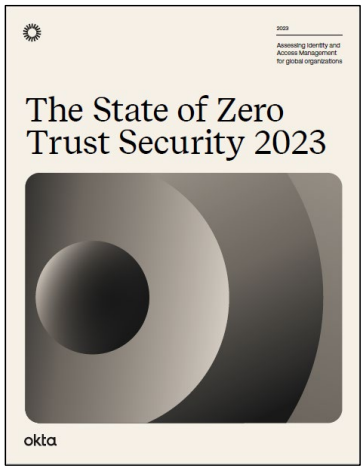


The State of Zero Trust Security 2023

Assessing Identity and Access Management for global organizations

Thank you for downloading this Okta Discovery Guide. Carahsoft is the distributor for Okta Cybersecurity solutions available via GSA, NASA-SEWP, ITES-Sw2, DoD ESI and other contract vehicles.

To learn how to take the next step toward acquiring Okta's solutions, please check out the following resources and information:

For additional resources:
carah.io/resources

For upcoming events:
carah.io/events

For additional Okta solutions:
carah.io/solutions

For additional Cybersecurity solutions:
carah.io/cybersecurity

To set up a meeting:
okta@carahsoft.com
833-674-3990

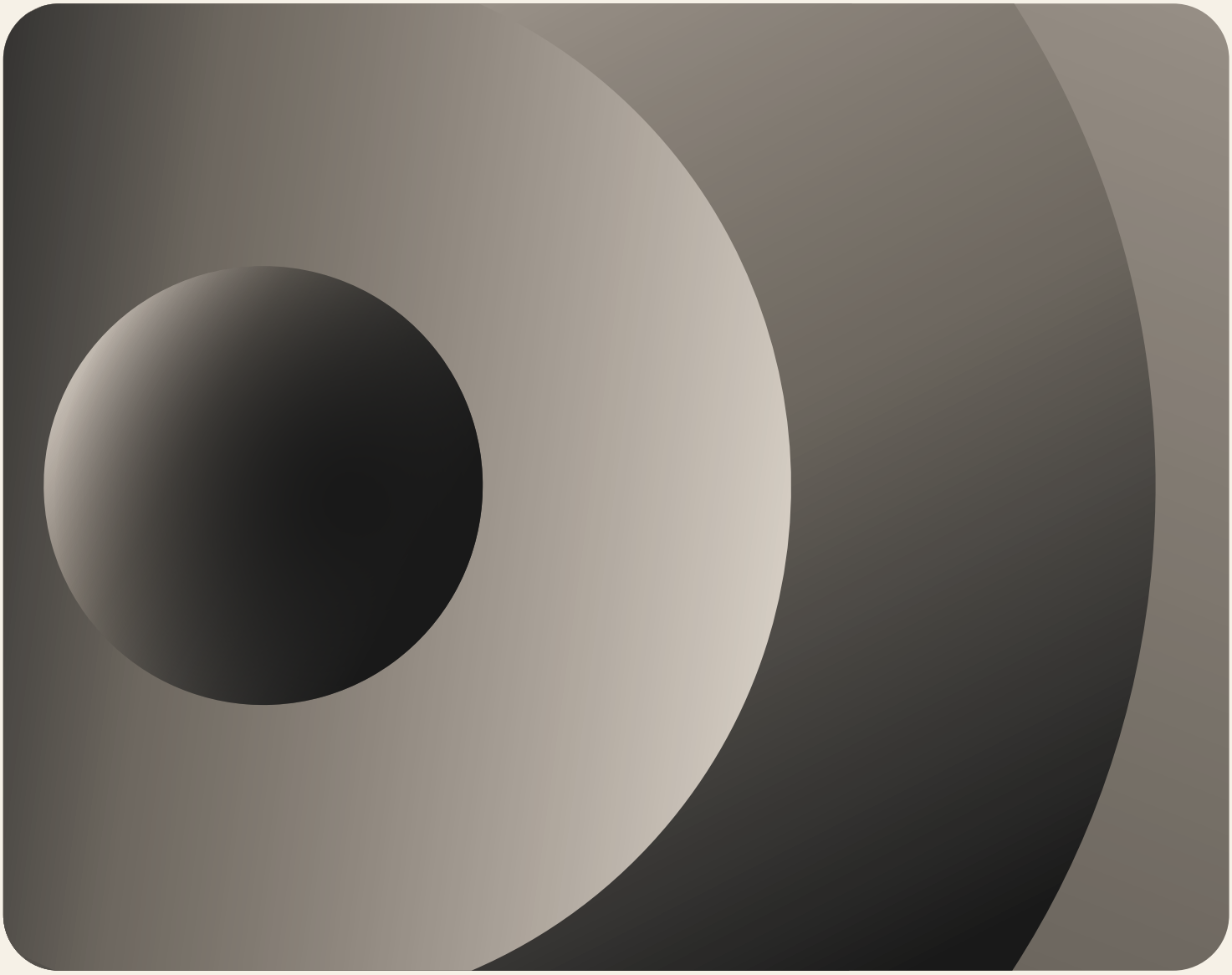
To purchase, check out the contract vehicles available for procurement:
carah.io/contracts

