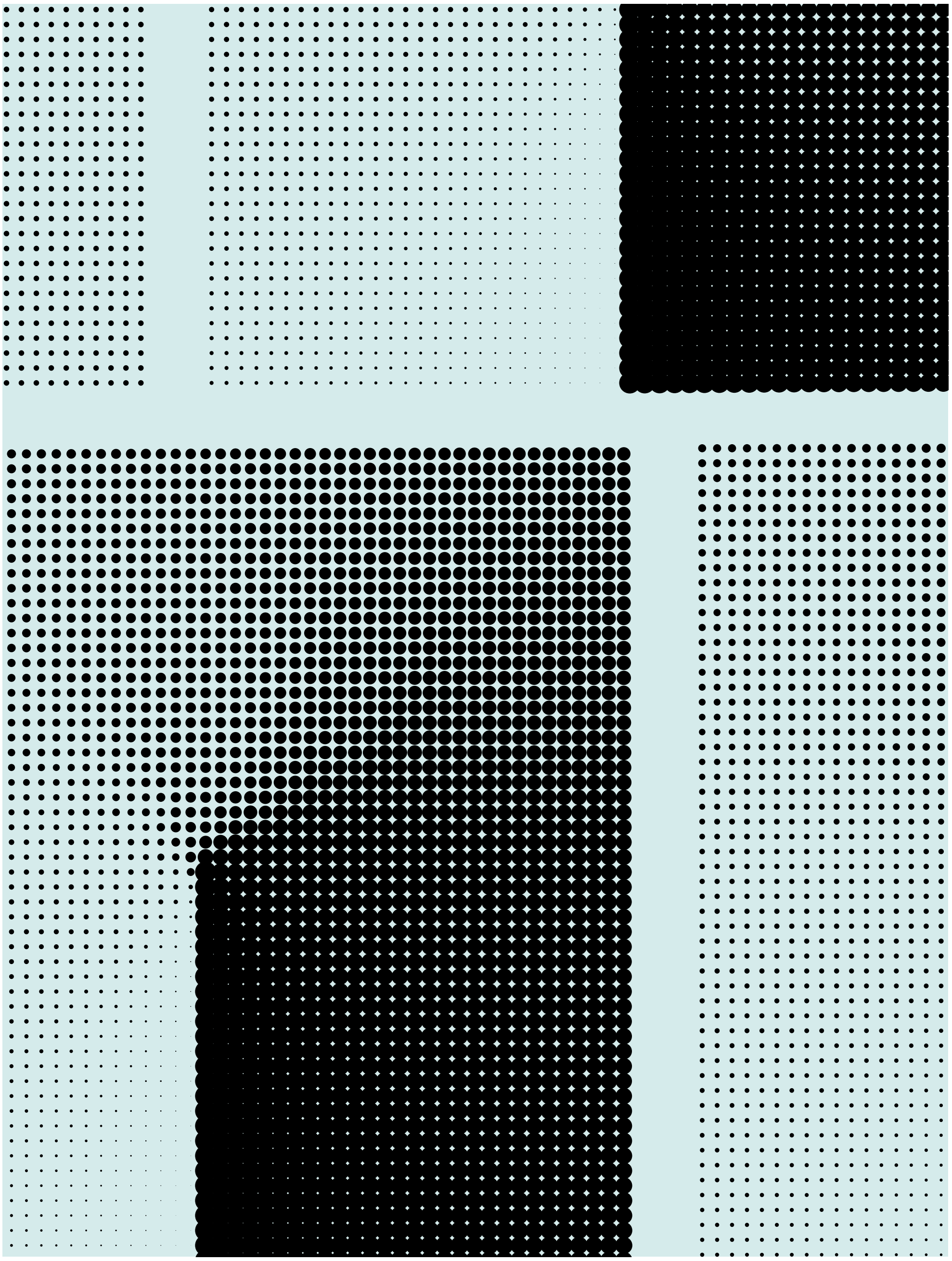
Whitepaper

June 2021

The State of Zero Trust Security 2021

Identity and access management maturity in global organizations

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



Contents

Zero Trust is Here to Stay

In recent years, “zero trust” has moved out of the realm of buzzwords to claim a permanent spot within modern information security. Since our 2020 report, several market factors drove a surge in zero trust security initiatives. Last year, the scope, scale, and perception of remote work each went through a massive shift. Now, 82% of company leaders plan to allow employees to work remotely at least part of the time after the pandemic, and 47% will allow them to permanently work from home full-time[1].

At the same time, identity-based attacks skyrocketed last year[2]. Almost 90% of web application breaches were caused by credential abuse and phishing was present in more than a third of all breaches — up from 25% last year[3]. Gaps in identity protection also introduce risks like the ransomware attacks that recently shut down schools and hospitals and affected the availability of fuel and food in the United States.

In order to better secure customers, employees, and businesses as mobile and cloud adoption skyrockets, the vast majority of technology and security leaders have moved past traditional security approaches. Rather than building a perimeter of protection around a “trusted” internal network vs. any “untrusted” external networks, they’re adopting the zero trust frameworks strongly recommended (and in some cases even mandated) by industry analysts and federal government agencies[4].

In today’s digital landscape, identity is the new perimeter. To meet the access and usability demands of modern users — and avoid becoming the next victim of a data breach or supply chain attack — organizations are moving towards a more robust and comprehensive security posture that’s centered around the zero trust principle of “never trust, always verify.” This requires companies to continually assess access privileges without adding friction for the user.

But no organization can achieve the promise of zero trust overnight. The best starting point for this journey is to nurture an identity-driven mindset that secures various user types regardless of their location, device, or network. To learn more about how organizations around the world are approaching zero trust today and where they’re headed over the next 12-18 months, Okta surveyed 600 global security leaders about their initiatives for this third annual report.

[1] Gartner, “**Gartner press release**,” July 14, 2020
[2] Federal Trade Commission, “**Consumer Sentinel Network Data Book**,” February 2021
[3] Verizon, “**Data Breach Investigations Report**,” May 13, 2021
[4] U.S. White House, “**Executive Order on Improving the Nation’s Cybersecurity**,” May 12, 2021

Top five security takeaways

The pandemic is fueling zero trust prioritization.
More than three-quarters (78%) of companies around the world say that zero trust has increased in priority and nearly 90% are currently working on a zero trust initiative (up from just 41% a year ago).

Zero trust adoption is on a tear.
This year, organizations dramatically accelerated their journey towards identity and access management (IAM) maturity and plan to progress by leaps and bounds by the end of next year. Every single recommended zero trust project across the identity maturity curve will have reached at least 25% adoption by 2023. That number jumps to nearly 40% for Forbes Global 2000 companies.

Identity is the new perimeter.
When asked to rank core zero trust requirements, the #1 priority was "people" for one-third of all organizations, followed by devices and data. Leading companies are adopting strong authentication across resources for employees, customers, partners, contractors, and suppliers, while moving from network-based to more individualized device-based access decisions.

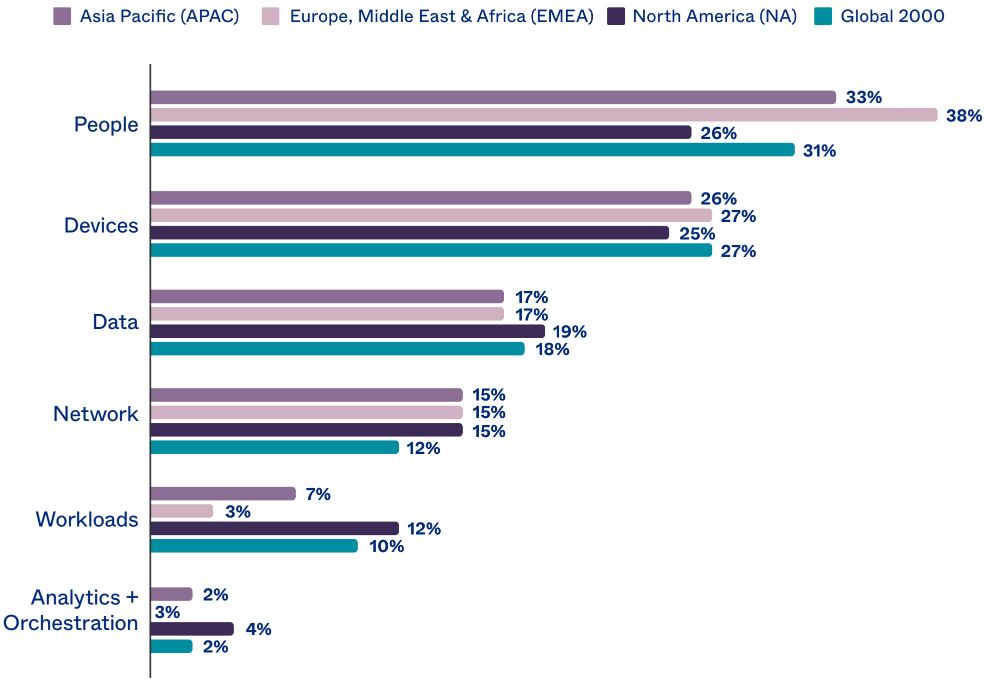
Organizations are upping their security game.
As IT and security leaders shift their collective focus beyond quick wins, the most common zero trust projects organizations are prioritizing over the next 12-18 months are those further along the IAM maturity curve. More than a third of all companies are prioritizing SSO and MFA for external users, context-based access policies, and automated account provisioning and deprovisioning.

Security posture varies across key verticals.
Nearly a third (30%) of healthcare organizations indicate that zero trust is now a top priority due to the pandemic, as compared with 17% globally. Amongst financial services businesses, 94% already have a zero trust plan in place or will have one in the next 12-18 months, compared to less than half in 2020. Meanwhile, the software industry has some catching up to do, but the good news is that it's ready. Almost four in five companies plan to adopt a zero trust security initiative by the end of next year, compared with just 9% that have an initiative in place today.

Identity: The Cornerstone of Zero Trust

With identity as your company's new perimeter, IAM becomes the central control point across users, devices, data, and their networks. In fact, Gartner recently singled out "identity-first" security as one of the top security and risk trends this year[5], since it provides visibility and control over which users have access to what resources, and minimizes risk such as compromised credentials or incorrect provisioning or authentication.

