Whitepaper

The State of Zero Trust Security 2022

Assessing identity and access management maturity in global organizations

Contents

Zero Trust Is Essential, Now

The philosophy of Zero Trust security—"never trust; always verify"—has certainly struck a chord. It took decades for organizations to move past the basic castle-and-moat security mindset, and to accept that in a cloud world, there is no perimeter to defend, and intruders are always on our networks. But today, boardrooms all over the world are embracing the security framework of Zero Trust, which has quickly evolved from quirky buzzword to strategic differentiator to business imperative. "Zero Trust is an information security model that denies access to applications and data by default," according to Forrester's 2022 definition. "...Zero Trust advocates these three core principles: All entities are untrusted by default; least privilege access is enforced; and comprehensive security monitoring is implemented." [1]

Today, Zero Trust is no longer a theoretical idea—it's an active initiative for virtually every company with a digital footprint, though many organizations still have a long way to go to truly reap the rewards of an advanced Zero Trust security architecture.

> Since the release of Okta's 2021 State of Zero Trust Security report last year, the percentage of companies with a defined Zero Trust initiative already underway more than doubled—from 24% to 55%.

Okta started issuing this State of Zero Trust Report in 2019, and many of the same challenges that dramatically accelerated the adoption of Zero Trust then are still in play today. Hybrid or remote knowledge workers spend 65% less time in offices than they did before the COVID-19 pandemic and meet with their teams in person two days a week.[2] Turns out this was not just a pandemic-driven spike in remote work: It was a fundamental shift in the way global workforces operate. Similarly, gaps in identity protection, sometimes exacerbated by accelerated shifts to cloud and digital, continue to challenge organizations large and small, as threat actors take advantage of disappearing network perimeters and fast-evolving ecosystems.

---

[1] Forrester, **"The Definition of Modern Zero Trust,"** Forrester Research, Inc., January 24, 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, June 9, 2022"

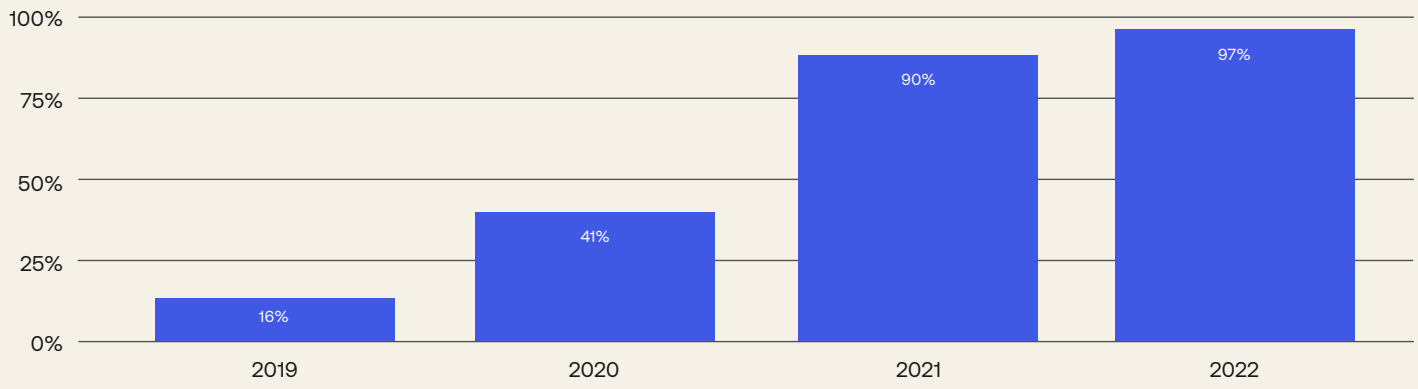
Identity is at the heart of the challenge: More than 80% of web app breaches last year resulted from credentials abuse, and stolen credentials were the No. 1 tactic used in ransomware attacks.[3]

To safeguard their systems, data, workforces, and customers in a changing world, organizations have had to quickly and dramatically alter their approach to cybersecurity, and move past legacy security solutions built for less complex times. Almost universally now, this means implementing Zero Trust. Adoption of a Zero Trust framework provides a methodology that makes it easier for organizations to continually assess their security posture and the relative maturity of their model, and pinpoint the right security solutions to accelerate their progress at every phase of their journeys.

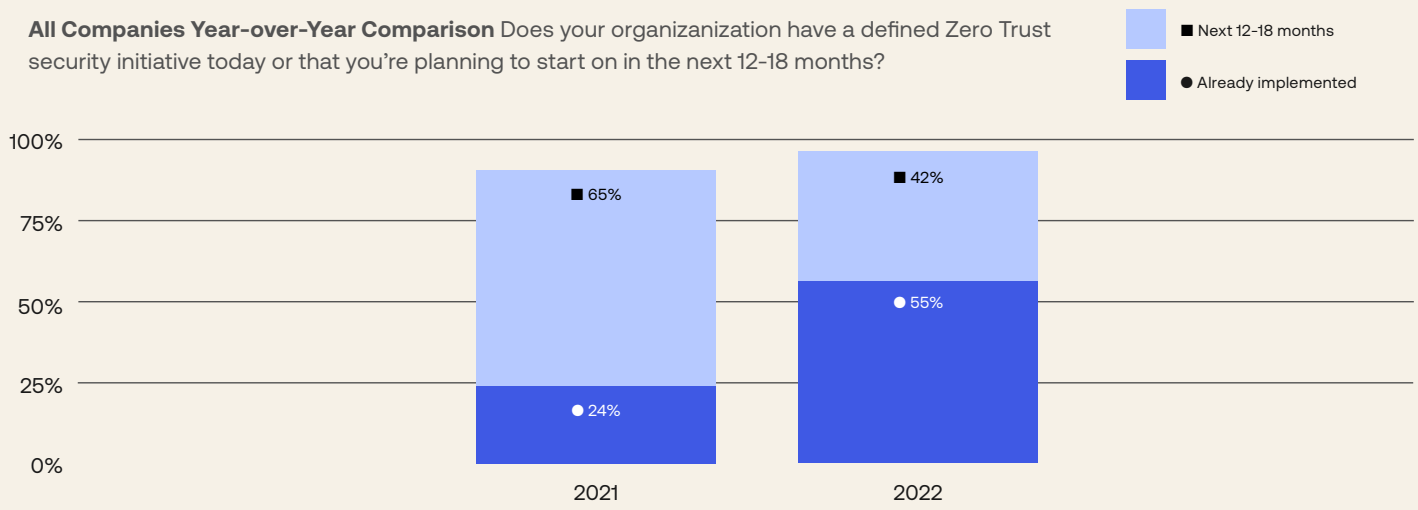
[3] Verizon, **"2022 Data Breach Investigations Report"**

> Four years ago, just 16% of companies surveyed said they either have a Zero Trust initiative in place or would have one in place in the coming 12–18 months. Today, that number is 97%.

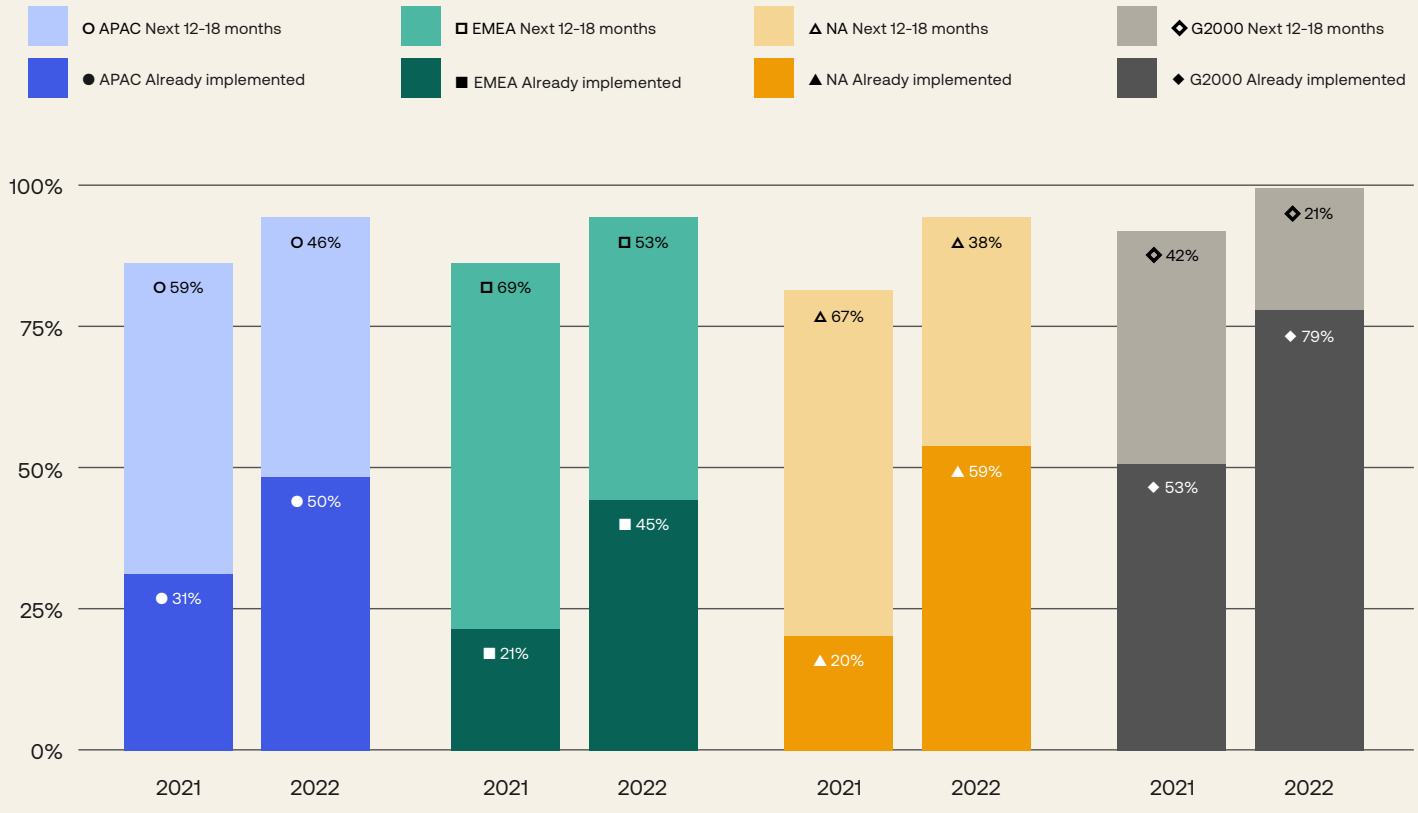
All Companies Year-over-Year Comparison Does your organizanization have a defined Zero Trust security initiative today or that you're planning to start on in the coming months?



All Companies Year-over-Year Comparison Does your organizanization have a defined Zero Trust security initiative today or that you're planning to start on in the next 12-18 months?



Year-over-Year Regional Comparison Does your organizanization have a defined Zero Trust security initiative today or that you're planning to start on in the next 12-18 months?

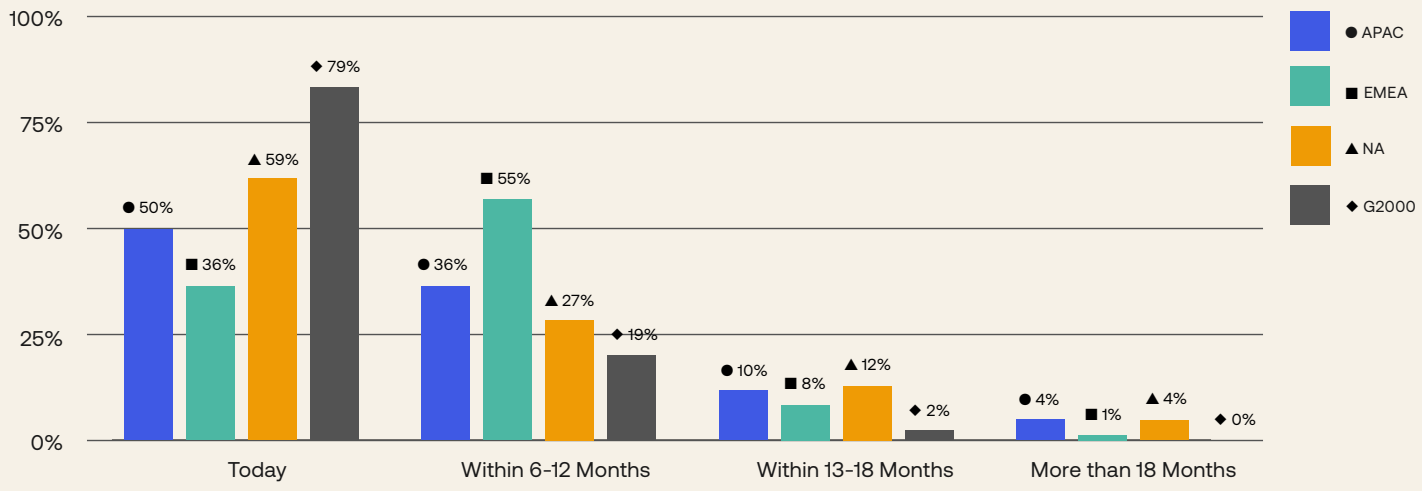


As this year's report makes clear, this mindset is essentially universal now: Nearly all organizations surveyed have either already started a Zero Trust initiative or have definitive plans to start one in the coming months. And the pressure is on to make progress quickly. As one example, in 2021 the U.S. federal government mandated, by executive order, the development of Zero Trust architecture across governmental agencies.

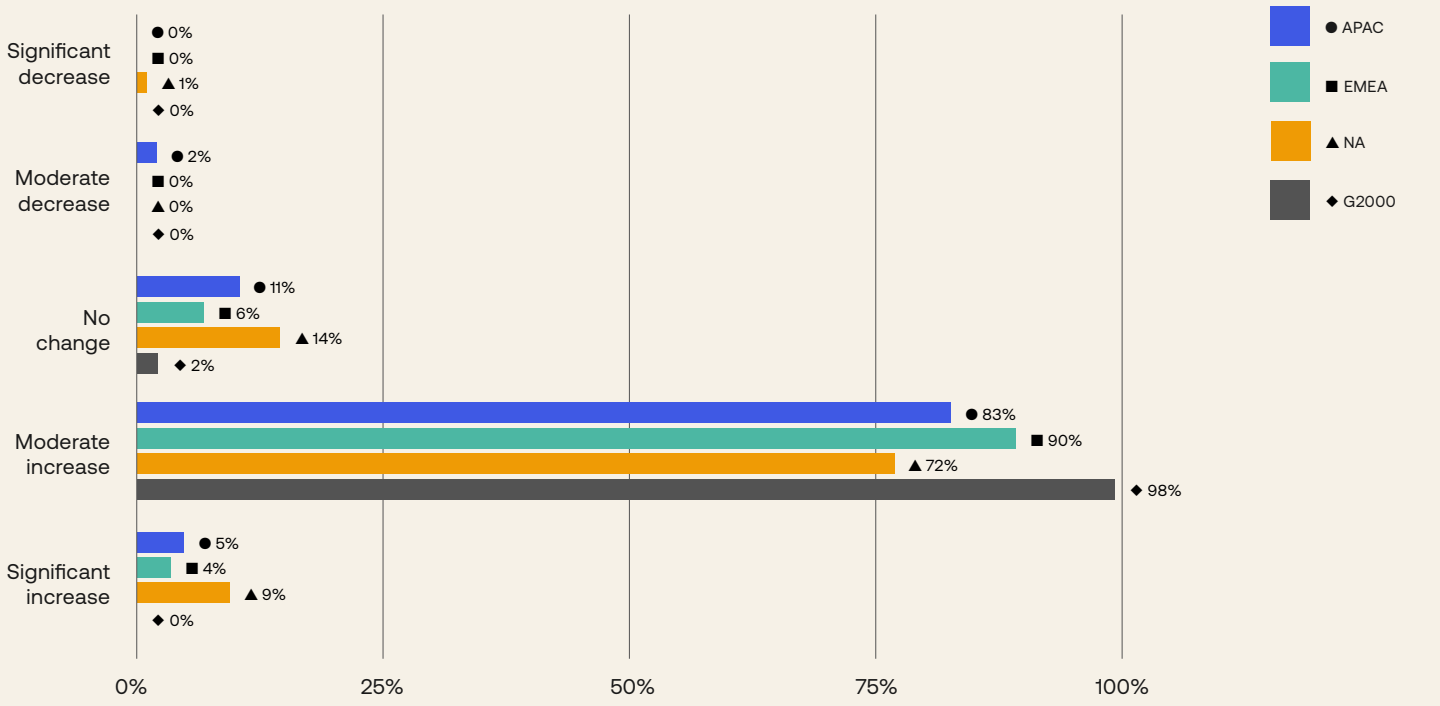
These aren't just plans: The speed at which organizations at large have been putting this philosophy into action is astounding. In 2021, 24% of organizations reported they had a Zero Trust initiative already in place; this year that number has more than doubled, to about 55%. In every region surveyed—Europe, Middle East, and Africa (EMEA); Asia-Pacific (APAC); and North America, as well as among the Global 2000 (G2000) companies—more than 85% of respondents said their organizations had allocated a moderate or, in some cases, a significant year-over-year increase in budget for Zero Trust initiatives.

Our survey of organizations around the world makes it clear that Zero Trust initiatives are not limited by company size, geographic location, or industry vertical; all respondents indicated that they are advancing steadily toward a Zero Trust future. In this report, we'll demonstrate how organizations are progressing today from an identity perspective—a core tenet of Zero Trust—and we'll check in on their progress toward completing their Zero Trust journeys more generally in the months and years to come.

Regional Comparison Does your organizanization have a defined Zero Trust security initiative today or that you're planning to start on in the coming months?

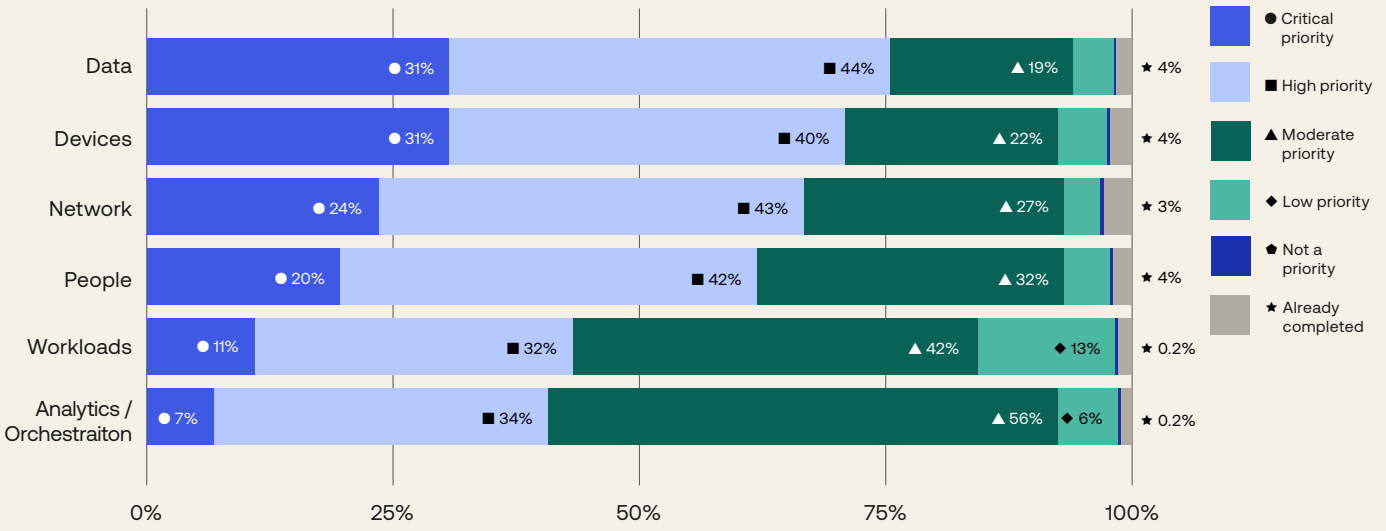


Regional Comparison How has your budget for Zero Trust changed (if at all) in the past 12 months?



For our fourth annual State of Zero Trust report, Okta surveyed 700 security leaders across the globe—more than ever before—to assess where they are on the journey toward a complete Zero Trust security posture. We asked about the specific initiatives they have in place already and how they're planning to prioritize these over the near and long term. We explored what priorities matter most today for Zero Trust initiatives, using the Zero Trust framework popularized by Forrester and the Cybersecurity and Infrastructure Security Agency (CISA). Not surprisingly, data, network, and devices categories continue to rank as the highest priorities among surveyed organizations, though we predict this may shift over time, with the People category gradually increasing in stature as organizations come to terms with an evolving security perimeter that places less emphasis on the network and more emphasis on the user. Identity is a powerful force multiplier for Zero Trust security initiatives, as we'll explore in detail later in this report.

All Companies Worldwide Rank the following Zero Trust requirements in terms of priority for your organization.



Key Takeaways

Every company forges its own path to Zero Trust, determined by industry practices and business priorities, budgets and existing infrastructure investments, and other contributing factors. But while their journeys are unique, the goal is the same: Organizations around the world have come to recognize that standing up a reliable Zero Trust infrastructure is the key to a secure, scalable future for their enterprises.

Zero Trust isn't just a buzzword anymore.

The adoption of a Zero Trust mentality for security has become the default security paradigm for organizations all over the world and the vast majority of these organizations already have initiatives in place and are actively looking for specific solutions to accelerate their journeys to Zero Trust. Security concerns are an increasingly strong motivator: Organizations have struggled to balance competing security and usability concerns for a long time, and while usability concerns have taken precedence in recent years, the scales have tipped this year and security projects on average represent a slightly higher priority for surveyed organizations.

There's no silver bullet for enterprise security.
Zero Trust is a solid guiding principle, but getting there is a complex proposition, requiring multiple deeply integrated best-of-breed solutions working seamlessly together. Every company has a different starting situation, different resources, and different priorities, leading to unique journeys to reach the same destination—true Zero Trust security.

Identity is the key to making Zero Trust a reality.
For all their differences, organizations around the world have come to realize that identity is critical for a successful security and Zero Trust strategy. Companies are working overtime to secure the new perimeter—identity—as part of their Zero Trust initiatives. And the specific identity and access management (IAM) strategies they're advancing to support those initiatives can be expressed in five distinct phases, as we detail in this report.

Identity's Role in Zero Trust

Identity: The Core of Zero Trust Solutions

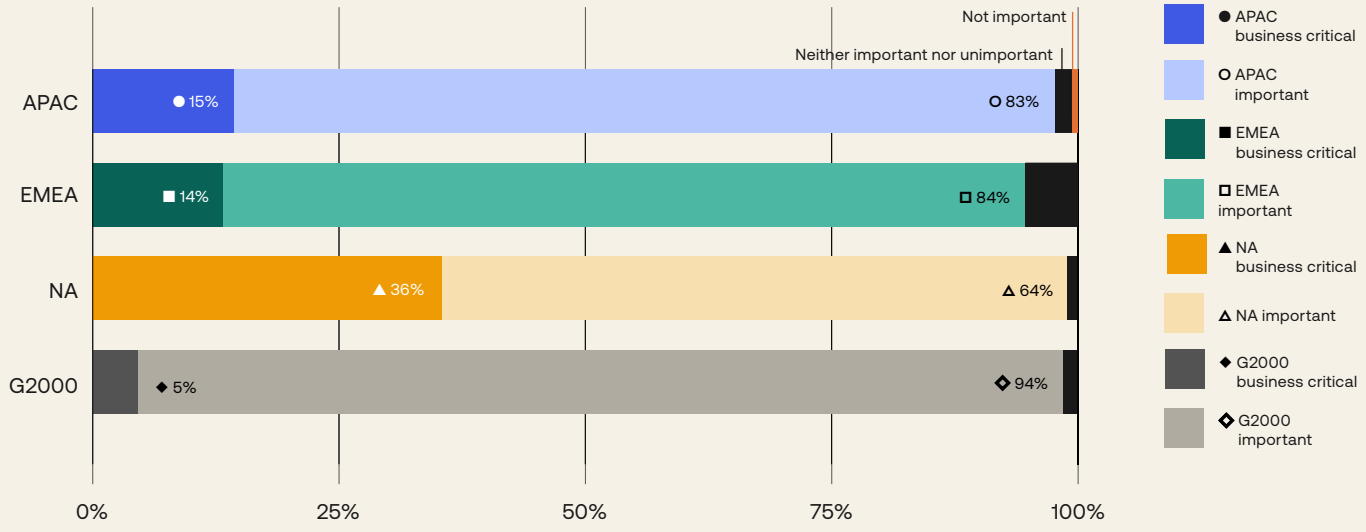
Identity isn't the only component of a comprehensive Zero Trust framework, but it's foundational to every Zero Trust strategy. Ensuring that each person always has the right level of access to the right resource at the right time has never been more important for security, management, compliance, and many other core business concerns. Each organization's Zero Trust journey is unique—different business imperatives, different existing tech stacks, different strategic priorities. But there is now a growing consensus among organizations around the world that an identity-first approach to Zero Trust lets organizations fully leverage IAM, by integrating it with other critical security solutions, into a powerful central control point for intelligently governing access among users, devices, data, and networks.