For more information, contact Carahsoft or our reseller partners:
okta@carahsoft.com | 833-674-3990

2023

Assessing Identity and Access Management for global organizations

The State of Zero Trust Security 2023



okta

Table of contents

Methodology

Survey methodology

In partnership with Qualtrics, Okta conducted a global survey of information security decision-makers across a range of industry verticals in April 2023. Decision-makers were defined as employees at the director level or higher who are responsible for making technology purchasing decisions. The survey was administered in English and Japanese via Qualtrics panels in 13 countries. 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."

Our survey respondents

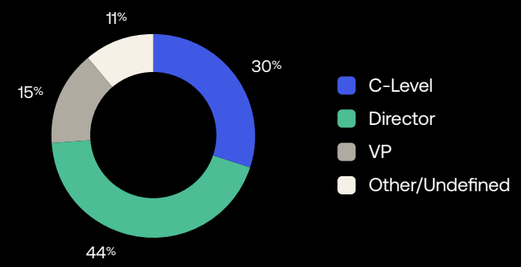
The total sample size was 860 information security decision-makers from North America (United States, Canada); EMEA (Denmark, Finland, France, Germany, Ireland, Netherlands, Norway, Sweden, United Kingdom); and APJ (Japan, Australia). This report focuses on the healthcare, public sector, financial services, and software verticals, but other industries are represented as well. (Regions and industries were self-reported by respondents.) Public sector includes organizations from all three global regions, but not state/local orgs. Surveyed groups included C-level executives, VPs, and directors. The survey did not target Okta employees or customers.

Methodology details

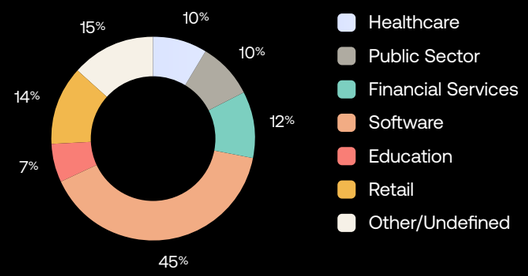
In the charts within, "Global" or "All" responses include respondents in all sectors (not just our four focus sectors) and all regions (whether or not they identified themselves as being in NAM, EMEA, or APJ). For convenience, we round all chart data to the nearest single digit, including rounding down to zero where numbers are less than 0.5; because of this, totals on some charts don't add to 100% exactly. Charts can also total more than 100% when respondents answered yes to multiple related questions (for example: indicating both that they've taken a specific initiative and that they plan to do so going forward). ■

Survey respondent demographics

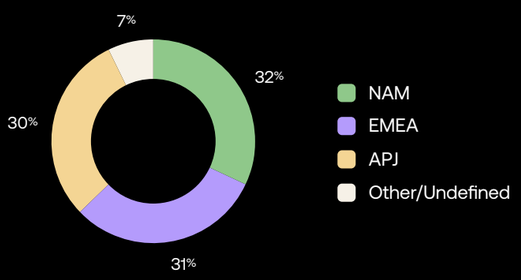
Respondent role



Company industry



Company region



Zero Trust moves from goal to plan

Organizations are deepening their embrace of Zero Trust as a way to keep their people, assets, and infrastructure safe.