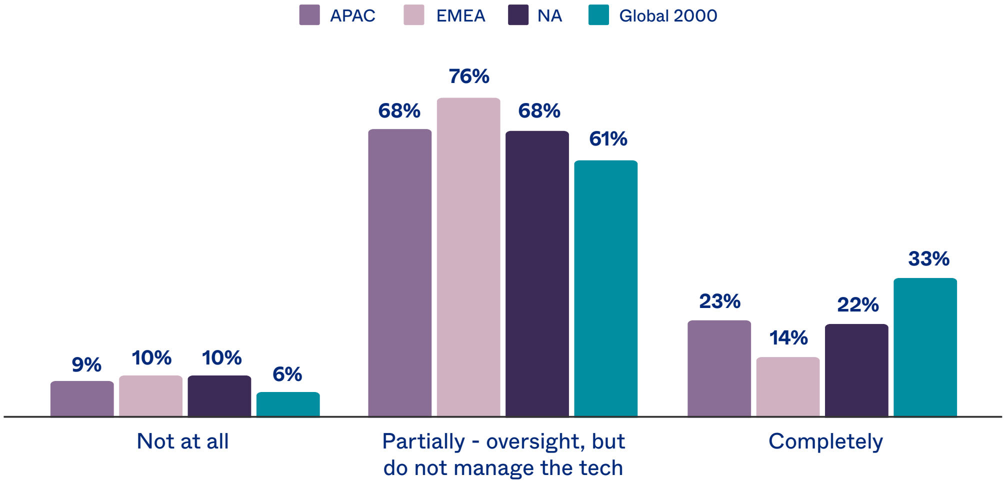
Rank core zero trust requirements in terms of priority for your organization



Given how interwoven identity and security are, zero trust strategies usually benefit from tight partnership between IT and security teams when it comes to IAM. Our research showed that security teams are more likely to own IAM technologies at the world's leading organizations (Forbes Global 2000) than in smaller companies, although more security teams worldwide are providing at least partial oversight of IAM. In EMEA and APAC particularly, we saw the percentage of companies where security at least partially oversees IAM increase over 11% year-over-year. And in APAC, the amount of security teams that completely own IAM increased over 4x since last year.

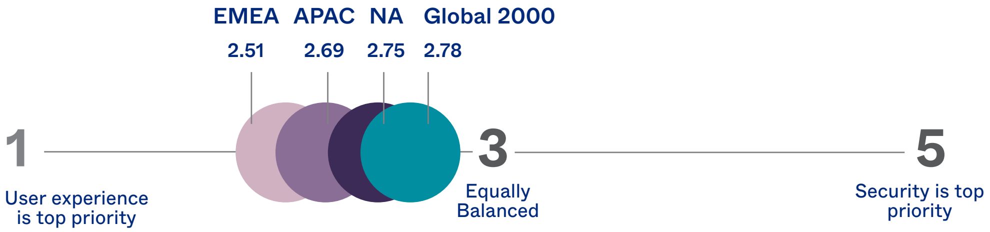
[5] Gartner, "**Top Security and Risk Trends for 2021**," April 5, 2021

To what extent does the security department own identity and access at your organization?



These teams must also work to strike the right balance between usability and security, while constantly keeping at least one step ahead of today's threats. Most respondents were confident they could optimize the user experience while moving to higher assurance factors and context-based access policies.

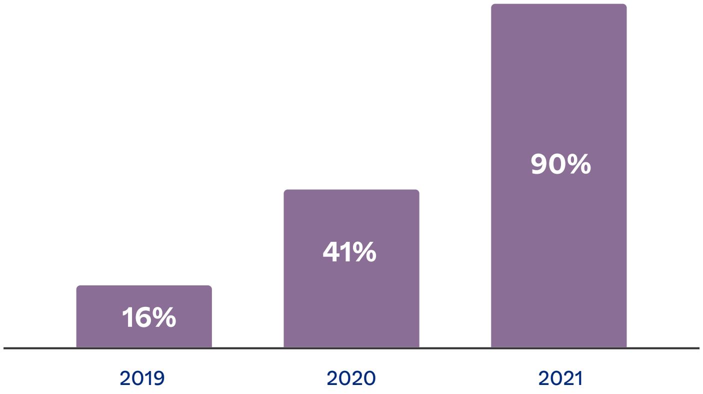
How do you weigh security in relation to usability at your organization?



The rise of identity-driven security

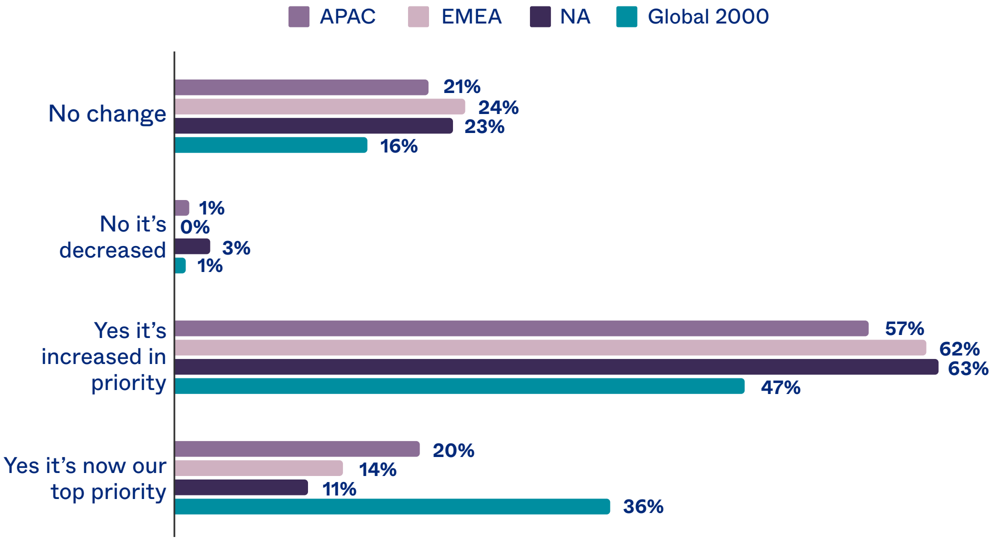
In observing how zero trust and IAM prioritization have shifted over the last year, it's clear that the pandemic supercharged organizations' move towards zero trust and many teams were allocated more budget to get there. Globally, about 90% said they're working on a zero trust security initiative today or plan to start one in the next 12-18 months, compared with just 41% in 2020.

Year-over-year comparison: Does your organization have a defined zero trust security initiative today or that you're planning to start on in the next 12-18 months?

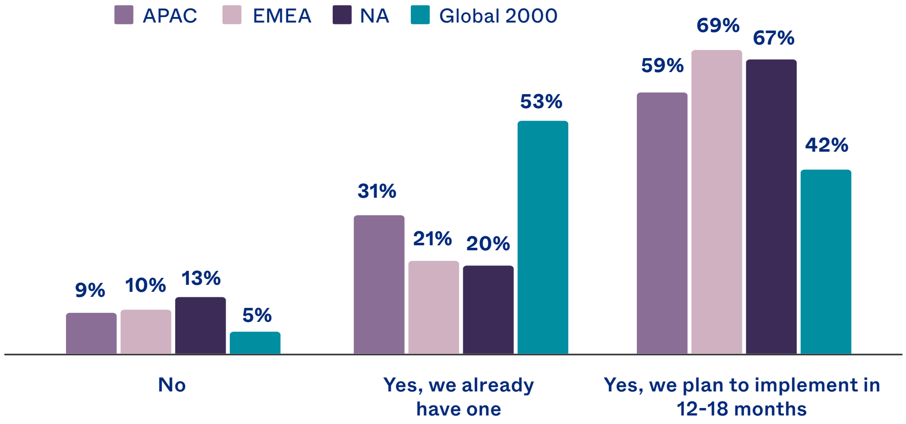


More than three-quarters of respondents believe zero trust is more of a priority due to COVID-19 and the remote work economy. In fact, 36% of Global 2000 companies and 30% of healthcare organizations indicated that zero trust security is now a top priority due to the pandemic, as compared with 17% globally.

Regional comparison: Has COVID-19 and the remote working economy accelerated zero trust as a priority at your organization?



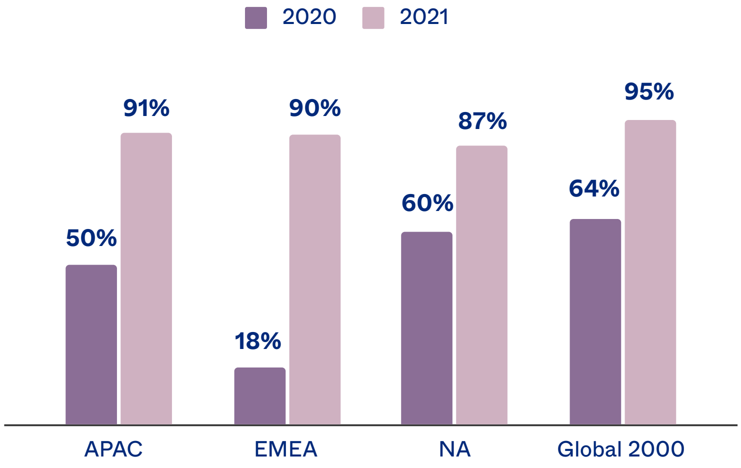
Regional comparison: Does your organization have a defined zero trust security initiative today or that you're planning to start on in the next 12-18 months?



Global 2000 organizations continue to lead the way in developing a robust security posture, with more than 50% of these respondents already having a zero trust security initiative in place, and another 42% planning one in the next 12-18 months. Perhaps unsurprisingly, we found that when the security team completely owns IAM at a Global 2000 company, they are more likely to already have a defined zero trust initiative in place — at 70% vs. 53% of companies where security is less involved with IAM.

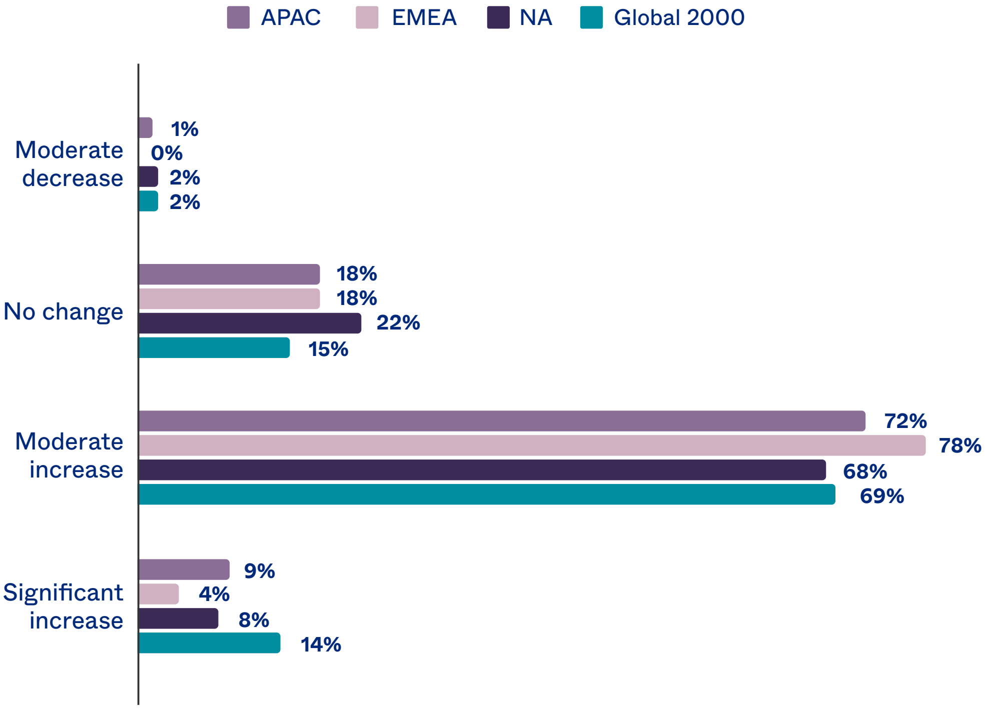
More regulated industries, like financial services, are also well along in their zero trust adoption, with 94% saying they already have zero trust in place or or have aggressive goals to get there. And companies in EMEA saw the largest jump in zero trust initiatives over the past year — from just 18% implementing or planning zero trust in 2020 to 90% in 2021. 21% of those companies say they already have zero trust security in place.