> "The days of castle-and-moat networking and perimeters are gone. Identity is the new perimeter.
>
> John McLeod, CISO, NOV Inc.

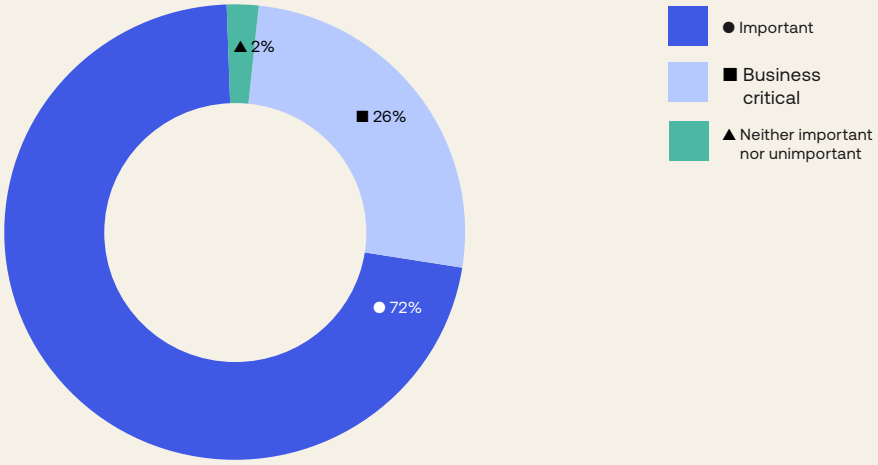
Just how important is identity? Looking at this year's survey, 80% of all organizations say identity is important to their overall Zero Trust security strategy, and an additional 19% go so far as to call identity business critical. That's a full 99% of organizations naming identity as a major factor in their Zero Trust strategy. Among chief information security officers (CISOs) and other members of the C-suite specifically, 26% deem identity business critical (among the 98% who say it's important). No wonder Gartner® recently identified "identity system defense" in its "7 Top Trends in Cybersecurity for 2022" article, noting that "Misuse of credentials is…a primary method that attackers use to access systems and achieve their goals."[4] While this has been the case for years, there has been a surprising recent increase around detection and disclosure, which has brought this to top of mind for many.

[4] Gartner®, "7 Top Trends in Cybersecurity for 2022," Susan Moore, April 13, 2022

Regional Comparison How important is identity to your overall Zero Trust security strategy?



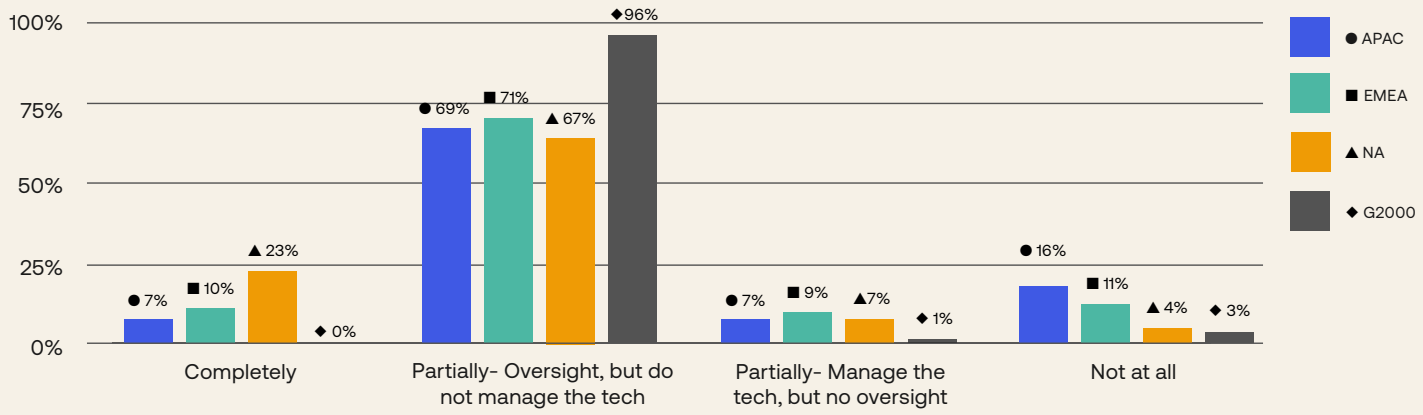
C-Level Respondents How important is identity to your overall Zero Trust security strategy?



As companies work to deploy identity solutions as part of their Zero Trust initiatives and overall security strategies, success means forging close partnerships between IT and security teams. Security has always been a team sport, but as threats grow ever more sophisticated, organizations need to create comprehensive cross-functional project plans that break down any remaining silos. This can create new issues, as we'll explain below, including the logistical challenge of bringing more and more people into alignment on identity-related decisions.

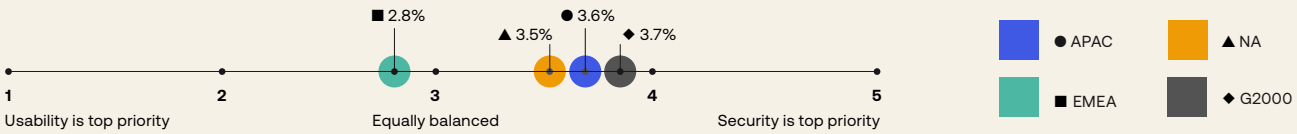
In this year's survey, we discovered that security teams are more likely to fully own IAM technologies in their security projects at Forbes Global 2000 companies than at smaller companies, although more security teams worldwide are providing at least partial oversight of IAM. In EMEA, 71% of security teams are providing at least partial oversight of the technology, which marks a slight decrease from last year's report. While in APAC and North America, the numbers are almost unchanged.

Regional Comparison To what extent does security own identity and access managementat your organization?



To stay secure but competitive today, organizations need to simultaneously make their assets available to authorized users while safeguarding them from threat actors. And finding that balance between usability and security concerns is an ongoing challenge. At the start of the COVID-19 pandemic, many organizations leaned harder into usability—they had little choice but to ensure that their newly remote workforces could easily access the tools and assets they needed to drive business results. In 2022, though, organizations began to flip the script, and a majority of them declared security to be a slightly higher priority than usability. The shift toward security is more pronounced in APAC and North America, with the EMEA region reporting a more balanced prioritization between usability and security. Why is the balance tipping in favor of security? Companies that have now firmly established remote and hybrid work practices are already leveraging pandemic-era investments in usability, and may be catching up on some security debt. But increasingly, companies are also realizing that stronger security and better usability aren't necessarily at odds anymore (consider passwordless authentication as an example). By prioritizing stronger security measures, they may gain improved usability at the same time.

Regional Comparison How do you balance the importance of security with the importance of usability at your organization?



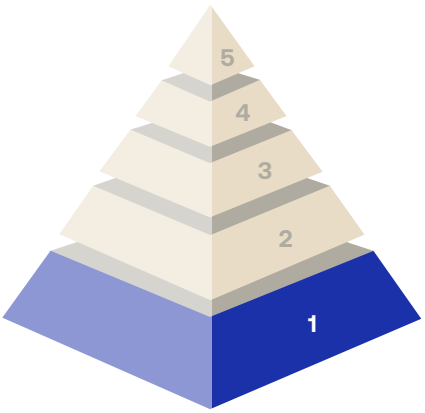
The Five Phases of Zero Trust Maturity

Organizations have fully embraced the basic philosophy of Zero Trust—and identity's crucial role within that framework—at the macro level. But are they taking action? We decided to explore some of the specific identity projects that companies are pursuing now and planning for tomorrow to support their Zero Trust initiatives, through the lens of Okta's Identity Adoption Model to Support Zero Trust Strategies. This model charts the path to Zero Trust as a five-phase journey, giving companies a way to understand how their peers are prioritizing identity projects: what they've already accomplished, what they've just begun, and which identity initiatives they plan to prioritize and focus on over the coming months.

> "Access management has become the source of trust for identity-first security.[5]"
>
> Gartner®, Magic Quadrant™ for Access Management

As organizations work to implement a leverageable Zero Trust architecture built around identity-driven security practices, we find they experience five distinct phases of maturity:

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

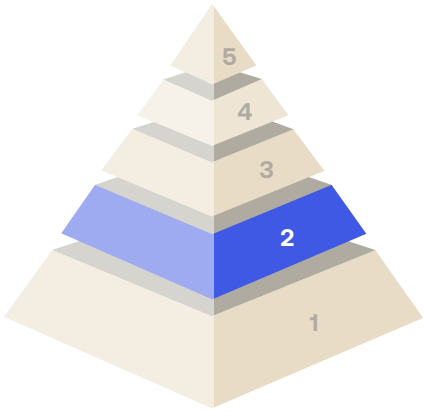


Phase 1: Traditional

Organizations at the beginning of their cloud transformation are either trying to anticipate the challenges of cloud adoption or already experiencing them: challenges like disconnected directories, a sprawled and growing risk surface, and an increasing incidence of identity-based attacks. Phase 1 is about taking the first steps toward true Zero Trust security.

Key identity projects that map to this phase:

- Connect employee directories to business-critical cloud apps for visibility into who's accessing what no matter where they are
- Implement multi-factor authentication (MFA) for employees to provide key protection from credential thieves

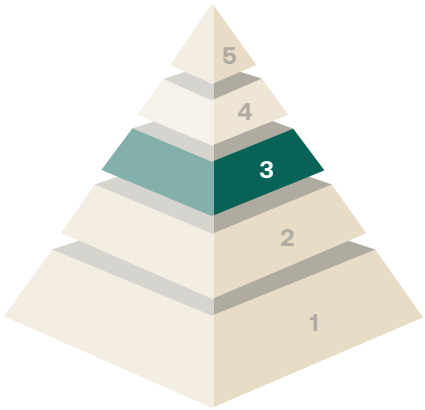


Phase 2: Emerging

In the Emerging phase, organizations are typically expanding their cloud environments and adoption, trying to lean into the efficiency and scalability of the cloud, while simultaneously trying to secure and simplify user access so their remote or hybrid workforces can stay safe and productive.

Key identity projects that map to this phase:

- Add MFA for external users, such as business partners and contractors
- Implement single sign-on (SSO) for employees for supported applications
- Enable self-service factor resets and reduce help desk costs
- Automate provisioning and deprovisioning for applications

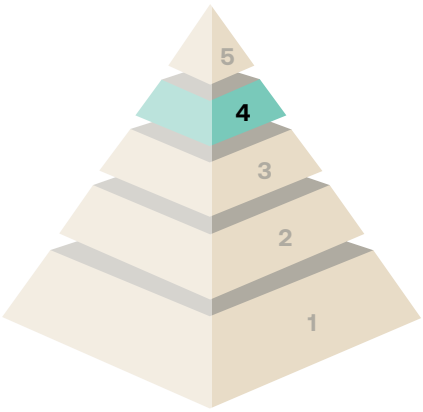


Phase 3: Maturing

In this phase, companies have developed processes and business imperatives around dynamic and remote work, and need tools to confidently extend appropriate 24/7 access to enterprise assets for a complex global workforce[5] while remaining compliant with regulatory requirements.

Key identity projects that map to this phase:

- Extend SSO to all authorized external users
- Automate provisioning and deprovisioning for employees and external users on a role-based model
- Build policy requirements around SSO support for new and existing applications
- Enable privileged access management to cloud infrastructure
- Integrate threat feeds from endpoints and cloud applications into security information and event management (SIEM) tools

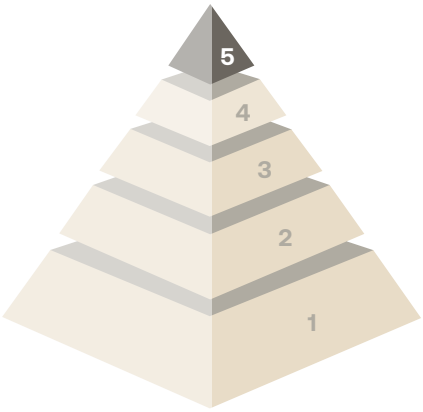


Phase 4: Elevated

Organizations in the Elevated phase are looking to consolidate their cloud wins by completing their digital transformation, by intelligently consolidating or deprecating outdated legacy tech as necessary, and by protecting key custom applications that may represent security weak points.

Key identity projects that map to this phase:

- Utilize different authentication factors across user groups based on risk and to reduce licensing costs
- Add secure access to application programming interfaces (APIs)
- Implement context-based access policies
- Deploy tools that act as a proxy to modernize legacy technologies
- Utilize security orchestration capabilities to dynamically respond to changes in the threat landscape



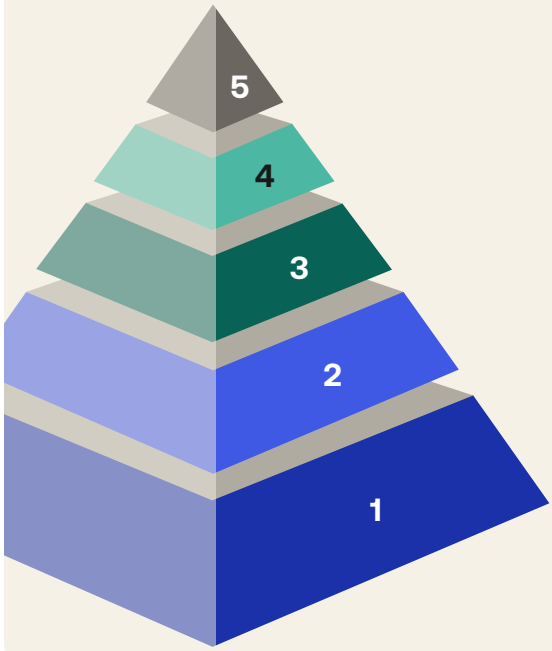
Phase 5: Evolved

Organizations in this phase have the basics of identity-first Zero Trust security in place, and can confidently leverage this real-time situational awareness to inform access decisions, and change existing decisions based on continuously updating information. They're able to focus on further refinements on an ongoing basis: making enterprise access safer, through edge security, and easier, by extending user-friendly passwordless access to all enterprise assets.

Key identity projects that map to this phase:

- Deploy secure passwordless access across the board
- Make access decisions at the data layer based on user and device posture position

Identity Adoption Model for Zero Trust Initiatives The five stages of Identity Adoption



Stage 1 - Traditional Model Early in the journey thinking about the role that identity plays in security strategies

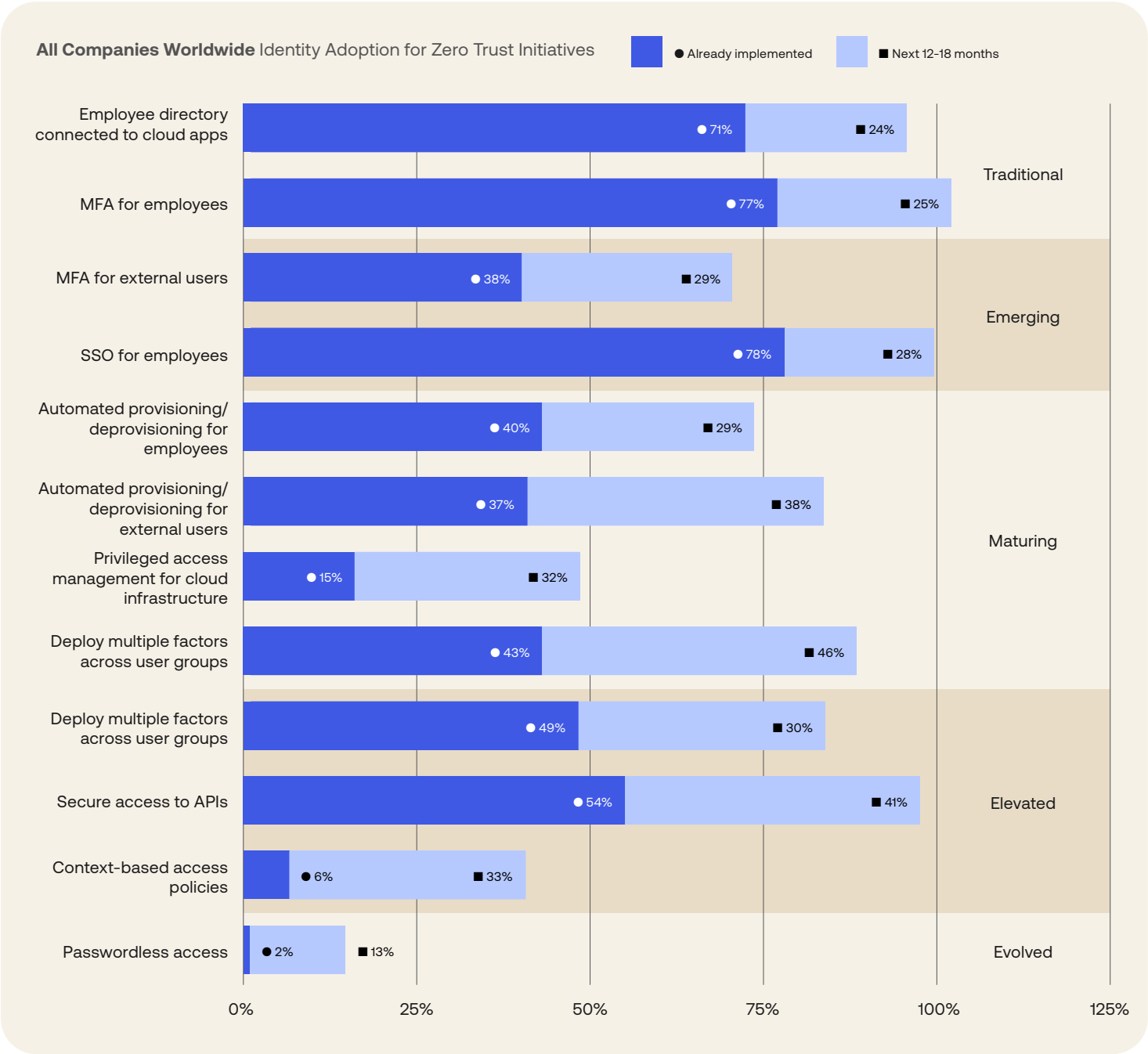
Stage 2 - Emerging Model Focused on streamlining user experience with security controls in place for cloud based applications

Stage 3 - Maturing Model Considers identity as a cornerstone element for security policies and user experience

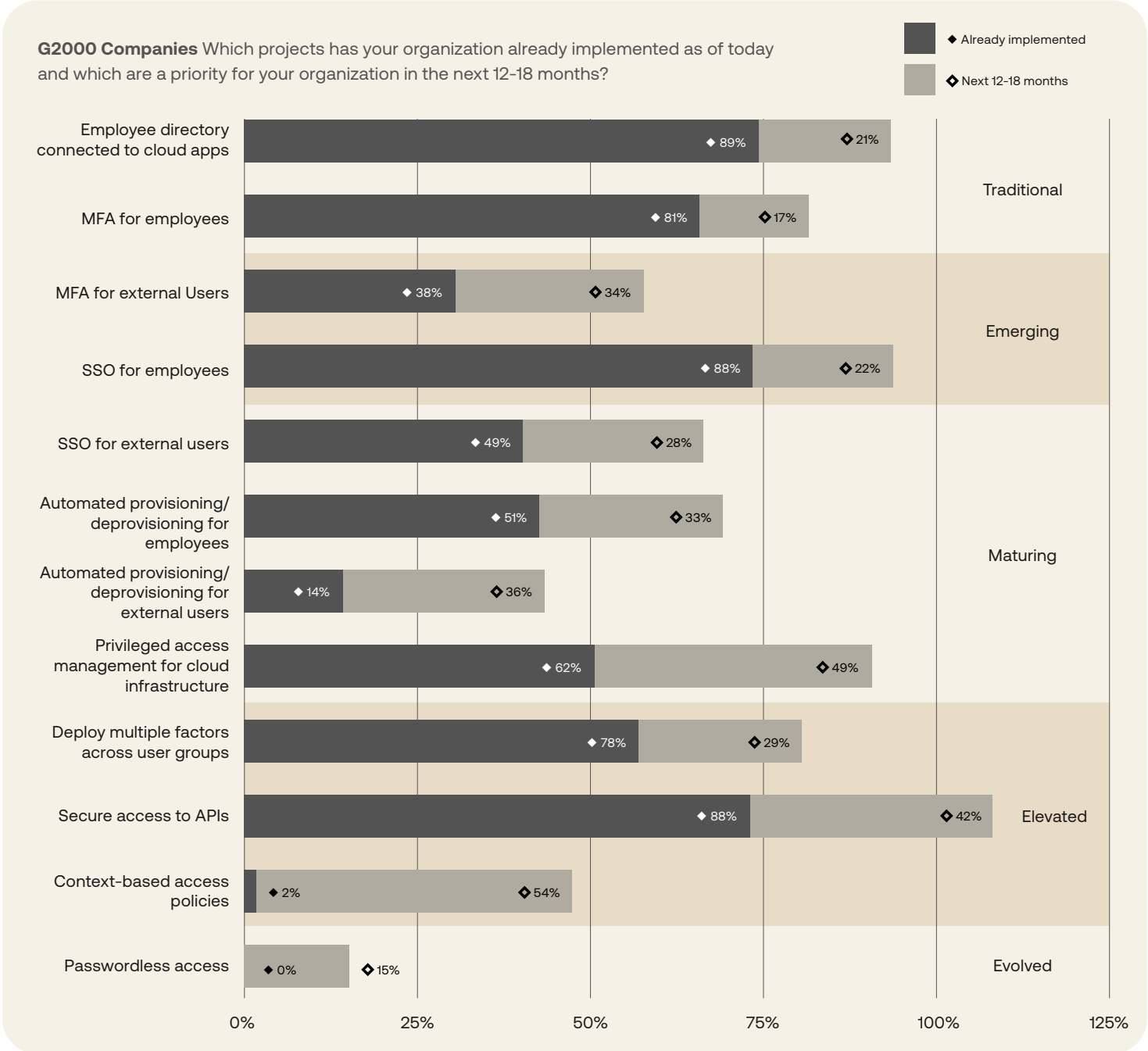
Stage 4 - Elevated Model Expanding protections to legacy technology and consolidating identity and security strategies

Stage 5 - Evolved Model Identity is integrated into a modern security practice supporting digital transformation and embracing the concept of least privileged access

When it comes to Zero Trust, companies are putting their money where their mouths are: The vast majority of organizations have at least begun their journeys to Zero Trust security, starting with critical identity initiatives. Our survey reveals that more than 70% of respondents worldwide have already advanced past Phase 1 (Traditional). A whopping 95% of respondents plan to complete the projects in Phase 1 over the next 12-18 months, and are firmly working on identity projects further along the maturity curve. When it comes to Phase 2 (Emerging) initiatives, the majority of respondents (nearly 80%) have extended SSO for their employees, but just 38% of respondents said their companies have extended MFA to external users, ensuring secure access to critical resources for authorized contractors, suppliers, and business partners. Zero Trust progress diverges after Phase 2, as detailed below, but nearly 50% of all respondents worldwide have completed multiple identity projects further along the maturity curve, and a large percentage of the remaining respondents plan to tackle these additional projects in the coming months.


All Companies Worldwide Identity Adoption for Zero Trust Initiatives
Already implemented
Next 12-18 months
Employee directory connected to cloud apps
71%
24%
MFA for employees
77%
25%
MFA for external users
38%
29%
SSO for employees
78%
28%
Automated provisioning/ deprovisioning for employees
40%
29%
Automated provisioning/ deprovisioning for external users
37%
38%
Privileged access management for cloud infrastructure
15%
32%
Deploy multiple factors across user groups
43%
46%
Deploy multiple factors across user groups
49%
30%
Secure access to APIs
54%
41%
Context-based access policies
6%
33%
Passwordless access
2%
13%
Traditional
Emerging
Maturing
Elevated
Evolved
0%
25%
50%
75%
100%
125%

Turning to the Forbes Global 2000 companies as a group, nearly 100% of these respondents plan to complete all Phase 1 identity projects within the next 18 months (if they haven't already done so). And at least half of the respondents from these companies plan to have completed all the projects in Phases 1-4, and to have begun working on Phase 5 projects, in that same time span.