Ten years ago, Zero Trust was a shimmering oasis on the security horizon. Forrester researcher John Kindervag is credited with coining the term, back in 2010, as a convenient encapsulation of the growing need for a "never trust, always verify" security ideal. But in the decade since, Zero Trust has progressed with rapid speed: from cool philosophy to stretch goal to everyday business reality. Today, as our annual State of Zero Trust survey demonstrates, more organizations than ever have fully embraced this ideal as a business strategy, and are taking concrete steps to fully implement Zero Trust security over the coming months.

In fact, for the first time since Okta started issuing the State of Zero Trust Report in 2019, we're seeing the number of organizations that already have a defined Zero Trust strategy in place far exceeding the number of organizations that are still in the planning stages (or that don't think it's important enough to focus on at all). The tide has clearly turned.

In light of the continued explosive growth of breaches and data theft, as well as prescriptive guidance by NIST and CISA, none of this should be terribly surprising. According to the Identity Theft Resource Center's 2022 Annual Data Breach Report, there were 1,802 data compromises in the U.S. last year, affecting more than 422 million individuals. Identity, as always, is at the heart of this onslaught: Javelin's 2022 Identity Fraud Study puts the cost of U.S. Identity fraud losses alone at $43 billion in 2022 — and that represents a hard-fought win over the $52 billion identity thieves took in 2021. "Identity fraud is a component of almost every major crime and felt throughout the world," according to a 2023 report from the U.S. Department of Justice, "posing a national and global threat to the security of all nations and their citizens."

To combat modern threats and sophisticated threat actors, we believe the best strategy for enterprise security teams is to adhere to Zero Trust's core "never trust; always verify" principle. A Zero Trust security strategy lays the groundwork for organizations to evolve beyond traditional approaches to cybersecurity that were not built for a cloud-security world, and to position Identity as the main driver of their security posture. For many organizations, Identity used to be wholly the province of IT teams; today, as our data shows, control has largely — and, in many cases wholly — shifted to the security team. But SecOps teams aren't the only beneficiaries of Zero Trust: Organizations embracing this best practice are better able to leverage Identity management across their entire network infrastructure, realizing new efficiencies and better workforce and customer experiences.

Macroeconomic trends and cloud innovation have led modern organizations to adopt more complex hybrid/multi-cloud ecosystems, with distributed resources and IT environments being accessed by diverse boundaryless workforces, including partners, contractors, and outside vendors. Identity is the common thread that holds all this together, and strong Identity management is now considered critical infrastructure to keep these complex global workforce teams collaborating securely and productively. As this year's data shows, organizations are busy strengthening their mobile device management, adding single sign-on (SSO) and multi-factor authentication (MFA) for external collaborators as well as employees, automating their provisioning/deprovisioning workflows, and otherwise putting strong Zero Trust initiatives in place to keep their enterprise assets — and people — safe.

Getting to Zero Trust is a journey: Upending decades-long practices and processes, rebuilding security stacks, and making tough investment and software deprecation decisions are challenging in the best of times. And, as a casual glance at the financial news will quickly reveal, these are not the best of times. But with the right technology and vendors, the global organizations in our annual survey are simplifying the challenge and progressing quickly. This report is meant to help organizations understand how and where today's forward-thinking growth companies are putting Zero Trust security initiatives into play, so they can identify the right steps as they move from goal stage to implementation of plans in their own organizational journeys.

Zero Trust initiatives continue to grow by leaps and bounds

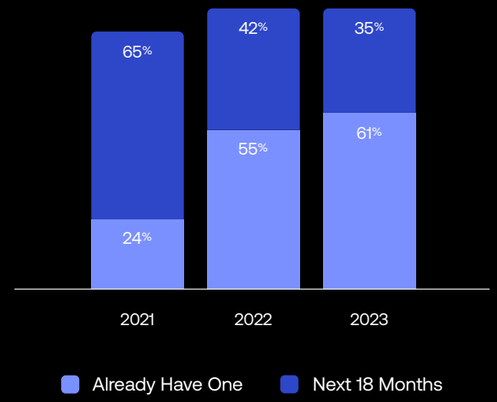
The number of organizations with a defined Zero Trust initiative in place continues to grow by leaps and bounds. Back in 2021, fewer than one in four of the organizations we surveyed had one in place; by 2022, more than half the organizations surveyed had one, and the number grew again this year, to 61%. The percentage of organizations still planning to implement a Zero Trust initiative over the next 18 months has correspondingly dropped, year-over-year, as companies rapidly put their plans into action. Today, more than six out of 10 surveyed organizations are already well into their Zero Trust journey, with most of the rest firmly in the planning stage.