Regional year-over-year comparison: Does your organization have a defined zero trust security initiative today or that you're planning to start on in the next 12-18 months?



Across regions and industries, over three-quarters of organizations have grown their budget for zero trust security initiatives despite the hardships of the past year. 83% of the world's largest organizations indicated a budget increase, with 14% even reporting a "significant" increase.

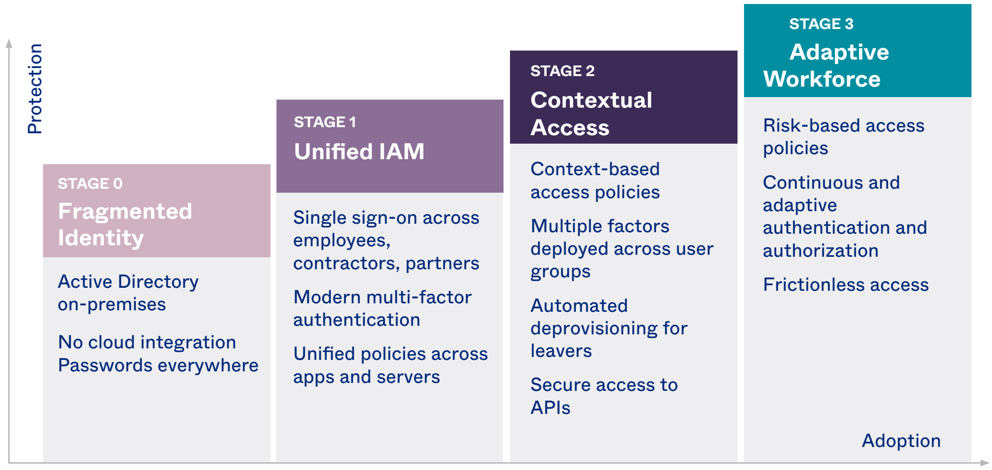
How has your budget for zero trust changed (if at all) in the past 12 months?



The Evolution of Zero Trust Maturity: 2021

Now that we've reviewed how companies are thinking about zero trust at the macro level, let's explore some of the specific zero trust projects they're actually pursuing, through the lens of Okta's IAM maturity curve. As organizations work to implement a zero trust architecture built around identity-driven security practices, we find they roughly follow four primary stages of maturity:

Identity and Access Maturity Curve

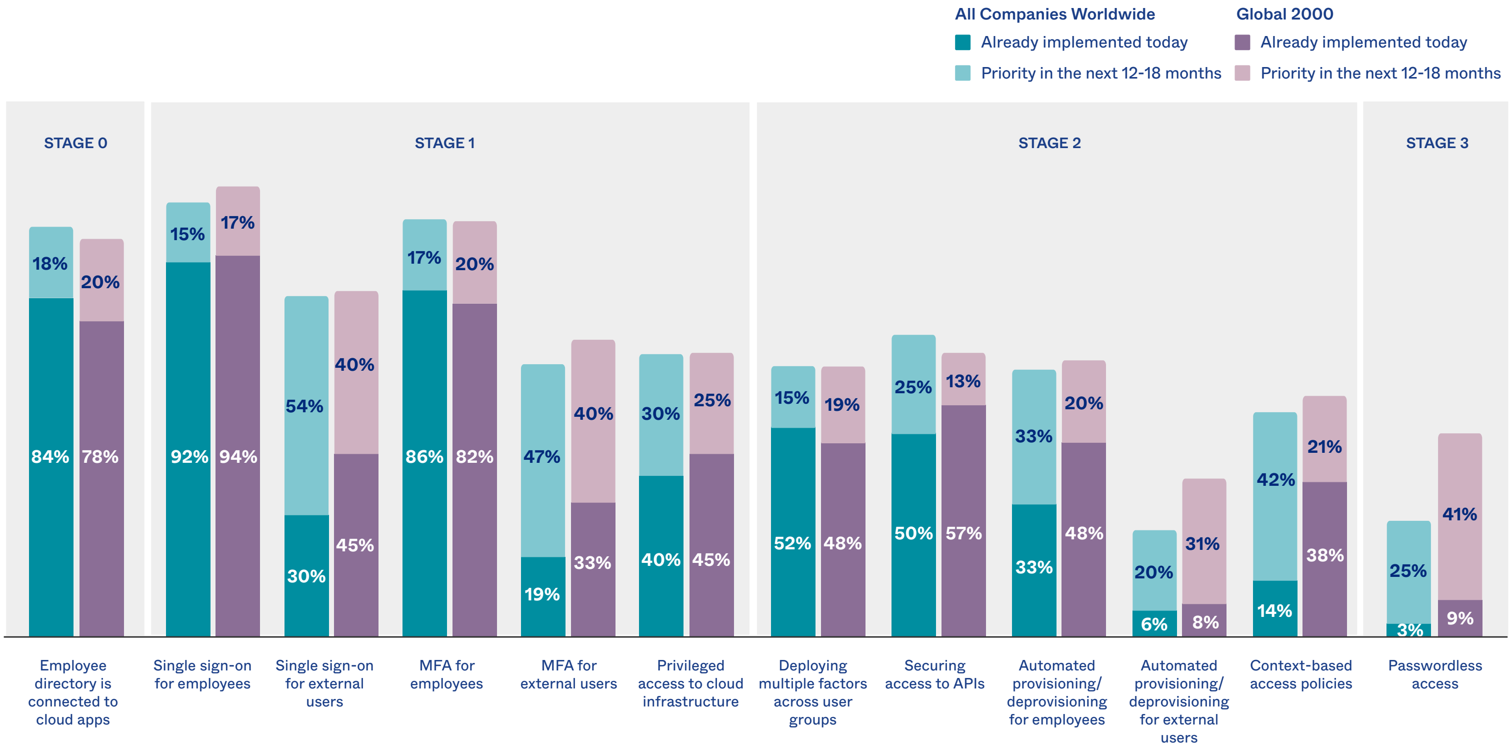

Protection
STAGE 0
Fragmented Identity
Active Directory on-premises
No cloud integration
Passwords everywhere
STAGE 1
Unified IAM
Single sign-on across employees, contractors, partners
Modern multi-factor authentication
Unified policies across apps and servers
STAGE 2
Contextual Access
Context-based access policies
Multiple factors deployed across user groups
Automated deprovisioning for leavers
Secure access to APIs
STAGE 3
Adaptive Workforce
Risk-based access policies
Continuous and adaptive authentication and authorization
Frictionless access
Adoption

Zero trust projects span everything from the types of resources an organization manages, to how they provision and deprovision users, which authentication methods they deploy, and more. Companies with a fragmented approach to identity really haven't started down the path towards zero trust yet. During Stage 0, they might begin to embrace cloud technologies, but don't yet integrate those solutions with an IAM platform or on-premises resources.

At Stage 1, teams start wrapping their arms around a unified IAM ecosystem and eliminating poor password hygiene by implementing single sign-on (SSO) and multi-factor authentication (MFA) for employees to access key resources. Moving into Stage 2, businesses adopt additional security best practices by extending access controls to other resources such as their APIs, and also using rich context and diverse factors to better inform authentication decisions. Once companies reach Stage 3, they've successfully adopted a full risk-based authentication approach to zero trust, including passwordless and continuous access solutions.

Unlike last year, when the majority of the companies we surveyed were still focused on Stage 0 or Stage 1 projects, this year all 100% of respondents expected to be firmly in Stage 1 by 2022. Impressively, each of the 12 projects on the maturity curve will have reached 25% adoption by the end of next year. The majority of Global 2000 businesses are already well on their way, moving at a steady clip from Stage 0 to Stage 3.

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?



In North America, companies are slightly behind their peers in other parts of the world, with only 74% having already connected their employee directory to their cloud apps (Stage 0). However, the majority do plan to accomplish this in the next 12-18 months. Meanwhile, each project in Stage 1 will have been adopted by two-thirds of all APAC organizations by the end of 2022.

93% of North American companies aim to complete Stage 0 in 2022

Stage 1 adoption will reach >67% of APAC companies by 2023

Zero trust projects that can expect the most progress in the years to come include SSO and MFA for external users, context-based access policies, and passwordless access. Global 2000 companies are especially focused on planning for these zero trust capabilities as well as projects much further along the maturity curve, such as automating the provisioning and deprovisioning of external user accounts.

Global 2000 Planned Zero Trust Adoption

85%	External SSO
73%	External MFA
59%	Context-based access
50%	Passwordless access
39%	Automated external provisioning/deprovisioning

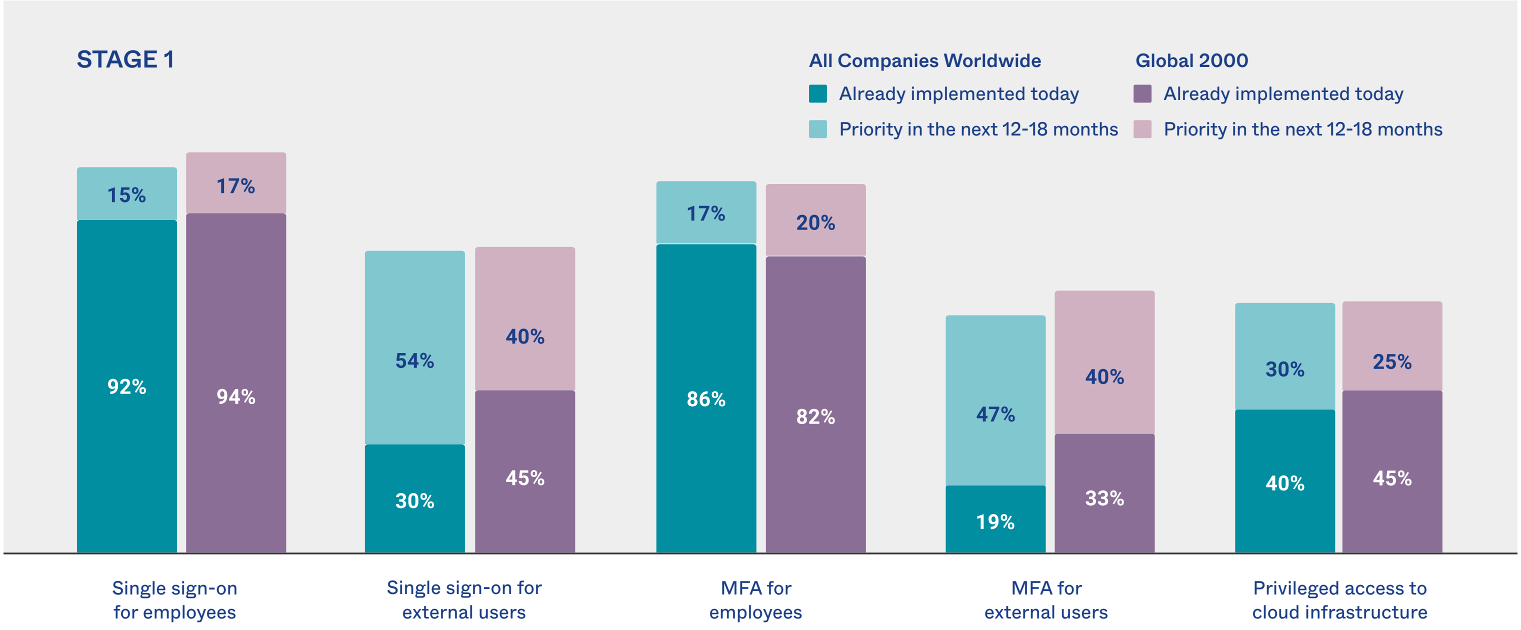
Stage 1: Unified IAM

To assess progress within the unified IAM stage, we asked whether businesses require SSO for employees or external users, are implementing MFA, and/or are managing privileged access to cloud infrastructure. By adding multiple layers of security to their authentication mechanisms, Stage 1 organizations are finding effective ways to give the right people access to the right resources, with minimal friction.