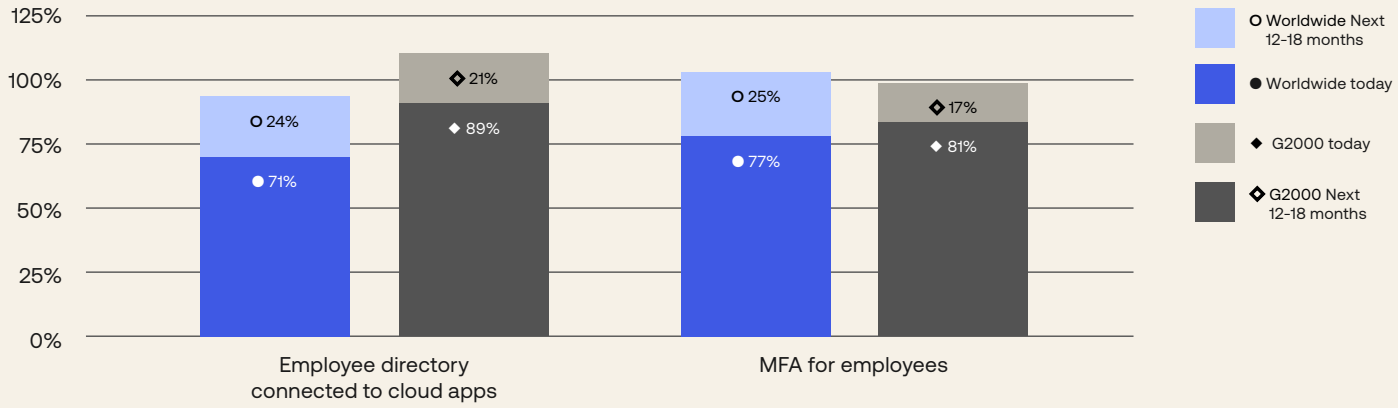


Phase 1: Traditional

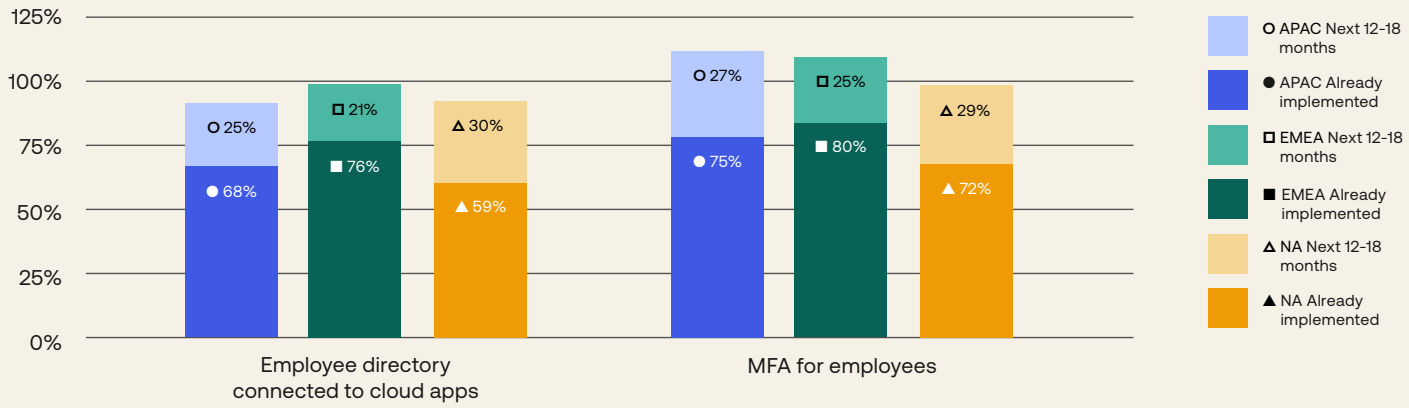
At the beginning of a Zero Trust journey, organizations face basic identity challenges like disconnected directories, a sprawling risk surface, and an endless onslaught of identity-based attacks. To measure progress in this phase of the maturity curve, we asked organizations whether their employee directories were connected to their cloud apps and if they had implemented MFA for their employees. We discovered that even in Phase 1, organizations are finding effective ways to give the right people access to the right resources by adding multiple layers of security to their authentication processes.

Our report shows that within the next 18 months, nearly 100% of respondents in companies worldwide and in Global 2000 companies plan to complete the identity projects in Phase 1. Extending MFA for employees is the most adopted identity project across the board, and within the next 18 months, 100% of respondents from all regions plan to have adopted MFA for employees as part of their overall identity strategy. Fewer respondents have indicated their company's directory is already connected to cloud apps, but many may still be in the process of cloud migration; they generally plan to advance toward completion of this identity project within the next 18 months.

Phase 1 at All Companies Worldwide and Global 2000 Companies Which projects has your organization already implemented as of today, and which are a priority for your organization in the next 12-18 months?



Phase 1 Regional Comparison Which projects has your organization already implemented as of today, and which are a priority for your organization in the next 12-18 months?

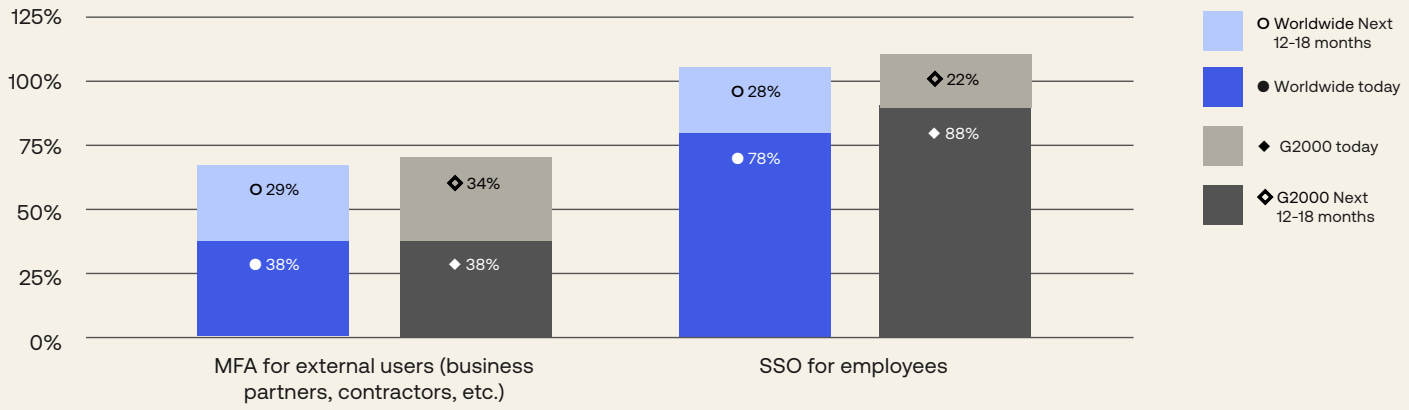


Phase 2: Emerging

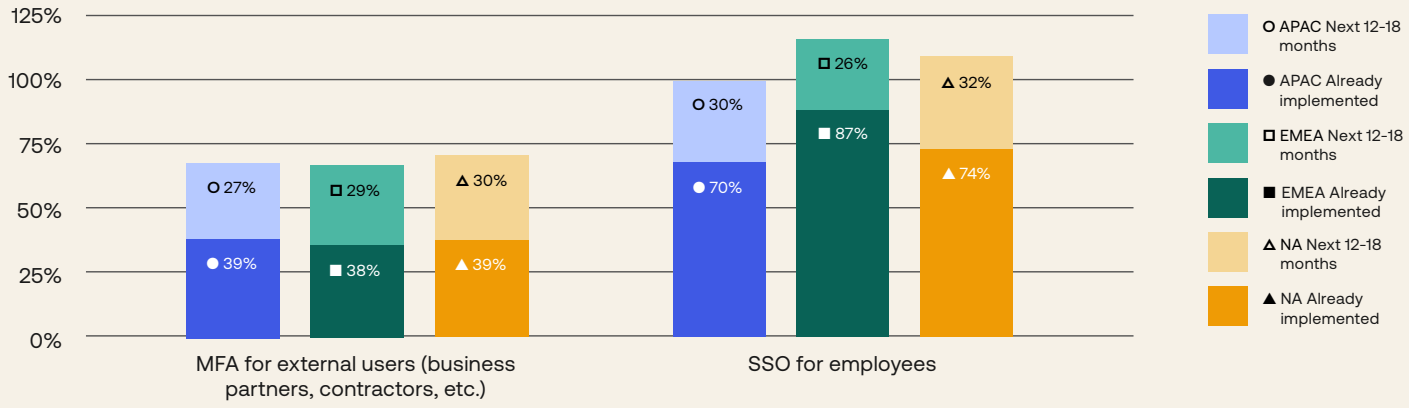
In the Emerging phase, organizations are typically attempting to correlate activity across disparate systems, resulting from changes like increased adoption of cloud apps and/or from mergers and acquisitions activity, that create a greater need to simplify user access. To evaluate progress in Phase 2, we asked respondents whether their organizations have yet to deploy MFA for external users, including their business partners and contractors, and if they've added SSO for employees to make it easier for them to access the tools they need to be productive.

According to our data, more than half of respondents from each region plan to complete the projects in Phase 2 within the next 12-18 months (if they haven't already). More and more companies are relying on not just remote employees, but on contractors, volunteers, suppliers, and other non-full-time employee partners. These individuals represent a growing security threat for organizations, and extending MFA to these external users is a major focus for all regions to help keep resources accessible yet safe. The numbers for MFA for external users are virtually identical for companies of all sizes, while SSO for employees is more likely to be in place at Global 2000 companies than at smaller companies (88% versus 78%).

Phase 2 at All Companies Worldwide and Global 2000 Companies Which projects has your organization already implemented as of today, and which are a priority for your organization in the next 12-18 months?



Phase 2 Regional Comparison Which projects has your organization already implemented as of today, and which are a priority for your organization in the next 12-18 months?



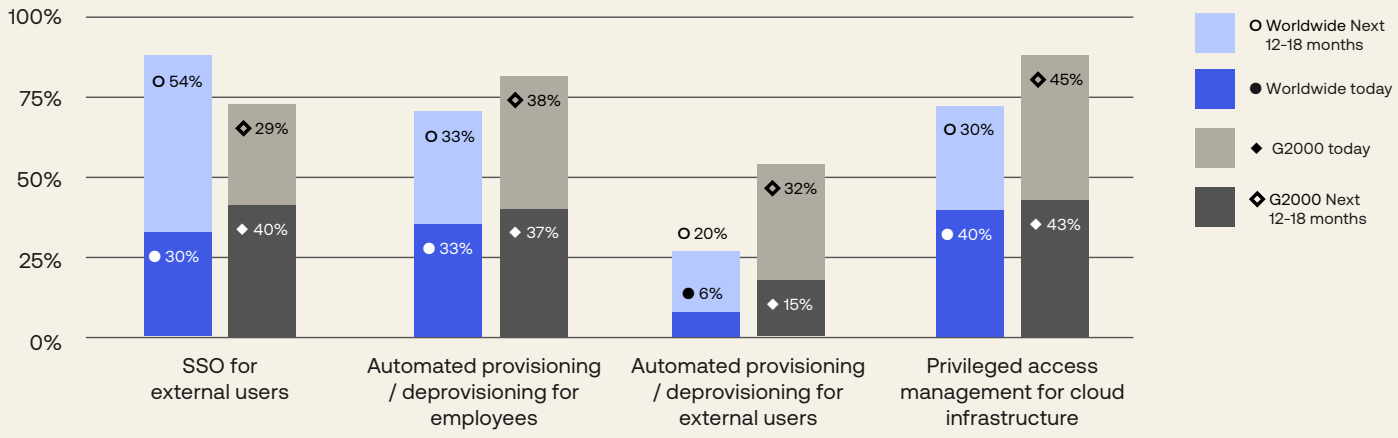
Phase 3: Maturing

Maturing organizations have complex challenges like increased compliance and regulatory requirements, a hybrid infrastructure, and the need to support a large, busy, dynamic, and partly or mostly remote workforce. Meeting these challenges means extending and expanding their IAM efforts beyond their employees and legacy network to accommodate a growing world of external users and an expanding cloud or multi-cloud infrastructure.

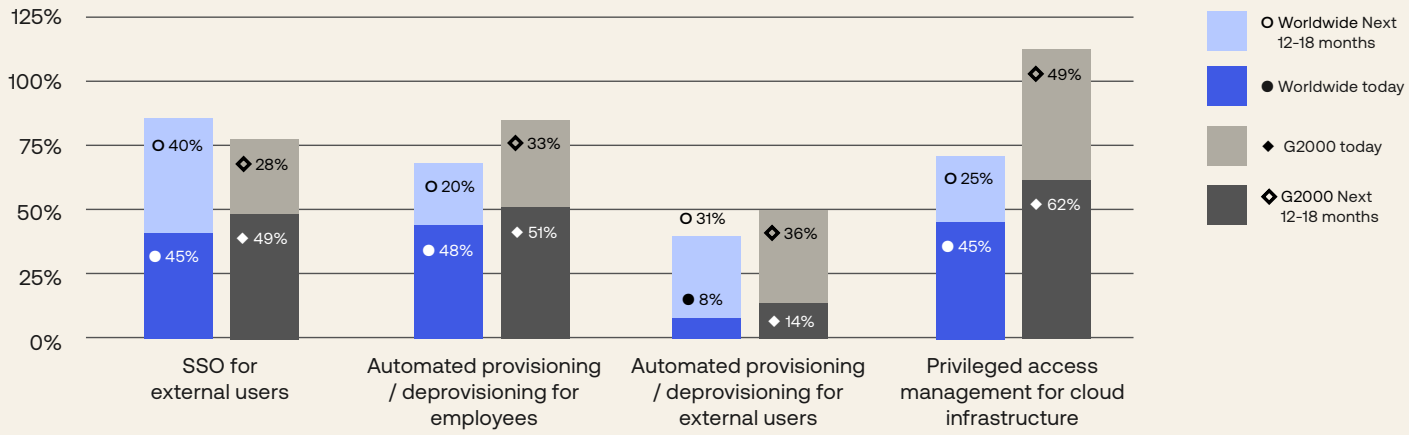
To evaluate progress in Phase 3, we asked respondents if they had yet automated provisioning and deprovisioning, both for employees and for external users, and whether they supplied privileged access management for their cloud infrastructure.

Fewer companies have reached this phase, but nearly half of respondents from companies worldwide and in Global 2000 companies plan to complete the Phase 3 initiatives by the end of 2023. Companies in the APAC region place a relatively greater emphasis on automating the provisioning and deprovisioning of employees and on working on privileged access for cloud infrastructure over the coming 18 months, with their responses forecasting an increase from 22% to 76% adoption and from 44% to 88% adoption, respectively. As a group, North American respondents are scheduled to double adoption for privileged access to cloud infrastructure, and plan to increasingly extend SSO for external users, all within the next 12-18 months. Likewise, respondents from companies in the EMEA region plan to more than double the adoption of privileged access to cloud infrastructure, with adoption scheduled to reach 100% over the next 18 months.

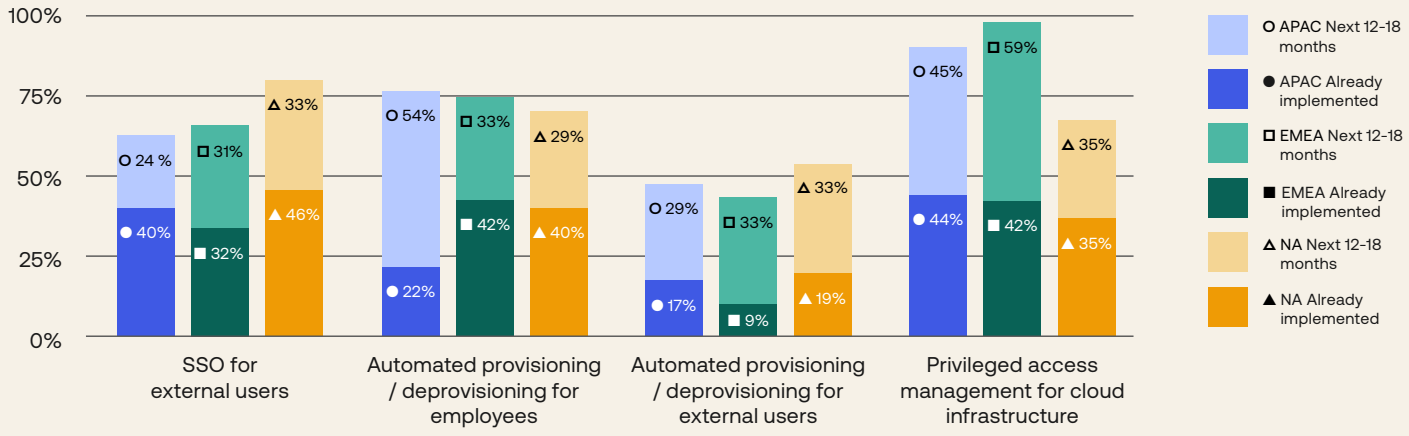
Phase 3 at All Companies Worldwide Year-over-Year Comparison Which projects has your organization already implemented as of today, and which are a priority for your organization in the next 12-18 months?



Phase 3 Global 2000 Companies Year-over-Year Comparison Which projects has your organization already implemented as of today, and which are a priority for your organization in the next 12-18 months?

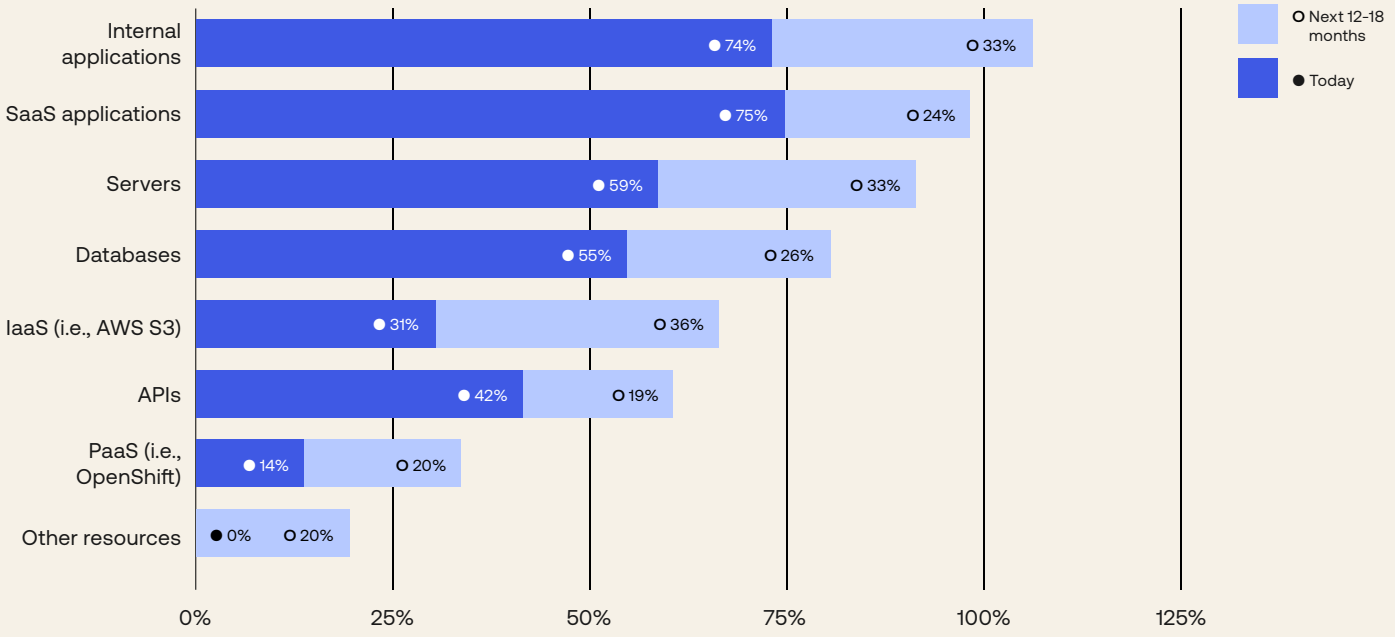


Phase 3 Regional Comparison Which projects has your organization already implemented as of today, and which are a priority for your organization in the next 12-18 months?



Extending MFA and SSO, the twin pillars of modern security and usability, to resources is well on its way toward becoming universal: Nearly 75% of all respondents worldwide say they've already extended MFA, SSO, or both to internal applications and software as a service (SaaS) apps, and at least 99% plan to do so within the next 12-18 months if they aren't already there. Extending SSO, MFA, or both to infrastructure as a service (IaaS) is set to experience a tremendous leap over the next 12-18 months, as companies around the world look to secure access to these important resources; adoption is set to more than double, from 31% to 67%, by 2023.

All Companies Worldwide Which classes of resources have you already extended SSO and/or MFA to? (Select all that apply)

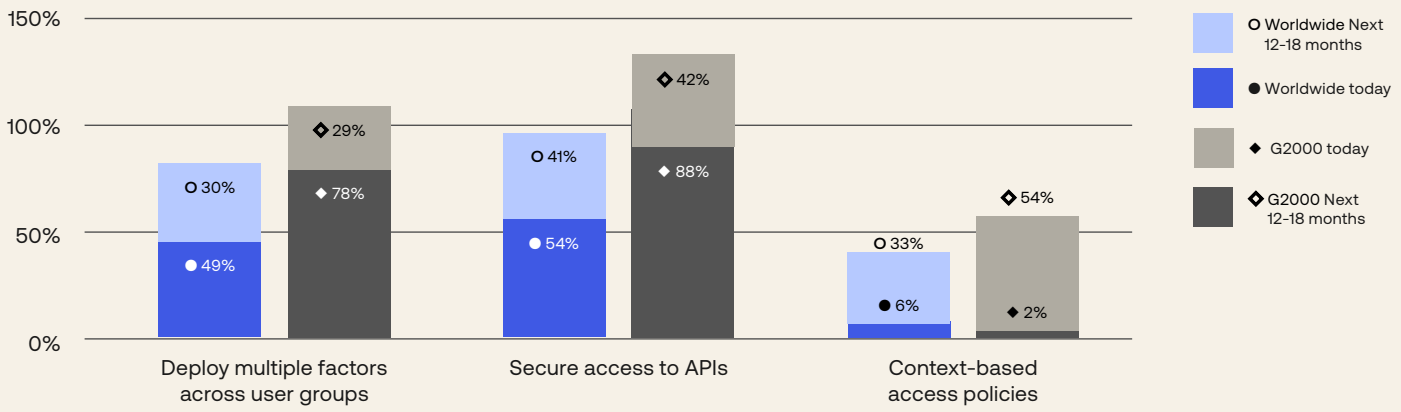


Phase 4: Elevated

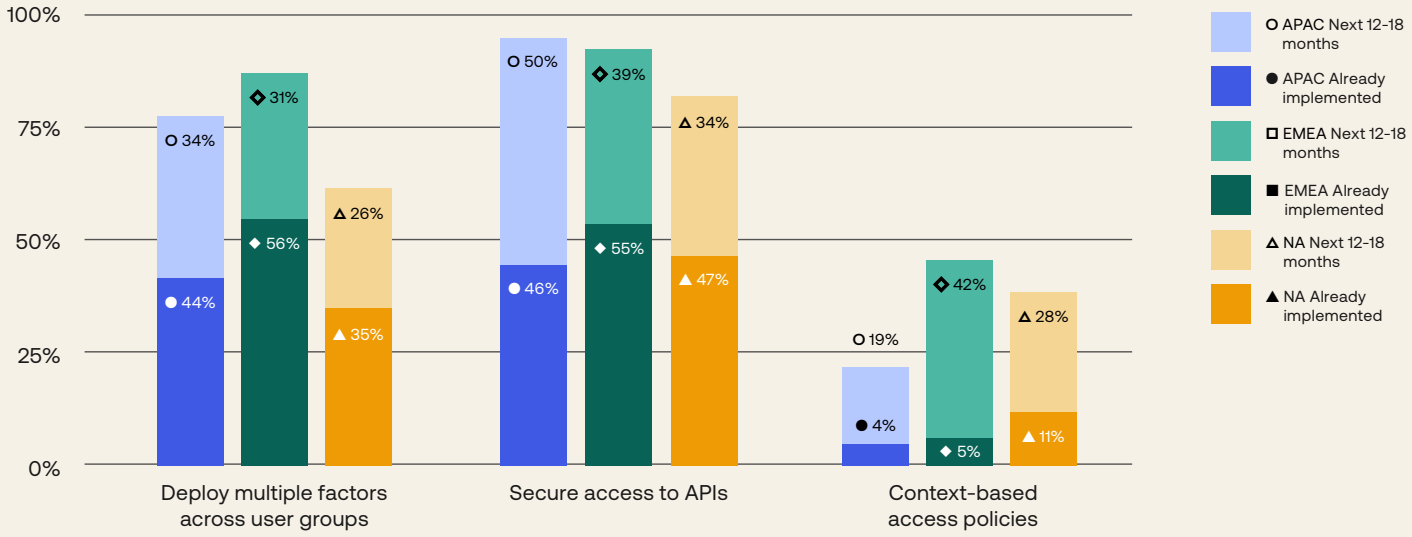
Organizations further along the maturity curve have conquered the basics of identity-based Zero Trust, and have the tools and processes in place to tackle ever more complex identity challenges. We gauged organizations' progress against the following Phase 4 initiatives: Are they set up to deploy multiple authentication factors across user groups to decrease user friction, increase remote productivity, and support "never trust, always verify" security? Have they added secure access to APIs? Have they implemented context-based access policies?

