dies innerhalb der kommenden 18 Monate tun wollen.

Der Finanzsektor hat also die Weichen für die branchenweite Einführung von Zero Trust gestellt. Mehr als 90 % der Befragten aus dieser Branche gaben zudem an, dass Identity für die Umsetzung ihrer Zero-Trust-Strategie eine sehr wichtige oder zumindest relativ wichtige Rolle zukommt – wobei fast die Hälfte der Befragten Identity eine Schlüsselrolle zuschreiben. Nur etwa 2 % der Befragten sind da gegenteiliger Meinung und halten den Faktor Identity für unwichtig.

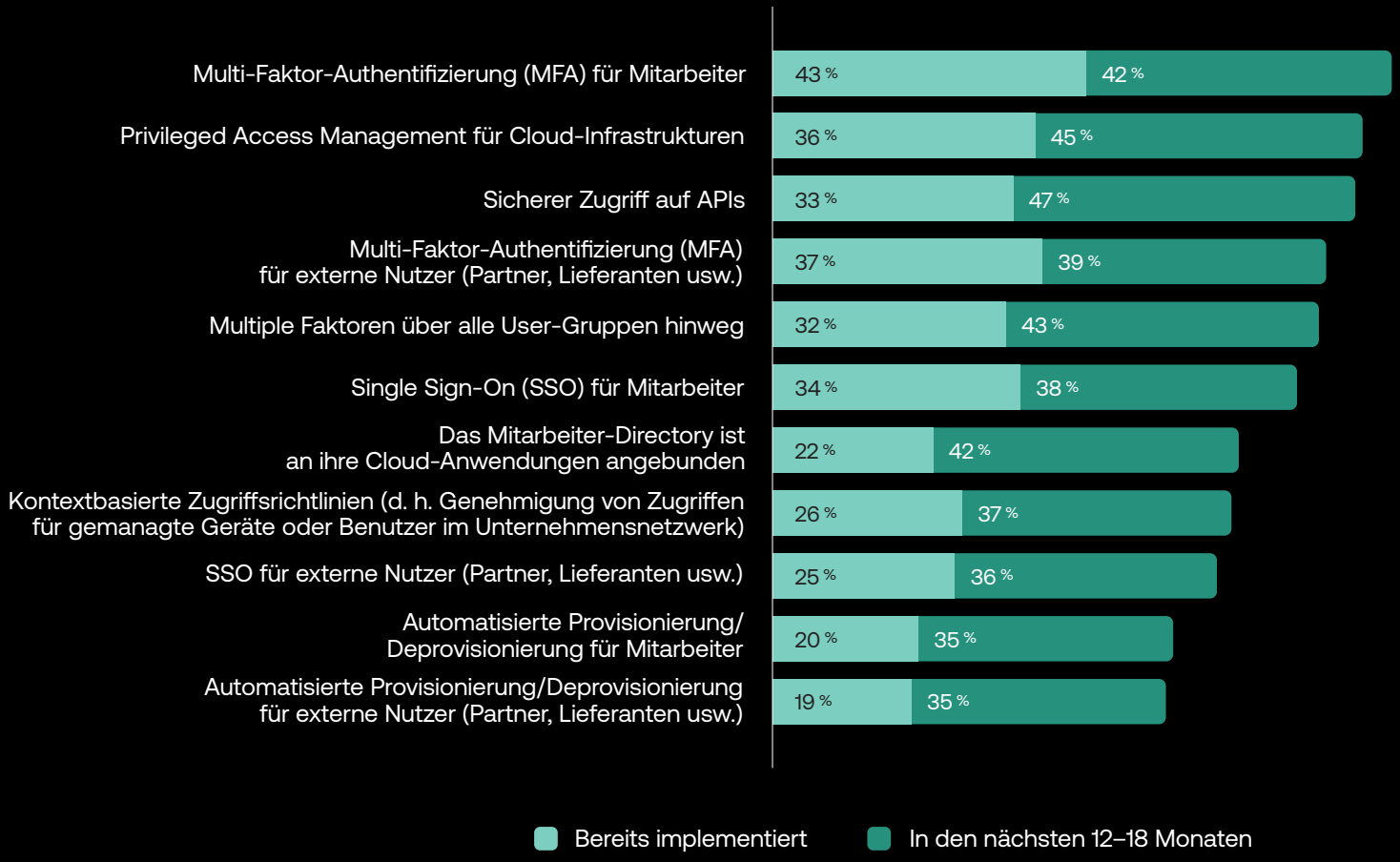
Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten 18 Monaten eines starten?
Finanzdienstleister im Jahresvergleich



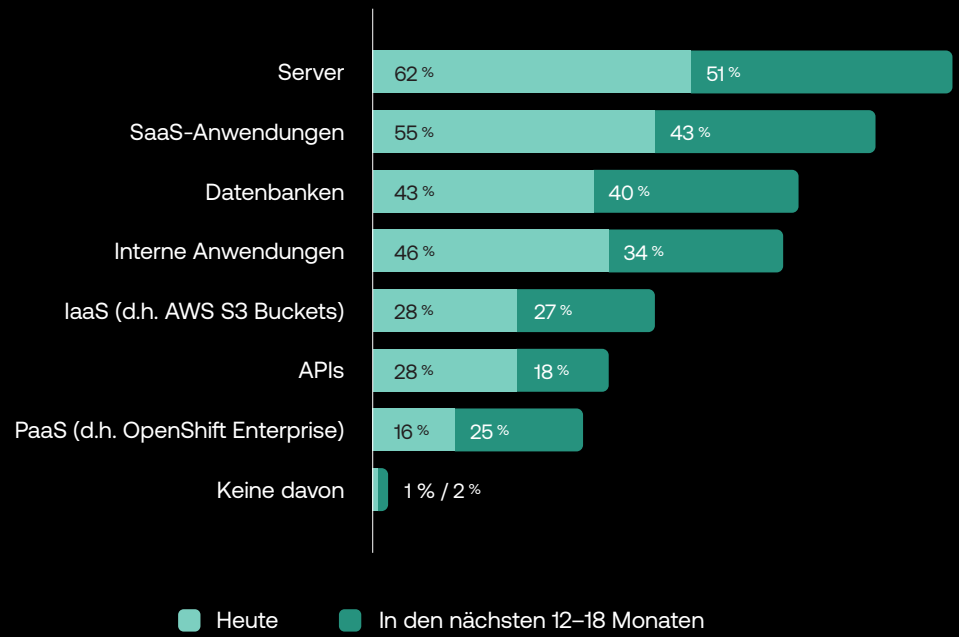
Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten Monaten eines starten?
Finanzdienstleister vs. Alle Befragten



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



Für den Zugriff auf welche Ressourcen verwenden Sie SSO und/oder MFA, und auf welche Ressourcen möchten Sie sie innerhalb der nächsten 12-18 Monate ausweiten?
Finanzdienstleistungen