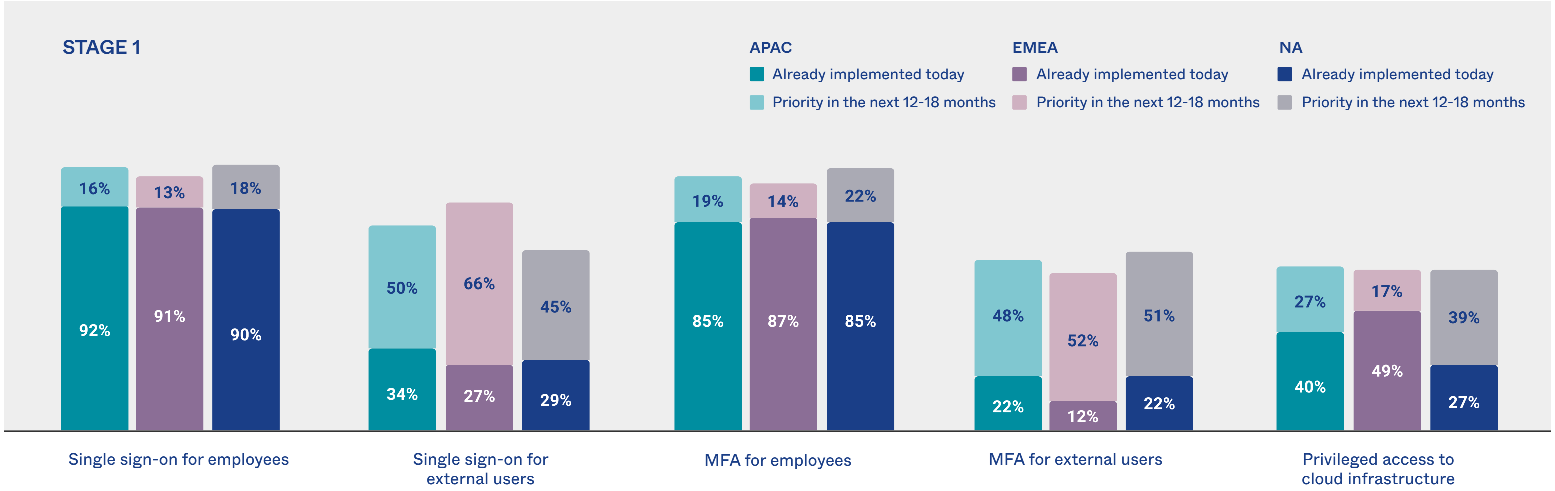
While at least three of the five projects in Stage 1 have been adopted by more than 40% of companies today, in the next 12-18 months, all five projects will have been implemented by at least two-thirds of all companies (for Global 2000 companies, adoption trends even higher, at 70% across projects).

Companies in EMEA and APAC are prioritizing tasks that secure access to external users like partners, contractors, and suppliers. Over the next year or so, 66% and 50% (respectively) of companies in these regions expect to kick off SSO projects, and 52% and 48% will pursue MFA projects. In North America, the biggest growth in Stage 1 will involve implementing MFA for external users — which is expected to increase to 51% of companies.

Stage 1 at All Companies Worldwide vs. 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?

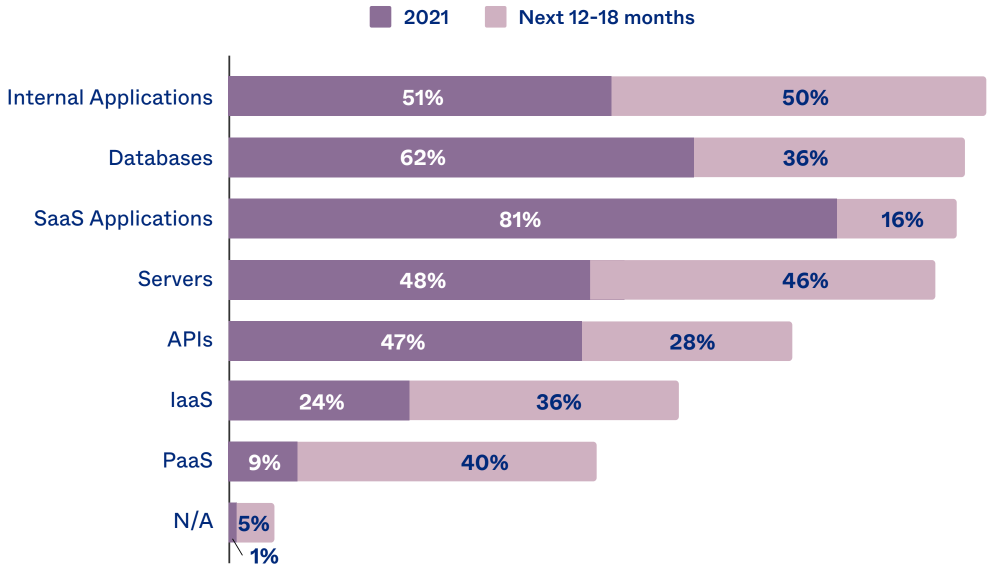


Stage 1 at EMEA, APAC & North American Companies: Which projects has your organization already implemented as of today, and which are a priority for your organization in the next 12-18 months?



In terms of creating unified access policies by extending SSO and MFA to apps, servers, and more, adoption varies across specific resource types. Since 81% of companies around the world have now extended SSO and MFA to their SaaS applications, most are starting to add these protections to additional resources, namely their internal applications, servers, databases, and APIs. While IaaS and PaaS aren't a current focus, more companies do plan to prioritize both of these resource types over the next 12-18 months.

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



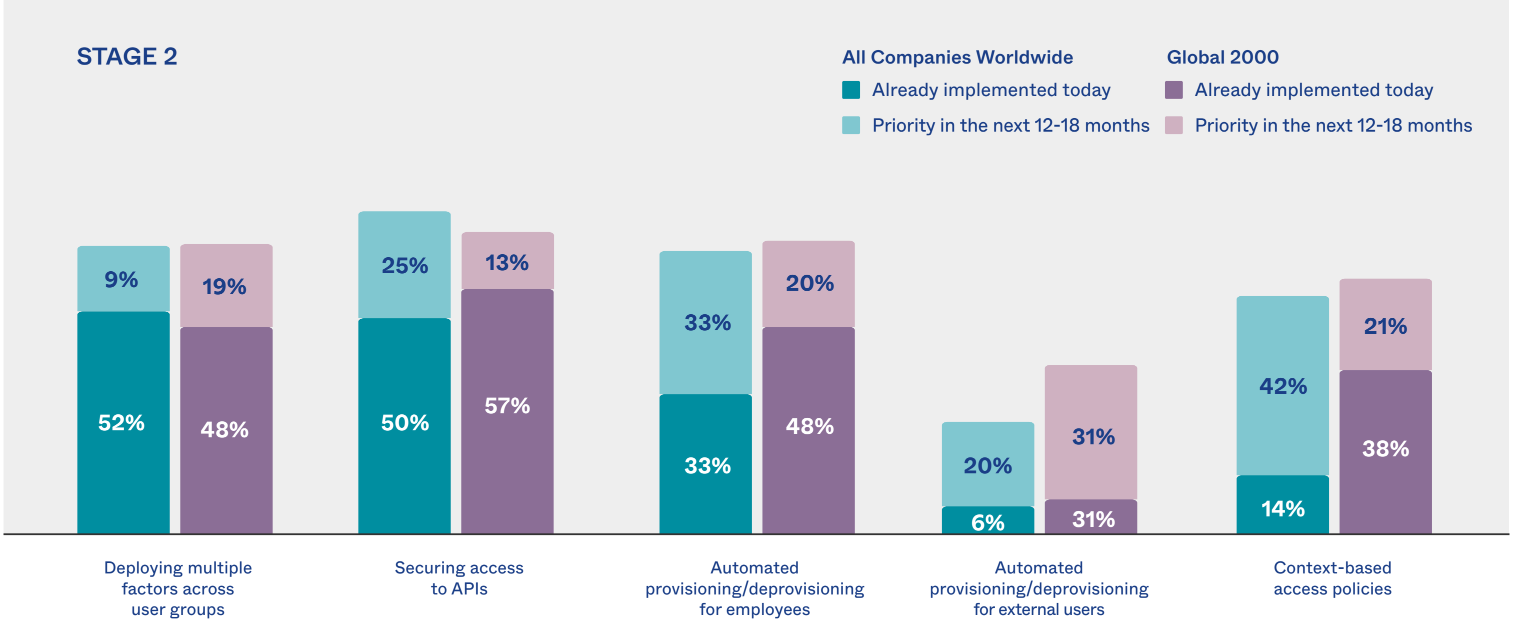
Stage 2: Contextual access

To evaluate Stage 2, we asked respondents whether their organizations deploy safeguards such as multiple factors across user groups, secure access to APIs, automated account provisioning and deprovisioning for employees and/or external users, or context-based access policies.