All Global 2000 companies surveyed plan to complete identity projects, including deploying multiple factors across user groups and securing access to APIs, over the next 12-18 months. At least half of these companies plan to have completed all identity projects in Phase 4 during that same time frame, with an emphasis on context-based access policies like how well a device is trusted at the time the user is trying to gain access, the location of the access attempt, the user and/or resource itself, and other critical inputs. Respondents from organizations in North America currently lag behind their counterparts in APAC and EMEA with regard to plans to deploy multiple factors across users and to secure access to APIs, but are poised to make a leap forward in the coming months.

All Companies Worldwide and Global 2000 Companies: Which projects has your organization already implemented as of today, and which are a priority for your organization in the next 12-18 months?



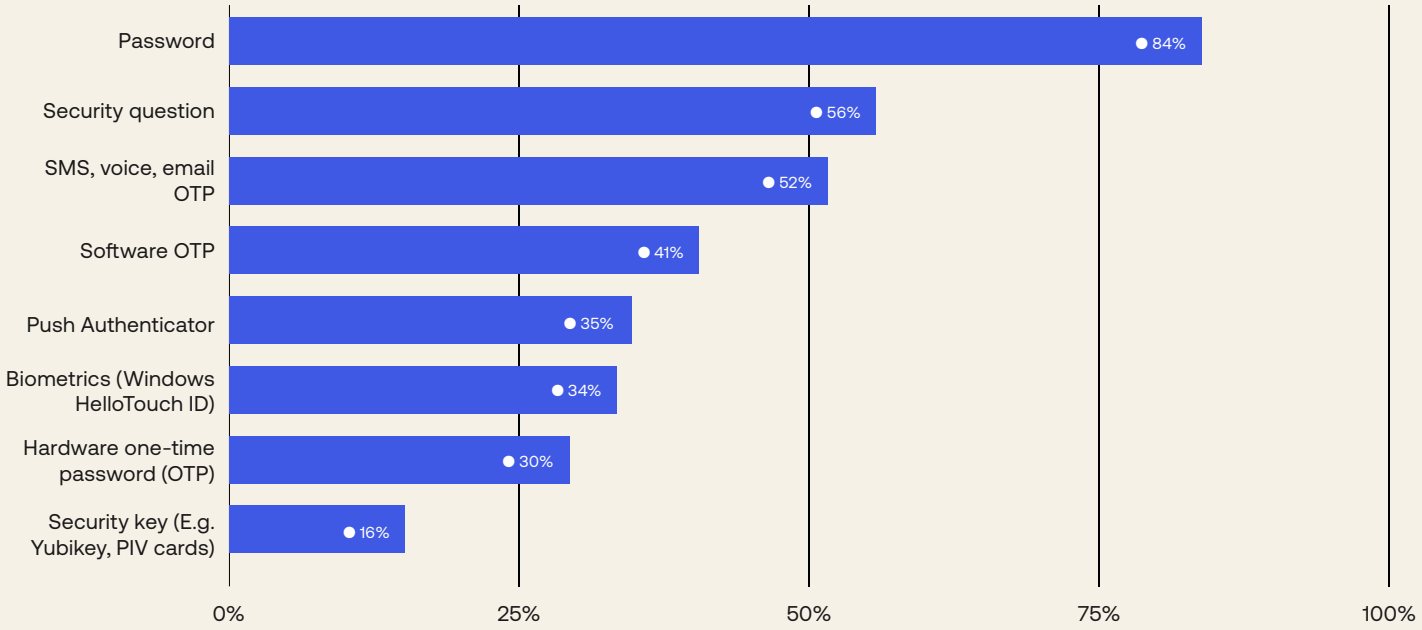
Phase 4 Regional Comparison Which projects has your organization already implemented as of today, and which are a priority for your organization in the next 12-18 months?



Unsurprisingly, passwords continue to be the most used security factor, which is an ongoing problem—an oft-cited data point is that "123456" stubbornly remains the most commonly used password.[6] On a more positive note, as pointed out in Okta's annual Businesses at Work report earlier this year, companies continue to increase their usage of MFA, and to steadily replace low-assurance factors like passwords with higher-assurance factors. The percentage of companies that still use passwords to verify internal and external users has dropped ten percentage points, to 84% this year; in the same time span, usage of the higher-assurance factor push authentication has increased more than 20 percentage points.

[6] Okta, **"Businesses at Work, 2022."**

All Companies Worldwide Select the authentication factors that your organization uses to verify internal and external users (Select all that apply)

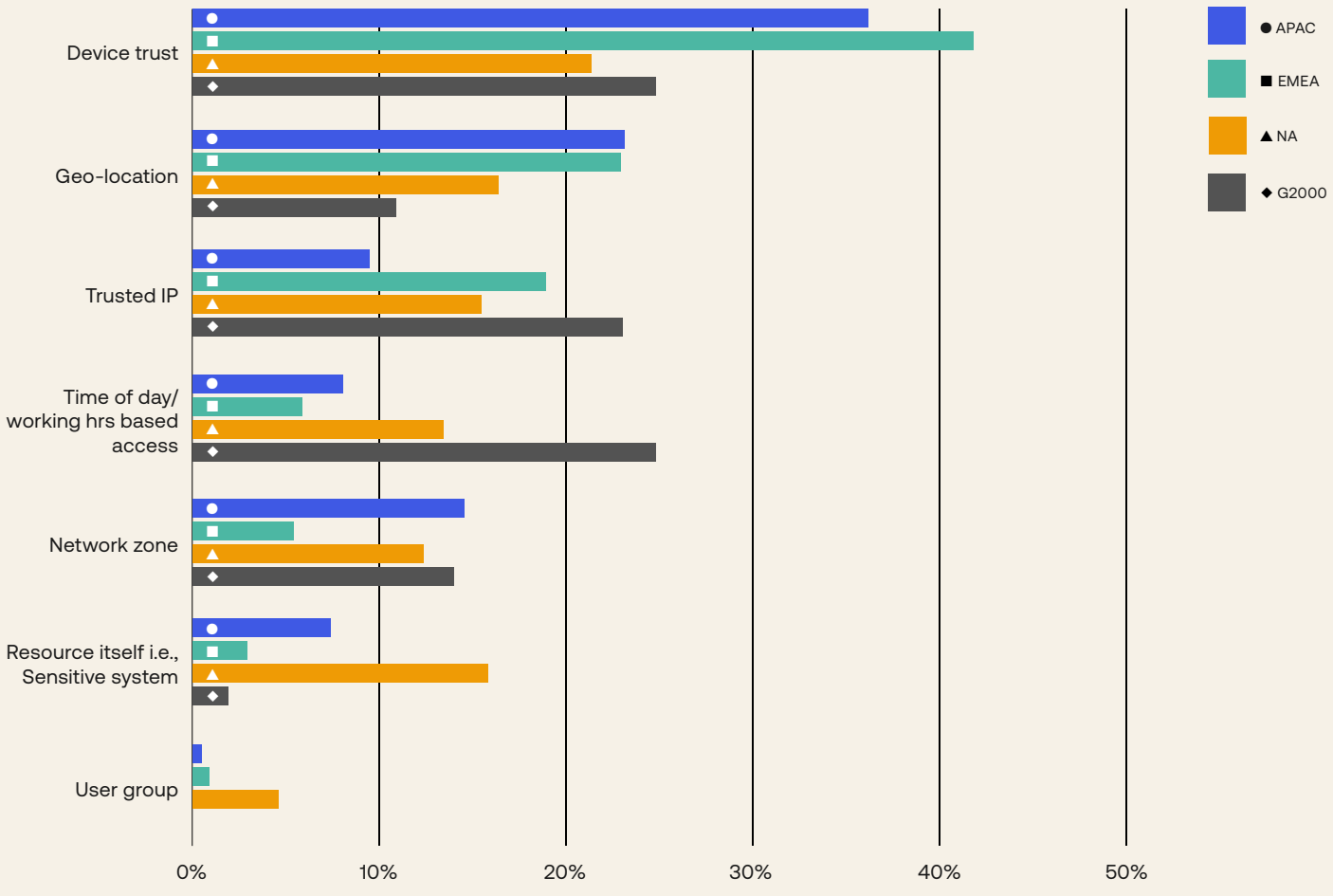


"Compromised passwords are typically the first step in the data breach kill chain. It's how an attacker gains initial access before moving laterally across the network looking to escalate privilege. Passwords alone are no longer defendable or adequate for authenticating our identities and protecting our digital assets."

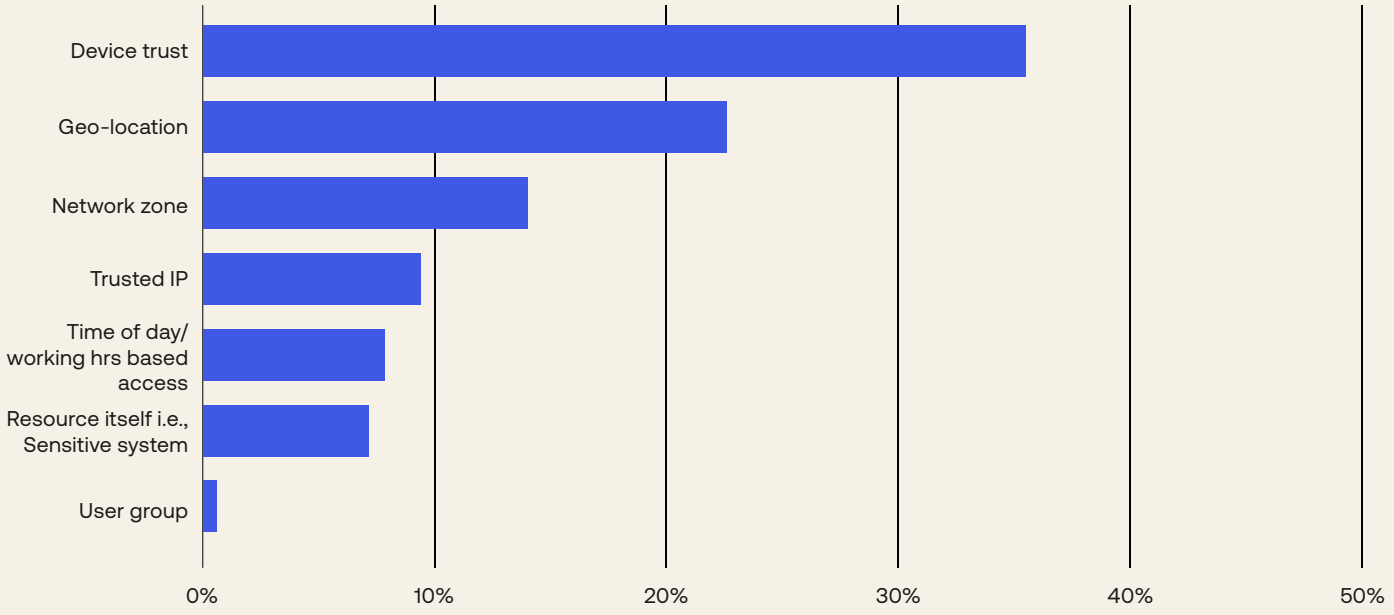
Trey Ray, Manager of Cybersecurity, FedEx

Worldwide, respondents ranked device trust, geographic location, and trusted IP as the most critical attributes for managing and approving access to internal resources. Device trust—including understanding whether the device is managed, whether the device is known, and whether the device is verified and healthy—was every region's No. 1 critical attribute. But there were regional variations: APAC respondents deemed the network zone a more critical attribute than a trusted IP, while in North America, the resource itself (e.g., a sensitive database) was judged to be essentially on par with geo-location and trusted IP. Among the Global 2000, geo-location was a far less critical factor: Time of day and network zone were deemed slightly more critical than trusted IP, leaving geo-location as only the fifth most important attribute.

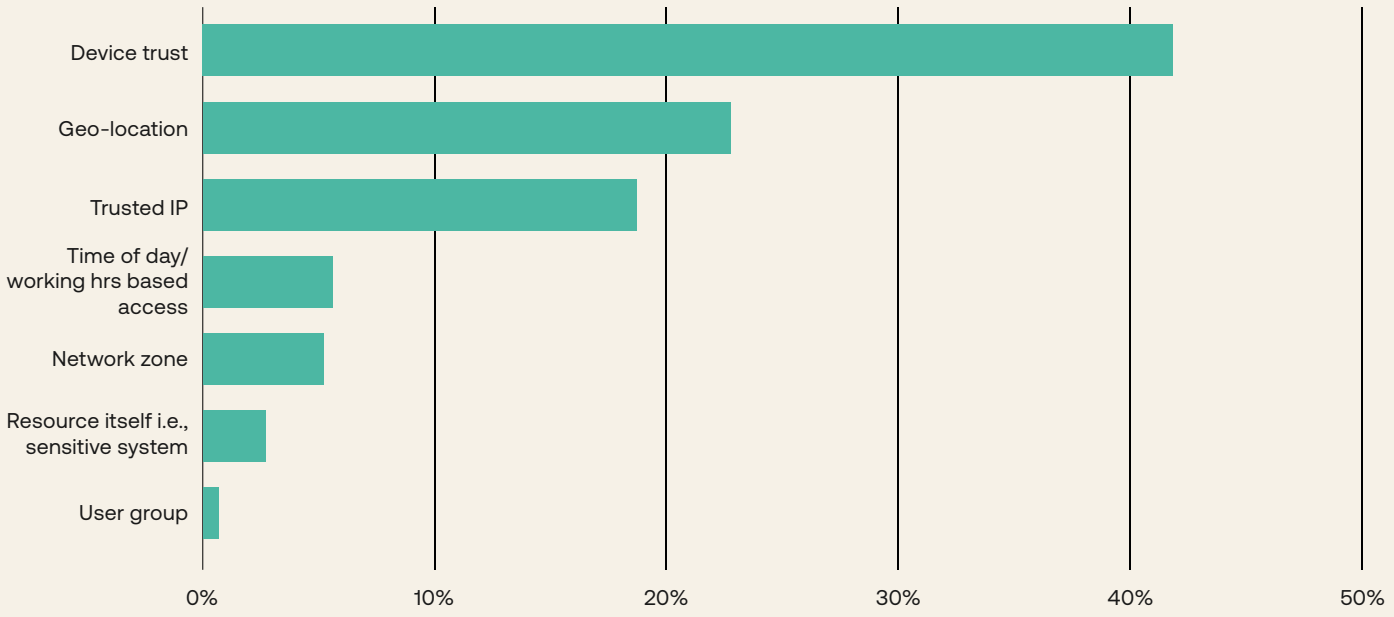
All Companies Worldwide Which classes of resources have you already extended SSO and/or MFA to? (Select all that apply)



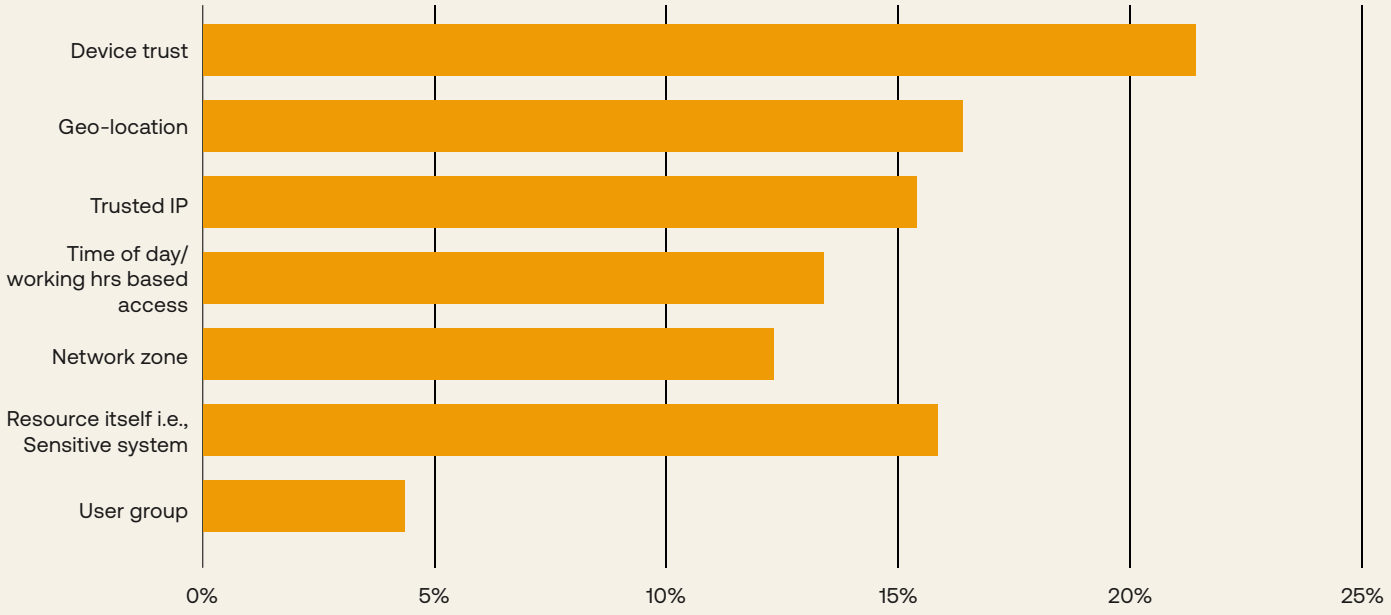
APAC Rank the most critical factors when controlling and approving access to your internal resources



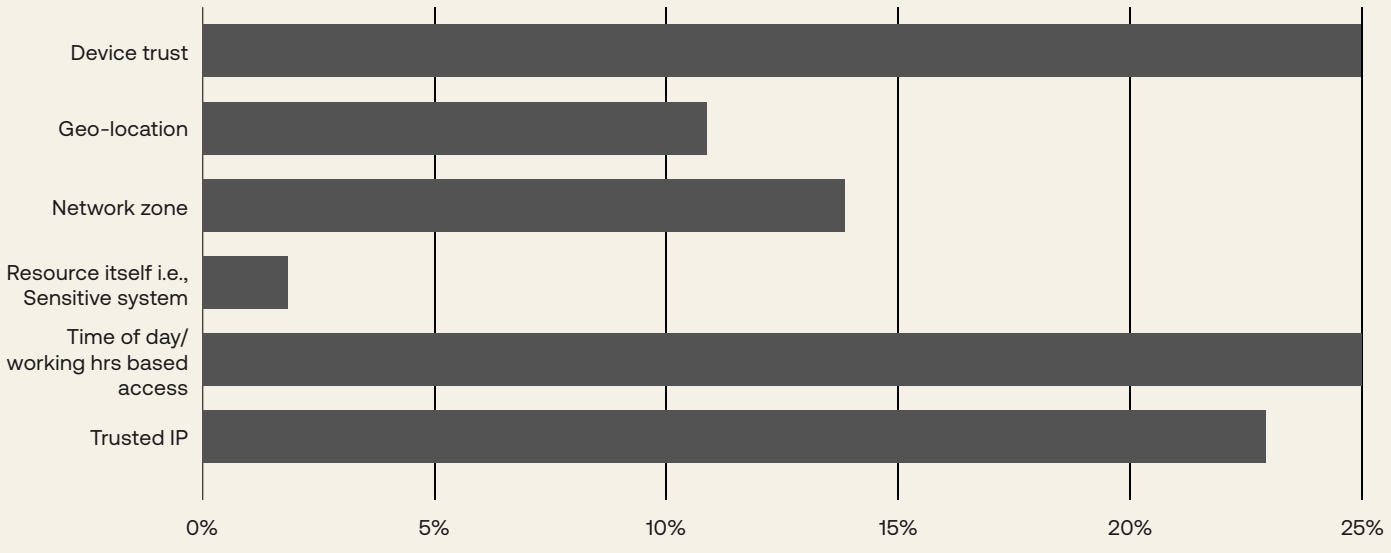
EMEA Rank the most critical factors when controlling and approving access to your internal resources



NA Rank the most critical factors when controlling and approving access to your internal resources



Global 2000 Companies Rank the most critical factors when controlling and approving access to your internal resources

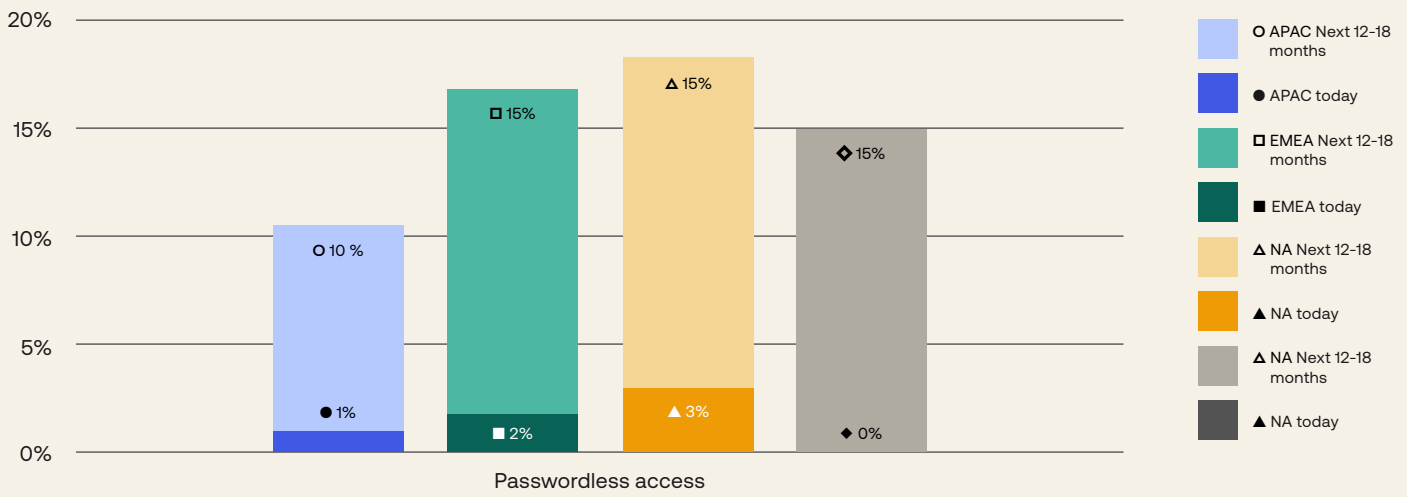


Phase 5: Evolved

Organizations in the Evolved phase have already shifted operations to cloud-based platforms like Amazon Web Services (AWS), Google Cloud (GCP), and Microsoft Azure, and they're focused on automation and adoption of edge security. Here, the focus shifts from implementing the core Zero Trust projects highlighted in earlier phases to optimizing user lifecycle management, applying security access control to servers, and implementing passwordless access using high assurance factors such as factor sequencing, biometric-based logins through web authentication (WebAuthn), and Universal 2nd Factor (U2F) security keys.