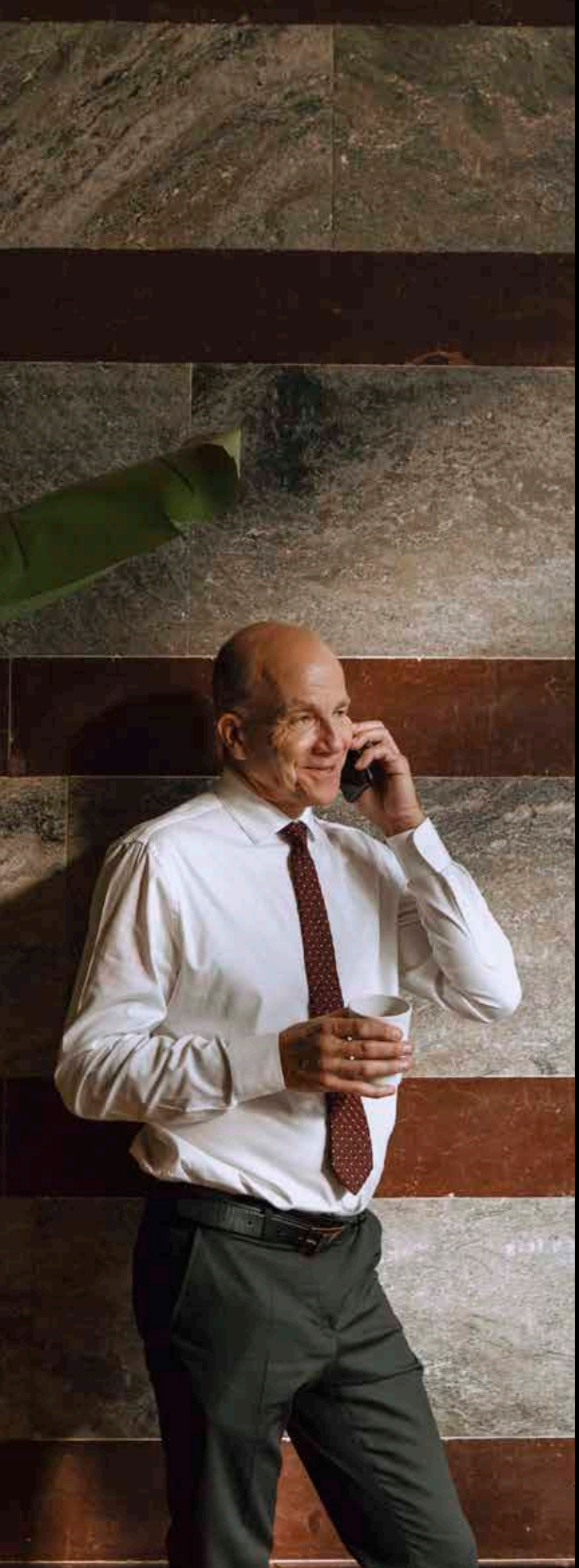
Hinweis: Die Gesamtsumme der Spalten kann 100 % übersteigen, da die Befragten beide Antwortmöglichkeiten gewählt haben.

Die wichtigsten Programme für Finanzdienstleister: MFA und Privileged Access Management

Das wichtigste Zero-Trust-Projekt im Finanzsektor ist in diesem Jahr MFA für Mitarbeitende. 43 % der Befragten haben dieses Sicherheits-Feature bereits implementiert, weitere 42 % wollen dies innerhalb der nächsten 12-18 Monate tun. 36 % der Befragten hat Privileged-Access-Management für die Cloud im Einsatz; weitere 33 % gaben an, den Zugang zu APIs gesichert zu haben. SSO für externe User und die Automatisierung der Provisionierung und Deprovisionierung haben geringere Priorität.

Die meisten Server und SaaS-Anwendungen sind durch SSO und/oder MFA geschützt

Finanzdienstleister haben ihre Server genauestens im Blick. 62 % schützen Zugriffe bereits mit SSO und/oder MFA. 51 % wollen den Schutz in naher Zukunft ausdehnen. (Die Befragten konnten auch beide Optionen wählen.) Und schließlich schützt man mitunter auch SaaS-Anwendungen, Datenbanken und interne Anwendungen durch diese Identity-Technologien (oder will dies künftig angehen).



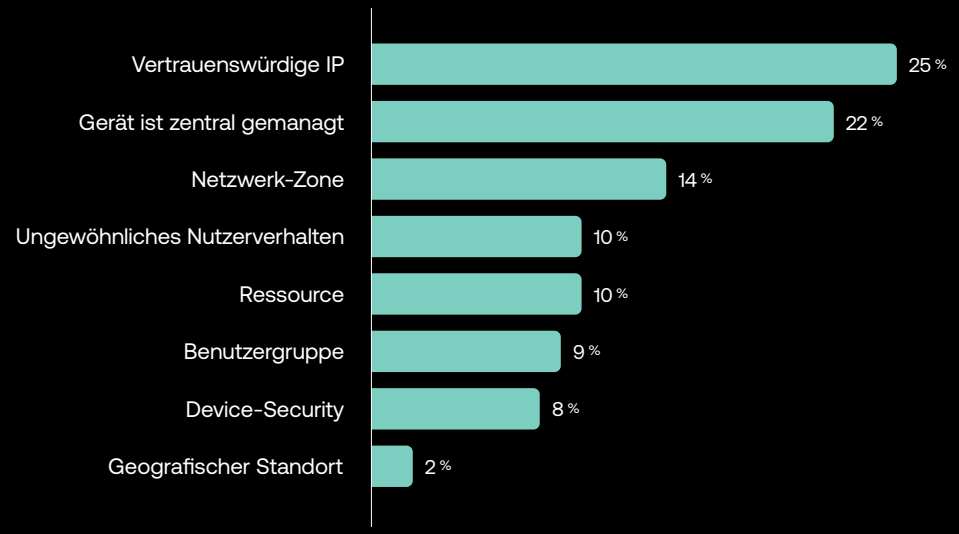
Vertrauenswürdige IP und Device-Management als Top-Kriterien für Zugangsgenehmigungen

Was die Kontrolle und Genehmigung von Zugriffen betrifft, nehmen Finanzdienstleister diese Themen sehr genau – und wollen exakt wissen, wo sich der jeweilige User befindet und welches Device er nutzt. Einer von vier Befragten definierte eine vertrauenswürdige IP-Adresse als wichtigsten Faktor, wenn es darum geht, einen Zugriff zu gestatten. Weitere 22 % halten das Device-Management für ausschlaggebend. Befragte nennen darüber hinaus die Netzwerk-Zone, eventuelle Anomalien im Nutzerverhalten und die Ressource selbst. Der geografische Standort nimmt den letzten Platz in diesem Ranking ein.

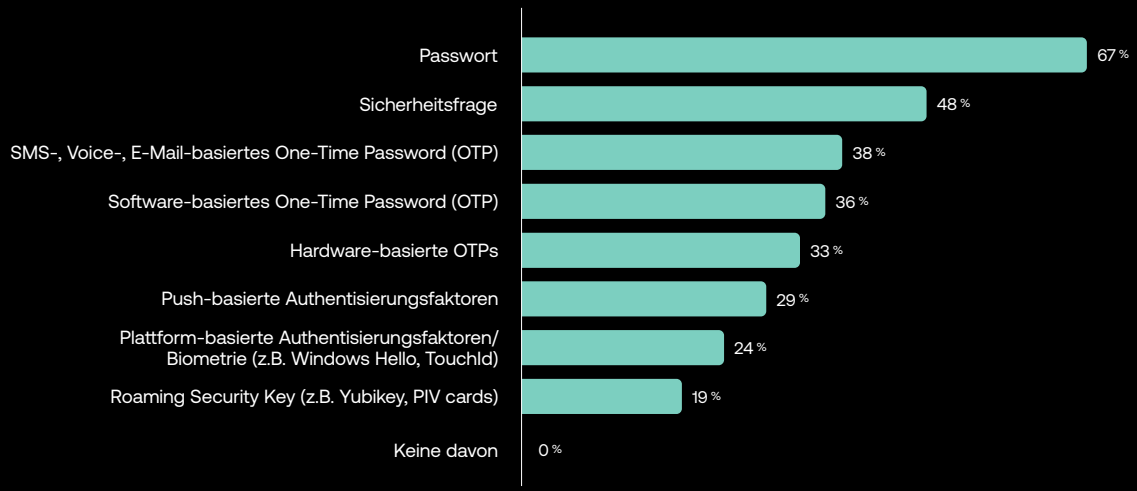
Die wichtigsten Authentifizierungsfaktoren im Finanzsektor: Passwörter und Sicherheitsfragen

Passwörter sind nach wie vor die beliebteste Authentifizierungsmethode von Finanzdienstleistern. Zwei Drittel der Befragten gaben an, primär Passwörter für die Authentifizierung zu nutzen. Platz zwei hinter den Passwörtern nehmen die wissensbezogenen Sicherheitsfragen mit 48 % ein, gefolgt von OTP-Optionen, die von einem Drittel der Befragten genannt wurden.