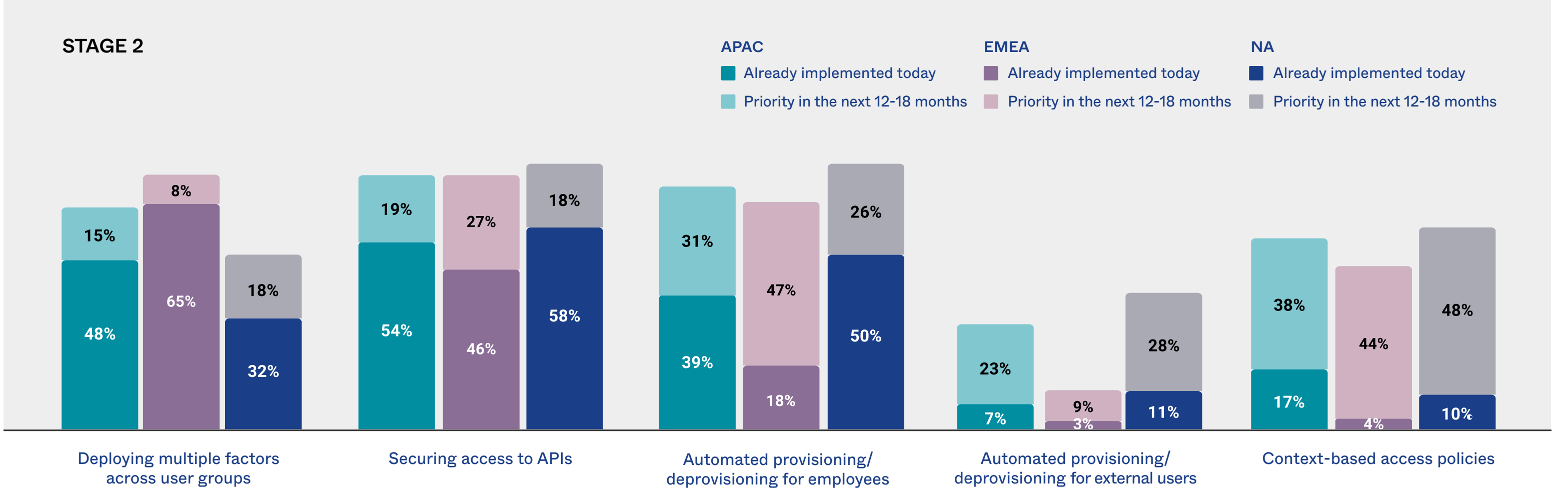
Globally, companies plan to make strides across Stage 2 projects, with adoption levels over the next year or two ranging from 26% to 75%. In EMEA and APAC, four out of these five projects will have been implemented by nearly half of companies by 2023, including a jump of 40% for EMEA in projects surrounding context-based access policies. Over this same timeframe, two of these projects (securing access to APIs and automating provisioning/deprovisioning) are expected to reach >70% adoption amongst APAC organizations.

While, last year, only 26% of North American businesses had implemented API security, that number more than doubled (58%) in 2021. It's no surprise to see this focus on securing APIs, since, as digital business models evolve, organizations require seamless connections with external supply chains, emerging data sources, and third-party technology systems. In this digitally connected environment, API security is absolutely critical.

Stage 2 at All Companies Worldwide vs. 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?



Stage 2 at EMEA, APAC & North American 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?



Three most adopted Stage 2 projects worldwide by 2022

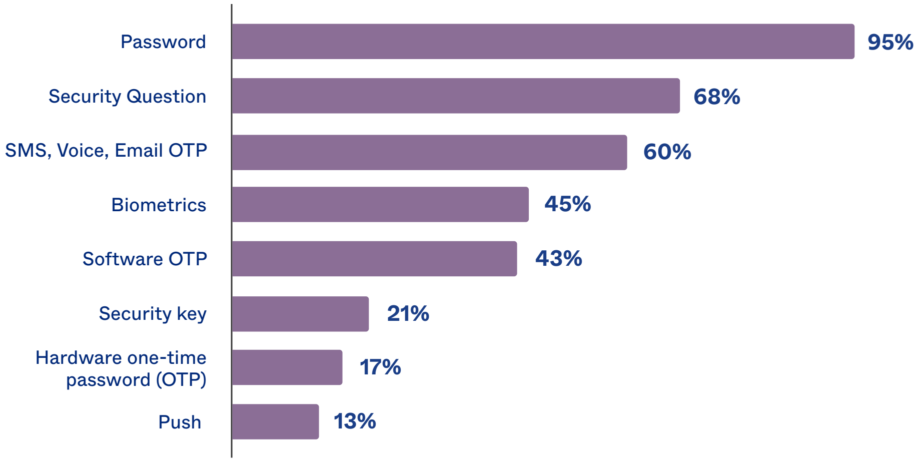
75%	Securing access to APIs
67%	Deploying multiple factors across user groups
66%	Automating provisioning & deprovisioning of employees

Automated provisioning for both internal and external users shows the most room for growth, especially in APAC and EMEA, as well as across software and healthcare organizations. In particular, few companies have yet recognized the opportunity to improve their security posture through external user provisioning, which can limit the risk of allowing access to critical resources by partners and contractors even after they stop working with the company. However, this is the lowest priority along the maturity curve — just 6% of companies have automated this task thus far, and a mere 20% are making it a priority over the next 12-18 months.

Security factors

Since 52% of all respondents indicate they've already implemented multiple factors to better inform authentication decisions across user groups, we decided to find out what their most-used security factors are.

Select the security factors your organization is using currently.



Impressively, 45% of global companies (over 50% in financial services and software) say they use biometrics, a high assurance factor. That said, the majority of companies still rely on low assurance factors, such as passwords and security questions that can be stolen through social engineering (at 95% and 68% adoption respectively). In the software industry, 71% of respondents noted that they use SMS, voice, and email one-time passwords (OTP). This enables step-up authentication based on the information sent to the user device.

Top 3 Security Factors

Healthcare	Financial Services	Software
1. Password	1. Password	1. Password
2. Security Question	2. Security Question	2. **SMS, Voice, Email OTP**
3. SMS, Voice, Email OTP	3. **Biometrics**	3. Security Question

Organizations looking to meet high levels of assurance should adhere to the National Institute of Standards and Technology's digital identity guidelines[6], which indicate that many of the common factors used by organizations today increase the probability of account takeovers.

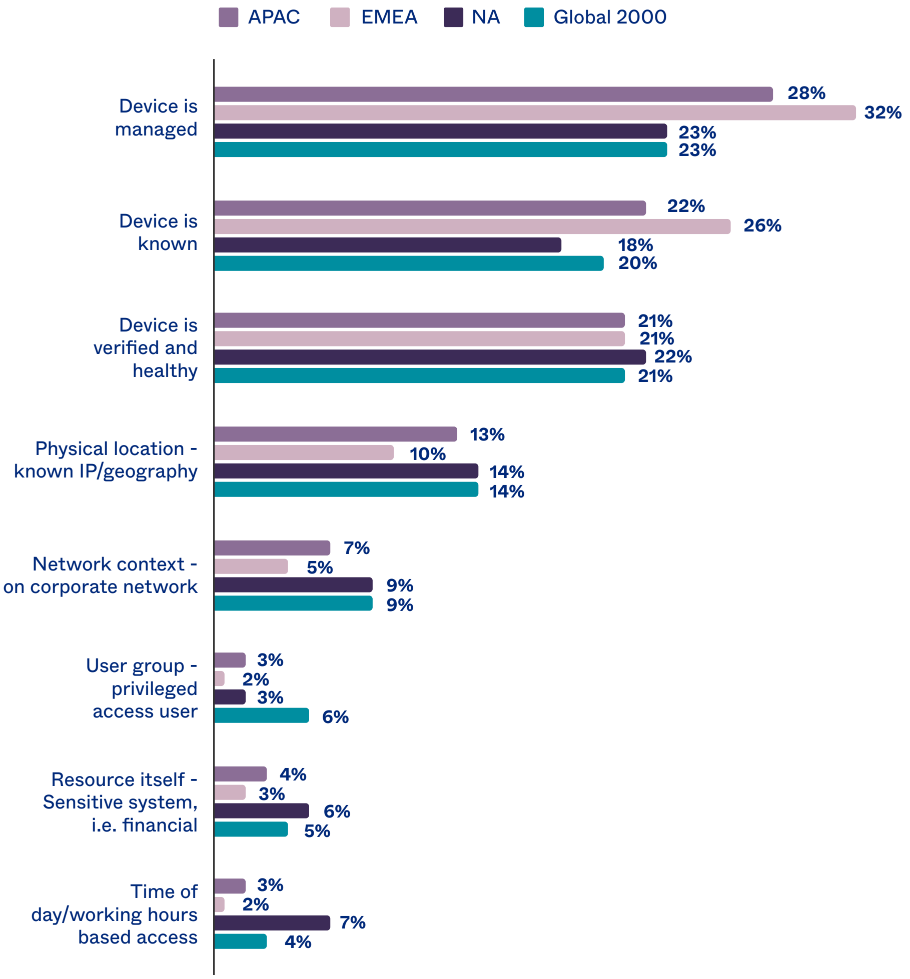
[6] NIST, "**Digital Identity Guidelines**" March 2, 2020

Amongst Okta's own customers, we've noticed that higher assurance factors like push notifications are on the rise compared to more brittle two-factor methods of authentication. Last year, our clients relied less on SMS and security questions and more on higher assurance factors. In the six months prior to the pandemic, use of Okta Verify grew by 28%, while from February to October 2020, it jumped 184%[7].

Access policies

Another key zero trust strategy is ensuring that people get the right level of access in the right context, so we also asked how teams are making their MFA policies context-aware. This involves setting access policies that can better assess users' devices, networks, locations, or the applications they're attempting to access. It's one area where respondents are clearly increasing their focus — up 40% in EMEA, 38% in North America, and 20% in APAC.

What are the top 3 most critical factors you think about when controlling and approving access to your internal resources?



[7] Okta, "**Businesses at Work Report 2021**," January 28, 2021

Another trend we noticed, both pre-COVID and over the past year, relates to how organizations make access decisions. This year, even more companies moved away from basing access grants on whether a user is accessing resources from a corporate network — from 21% in 2020 down to 7% in 2021. Interestingly, organizations are placing even less emphasis (from 28% last year to 3% currently) on a person's privileged access user group.

In line with established zero trust best practices, respondents told us the more important factors they use in access decisions are related to device posture, such as whether a user's device is managed, known, and/or verified as healthy. The most critical attribute in approving access to internal resources is confirming if the user's device is managed.