When we zoom in closer and look at the data by company size, we can see that smaller organizations (those with 500–999 employees) are less likely to have a defined Zero Trust security initiative in place than larger enterprises. The sweet spot is companies with between 5,000 and 9,999 employees, where three out of four report having a defined Zero Trust initiative in place. At all levels, only a very small minority of organizations (less than 10% in all cases) neither have a Zero Trust initiative nor plan to develop one in the next 18 months.

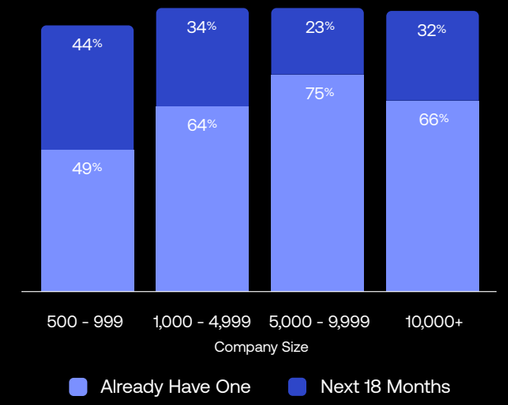
Around the world, Zero Trust plans are becoming an everyday business reality

Globally, 61% of all organizations now already have a defined Zero Trust security initiative in place; another 28% plan to implement one within the next 6–12 months, and another 7% plan to implement one within the next 13–18 months. This general trend holds across all regions: The North American region is maintaining a solid lead in terms of initiatives already in place, but EMEA- and APJ-based organizations are quickly gaining ground, and nearly all of the holdouts in both regions plan to adopt a Zero Trust initiative within the next 6–12 or 13–18 months.

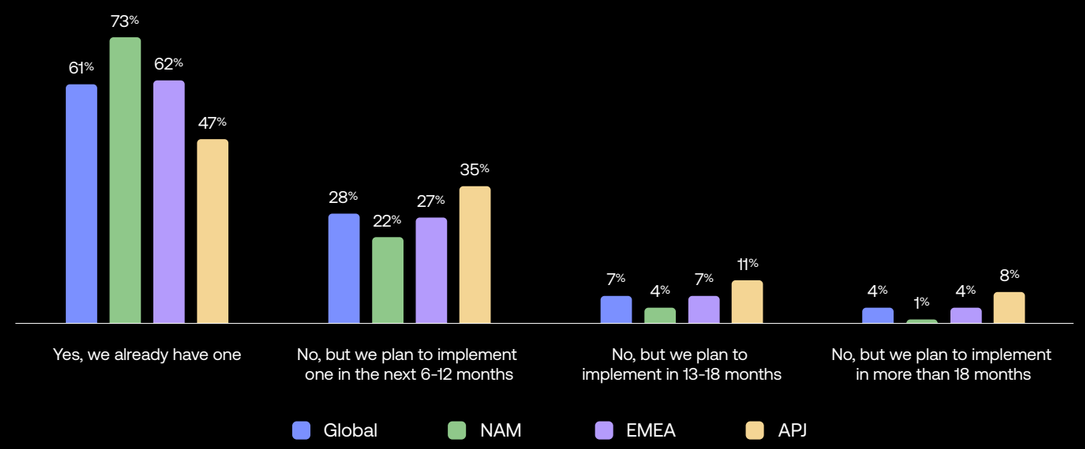
Does your organization have a defined Zero Trust security initiative today, or do you plan to implement one within the next 18 months?
All respondents