Geben Sie an, welcher Faktor für Sie bei Kontrolle und Genehmigung des Zugriffs auf interne Ressourcen ausschlaggebend ist.
Finanzdienstleistungen



Welche Sicherheitsfaktoren nutzen Sie aktuell zur Verifikation interner und externer Nutzer?
Finanzdienstleistungen



Zero Trust – Entwicklung nach Branche

Software

In den vergangenen Jahren blieben die Software-Unternehmen in der Regel ein wenig hinter den anderen Branchen zurück. Allerdings hat auch diese Branche in den letzten Jahren in puncto Zero-Trust-Umsetzung gewaltig aufgeholt und liegt mittlerweile über dem Durchschnitt – obwohl die zusätzlichen Anreize durch starke Regulierung fehlen. Software-Unternehmen entwickeln ihre Authentifizierungsmethoden stetig weiter und setzen – im Vergleich zu den anderen Branchen, die für die diesjährige Umfrage berücksichtigt wurden – auf Technologien mit starker Sicherheit.

Zwei Drittel der Software-Unternehmen setzen auf Zero-Trust

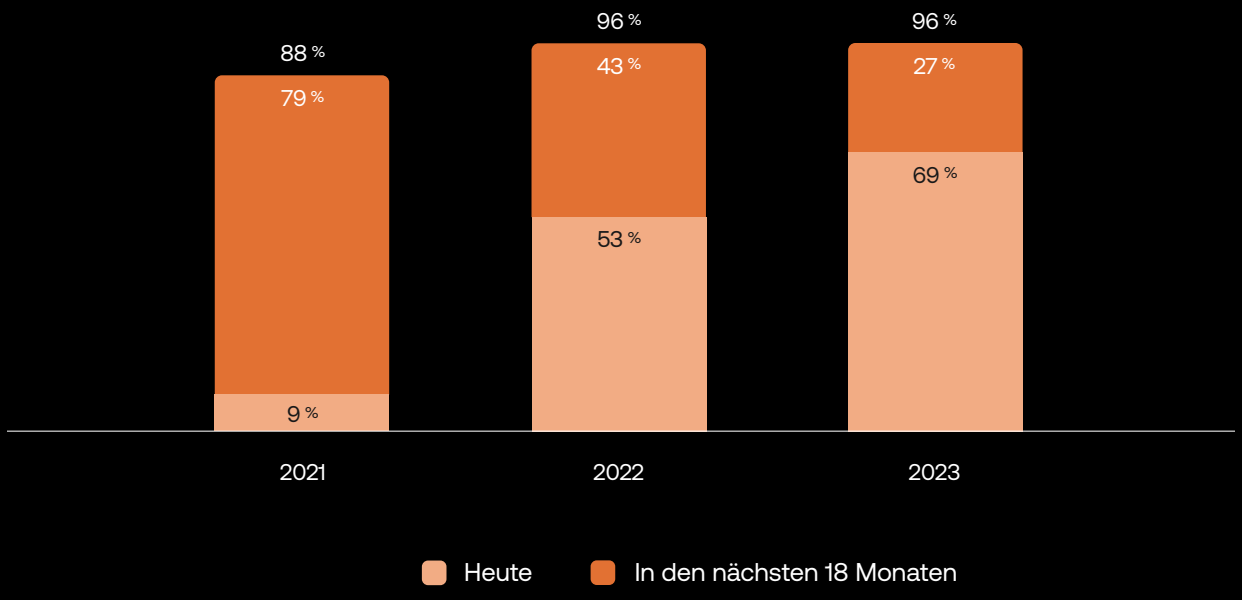
Software-Unternehmen machen bei der Zero-Trust-Umsetzung im Vergleich zu anderen Branchen Boden gut. Während im Rahmen des Reports, der 2021 erstellt wurde, noch weniger als einer von zehn befragten Softwareanbietern eine Zero-Trust-Strategie präsentieren konnte, ist nun das Gegenteil der Fall. 70 % der Befragten haben bereits Zero-Trust-Modelle eingeführt – die übrigen Anbieter planen dies für die nahe Zukunft. Nur 4 % der Befragten setzen nicht auf Zero Trust und planen auch nicht, in den nächsten 18 Monaten daran etwas zu ändern.

Software-Unternehmen überholen ihre Mitstreiter bei der Einführung von ZT-Modellen

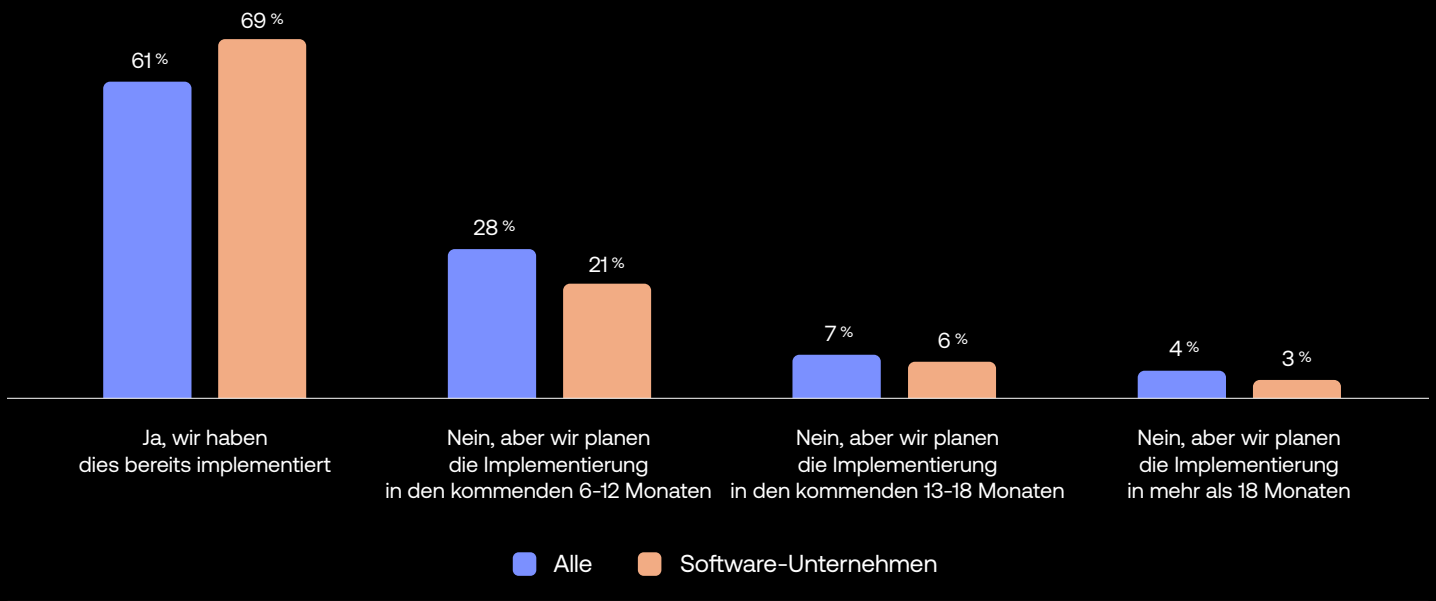
Software-Unternehmen liegen bei der Einführung konkreter Zero-Trust-Modelle über dem globalen Durchschnitt: 69 % im Vergleich zu 61 % bei allen Befragten weltweit. Die bislang unentschlossenen Unternehmen planen die Einführung einer Zero-Trust-Strategie entweder in den nächsten 6-12 Monaten (21 %), 13-18 Monaten (6 %) oder später (3 %).