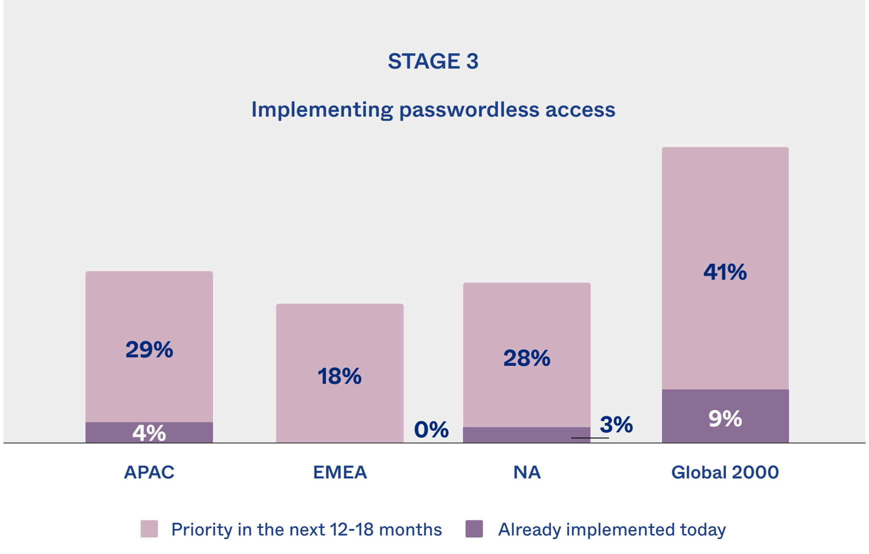
While this was likely the primary context organizations relied on prior to the pandemic, many IT staff had to rush to enable the workforce with whatever devices were available at the onset of the lockdown in 2020. It's probable that many chose "device is known" as their next best attribute in this situation. Increasingly, organizations are now looking to whether these known devices are verified and healthy: two key contexts for enabling zero trust.

Stage 3: Adaptive workforce

Going beyond the core zero trust projects outlined in Stages 0-2, one way that organizations can increase flexibility is by embracing passwordless access using high assurance factors. Given the inherent insecurity of passwords — particularly since 73% of online accounts use duplicated passwords[8] — credential harvesting tends to be the most fruitful tactic for today's threat actors. More than 60% of all data breaches involve stolen or weak credentials[9], and the best way to protect against compromised user information is by securing authentication through continuous assurance.

Relying on passwords alone leaves organizations vulnerable to password spraying and credential stuffing. Multiple high assurance factors such as factor sequencing, biometric-based logins through WebAuthn or U2F security keys can mitigate these risks and provide the flexibility for passwordless authentication in scenarios where a password isn't required. This is a big help in preventing account takeovers, so it is promising to see passwordless adoption picking up steam.

Stage 3 Across Segments: Which projects has your organization already implemented as of today, and which are a priority for your organization in the next 12-18 months?



This year, more than a quarter of companies say they either have, or will soon implement, passwordless access options for their users. Amongst Global 2000 organizations, 9% have passwordless access today, while 41% plan to by the end of 2022, and in the financial services industry, adoption will jump from 1% to 43%. In North America, we're seeing uptake go from 3% to 28% of companies, while EMEA and APAC businesses expect to shift from minimal adoption to 18% and 29%, respectively.

[8] TeleSign, "**2016 Consumer Account Security Report**," November 16, 2016
[9] Verizon, "**Data Breach Investigations Report**," May 13, 2021

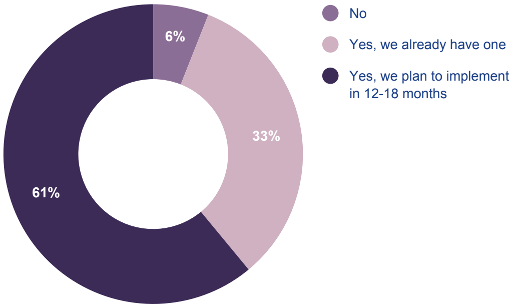
Zero Trust Adoption Varies by Industry

Every industry (and every company, for that matter) tends to follow a slightly different route to zero trust. In this year's study, we took a deeper dive into three key verticals — finance, banking, and insurance (financial services), healthcare and social assistance, and software — to better understand how these organizations' unique needs might influence their zero trust adoption.

Financial Services

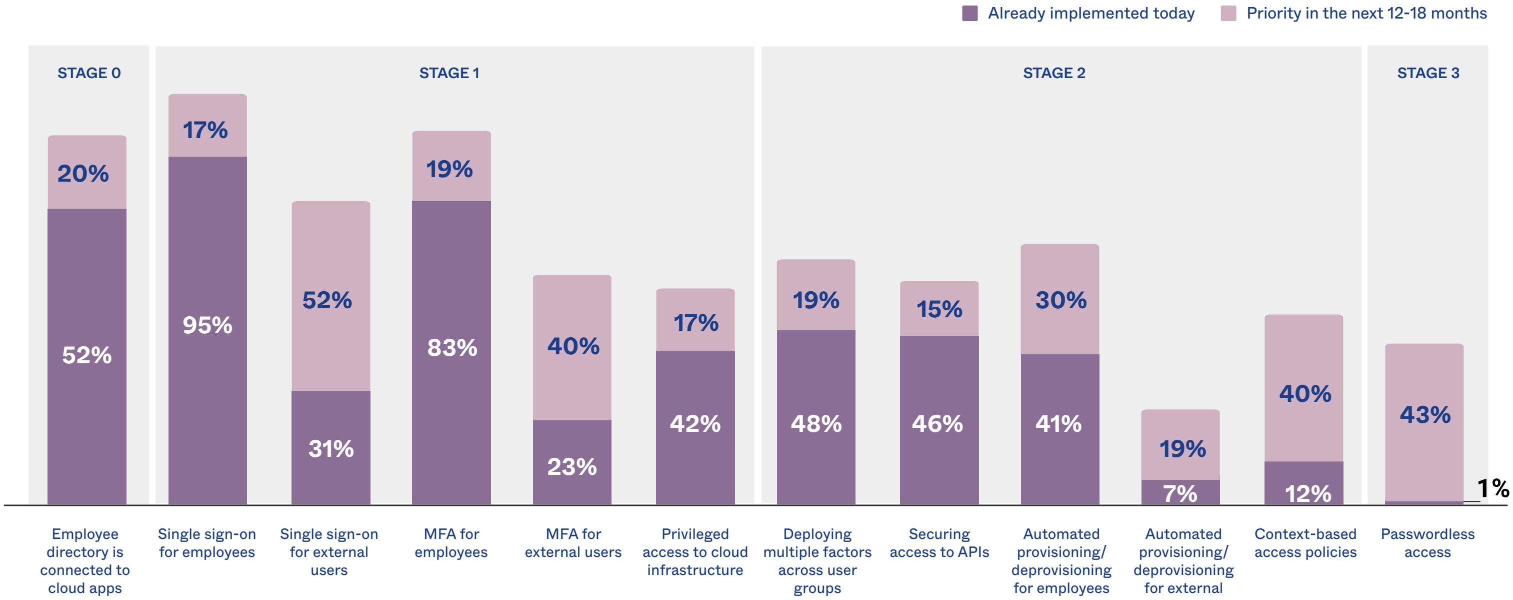
Financial Services: Does your organization have a defined zero trust security initiative today or that you're planning to start on in the next 12-18 months?

Chart 8



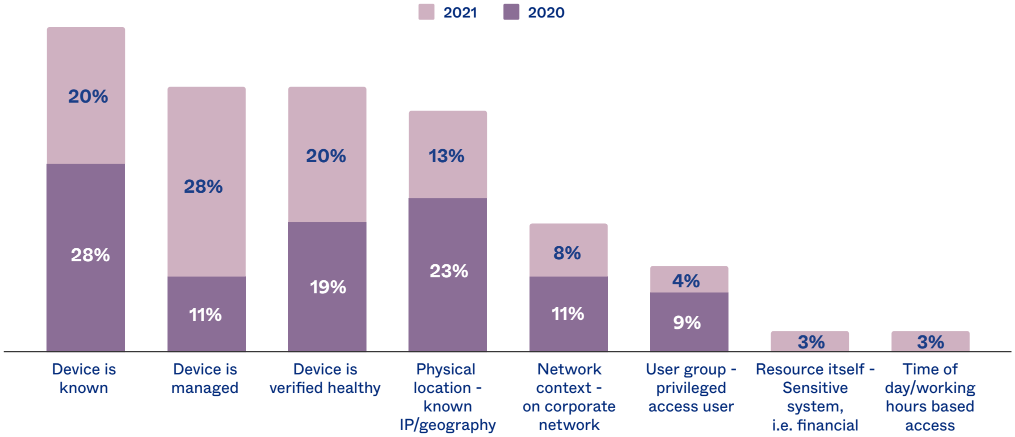
Within financial services, we saw a large year-over-year increase in the number of companies that told us they already have a zero trust initiative in place or plan to implement one in the next 12-18 months (from 48% in 2020 to 94% in 2021). And while less than half of companies in this industry have implemented the majority of projects on the maturity curve today, they definitely plan to advance these efforts over the coming years. By 2023, all five of the projects in Stage 1 and at least four of the five projects in Stage 2 will be underway at more than half of all financial services companies.

Financial Services: Which projects has your organization already implemented as of today, and which are a priority for your organization in the next 12-18 months?



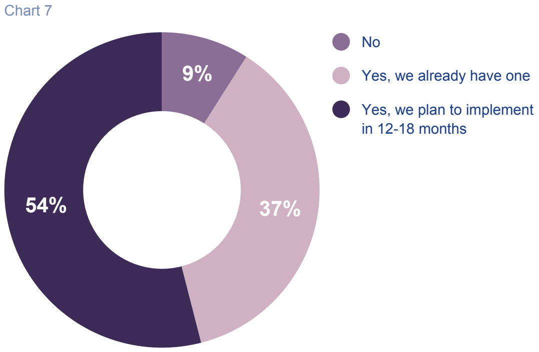
Going forward, their top areas of focus are SSO for external users (from 31% to 52%), context-based policies (from 12% to 40%), and passwordless access (from 1% to 43%). When it comes to access policies, we also saw a big jump in how many financial companies considered “device is managed” to be a critical factor in controlling and approving access to internal resources.

Financial Services: What are the top 3 most critical factors you think about when controlling and approving access to your internal resources?