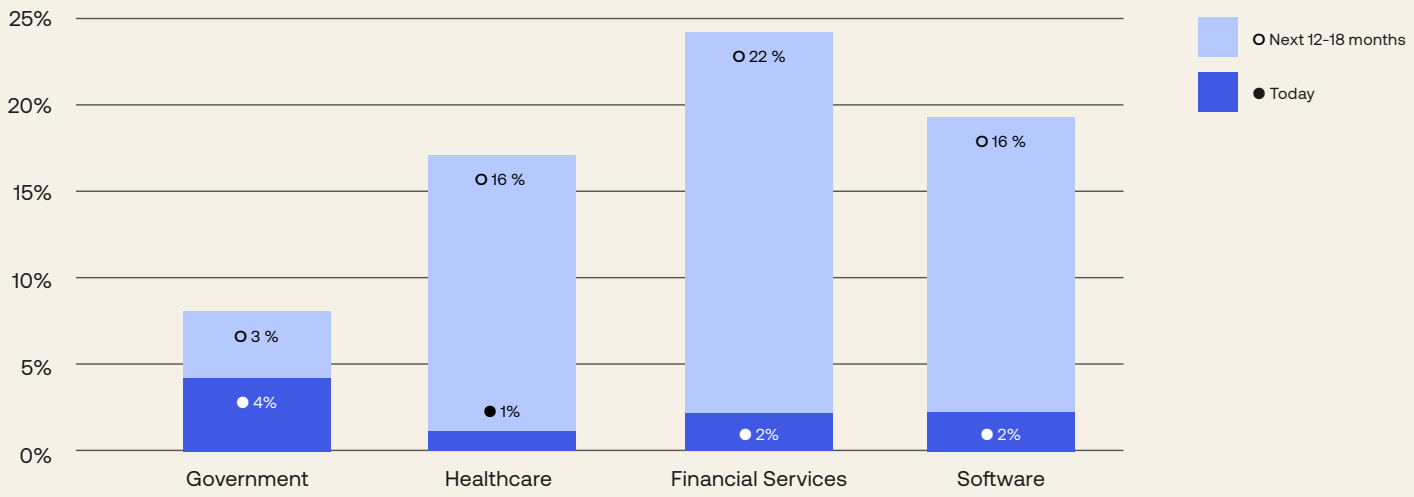
Encouragingly, respondents from all regions plan to ramp up adoption of passwordless access in the coming 12-18 months. This is especially positive considering that more than half of all data breaches today involve weak or stolen credentials, with credential abuse responsible for much of the increasing incidence of ransomware and other identity-based attacks.3 North American companies are leading the charge, having already adopted passwordless access options at a higher rate; many respondents in that region have definitive plans to follow suit over the coming months.

Regional Comparisons Have you already implemented passwordless access options or plan to do so in the next 12-18 months?



Looking at the data by industry, nearly 22% of respondents from financial services companies indicated that they plan to adopt passwordless access options in the coming 12-18 months, while 16% of healthcare and software companies plan to follow suit. Government institutions lag behind, with only around 7% either already having passwordless access in place or planning to do so in the coming months.

Industry Comparisons Have you already implemented passwordless access options or plan to do so in the next 12-18 months?



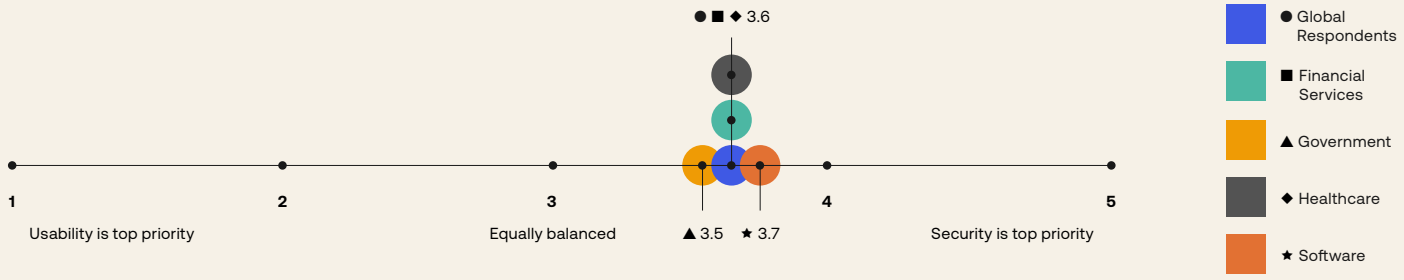
Industry Verticals

Zero Trust Progress by Industry Vertical

Every industry (and every organization, for that matter) has different practices, priorities, and obligations, and tends to follow a slightly different route to Zero Trust. In this year's study, we took a deeper dive into four key verticals—healthcare, financial services, software, and for the first time, government—to try to better understand how the unique needs of organizations in these sectors influence the adoption of Zero Trust solutions. In particular, we were interested in discovering how these four verticals balance the often opposing forces of security vs. usability.

Organizations are of course finding ways to fulfill both requirements. Interestingly, respondents this year, on average, considered security a slightly higher priority than usability—a change from 2021 data, when usability slightly outpaced security. An example of increased security focus: Industries like healthcare are reducing their dependence on low-assurance factors like passwords, which are highly vulnerable to credential-based attacks. Across all our target industry verticals, the top four challenges to implementing a Zero Trust security strategy were remarkably consistent: The biggest challenge this year is a talent and skill shortage, followed by stakeholder buy-in, cost concerns, and awareness of security solutions that support Zero Trust.

How do you balance the importance of security with the importance of usability at your organization?

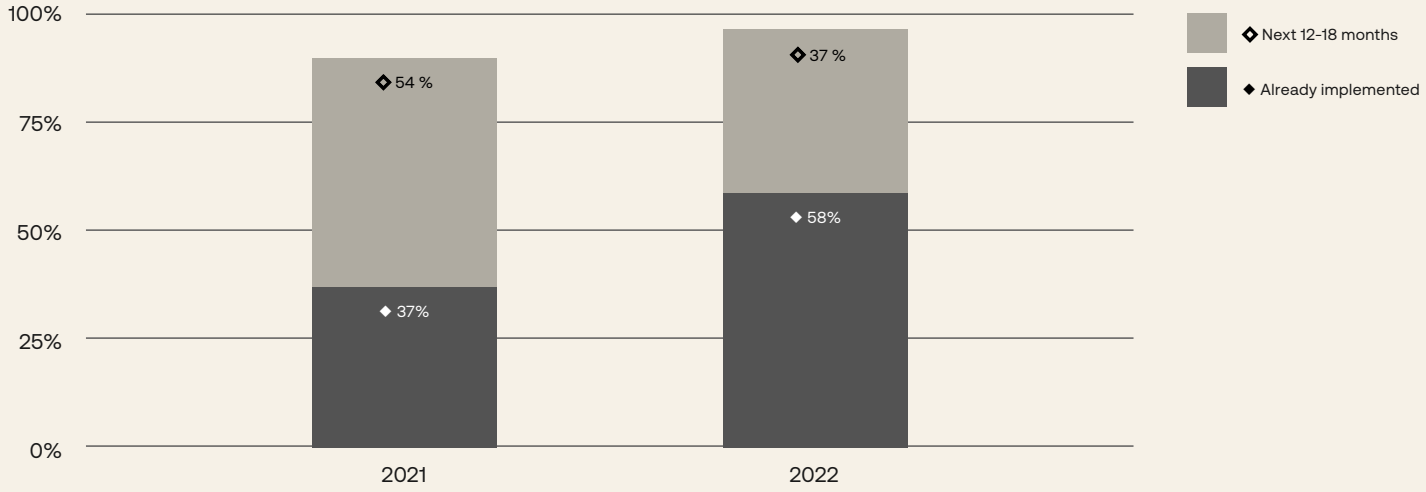


Key Verticals

Healthcare

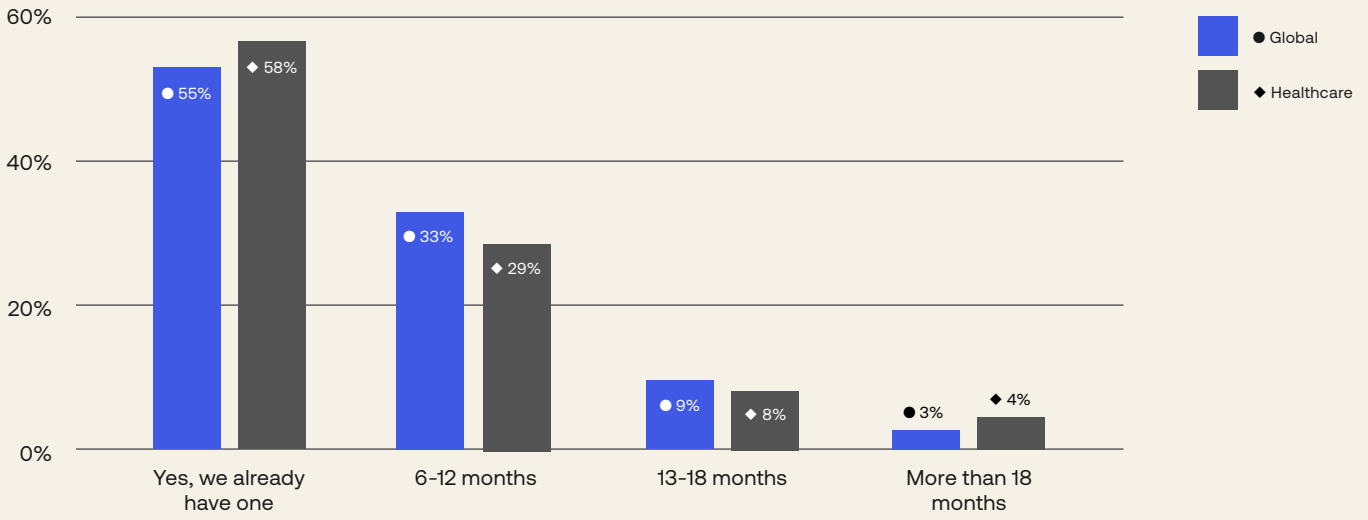
The last holdouts in the healthcare sector are getting their Zero Trust adoption plans in place: The number of healthcare respondents who either have a Zero Trust initiative in play or are planning to start over the next 12-18 months has climbed from 91% in 2021 to 96% in 2022. An impressive 58% of respondents in healthcare have already begun implementing their Zero Trust initiatives, representing a nearly 21-percentage point increase over the 37% who had begun by the time of last year's report. The majority of respondents from healthcare organizations that do not yet have a defined Zero Trust initiative in place plan to have one within the next 6-12 months, continuing the momentum for execution in the short term.

Healthcare Year-over-Year Comparison Does your organization have a defined Zero Trust security initiative today or that you're planning to start in the next 12-18 months?

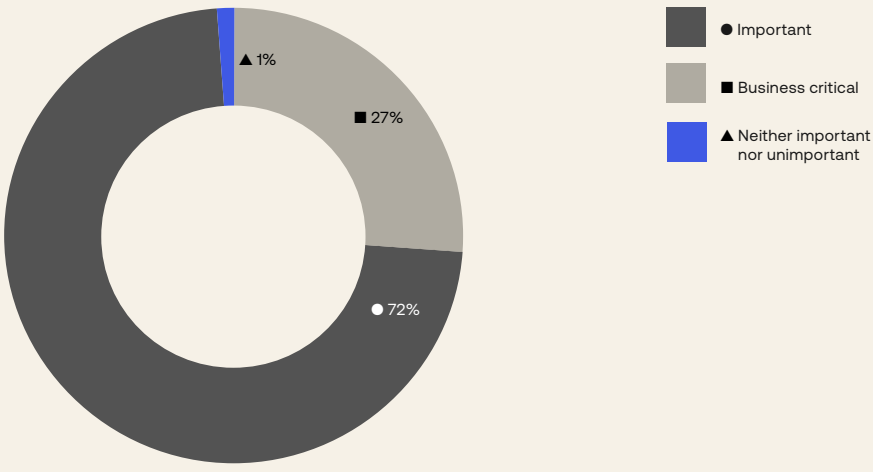


A full 98% of the respondents in this sector say identity plays a meaningful role in their overall Zero Trust security strategies, with 72% calling identity important and 27% calling it business critical. And they're putting these strategies into action: The majority of healthcare respondents already have a Zero Trust initiative in play, and most of the rest plan to start theirs within the next 6-12 months. Key identity projects they expect to complete in that time frame include extending SSO for employees and securing access to APIs.

All Companies Worldwide and Healthcare Companies Comparison Does your organization have a defined Zero Trust security initiative today or that you're planning to start on in the coming months?



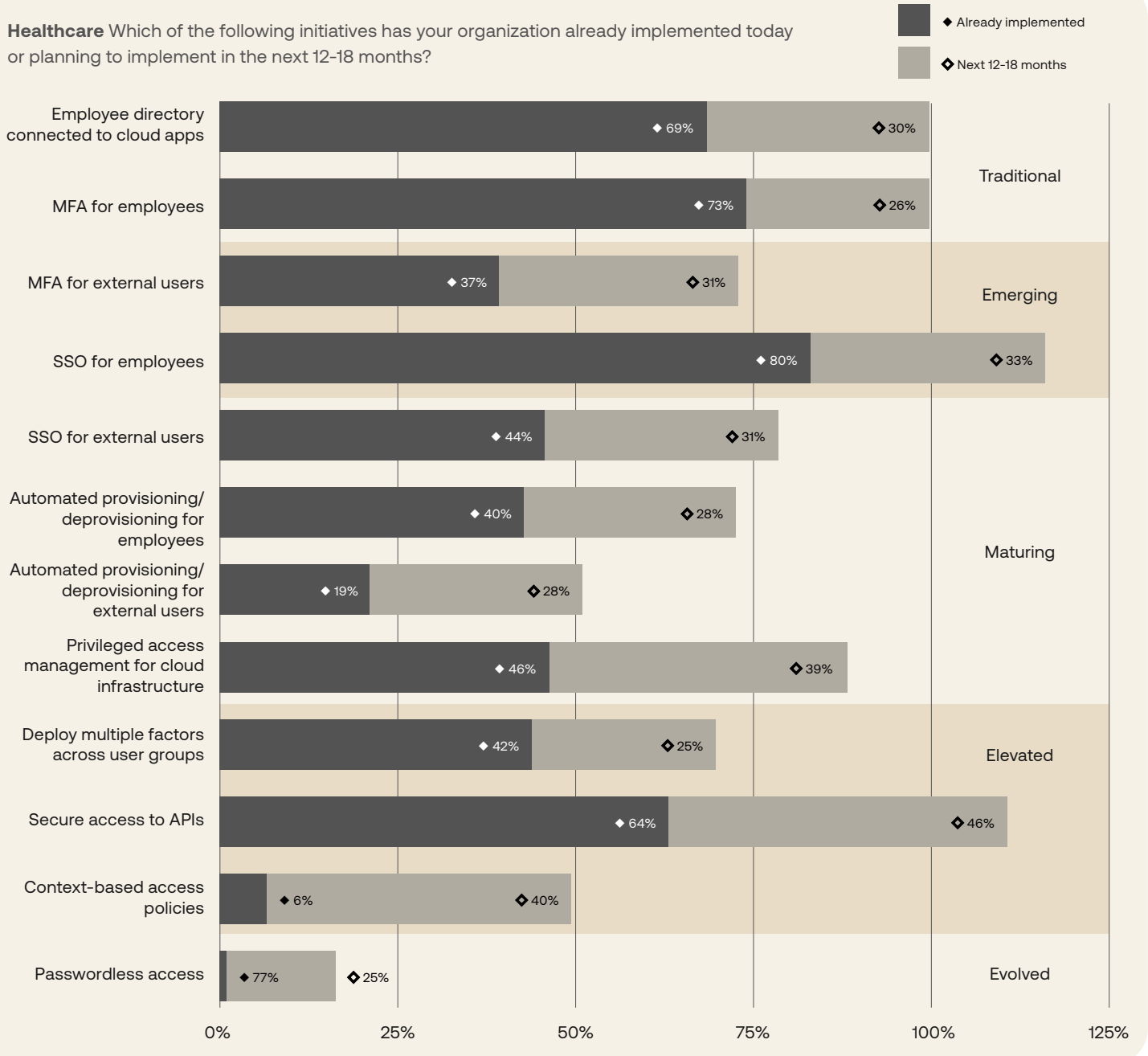
Healthcare How important is identity to your Zero Trust security strategy?



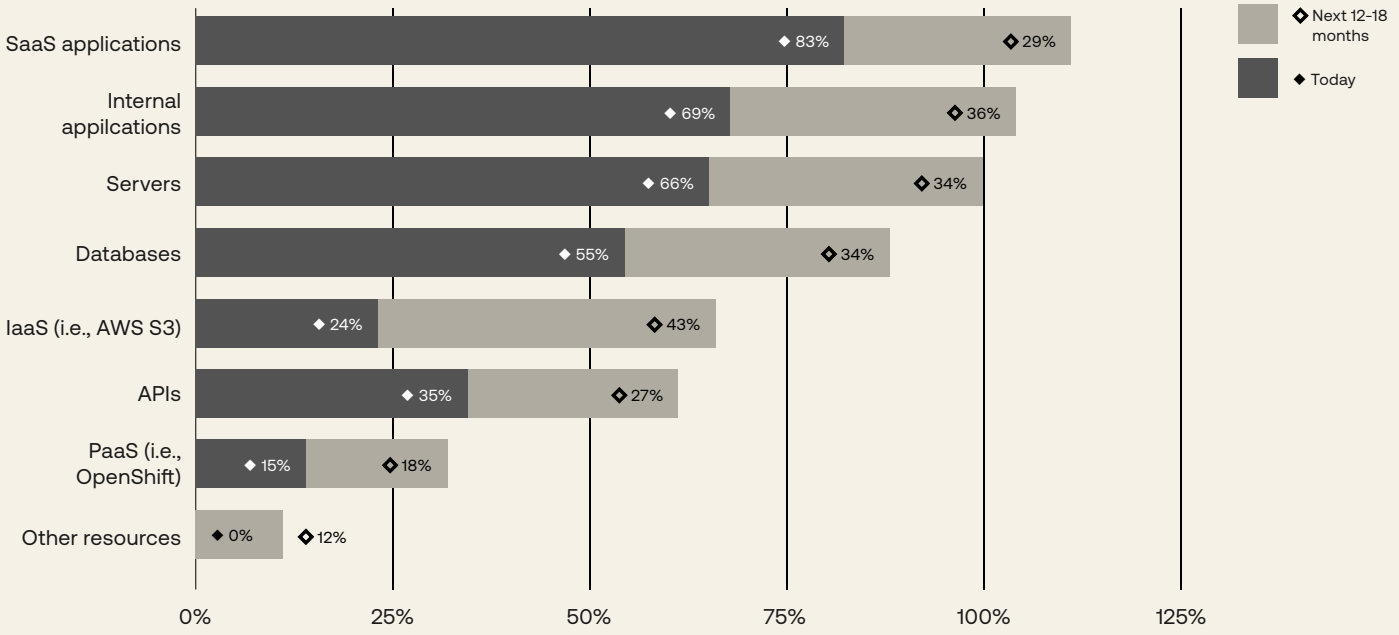
One of the biggest jumps in identity project adoption in the coming months for this sector will be to add context-based access policies: Just 6% of respondents say they have these policies in place already, but another 40% expect to roll them out in the next 12-18 months.

All healthcare respondents said they plan to have extended SSO, MFA, or both to SaaS apps, internal apps, and servers in the coming 12-18 months. Healthcare organizations are also focusing on IaaS; among those surveyed, the number who plan to extend SSO, MFA, or both to this resource class is expected to nearly triple in the coming months.

Healthcare Which of the following initiatives has your organization already implemented today or planning to implement in the next 12-18 months?

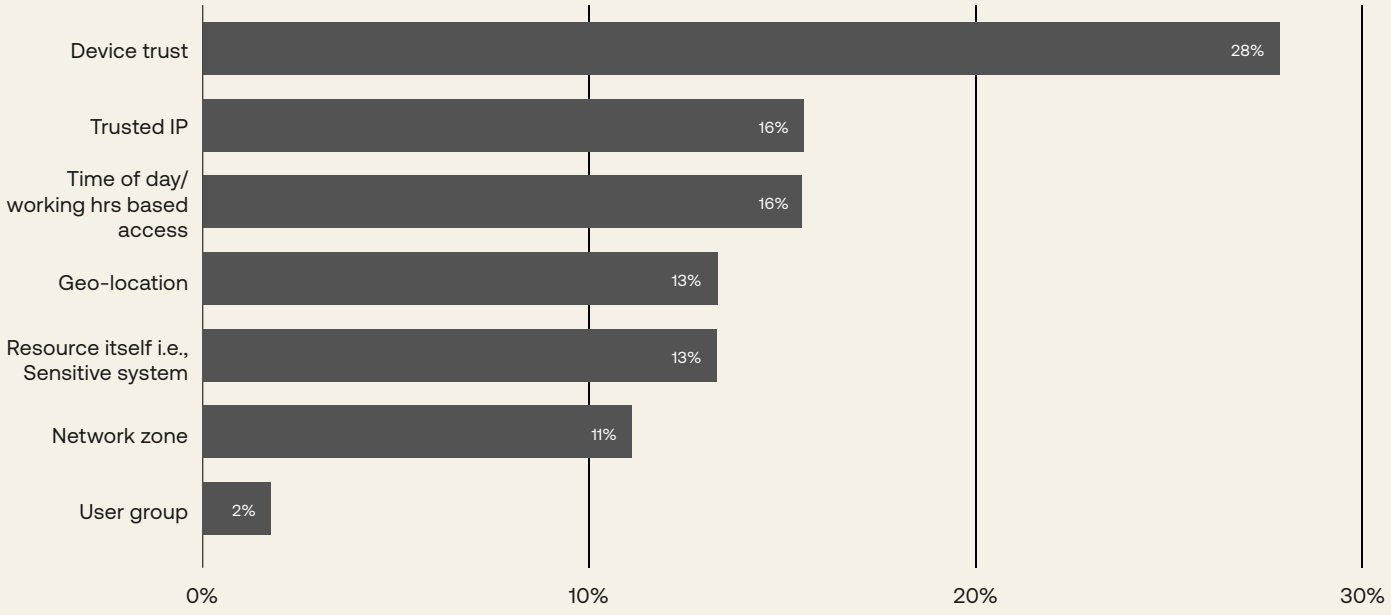


Healthcare Which classes of resources have you already extended SSO and/or MFA to?



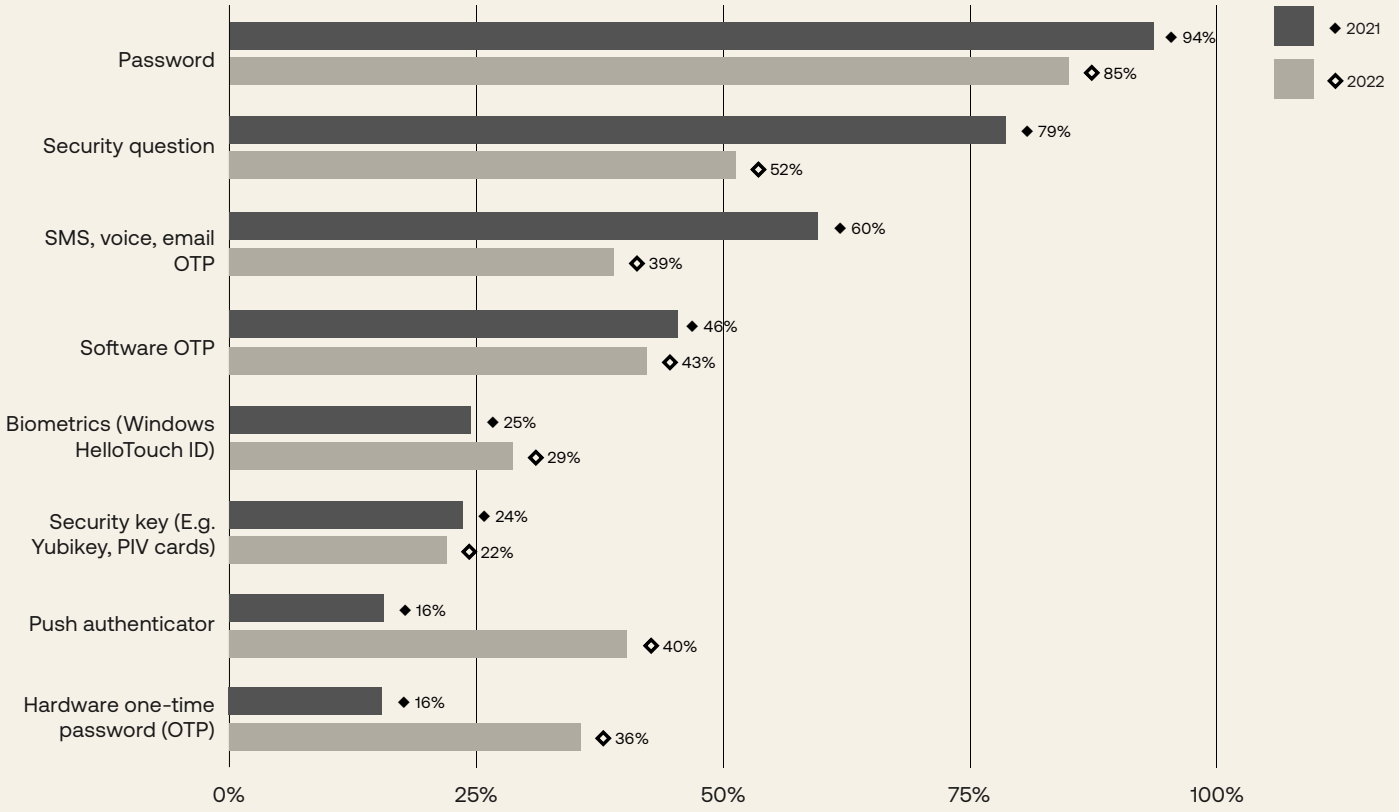
The three factors deemed most critical by healthcare organizations for controlling and approving access to internal resources in 2022 were device trust, geographic location, and trusted IP. While device trust has a significant lead in terms of rank, other factors that are nearly as important to healthcare organizations include the time of day or working hours-based access, and the resource itself like whether it is highly sensitive.