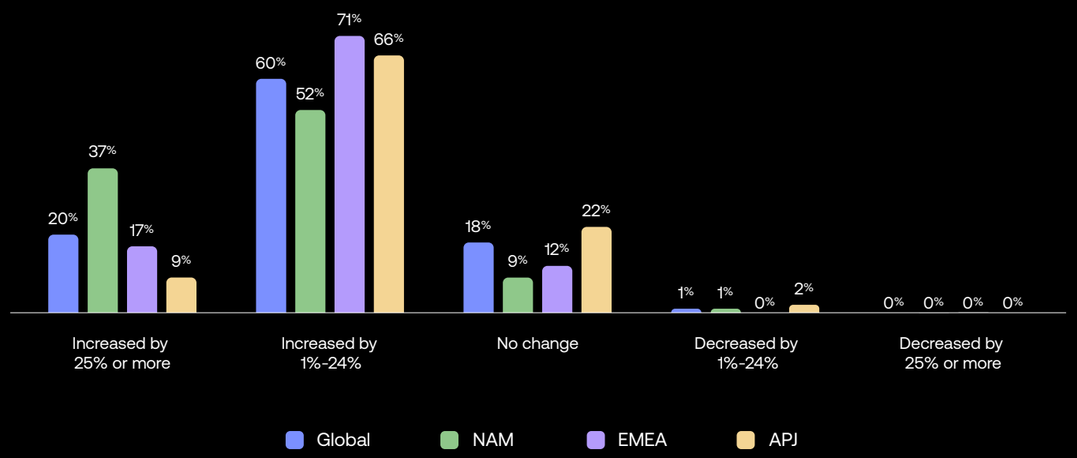
Does your organization have a defined Zero Trust security initiative today, or that you're planning to start in the next 18 months?
Comparison by company size



Does your organization have a defined ZT security initiative today or one you're planning to start on in the next 18 months?
Regional comparison



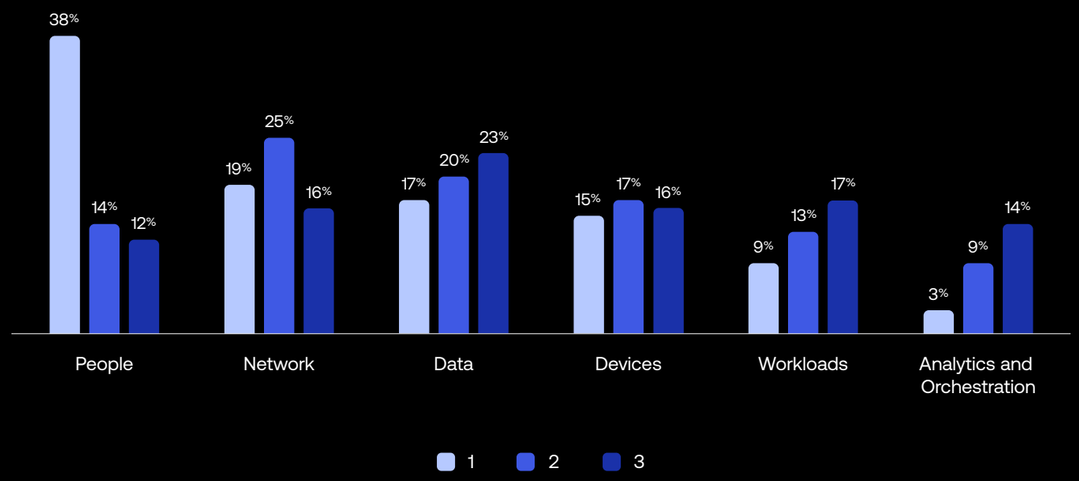
How has your budget for Zero Trust changed (if at all) in the past 12–18 months?
Regional comparison



Budgets are staying healthy for Zero Trust initiatives

In an age where macroeconomic factors are driving staffing and cost-cutting across all regions and industries, the budgets for Zero Trust security initiatives seem virtually untouchable. In fact, for the overwhelming majority of companies surveyed, these budgets aren't just holding steady — they've actually increased over the past 12–18 months. Globally, 60% of organizations have seen a 1–24% increase in these budgets since last year, and another one in five has increased by even more. Fewer than 3% of surveyed organizations in any region saw any budget decrease.

Rate the following areas in terms of priority for your organization's security projects (1 = highest, 3 = lowest)
All respondents



People remain the top priority for security projects

When we asked respondents to rank their organizations' top three areas of security concern, "People" was the runaway favorite category this year, with "Network" and "Data" coming in a distant second and third. "People" has always been rated a top priority, but this year it's an unusual outlier, reflecting an increasing understanding of Identity's critical function in Zero Trust security initiatives.