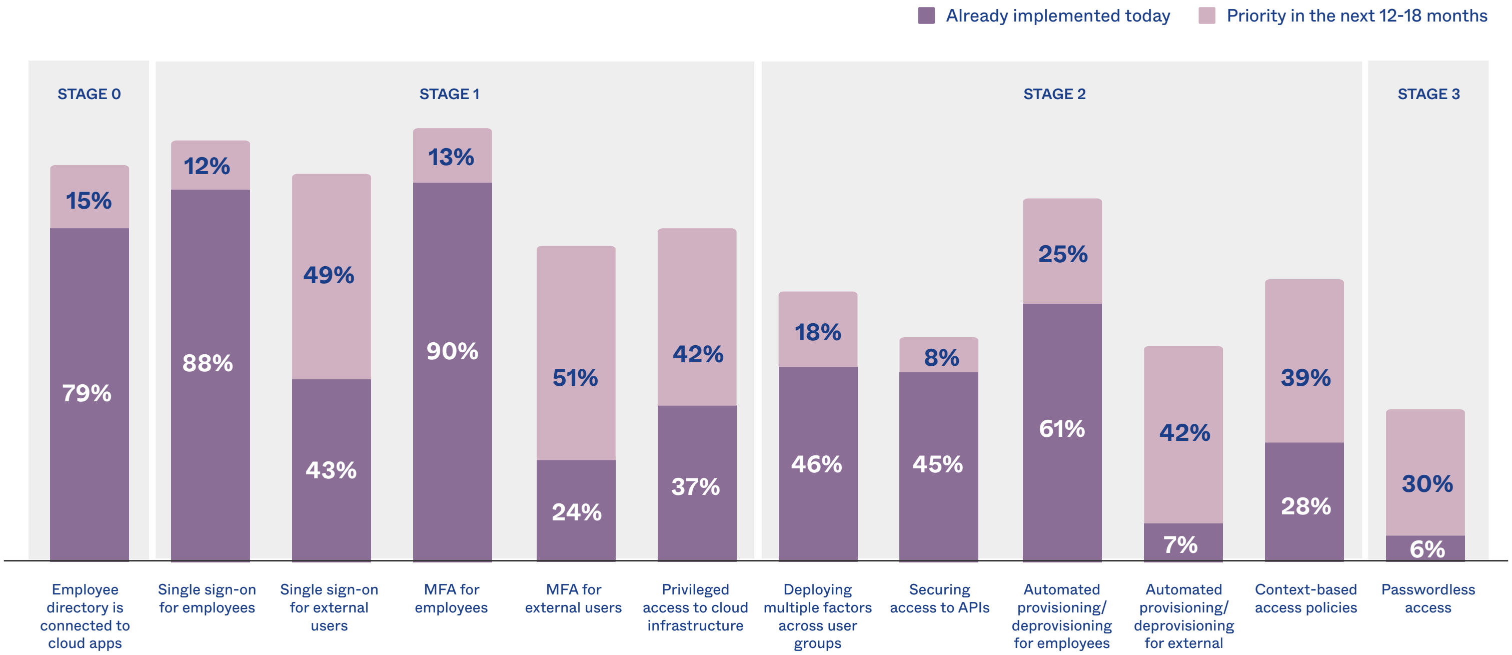
Healthcare & social assistance

Healthcare: Does your organization have a defined zero trust security initiative today or that you’re planning to start on in the next 12-18 months?



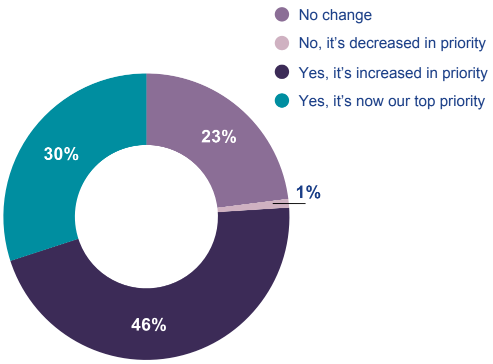
Similar to financial services, there was a large increase in the percentage of healthcare organizations that now have a zero trust initiative in place or underway — up from 44% last year to 91% today. Overall, this industry tends to be further along on the zero trust maturity curve, with at least 75% adoption expected across all five projects in Stage 1 over the next 12-18 months, and more than 50% adoption across Stage 2 projects.

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

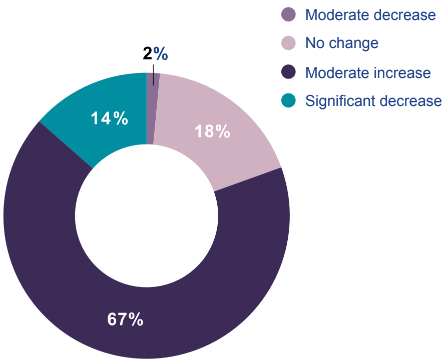


The top priorities for healthcare in the coming years include implementing MFA for external users (increased from 24% to 51%), automating the provisioning and deprovisioning of external users like supply-chain partners (from 9% to 42%), and implementing passwordless access (from 6% to 30%). Healthcare respondents noted that their biggest challenges in embracing a zero trust security model are a talent/skill shortage, followed by stakeholder buy-in. Meanwhile, 30% say that implementing zero trust is now their top priority in light of the impacts of COVID-19.

Healthcare: Has COVID-19 and the remote working economy accelerated zero trust as a priority at your organization?



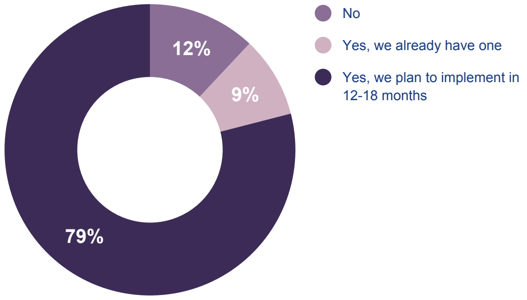
Healthcare: How has your budget for zero trust changed (if at all) in the past 12 months?



Software

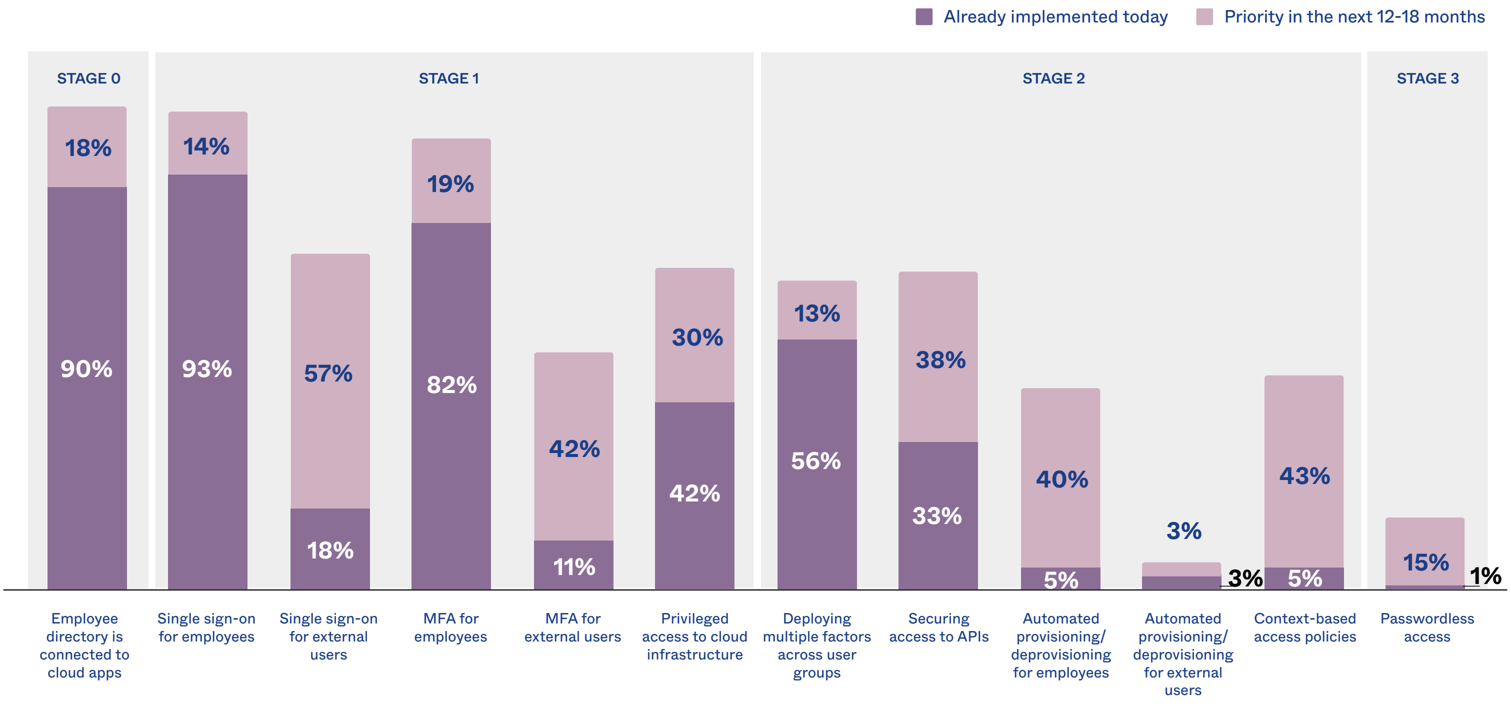
Software: Does your organization have a defined zero trust security initiative today or that you're planning to start on in the next 12-18 months?

Chart 9



On the other hand, the software industry is working to catch up with peers in financial services and healthcare. While 88% of these companies indicate they'll have zero trust security in the next 12-18 months (up from just 48% last year), 91% haven't yet started. That said, if the industry's plans play out, the security posture at most software companies will match their counterparts in highly regulated industries over the next couple years.

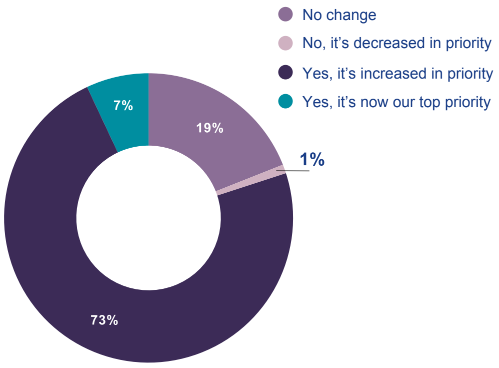
Software: Which projects has your organization already implemented as of today, and which are a priority for your organization in the next 12-18 months?



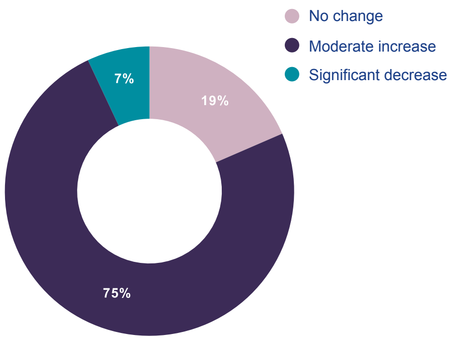
Today, most of software's zero trust projects are focused in the very early stages of the maturity curve, and at least half of the projects we asked about currently have less than 20% adoption in this industry. However, by 2023, 10 of the 12 projects we identified will be approaching adoption rates of 45% or more across software businesses. To get there, software companies are currently focusing on:

1. SSO for external users
2. Automating provisioning/deprovisioning for employees
3. Setting context-based access policies

Software: Has COVID-19 and the remote working economy accelerated zero trust as a priority at your organization?



Software: How has your budget for zero trust changed (if at all) in the past 12 months?