Healthcare Rank the number one factor when controlling and approving access to your internal resources



Year over year, the percentage of healthcare organizations that use passwords (low assurance) has dropped, while push authentication adoption (higher assurance) jumped from 16% last year to over 40% this year—a healthy increase.

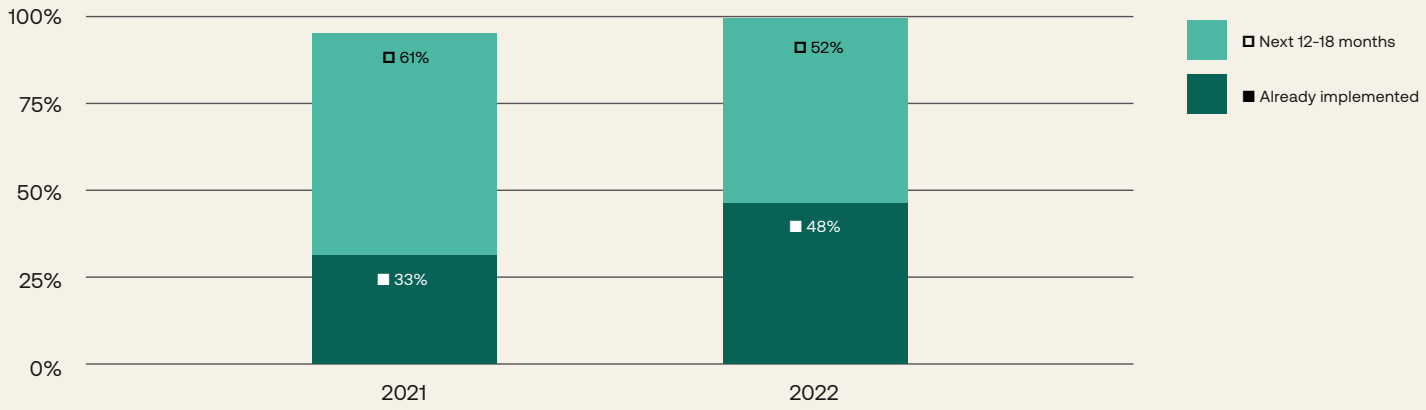
Healthcare Year-over-Year Comparison Select the authentication factors that your organization currently uses to verify internal and external users



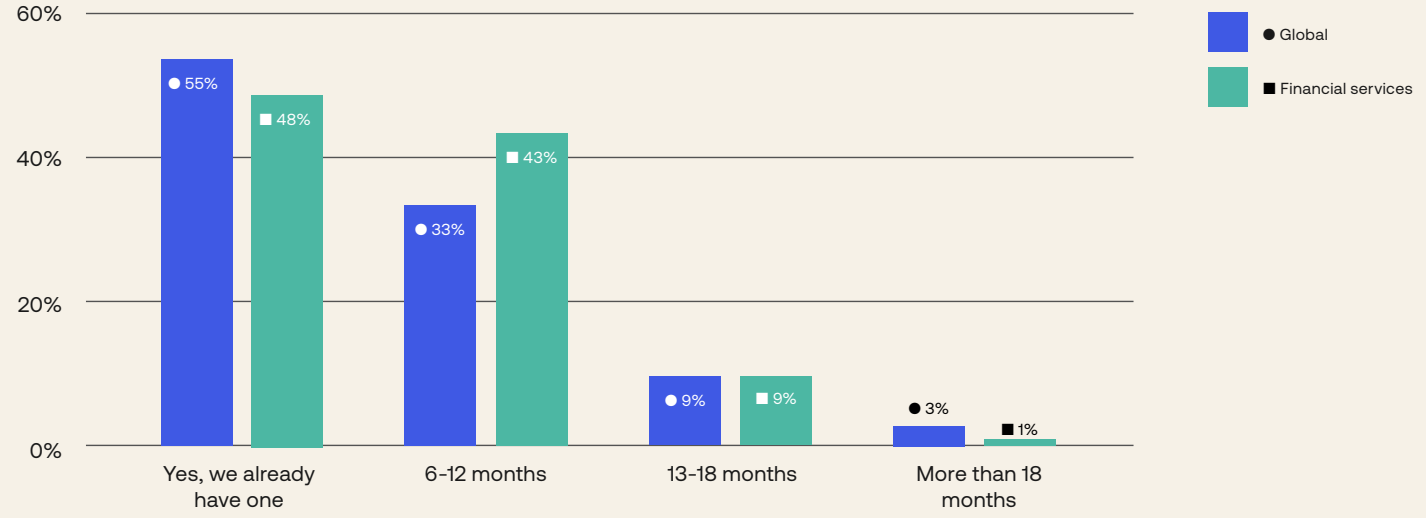
Financial Services

Zero Trust is clearly on the minds of financial services organizations: Within the next 12-18 months, nearly 100% of financial service respondents plan to have a Zero Trust initiative underway. In fact, nearly half of respondents (48%) already have such an initiative in place today, up from about a third of respondents last year–a healthy 15-percentage-point increase.

Financial Services Year-over-Year Comparison Does your organization have a defined Zero Trust security initiative today or that you're planning to start in the next 12-18 months?

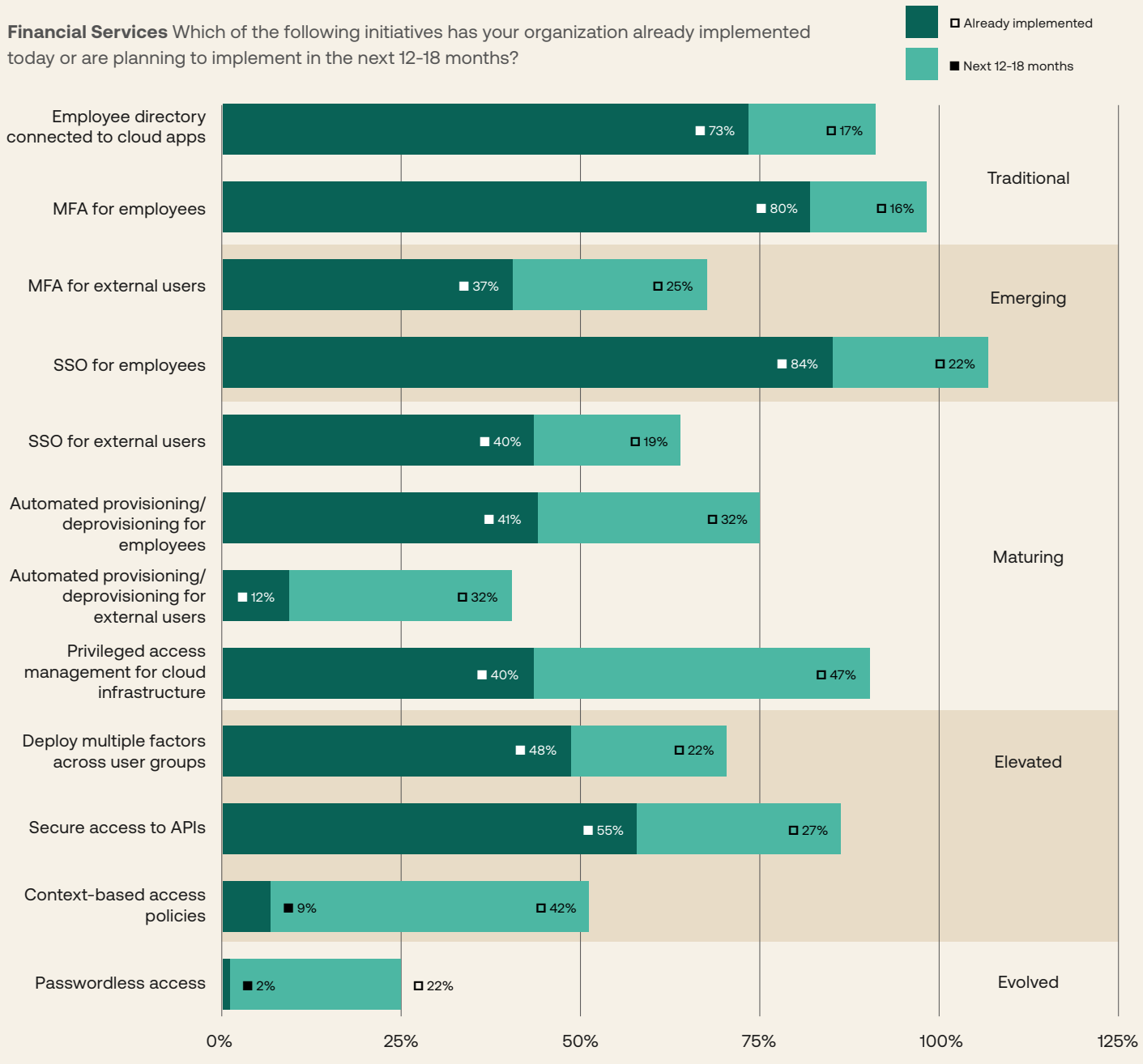


All Companies Worldwide and Financial Services Companies Comparison Does your organization have a defined Zero Trust security initiative today or that you're planning to start on in the coming months?

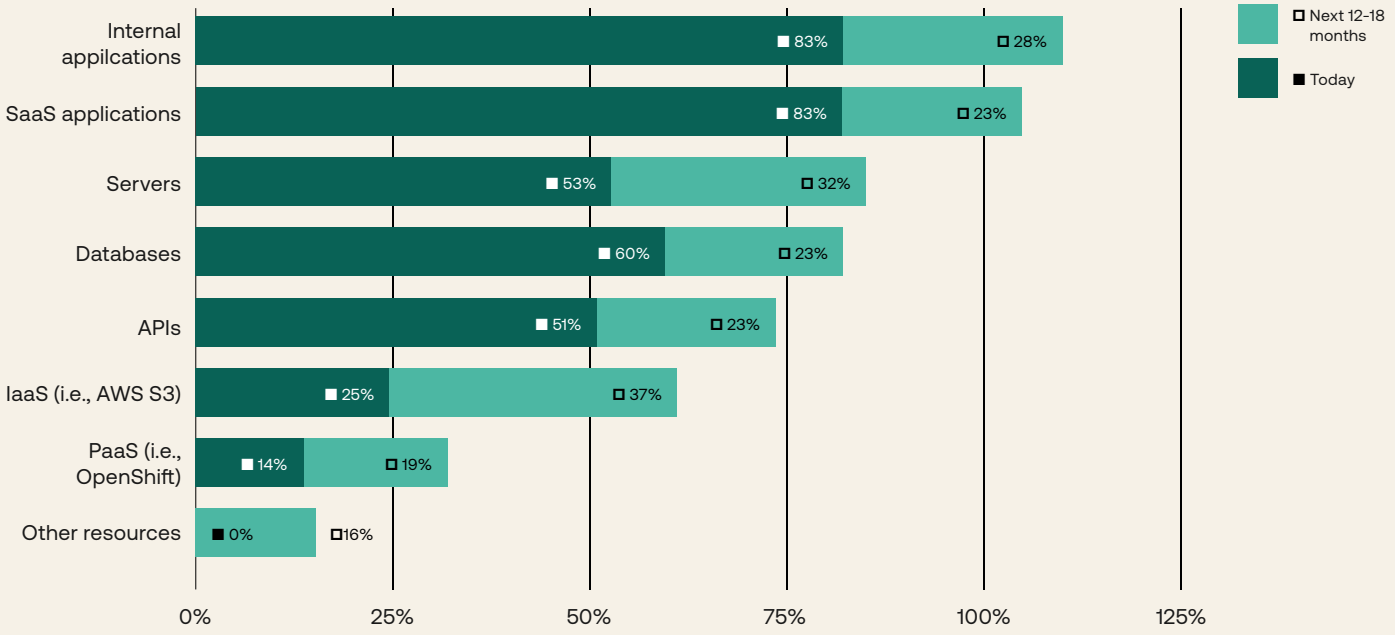


Most of the definitional work to get Zero Trust initiatives in the works for financial services organizations is already happening. The vast majority of respondents in the sector who don't already have a defined Zero Trust initiative in place plan to have one within the next 6-12 months. Financial services organizations as a whole may be slightly behind in their Zero Trust maturity relative to some other sectors today, but have specific and active plans to make significant strides to catch up in the near term.

Financial Services Which of the following initiatives has your organization already implemented today or are planning to implement in the next 12-18 months?



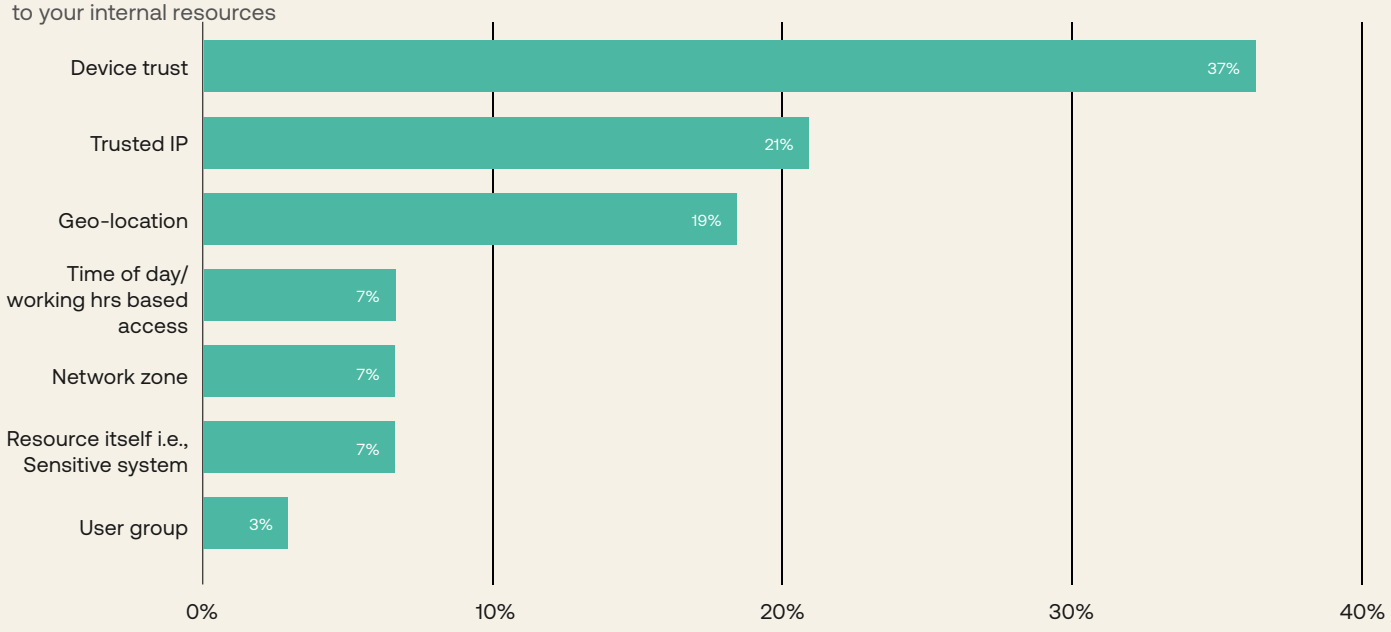
Financial Services Which classes of resources have you extended SSO and/or MFA to already, or plan to in the next 12-18 months?



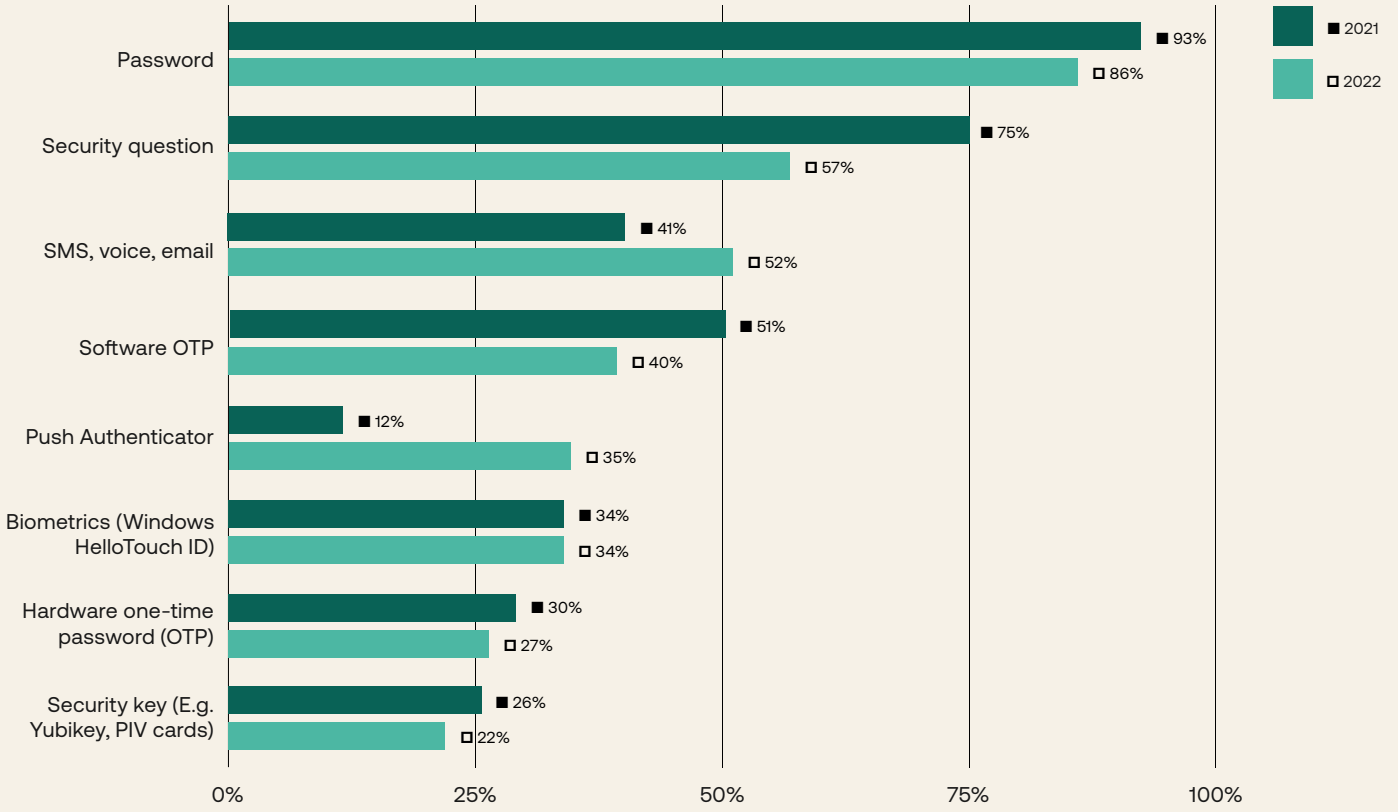
For financial services respondents, device trust is the most critical factor when controlling and approving access to internal resources; more than 36% of financial services respondents cited this as their No. 1 authentication factor. The number of financial services respondents using passwords and security questions as authentication factors has decreased since last year, while there has been an increase of more than 20 percentage points in the respondents using push authentication, a higher assurance factor.

All the financial services organizations we surveyed have either already extended SSO, MFA, or both, to SaaS apps and internal apps or plan to in the coming 12-18 months. Digging into the details, financial services companies plan to increase their verification factors on authentication. This means extending SSO to all endpoints wherever possible, including SaaS and on-prem applications, as well as moving to multi-factor authentication wherever possible, particularly on sensitive applications that include money moving and payments, and for all privileged access. IaaS is another identity project that financial services organizations are focusing on in the coming months; plans in place now would more than double the current rate of IaaS adoption by the end of 2023. Overall, nearly 75%, if not more, of financial services companies expect to have SSO, MFA, or both extended to servers, databases, and APIs within 18 months.

Financial Services Rank the most critical factors when controlling and approving access to your internal resources



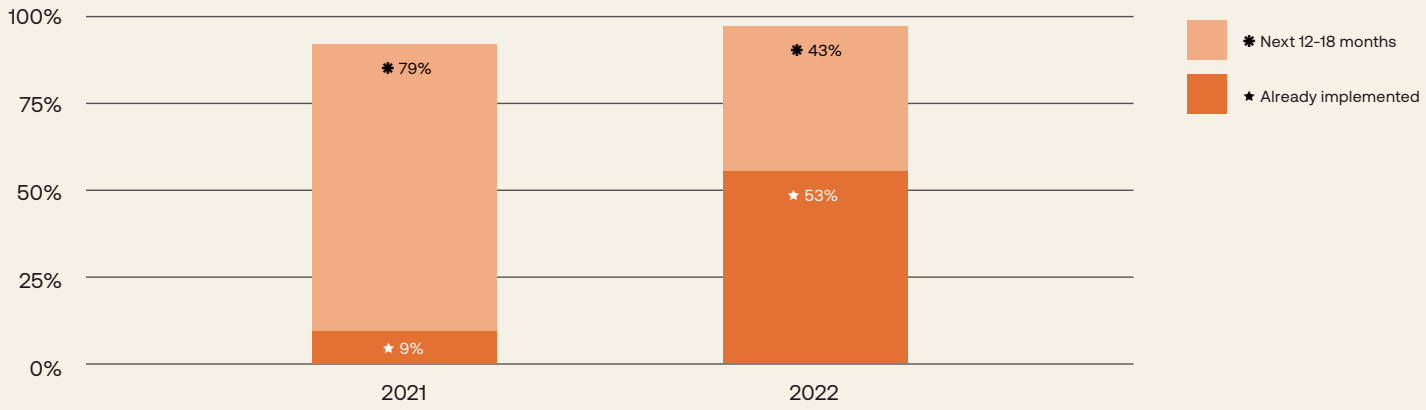
Financial Services Year-over-Year Comparison Select the authentication factors that your organization currently uses to verify internal and external users



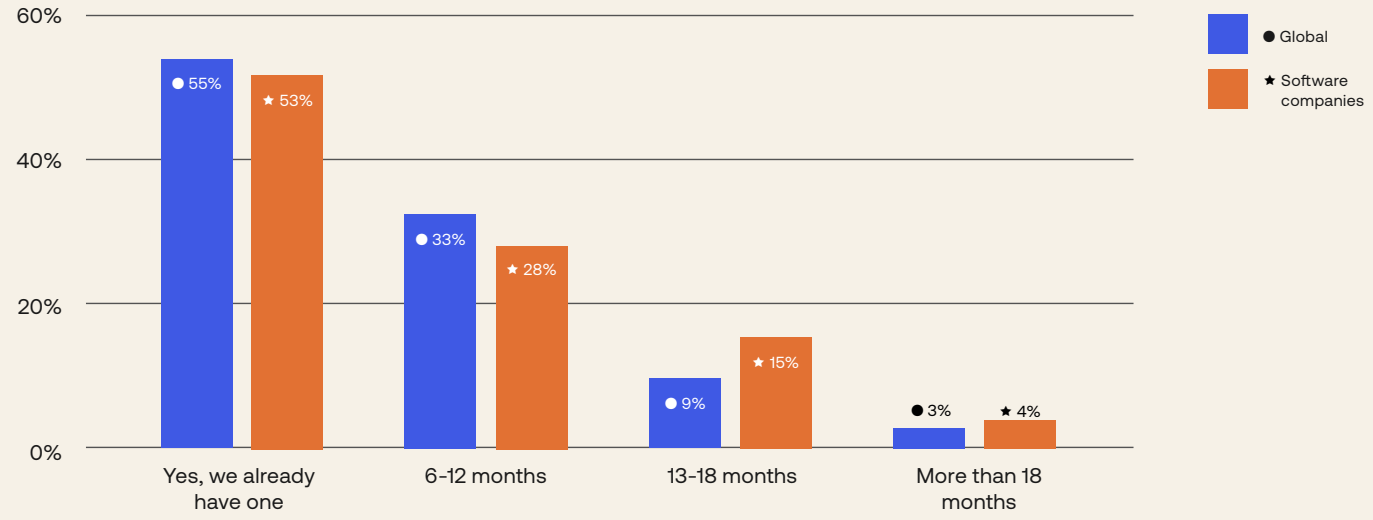
Software

In last year's report, the software industry lagged significantly behind the other target industries we surveyed. But in that report, software company respondents promised they would make significant strides in Zero Trust security initiatives over the ensuing 12-18 months–and they have come through with flying colors. In 2021, just 9% of software organizations surveyed had a defined Zero Trust initiative already in place, but another 79% planned to start one. This year, the number of organizations with an initiative underway climbed to almost 53%, and with another nearly 43% planning to get a defined initiative in place over the next 12-18 months, so a full 96% of software companies have at least begun their journeys. We've seen the same quick uptake in Zero Trust adoption: Software companies intend to move quickly. The speed at which they're defining their Zero Trust strategies has increased, and they generally expect to implement a Zero Trust initiative in the next 6-12 months.