Niemand weiß besser als Software-Entwickler, wie wichtig starke Identitäten für Zero Trust sind. Bezüglich der Frage, wie wichtig Identity für Zero-Trust-Modelle ist, gaben mehr als 9 von 10 Befragten an, dass Identity extrem wichtig (54 %) oder relativ wichtig (37 %) ist – weniger als 1 % schätzt Identity als unwichtig ein.

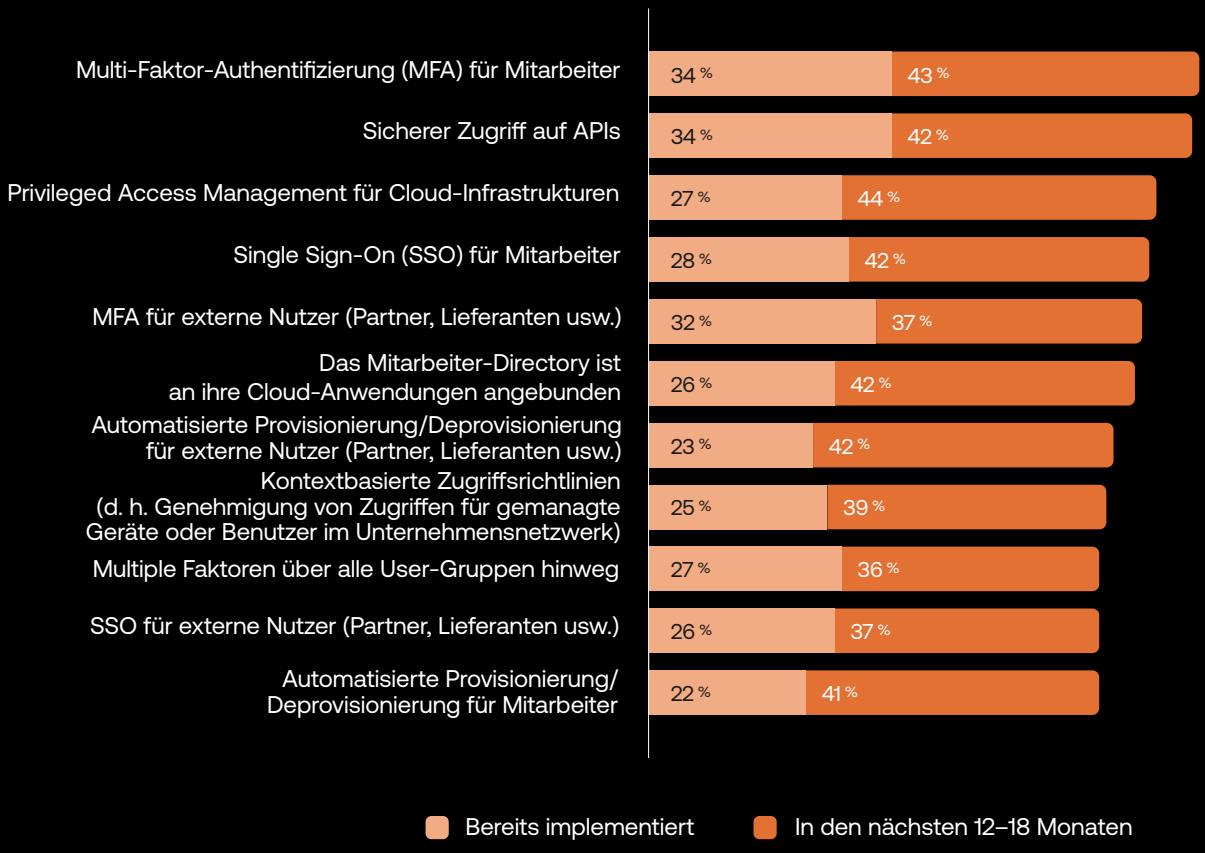
Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten 18 Monaten eines starten?
Software-Unternehmen im Jahresvergleich



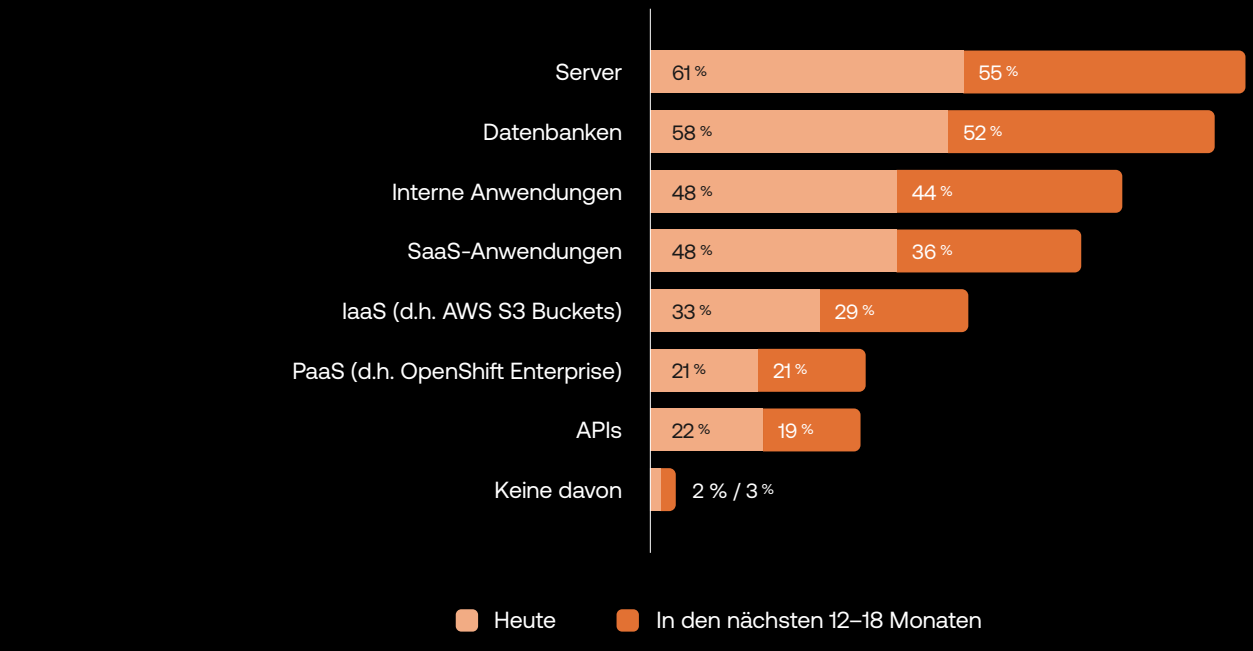
Hat Ihr Unternehmen aktuell ein konkretes Zero-Trust-Security-Programm eingeführt oder wollen Sie in den nächsten Monaten eines starten?
Softwareanbieter vs. Alle Befragten



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



Für den Zugriff auf welche Ressourcen verwenden Sie SSO und/ oder MFA, und auf welche Ressourcen möchten Sie sie innerhalb der nächsten 12-18 Monate ausweiten?
Software



Hinweis: Die Gesamtsumme der Spalten kann 100 % übersteigen, da die Befragten beide Antwortmöglichkeiten gewählt haben.