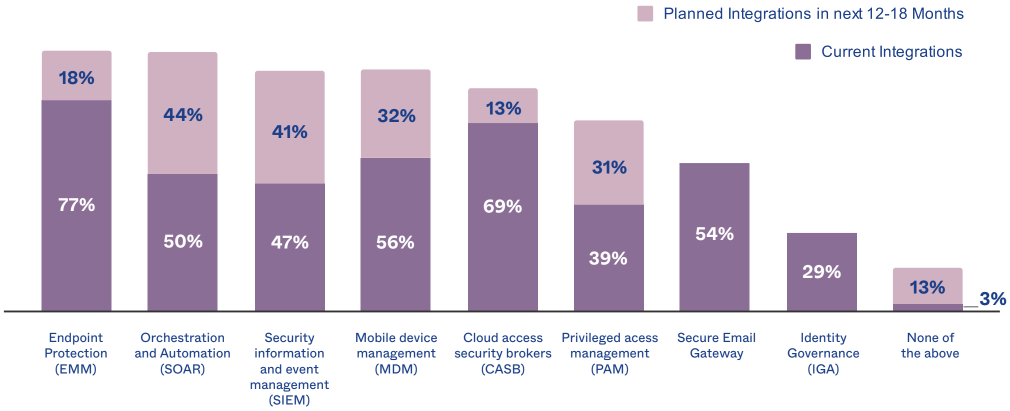
Nearly three-quarters of software companies indicated that zero trust initiatives have increased in priority, yet only 7% noted that it's now a top priority following the pandemic-driven shift to remote work. This could be due to the fact that software companies are more likely to embrace cloud applications, so the shift to remote work might not have impacted them as much as companies in highly regulated industries.

A Best-in-Class Zero Trust Ecosystem

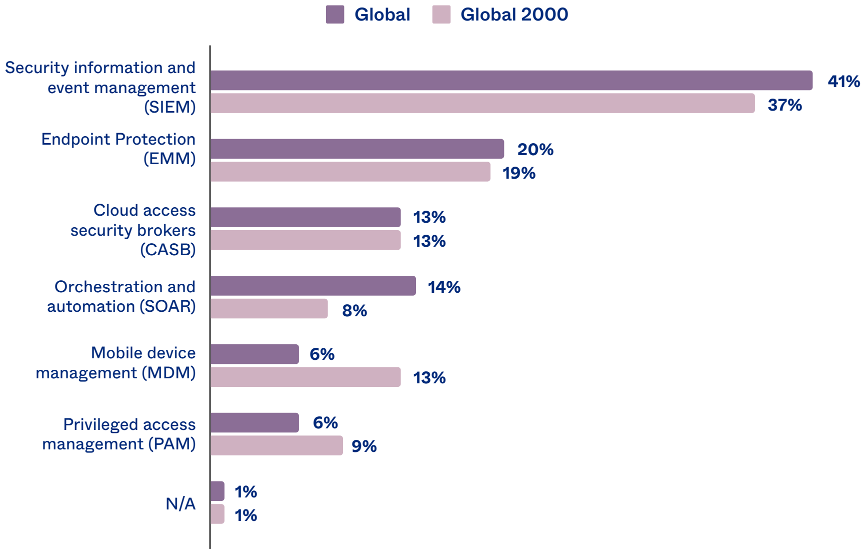
No single solution automates all of the zero trust recommendations promoted by Forrester, NIST, and others. A critical best practice in any industry is to leverage identity as a foundational technology across the security stack. Integrating your entire security architecture — including **security information and event management** (SIEM), **orchestration and automation** (SOAR), **endpoint protection** (EMM), **mobile device management** (MDM), **cloud access security brokers** (CASB), and **privileged access management** (PAM) — with an IAM solution helps establish a holistic, in-depth approach to your zero trust defense.

With this in mind, we asked security leaders what other tools they have integrated or plan to integrate with their IAM system, and found that the most common integrations in place today were EMM and CASB — at 77% and 69% of companies. The majority of companies selected SIEM as the single most important security integration.

Which tools have you integrated with your identity and access solution, and which are you planning to integrate with your IAM solution in the next 12-18 months?



Which tools do you see as most important to integrate with an IAM solution to support zero trust security?

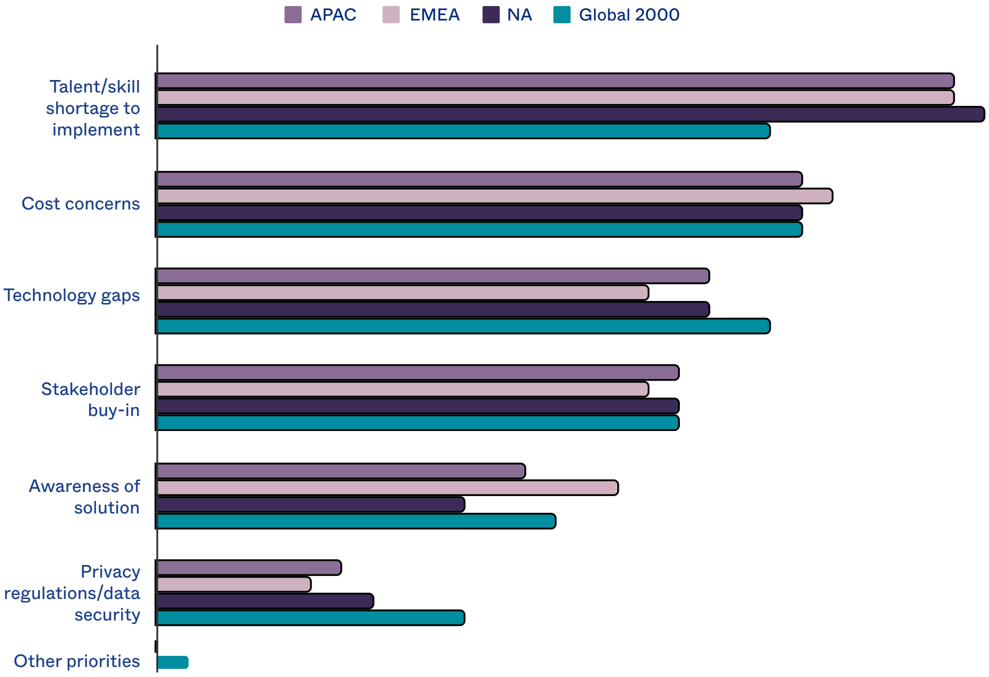


At least three-quarters of companies around the world say they'll have integrations between their IAM and EMM, SOAR, SEIM, MDM, and CASB systems within the next 12-18 months. Of those, about 95% of companies will have integrations with the top two solutions: SOAR and EMM. Global 2000 companies tend to have more of these integrations in place already, with at least half indicating current integrations with six security solutions (SEIM, SOAR, EMM, MDM, CASB, PAM). By the end of 2022, that number will jump to 80% of the world's largest organizations.

What's Next for Zero Trust?

While companies around the globe have made significant progress on their zero trust strategies since last year, there are still many opportunities and challenges ahead.

2021: What challenges does your organization face in implementing a zero trust model?



Thankfully, budget increases for zero trust security projects, industry momentum towards more sophisticated security practices, and even recent government mandates will all lend support to organizations as they progress along their zero trust journeys.

Key lessons learned

When it comes to implementing zero trust, there is no silver bullet. Even companies with the greatest resources to throw at the task won't achieve full maturity overnight. However, the digital nature of our modern economy means that security threats will only intensify, so no business can afford to stand still. If your organization is ready to accelerate its zero trust strategy, there are several ways you can make inroads with identity-driven security.

Important steps to mature your zero trust security posture:

- Recognize that people are the new perimeter, and adopt strong authentication across all your services, everywhere — from on-premises, to cloud, to mobile, and for employees as well as customers, partners, contractors, and suppliers.
- Centralize your identity and access control across the enterprise so you can more easily manage risk.
- Reduce risk by reviewing the IAM maturity curve, determining where your organization is, and finding some immediate wins to quickly advance your position through an identity-first approach to zero trust.
- Extend your security ecosystem by integrating key tools with your IAM solution, thus enabling holistic security visibility and collaboration across the organization.
- Consider even more advanced projects you can plan that will further increase security over time, such as adopting passwordless authentication and context-based access policies, as well as shifting beyond protecting employee accounts to also securing access for partner accounts.

As your organization takes steps to up its security game, it can be very helpful to benchmark this work against your peers. Check out **Okta's zero trust assessment tool** for a prescriptive roadmap to putting zero trust identity and access controls in place. Based on the IAM maturity curve detailed above, our assessment will review your practices surrounding everything from the type of resources you manage, to how your IT department provisions and deprovisions users, which authentication methods you deploy, and your future business priorities. We'll determine your current maturity and offer actionable recommendations on where you can go from here.

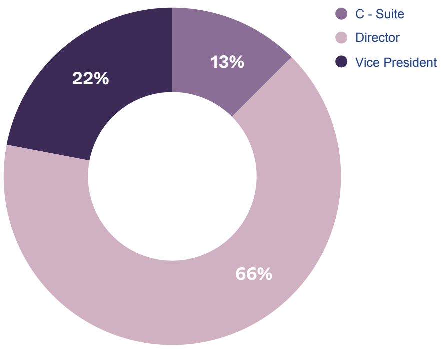
Survey methodology

Commissioned by Okta, Pulse Q&A conducted a survey of 600 director and above security decision makers at global companies across multiple industries. Decision makers were defined as someone responsible for making technology purchasing decisions, and Pulse collected responses in early 2021. We refer to this survey as “our survey” and “survey,” and refer to the people who responded as “survey respondents” or “respondents.”

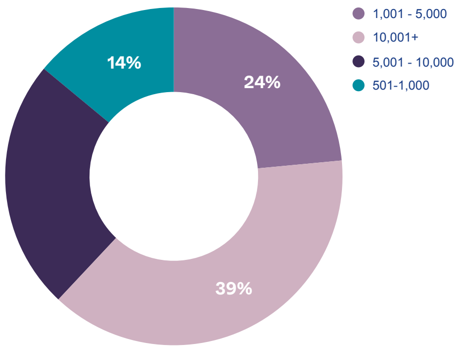
Who took the survey?

Here is a look at the 600 survey respondents and the companies they represent. For industry data, we used percentages within each segment to normalize and compare responses across the top three industries.

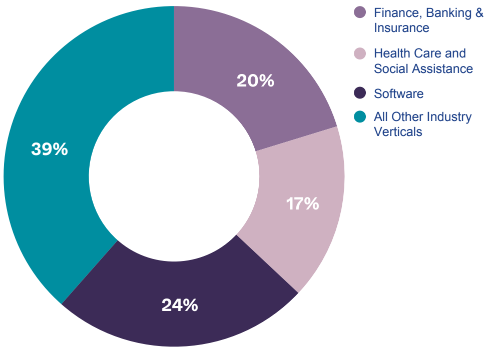
Respondent Roles



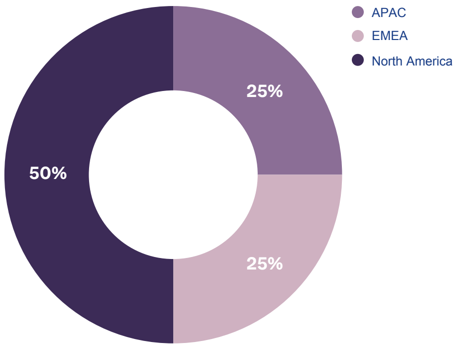
Organization Size



Industry



Geographic breakdown



About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 7,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 10,000 organizations, including JetBlue, Nordstrom, Slack, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers. For more information, go to **okta.com**.