Software Year-over-Year Comparison of Phase 3 Which of the following initiatives has your organization already implemented today or plan to implement in the next 12-18 months?

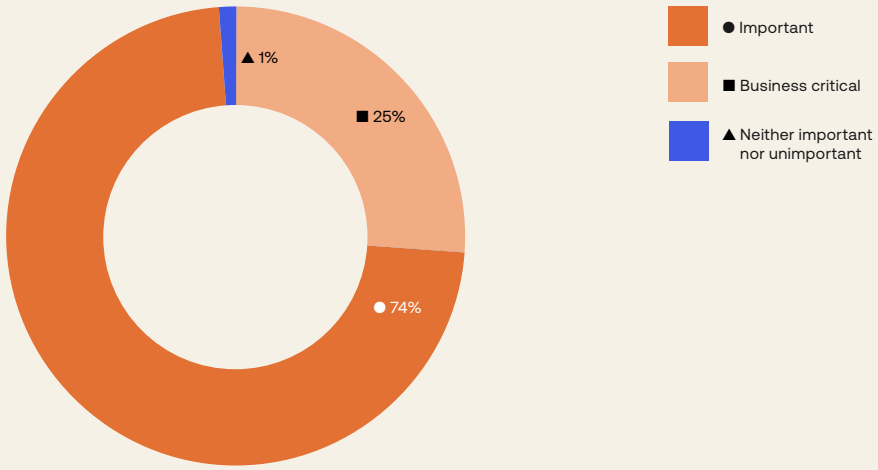


All Companies Worldwide and Software Companies Comparison Does your organization have a defined Zero Trust security initiative today or that you're planning to start on in the coming months?



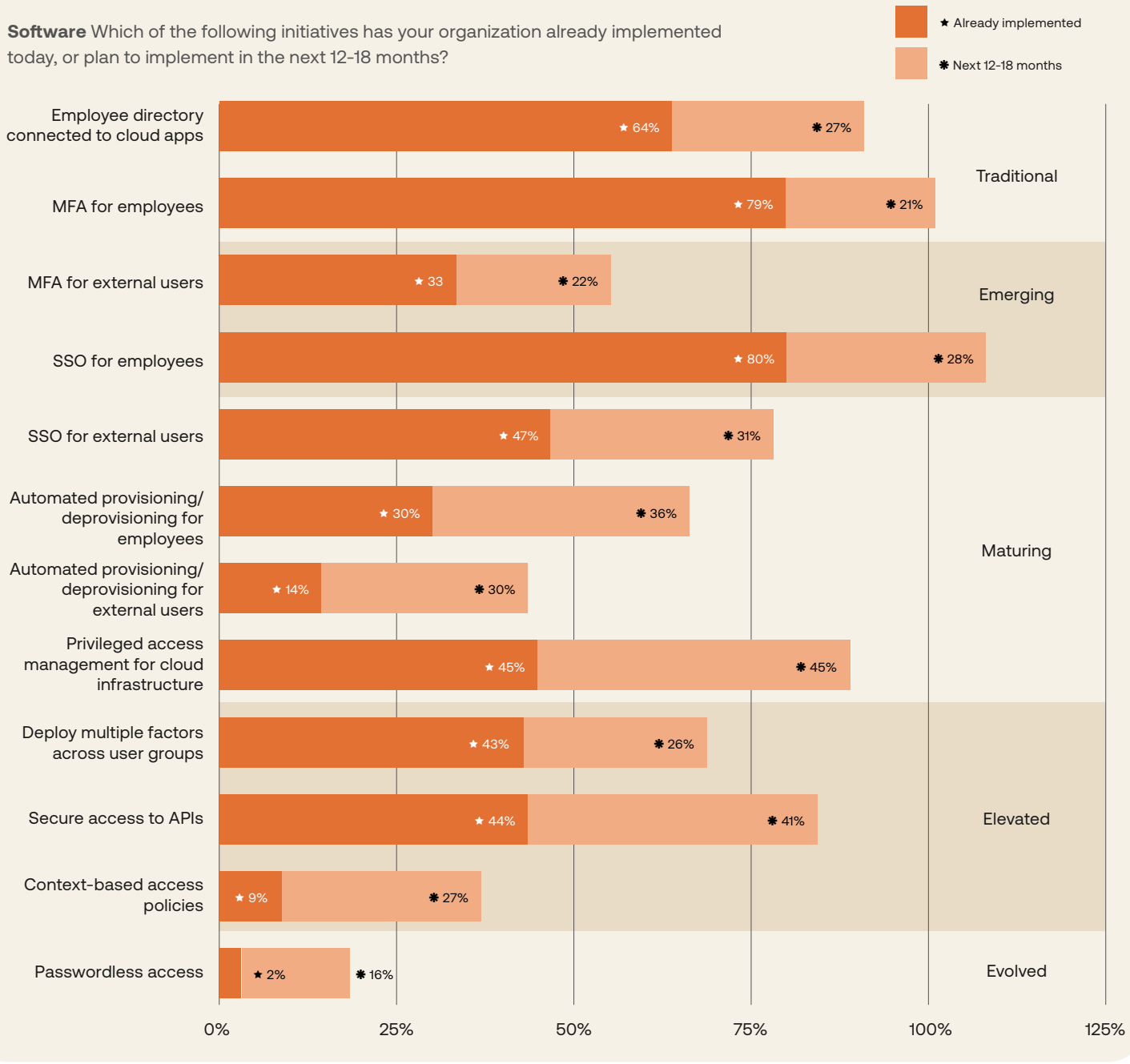
Of the respondents in the software sector, 99% reported that identity is either important or business critical to their overall Zero Trust strategy, with 25% declaring it business critical.

Software How important is identity to your Zero Trust security strategy?

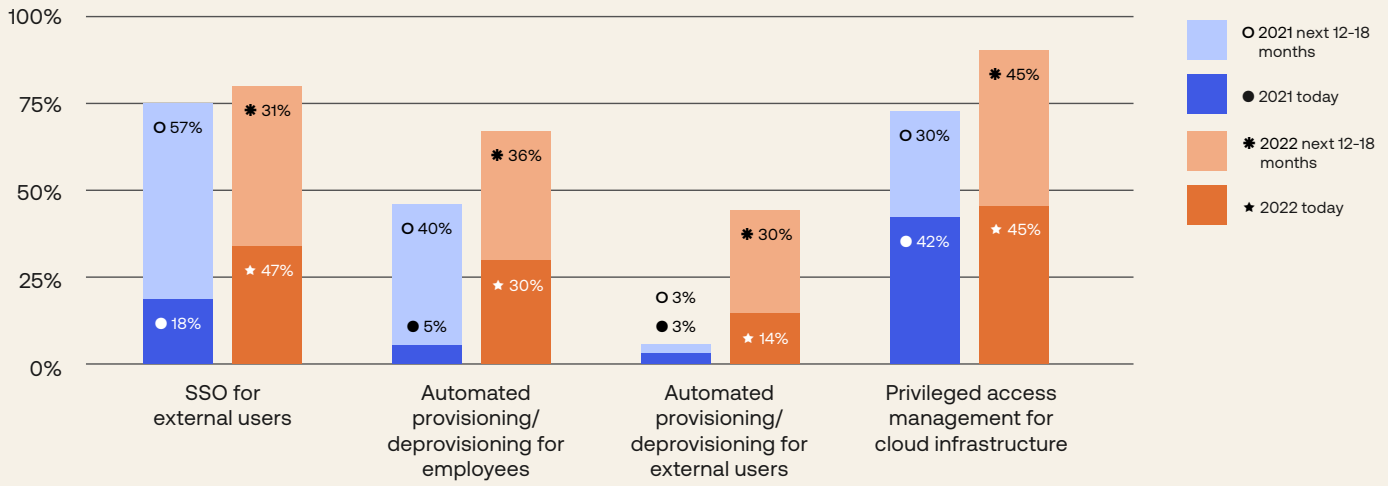


Among all industry verticals surveyed, software companies showed the most progress year over year in the initiatives of Phase 3 of the maturity curve. They've made good progress in adopting identity projects across the board, with implementing SSO for external users and automating provisioning and deprovisioning of all users a standout success. Nearly 100% of software companies surveyed indicated that they expect to have privileged access to cloud infrastructure in place by the end of 2023.

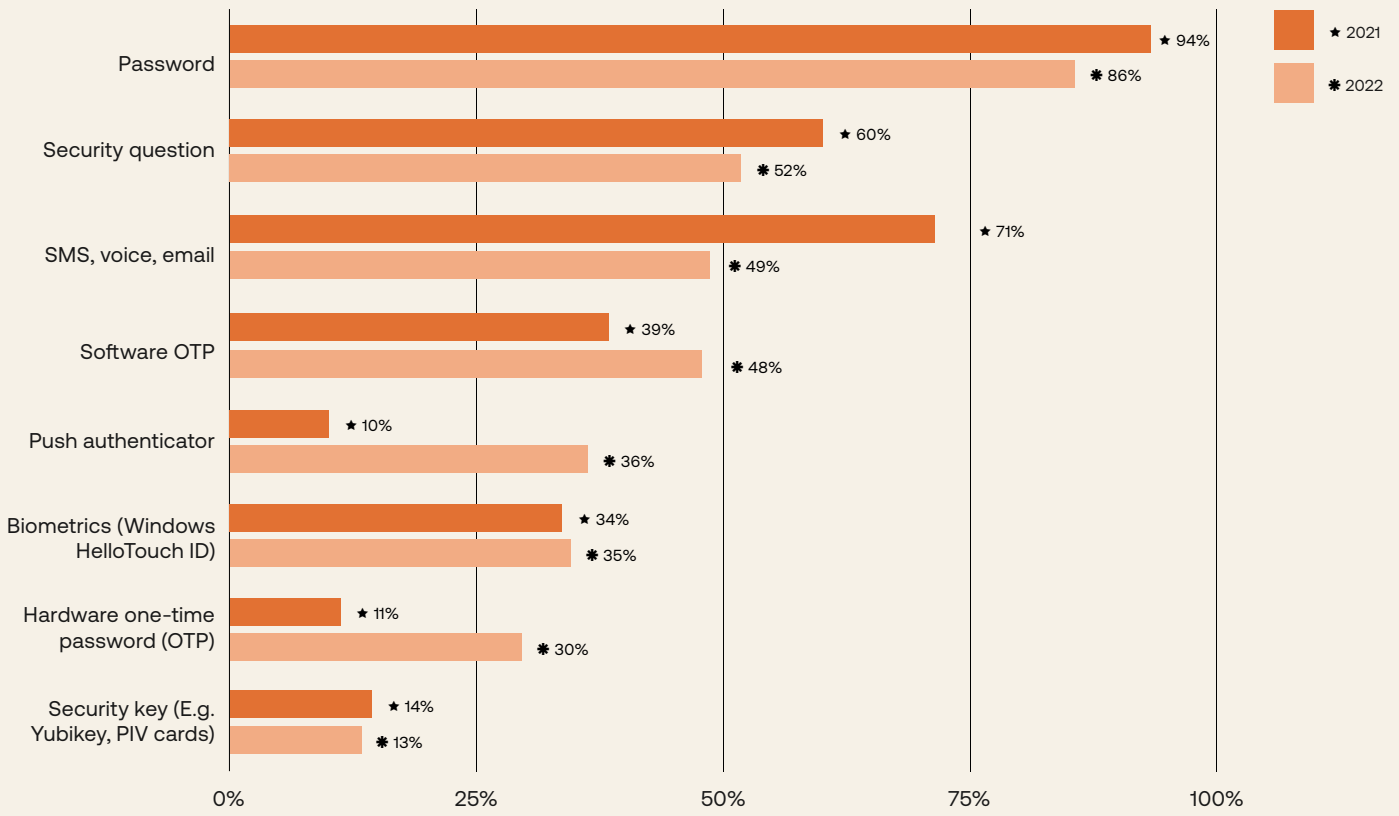
Software Which of the following initiatives has your organization already implemented today, or plan to implement in the next 12-18 months?



Software Year-over-Year Comparison Does your organization have a defined Zero Trust security initiative today or that you're planning to start in the next 12-18 months?



Lower-assurance authentication factors, including passwords; security questions; and SMS, voice, and email, all saw a slight drop compared to 2021 for software companies, while there has been a significant rise in the use of push authentication.

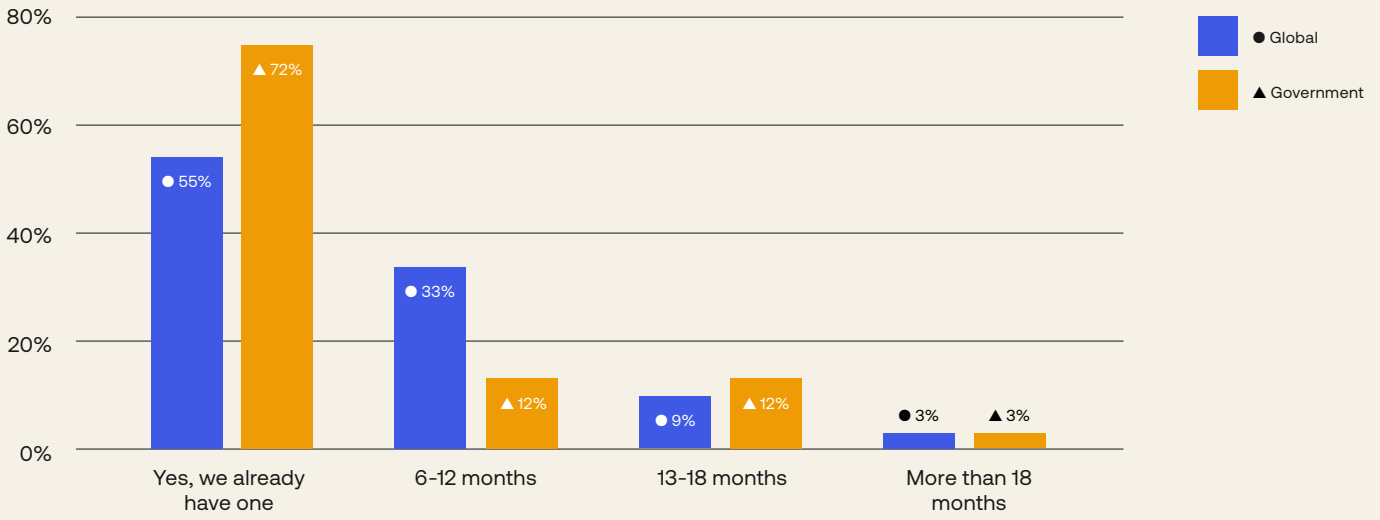


Government

Government organizations are ahead of their peers generally in their adoption of Zero Trust initiatives, and have plans to make steady progress adopting specific identity projects that support a Zero Trust strategy over the next several months. In the U.S., one accelerant has been recent government mandates demanding bold, swift action on cyber modernization (and not just incremental improvements), including clear actions that federal agencies must meet in the not-too-distant future. Other government organizations worldwide are similarly overhauling their approach to Zero Trust imperatives—in the U.K., for example, the National Cyber Security Centre issued a helpful set of eight Zero Trust architecture design principles, including identity-first recommendations like, "Don't trust any network, including your own."[7]

[7] **" Zero Trust Architecture Design Principles."** National Cyber Security Centre, 23 July 2021, Ncsc.gov.uk/collection/zero-trust-architecture/dont-trust-any-network. Accessed 10 Aug. 2022.

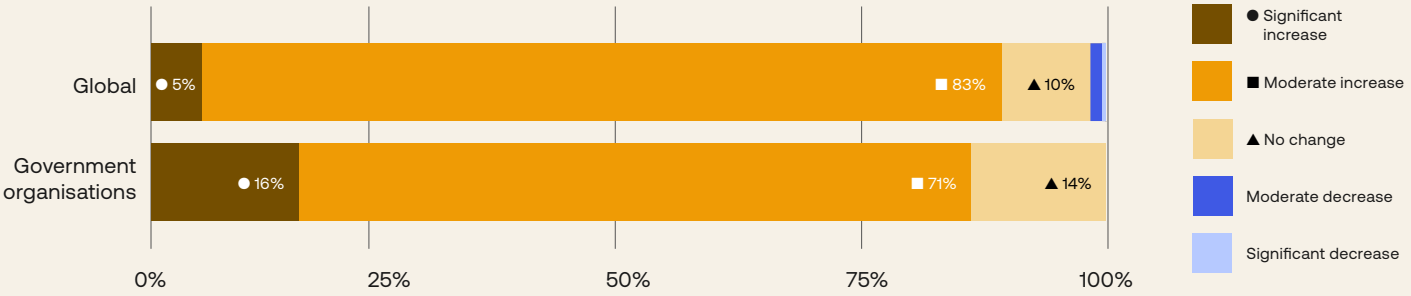
All Companies Worldwide and Government Organizations Comparison Does your organization have a defined Zero Trust security initiative today or that you're planning to start on in the coming months?



Around the world, a higher percentage of government organizations experienced a significant increase in budget over the past 12 months to support their Zero Trust initiatives. In the case of the U.S. government, the White House's federal Zero Trust strategy is unfunded, but agency applicants can access funding to support Zero Trust initiatives via the Technology Modernization Fund (TMF).[8]

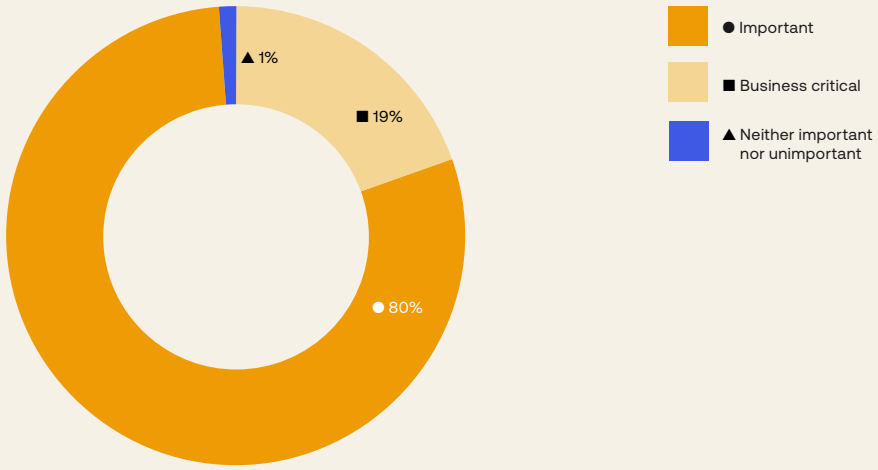
[8] FCW.com, **How the TMF Helps Agencies Pave the Way Toward Zero Trust,** 2022

All Companies Worldwide and Government Organizations Comparison How has your budget changed for Zero Trust security initiatives in the past 12 months?

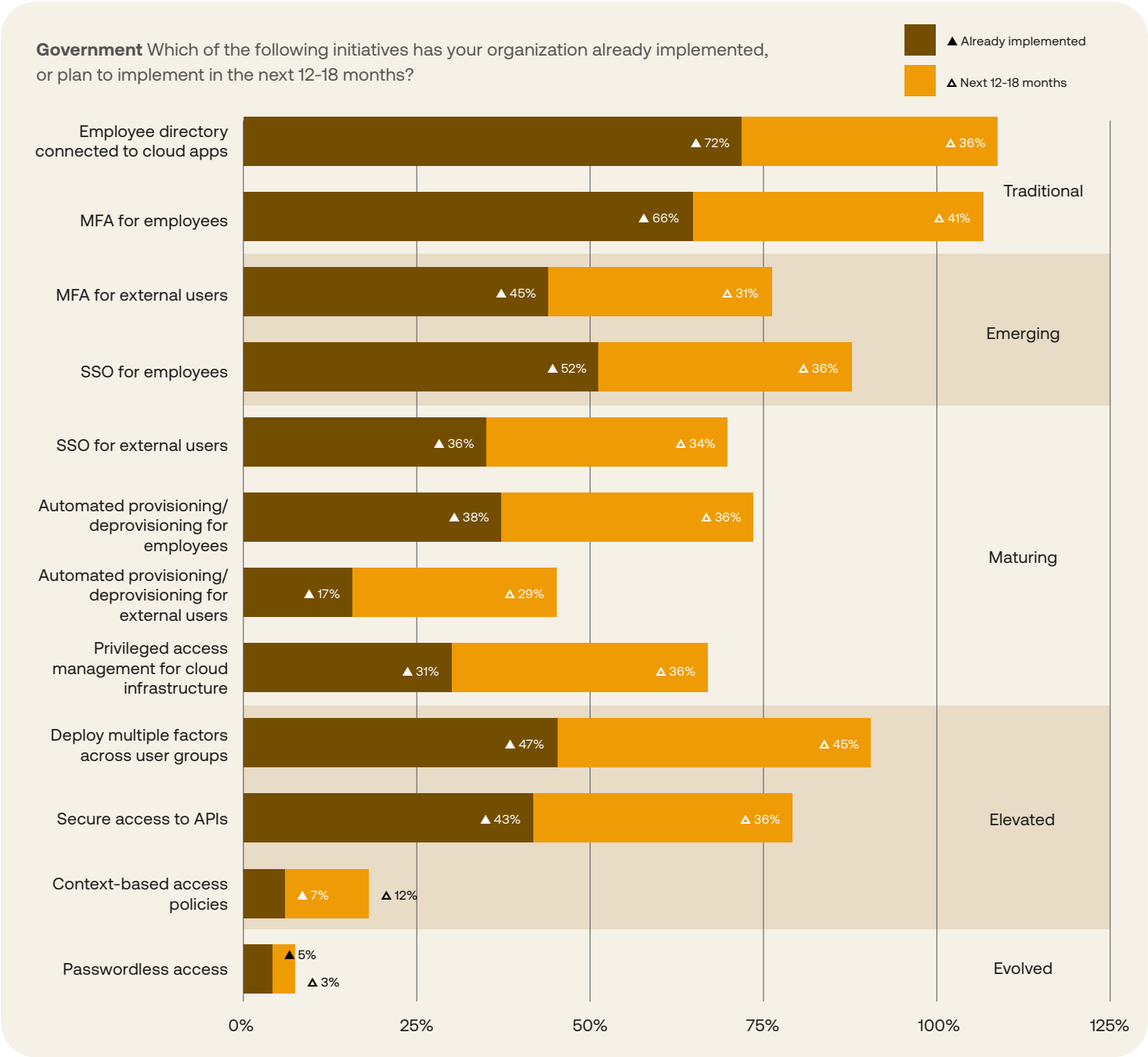


Nearly all government respondents around the world said that identity is an important part of their overall Zero Trust strategy, with 19% deeming it business critical. (In the U.S., a new federal Zero Trust strategy specifically calls out phishing-resistant MFA as a requirement for the workforce, and an available option for public customers.) In addition, identity is the first pillar of Zero Trust in the CISA Zero Trust Maturity Model, comparable to the "User" pillar of the U.S. Department of Defense Zero Trust Reference Architecture.