Die wichtigsten Projekte in der Software-Branche: MFA für Mitarbeitende und API-Security

Die befragten Software-Unternehmen gaben an, dass MFA für Mitarbeitende und sichere API-Zugriffe gleichsam bedeutend für sie sind. In beiden Fällen gaben 34 % der Befragten an, bereits ein entsprechendes Projekt gestartet zu haben, und für mehr als zwei von fünf Unternehmen steht bereits fest, dass sie in den nächsten 12-18 Monaten ein solches Modell – für einen oder auch beide Bereiche – einführen wollen. MFA für externe User lag an nächster Stelle: 32 % der Unternehmen gaben an, bereits ein ZT-Modell hierfür zu nutzen.

Die wichtigsten Ressourcen für den Einsatz von SSO/MFA: Server und Datenbanken

Software-Unternehmen war es in diesem Jahr besonders wichtig, ihre Server (61 %) und Datenbanken (58 %) mithilfe von Single Sign-On (SSO) und Multi-Faktor-Authentifizierung (MFA) zu schützen. Weitere 48 % der Befragten gaben an, interne Anwendungen durch SSO und/oder MFA schützen zu wollen. Derselbe Prozentsatz gab an, SaaS-Anwendungen mit SSO und/oder MFA schützen zu wollen.

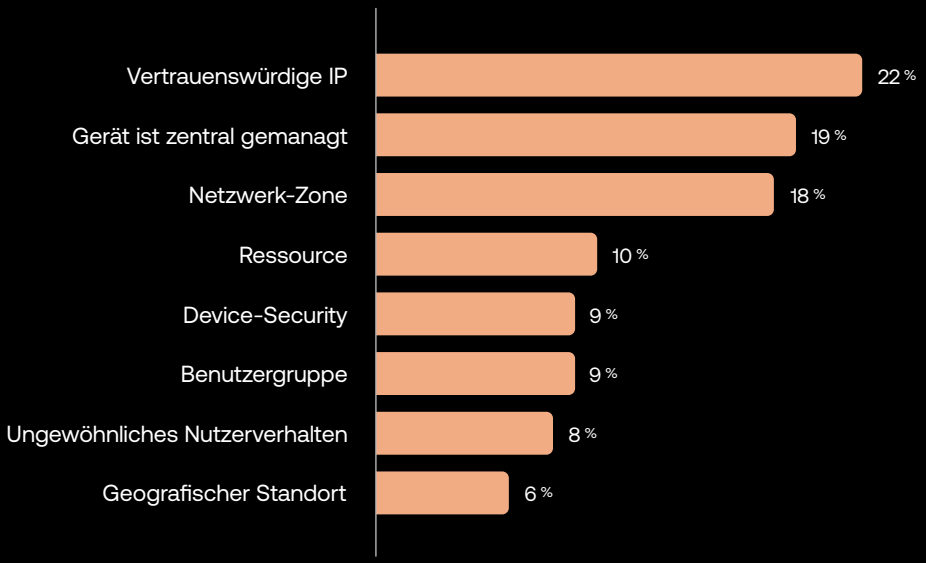
Die wichtigsten Faktoren beim Zugriff auf Ressourcen: Vertrauenswürdige IP und Device-Management

Software-Unternehmen achten bei der Kontrolle und Genehmigung des Zugriffs auf interne Ressourcen vor allem auf eine vertrauenswürdige IP (22 %). Platz zwei belegt das Device Management (19 %) und Platz drei die Netzwerk-Zone (18 %). Etwa jeder Zehnte nennt individuelle Ressourcen (z.B. kritische Systeme) als wichtigsten Faktor, während 9 % den Status der Devices oder die User-Gruppe als Schlüsselfaktor sahen. Der geografische Standort belegte in diesem Ranking den letzten Platz.

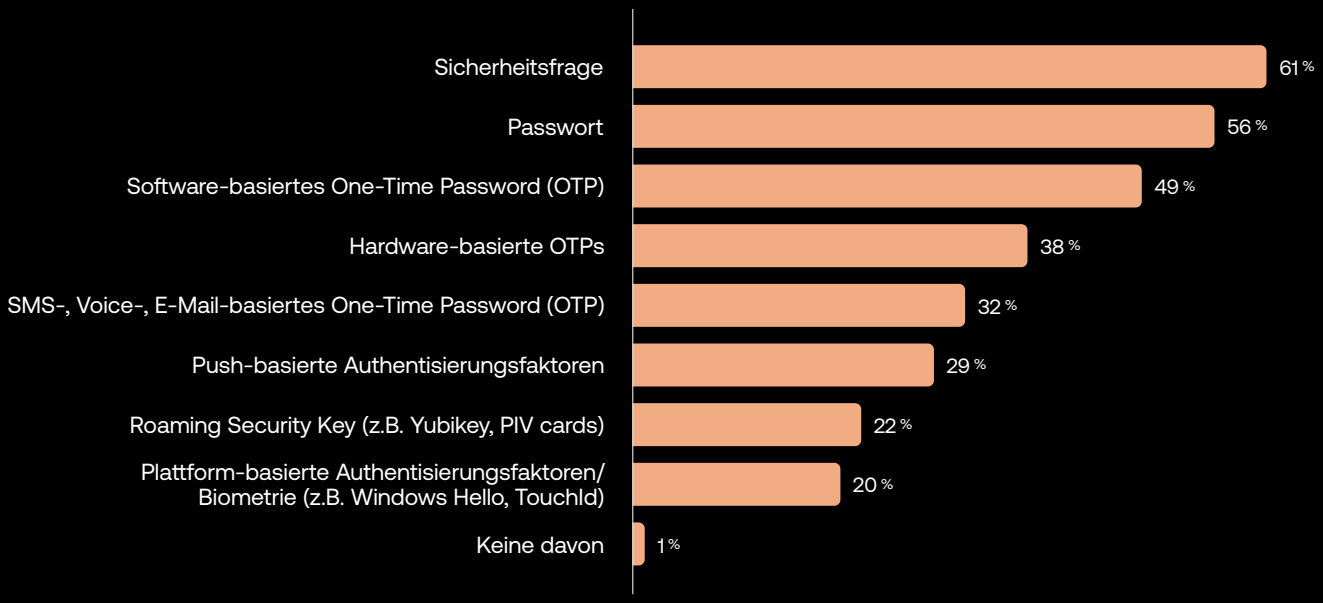
Sicherheitsfragen als die Nummer 1 unter den Authentifizierungsmethoden in der Software-Branche

Die Software-Branche ist die Einzige unter den befragten Branchen, die nicht auf riskante und unsichere Passwörter bei der Authentifizierung setzt. Passwörter rangieren mit 56 % zwar nur knapp hinter den Sicherheitsfragen, welche von 61 % der Befragten genannt wurden – aber schon die Tatsache, dass sie „nur“ Platz zwei belegen, gibt Anlass zur Hoffnung. Um es ganz klar zu sagen: Weder Passwörter noch Sicherheitsfragen bieten ein ausreichendes Maß an Schutz und sollten daher durch OTP und andere sicherere Faktoren – die sich immer größerer Beliebtheit erfreuen – abgelöst werden.

Geben Sie an, welcher Faktor für Sie bei Kontrolle und Genehmigung des Zugriffs auf interne Ressourcen ausschlaggebend ist.
Software



Welche Sicherheitsfaktoren nutzen Sie aktuell zur Verifikation interner und externer Nutzer?
Software



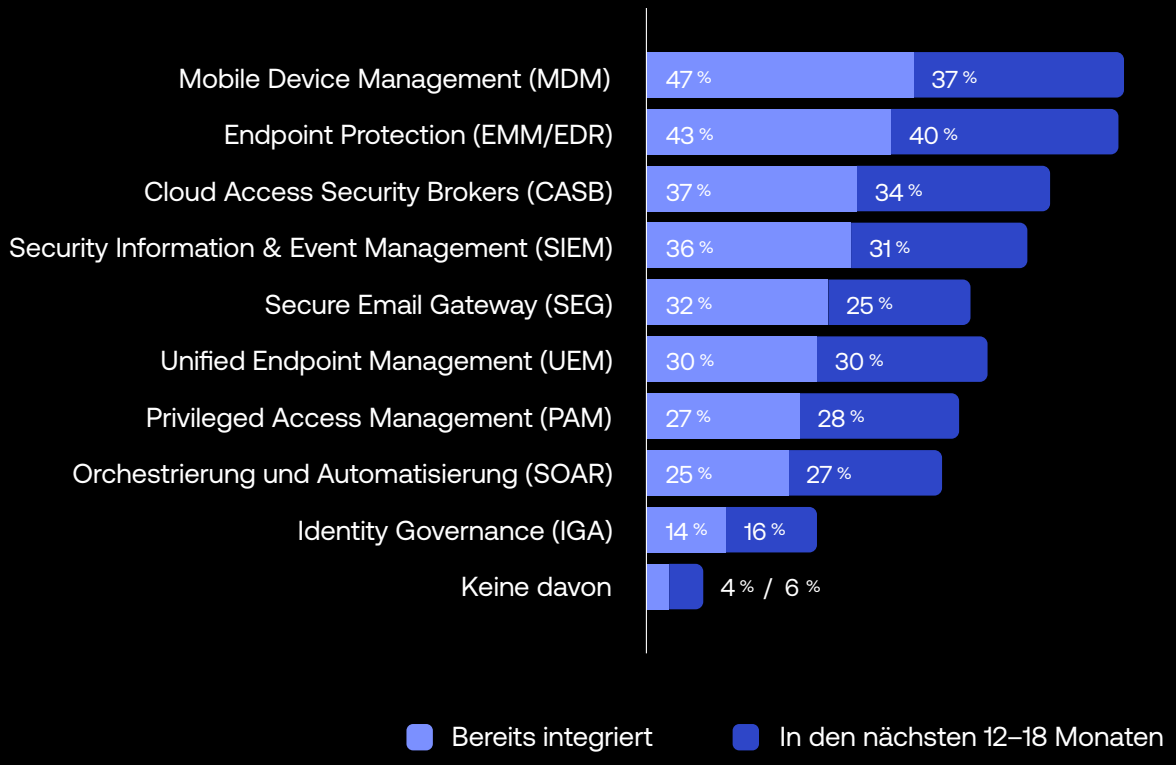
Identity-zentrierte Security

Die dynamischen Ökosysteme der Unternehmen

Wenn Identitäten der neue Security-Perimeter sind, rückt das Management der Identitäten ganz automatisch in den Fokus der Security-Strategie. Hybrid- und Multi-Cloud-Unternehmen müssen heute sicherstellen, dass ihre IAM-Lösung nahtlos mit der Security-Infrastruktur integriert ist. Nur so können ihre Security-Teams externe und interne Bedrohungen erkennen und stoppen, ohne dabei die Produktivität der Mitarbeitenden zu beeinträchtigen. Mit anderen Worten: Ein funktionierendes Zero-Trust-Ökosystem setzt voraus, dass das Identity-Management nahtlos in den Security-Stack eingebunden ist.

Wir haben Security- und IT-Verantwortliche gefragt, welche Tools sie bereits in ihre IAM-Systeme integriert haben und welche noch folgen sollen. Hier haben sich seit dem Vorjahr – in dem das Security Information & Event Management (SIEM) den ersten Platz belegte – einige Veränderungen ergeben. Platz eins bei den integrierten Systemen belegt jetzt das Mobile-Device-Management (MDM). SIEM, MDM und Endpoint Protection führen die Liste der Lösungen an, die priorisiert in das IAM integriert werden.

Welche der folgenden Lösungen haben Sie bereits in Ihre ID- und Zugangslösung integriert und bei welchen wollen Sie dies in den nächsten 12-18 Monaten tun?
Alle Befragten



Die wichtigsten Lösungsintegrationen 2023: Mobile Device Management

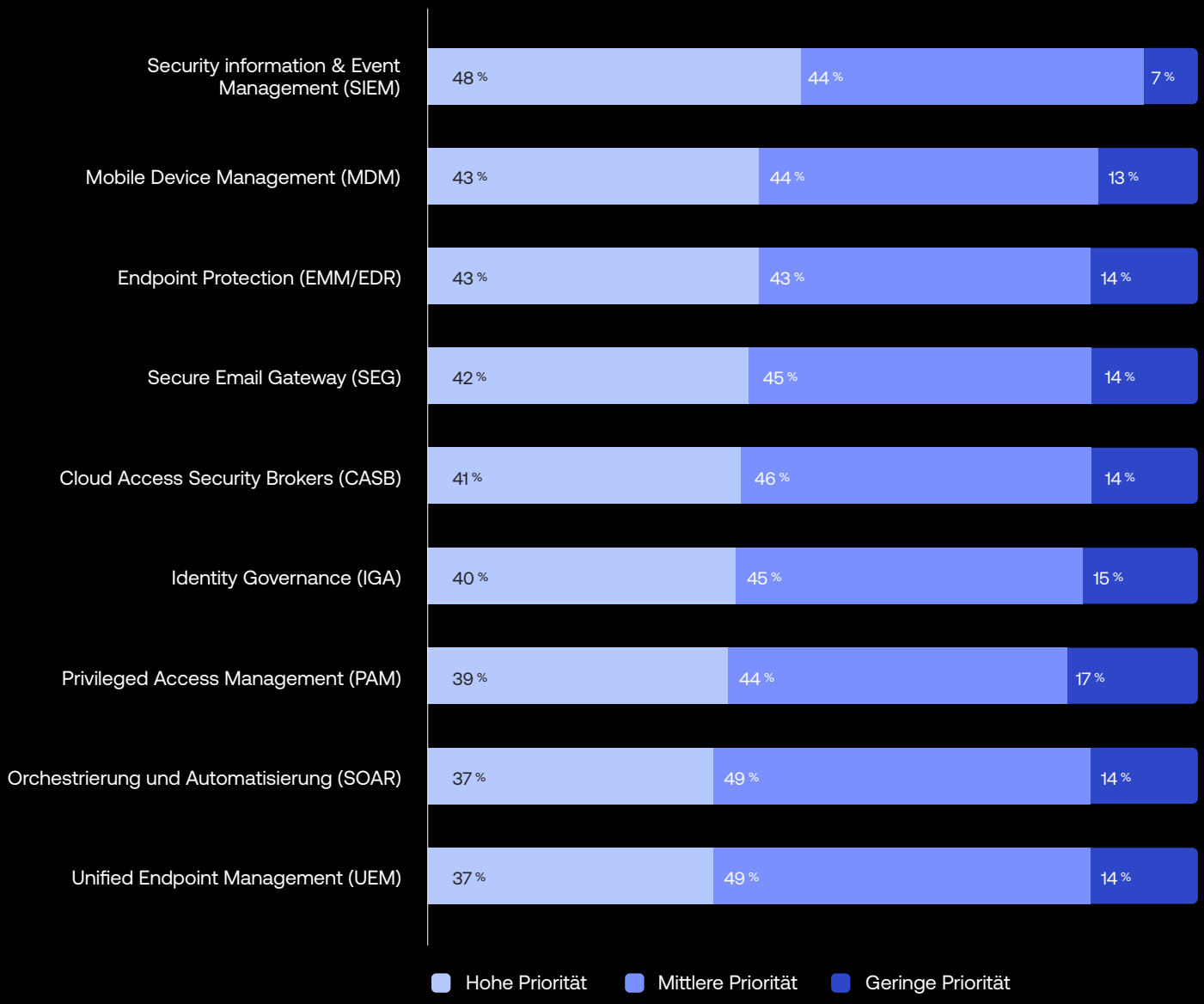
Das Mobile Device Management ist die am häufigsten in ein IAM integrierte Lösung. 2021 belegte MDM noch den siebten Platz, im letzten Jahr den vierten. Im Jahr 2021 hatten 11 % der Befragten MDM in ihrem IAM integriert, heute sind es schon 47 %. Weitere 37 % planen die Integration eines MDM in den nächsten 12-18 Monaten. Bei den künftig geplanten Integrationen liegt der Fokus auf hochwertigen Monitoring- und Security-Systeme sowie auf dem Endpoint-Management.