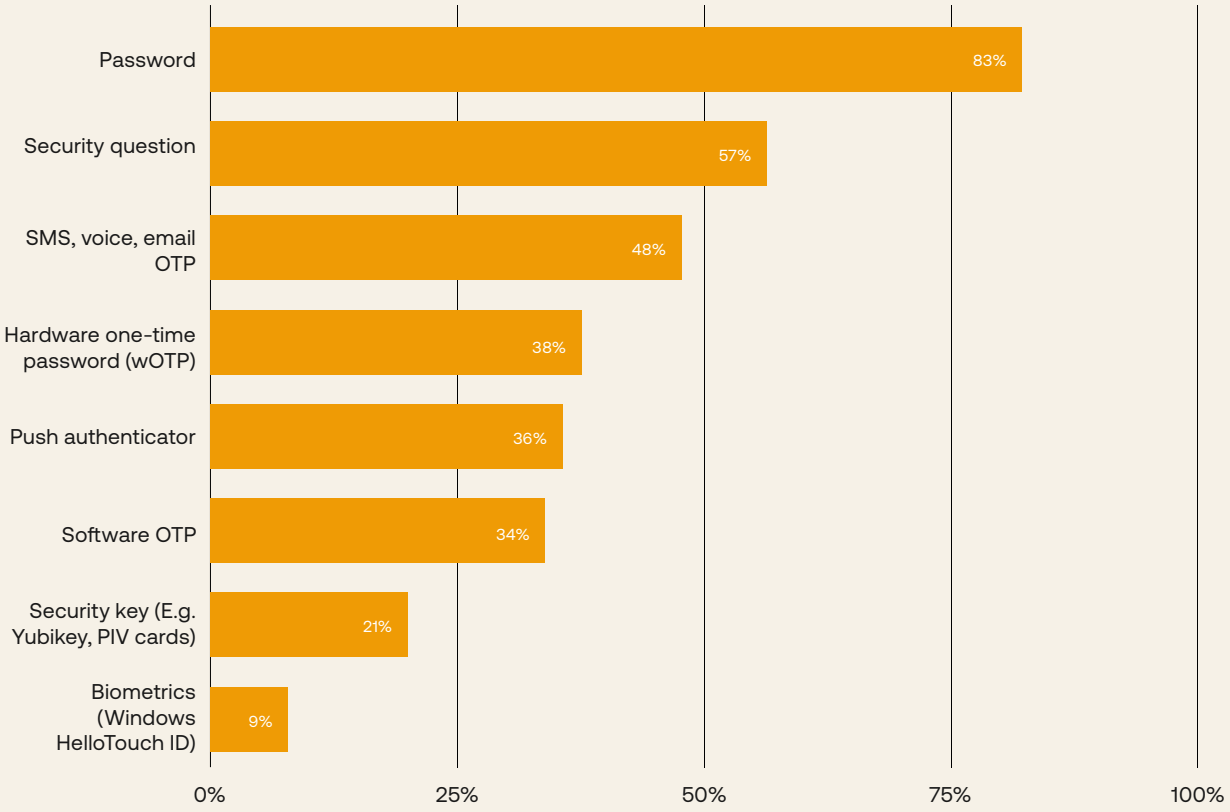
Software How important is identity to your Zero Trust security strategy?



Government respondents plan to make significant strides across the maturity curve in the coming 12-18 months. Specifically, their plans amount to nearly doubling progress against six of the 12 identity projects on the curve, prioritizing initiatives like deploying MFA for employees and user groups. Government organizations seem to be behind all other respondents on identity projects earlier on the curve, such as MFA and SSO, but indicate they'll work to not only adopt these projects, but also many more in the coming months.


Government Which of the following initiatives has your organization already implemented, or plan to implement in the next 12-18 months?
▲ Already implemented
△ Next 12-18 months
Employee directory connected to cloud apps
▲ 72%
△ 36%
MFA for employees
▲ 66%
△ 41%
Traditional
MFA for external users
▲ 45%
△ 31%
SSO for employees
▲ 52%
△ 36%
Emerging
SSO for external users
▲ 36%
△ 34%
Automated provisioning/ deprovisioning for employees
▲ 38%
△ 36%
Automated provisioning/ deprovisioning for external users
▲ 17%
△ 29%
Privileged access management for cloud infrastructure
▲ 31%
△ 36%
Maturing
Deploy multiple factors across user groups
▲ 47%
△ 45%
Secure access to APIs
▲ 43%
△ 36%
Context-based access policies
▲ 7%
△ 12%
Elevated
Passwordless access
▲ 5%
△ 3%
Evolved
0%
25%
50%
75%
100%
125%

Government Organizations Select the authentication factors that your organization currently uses to verify internal and external users



Zero Trust Today

Today's Identity-First Security Ecosystem

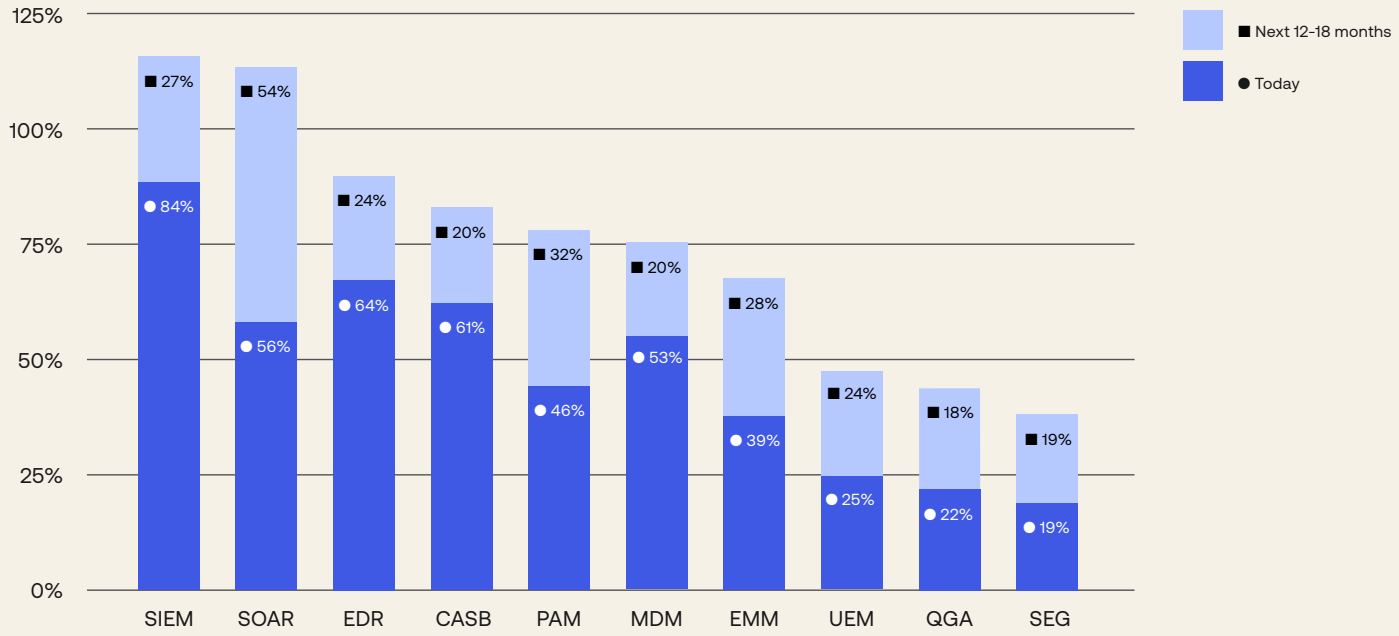
No single solution can accommodate every aspect of the Zero Trust recommendations promoted by Forrester, National Institute of Standards and Technology, and others. However, identity has emerged as a fundamental technology across the security stack, and it's becoming ever clearer that identity needs to be central to security planning, rather than an afterthought to bolt on later.

The Zero Trust defense an organization establishes is simply more effective and more efficient if it can integrate its IAM solution across the entire security architecture— including SIEM; security orchestration, automation and response (SOAR); enterprise mobility management for endpoint protection; mobile device management; cloud access security brokers (CASB); and privileged access management (PAM).

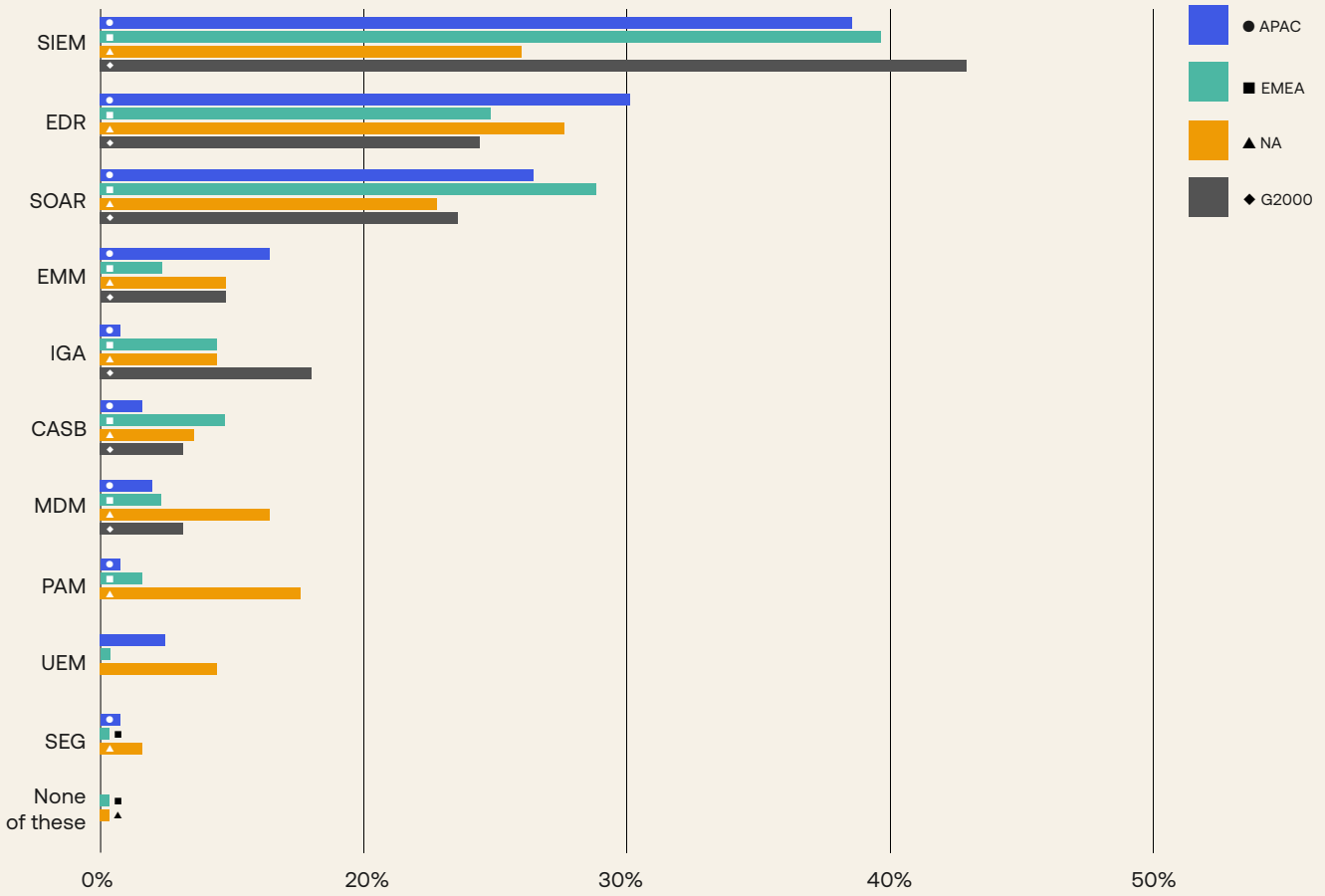
Coordinating IAM with SIEM can help organizations intelligently triage potential security events, for example; integrating IAM with SOAR can enable better-informed automated security responses; and integrating IAM with EDR can use identity to centrally correlate independent data points that together indicate an attack is in progress.

We asked security leaders which tools they thought were most important to integrate with their IAM solutions in support of establishing Zero Trust security. In our survey, SIEM was deemed the most critical element to integrate in almost every region, as well as by more than 40% of the Global 2000 companies we surveyed. The only region not to name SIEM the most critical element was North America, where EDR edged out a slim victory. In terms of current IAM integrations, the most common integrations in place today are SIEM, EDR, and CASB—these three are already operational today at more than three out of five companies we surveyed.

All Companies Worldwide Which of the following have you integrated with your identity and access solution or that you plan to implement within the next 12-18 months? (Select all that apply)



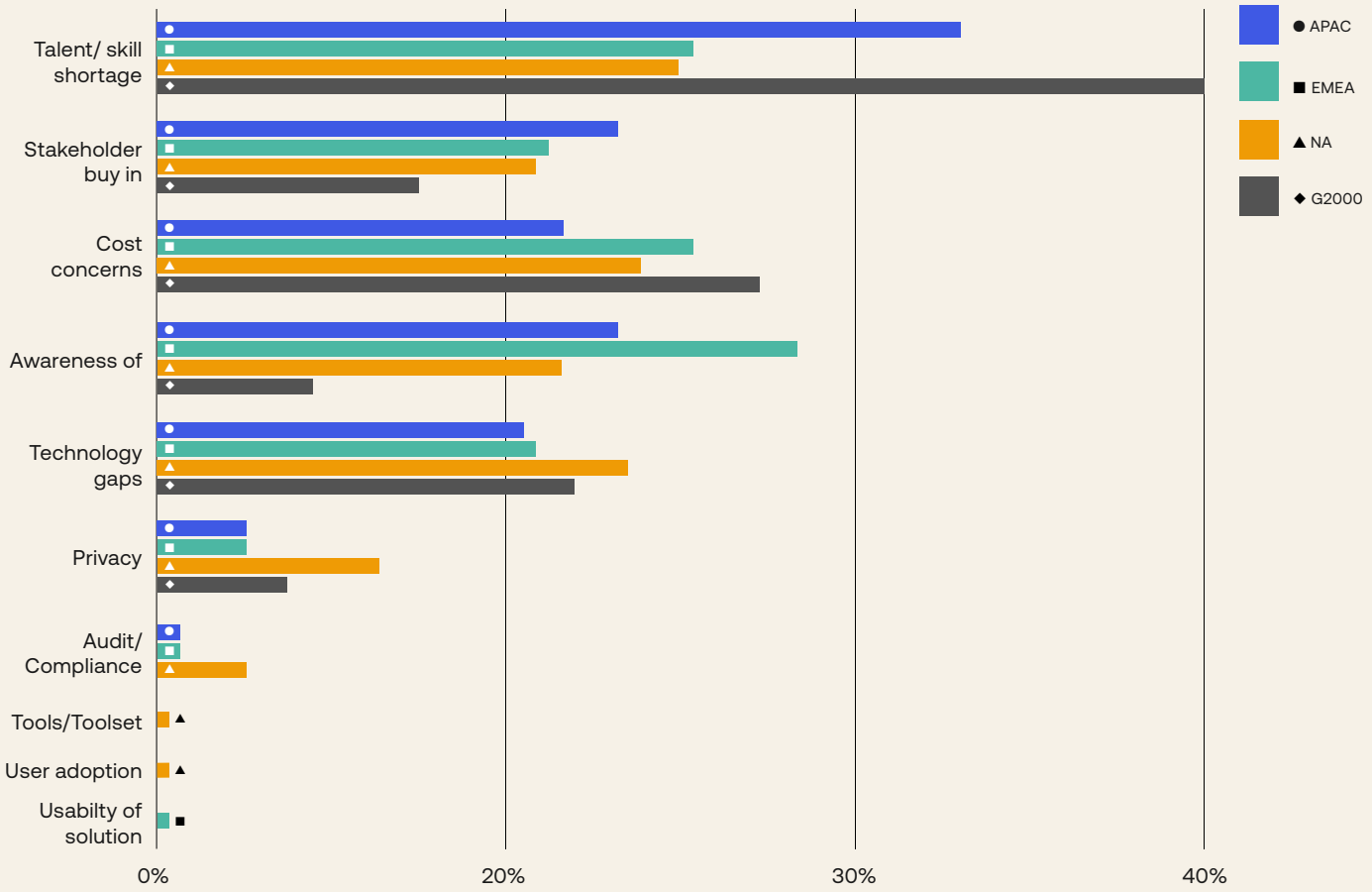
Regional Comparison Which of the following do you see as most important to integrate with an IAM solution to support Zero Trust security?



The Promises (and Challenges) of Zero Trust

Organizations around the globe have made significant progress in their Zero Trust initiatives since last year, but they still face a number of sobering challenges, like making significant investments to help their teams implement new technology. When we asked security leaders their top challenges to implementing specific Zero Trust initiatives, their answers were revealing. Talent/Skill shortage was listed as the top challenge in North America, APAC, and among the Global 2000; but in EMEA, Cost Concerns were judged to be an equivalent challenge, and Awareness (of a solution to support Zero Trust) was ranked even higher. Looking at each group's top three challenges, Talent/Skill Shortage and Cost Concerns were in everybody's top three, rounded out by Technology gaps in North America and APAC, and by Stakeholder Buy-In in EMEA and amongst the Global 2000.

Regional Comparison What challenges does your organization face in implementing a Zero Trust security model?



Top Challenges To Implement a Zero Trust Initiative Rank your org's top 3 challenges to implementing a Zero Trust security initiative (Rank 3)

APAC
1. Talent/Skill shortage to implement
2. Technology gaps
3. Cost concerns

EMEA
1. Talent/Skill shortage to implement
2. Stakeholder buy in
3. Cost concerns

North America
1. Talent/Skill shortage to implement
2. Technology gaps
3. Cost concerns

Global 2000
1. Talent/Skill shortage to implement
2. Stakeholder buy in
3. Cost concerns

All Respondents Global
1. Talent/Skill shortage to implement
2. Stakeholder buy in
3. Cost concerns

What Lies Ahead for Zero Trust

In light of the talent/skill shortage faced around the world, organizations need to find solutions that help them progress along their Zero Trust journeys without creating the need for additional budgets, head count, or training resources. They need to find solutions that integrate with their existing security ecosystems to extract the most value. And these solutions need to be easier and quicker to deploy, being able to scale as organizations grow and advance Zero Trust strategies. Stakeholder buy-in concerns may, in some cases, be a result of security departments not having full ownership over their IAM solutions, and possibly other security-related solutions in their environments. Other departments less invested in Zero Trust initiatives may be reluctant to reallocate resources to such efforts.

Within these challenges are opportunities. Organizations need to educate the departments they work with to build consensus and establish the need to advance Zero Trust initiatives. They need to look to their peers within other enterprises to find inspiration to help orchestrate their organizational approach. And, perhaps most importantly, they need to work with the right partners to implement Zero Trust solutions that they can leverage wherever they are on their journeys to find the specific solutions they need at each phase of the maturity curve that can be integrated with their existing security infrastructure to help them conquer remaining challenges.

Reiterating the Key Takeaways

First, Zero Trust isn't just a buzzword anymore—it has progressed in record time from an intriguing idea and security theory to a critical business imperative–and organizations around the world have their plans underway.

Second, there's not one straightforward path to achieving Zero Trust. Every company has a different starting point and priorities, requiring a different, specific set of solutions that ultimately needs to be integrated seamlessly into a simpler, more efficient, and effective security program.

Third, identity is what makes Zero Trust work. It's how you efficiently connect your complex solution, protect the new perimeter, balance security with usability, and keep your assets secure but accessible for your modern, remote workforce.

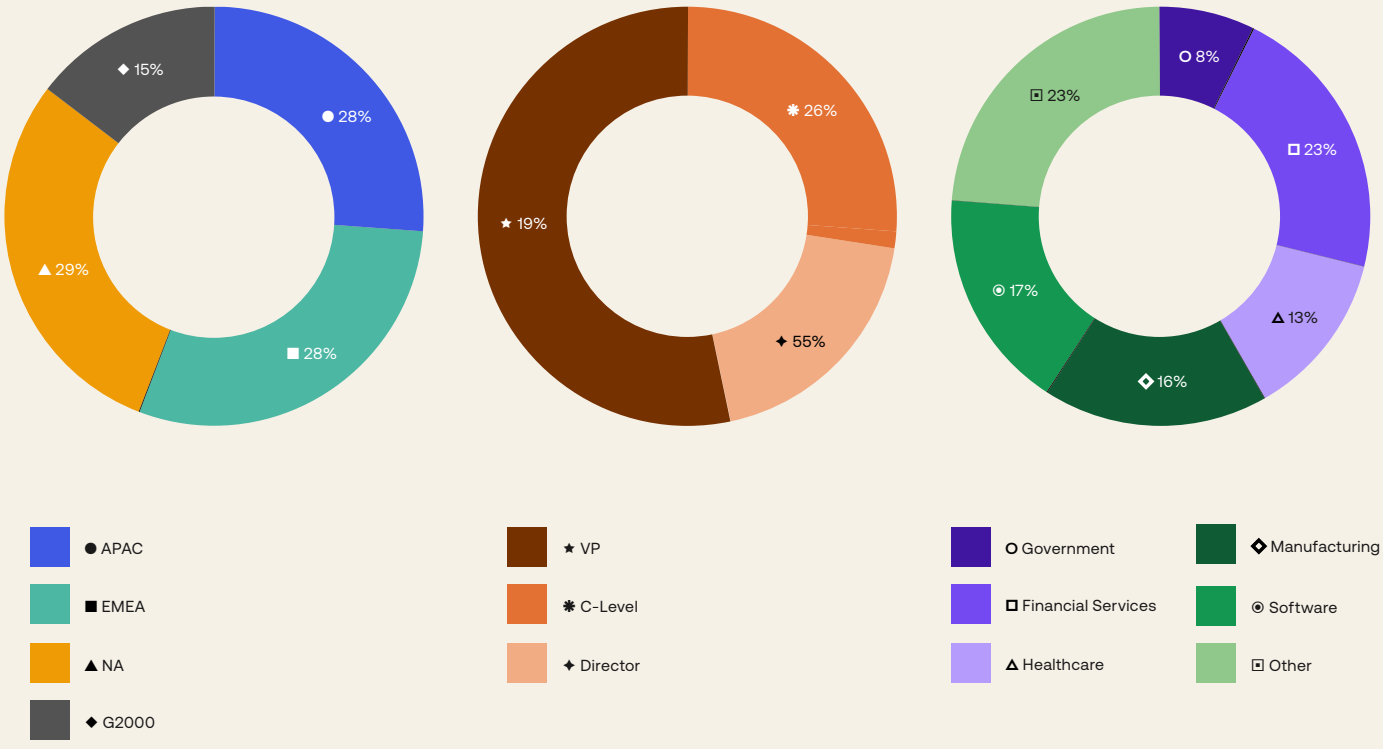
When you're ready to take action to find out where your organization is on the maturity curve, we have a resource that can help.

Survey Methodology

Commissioned by Okta, Pulse Q&A conducted a global survey of 700 security decision makers at the director level or higher across many organizations and industries. Decision makers were defined as people responsible for making technology purchasing decisions, from which our survey partner, Pulse, collected responses in early 2022. We refer to this survey as “our survey” and “survey” throughout, and refer to the people who responded on behalf of their organizations as “survey respondents” or “respondents.”

Who took the survey?

Here is a look at the 700 survey respondents and the companies they represent. For industry data, we focused on four industry verticals and three geographical regions, as well as the companies in the Forbes Global 2000. The security leaders that were surveyed were VPs, directors, or C-level executives, and we used percentages within each segment to normalize.



Whitepaper

The State of Zero Trust Security 2022

About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 16,400 organizations, including JetBlue, Nordstrom, Siemens, Slack, Takeda, and Teach for America, trust Okta to help protect the identities of their workforces and customers. To learn more visit okta.com. okta.com

okta

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871