Die größten Bedenken nach Region:

- NAM: Mobile Device Management, CASB und Endpoint Protection
- EMEA: SIEM, Secure E-Mail Gateway und Unified Endpoint Management
- APJ: Mobile Device Management, SIEM, SOAR und Endpoint Protection

Diese IAM-Integrationen vereinfachen – wenn sie nahtlos ineinandergreifen – die Management-Prozesse und gewährleisten eine zuverlässige Zugriffskontrolle auf der Basis der geltenden Richtlinien sowie granulare Autorisierungsprozesse. Überdies erschließen sie den Unternehmen eine Reihe attraktiver Automatisierungspotenziale.

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



Auf der Wunschliste der IAM-Integrationen stehen SIEM, MDM und Endpoints ganz oben

Auf die Frage, wie sie die möglichen IAM-Integrationen priorisieren, nannten 48 % der Befragten (weltweit) SIEM als Integration mit hoher Priorität. Auf MDM und Endpoint Protection entfielen jeweils 43 %. Der Einbindung von SOAR und UEM wird mittlere Priorität eingeräumt. Immerhin wurde aber keine der Lösungen von mehr als 17 % der Befragten mit dem Label „geringe Priorität“ markiert. ■

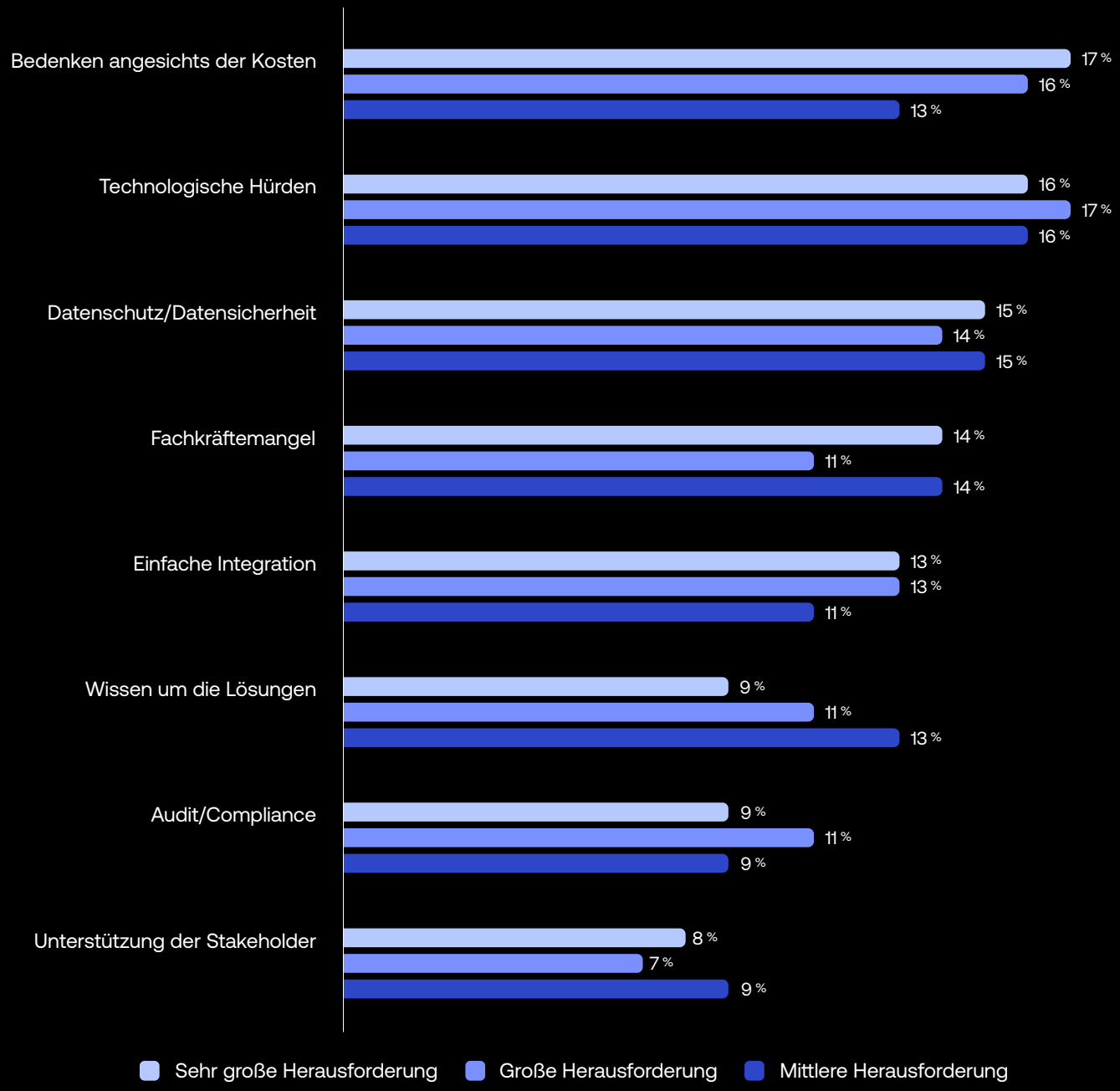
Bitte beachten Sie, dass die Werte in einer Spalte aufgrund der Rundung auf ganze Zahlen aufsummiert nicht genau 100 % ergeben müssen.

Der lange Weg zu Zero Trust

Unternehmen meistern systemische Hürden und starten geschäftskritische Zero-Trust-Projekte.

Für moderne Hybrid-/Multi-Cloud-Unternehmen führt kein Weg an Zero Trust vorbei – denn nur so werden sie in der Lage sein, die Zugriffe und die Provisionierung für ihre global verteilten Teams zu automatisieren und interne und externe Bedrohungen zu stoppen. Der Ansatz hat sich inzwischen etabliert und über nahezu alle Unternehmensgrößen, Branchen und Regionen hinweg treiben die Verantwortlichen entsprechende Projekte voran. Ohne die richtige Software, die richtigen Partner und die richtigen Prozesse ist es aber alles andere als einfach, Zero Trust umzusetzen und das volle Potenzial dieses Ansatzes zu erschließen. Die Ergebnisse der diesjährigen Umfrage legen nahe, dass Unternehmen auch heute noch mit einer Reihe von Problemen kämpfen – darunter Security-Herausforderungen, Finanzierungslücken, technologische Hürden, Fachkräftemangel und viele mehr.

Die drei größten Herausforderungen bei der Einführung von Zero Trust:



Die größten Herausforderungen dieses Jahres bei der Einführung von Zero Trust: Bedenken aufgrund der Kosten und technologische Hürden

Die Befragten nannten 2023 die Faktoren Kosten, technologische Hürden und Datenschutz/Compliance als größte Herausforderungen bei der Umsetzung von Zero-Trust-Konzepten. Der Aspekt Datenschutz/Compliance ist in diesem Jahr neu auf der Liste, die Kosten hingegen waren schon immer ein Problem. Im Jahr 2021 belegte der Kostenfaktor Platz zwei unter den größten Herausforderungen – nach dem Faktor Fachkräftemangel und vor den technologischen Hürden. Im Jahr 2022 stand der Kostenaspekt an dritter Stelle der Rangliste – hinter den Faktoren Fachkräftemangel und fehlende Akzeptanz der Stakeholder. Während der Fachkräftemangel auch in diesem Jahr ein Problem zu sein scheint, haben die Probleme bei der Einbindung der Stakeholder abgenommen. Das ist vermutlich darauf zurückzuführen, dass sich so viele Experten für den Zero-Trust-Ansatz stark machen.

Berücksichtigt man bei der diesjährigen Auswertung die Position der Befragten, stellt man fest, dass sich die Trends insgesamt verlagert haben: Für die befragten CXO's nehmen die Aspekte Datenschutz und Fachkräftemangel eine Schlüsselrolle ein. Die VPs bezeichnen die Einfachheit der Integration und den Datenschutz als problematisch, während die Bereichsleiter Compliance und eine einfache Integration als zentrale Anliegen nennen.

Der lange Weg zu Zero Trust

Was die Zukunft für Zero Trust bereithält

Der Weg zu Zero Trust ist für jedes Unternehmen einzigartig. Für Unternehmen, die eigene Modernisierungsvorhaben vorantreiben wollen und versuchen, der dynamischen Bedrohungslandschaft einen Schritt vorauszubleiben, ist die Umsetzung eines derart komplexen und strategischen Projekts oft eine erhebliche, jahrelange Herausforderung. Dennoch treiben die Unternehmen die entsprechenden Pläne trotz unsicherer wirtschaftlicher Lage kontinuierlich voran. Sie reservieren mehr Budget für Zero Trust und verbessern erfolgreich ihre Cloud-Security.

Für die erfolgreiche Umsetzung von Zero Trust ist es entscheidend, dass die Unternehmen alle Datenschutz-Vorgaben einhalten und die Produktivität ihrer Mitarbeitenden nicht beeinträchtigen. Um das Potenzial ihrer Investitionen voll auszuschöpfen, benötigen Unternehmen Lösungen, die sich einfach in den bestehenden Tech-Stack und das bestehende Ökosystem implementieren lassen. Und sie müssen alle die jahrelangen Hemmnisse – etwa mit Blick auf den Fachkräftemangel – ausräumen.

Glücklicherweise werden die Vorteile eines starken Identity-Managements immer deutlicher – und es wird immer einfacher, Stakeholder für Zero-Trust zu gewinnen. Die meisten Entscheider haben inzwischen verstanden, dass Zero Trust weit über die Security hinaus ausstrahlt. Zero Trust ist auch ein strategischer Business-Treiber, der die User-Experience für Mitarbeitende und Kunden prägt, die Zusammenarbeit in hybriden Teams vereinfacht und reibungslose und sichere Abläufe sicherstellt, mit denen Sie das Vertrauen Ihrer Kunden gewinnen.

Der Schutz des neuen Perimeters – der Identitäten – ist die vielleicht größte Herausforderung, vor der Unternehmen heute stehen. Die erfolgreiche Einführung eines Identity-basierten Zero-Trust-Modells erschließt Unternehmen eine Vielzahl von Vorteilen: Sie können das Potenzial der Cloud ausschöpfen, profitieren von einer neuen Flexibilität, können Innovationen schneller vorantreiben und stellen so die Weichen für ihre weiteres Wachstum.

Der lange Weg zu Zero Trust

Die wichtigsten Erkenntnisse im Überblick

- **Zero Trust ist kein Maßnahmenkatalog mehr – sondern Teil des täglichen Geschäfts.**

  Zero Trust lag früher in weiter Ferne, ist heute aber tägliche Realität. Die meisten Unternehmen verlassen sich auf einen Zero-Trust-Ansatz, um sicher und wettbewerbsfähig zu bleiben. Und diejenigen, die diesen Schritt noch nicht gegangen sind, haben sich die Einführung eines Zero-Trust-Modells zumindest auf die Agenda geschrieben

- **Die Identität gilt inzwischen als der Schlüssel für die Zero-Trust-Umsetzung.**

  Für die dynamischen hybriden und Multi-Cloud-Unternehmen von heute ist Identity der neue Perimeter. Ein starkes Identity-Management ist damit die Grundlage für ihren Erfolg – und das daraus resultierende Wachstum.

- **Die Zero-Trust-Budgets steigen weiter – ungeachtet aller Markt-Trends.**

  Externe Angriffe und Insider-Attacken sind auch in den unsicheren Zeiten von heute bittere Realität. Daher ist es unerlässlich, dass die Unternehmen ihre Security-Budgets erhöhen – und ihre Systeme durch robuste, Identity-basierte Security-Modelle stärken.

- **Die Einführung von Zero Trust ist nach wie vor kein Selbstläufer.**

  Die Entwicklung, Planung und Umsetzung einer Zero-Trust-Strategie ist ein komplexes Projekt und erfordert die Einbindung vieler Stakeholder. Der Weg zur erfolgreichen Einführung ist von Unternehmen zu Unternehmen verschieden – zumal es zahlreiche individuelle Herausforderungen zu meistern gilt: von der Einhaltung von Compliance-Vorgaben über technologische Hürden bis hin zu hohen Kosten.

Möchten Sie mehr über das Thema hören und erfahren, wo Sie im Okta Workforce Reifegrad-Modell stehen? Wir helfen gern.

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 dazu unter okta.com/de.

Disclaimer:

Dieses Dokument und die darin enthaltenen Empfehlungen zu Sicherheitsmaßnahmen stellen keine Rechts-, Sicherheits- und Business-Beratung dar. Dieses Dokument dient nur zu allgemeinen Informationszwecken und gibt womöglich nicht den aktuellen Stand aller relevanten Sicherheits- und Rechtsfragen wieder. Es liegt in Ihrer Verantwortung sich rechtlich, sicherheitstechnisch oder geschäftlich beraten zu lassen. Stützen Sie sich nicht allein auf die enthaltenen Empfehlungen. Okta übernimmt keine Haftung für Verluste oder Schäden, die sich potenziell aus der Umsetzung der Empfehlungen in diesem Dokument ergeben haben.

okta

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