Zero Trust moves from goal to plan

Key takeaways

Zero Trust has shifted quickly from a plan of action to business as usual.

Organizations that once saw Zero Trust as a hypothetical framework have by and large put those plans into action, or are well on their way to doing so. The rise has been dramatic: In 2021, just 24% of our respondents reported having a Zero Trust strategic initiative in place; that figure climbed to 55% last year, and to 61% this year. It's a trend we're seeing across all regions and organization sizes. Among our four focus industries, financial services holds a narrow lead, with 71% of organizations already having a Zero Trust initiative in place, over software, with 69%. By region, North America leads the pack, with 73% of organizations having a defined Zero Trust initiative in place; APJ is least likely to have one, at 47%, but most likely (at 35%) to plan to implement one over the next 6–12 months.

Identity is now widely understood to be mission critical for Zero Trust strategy.

What a difference a year makes: Last year, 71% of our respondents deemed Identity important to Zero Trust security strategy, but only 27% of respondents thought it was business critical. This year, the tables have turned, with 51% of respondents saying Identity is "extremely important," and 40% deeming it "somewhat important." We're not surprised to see this change of heart, as more and more organizations come to realize that strong Identity Access Management (IAM) is a fundamental strategy to keep people and assets safe in a hybrid/multi-cloud world.

Zero Trust budgets are still rising, stubbornly resisting market forces.

Budgets are tightening all over the world due to a variety of macroeconomic pressures, yet Zero Trust spending continues to grow. This year, a full 80% of survey respondents reported that their budgets for Zero Trust security initiatives had increased over the previous year: 60% reported budget increases of between 1% and 24%, and another 20% increased dramatically (by 25% or more). Cost concerns have been a major consideration for three years running in this report, but endless fraud and insider threats, plus the demand for hybrid work and unfettered cloud access, are forcing businesses of all sizes and in all industry sectors to apply focus — and budget — toward Identity-backed security measures.

Companies trying to adopt Zero Trust still face some uphill battles.

This year, our respondents named cost concerns and technology gaps as their top challenges to establishing Zero Trust, followed by privacy regulations/data security and a talent skills shortage. But the landscape has shifted: In previous years, a single concern has tended to far outweigh other concerns. This year, the challenges are more evenly distributed and include ease of integrations, awareness of solution, audit compliance, and stakeholder buy-in. In related news, team control over IAM within companies has largely shifted from IT's domain to a shared responsibility run mainly by security teams. ■

Identity: The core of Zero Trust

Organizations around the world are embracing Identity's central role in modern security.

In a world where traditional network perimeters have all but disappeared, Identity has emerged as the new perimeter — the place where defense has to start. Verifying the identity of every human and machine on every single attempt to access your resources — from anywhere in the world and on a wide array of sanctioned and unsanctioned devices — is the challenge of our times.

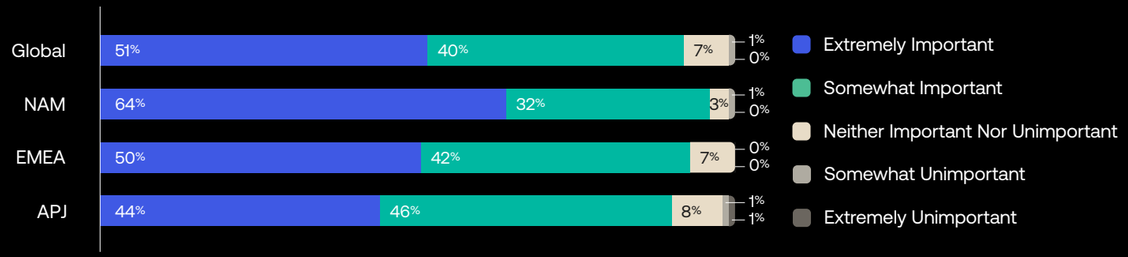
But the prize is nothing less than business success. As this year's data demonstrate, companies of all sizes across industries are increasingly understanding that Identity isn't just a security play but the path to safely scaling business so they can drive more revenue, increase customer loyalty, safeguard their assets and brand reputation, and a lot more.

These trends are reflected in our 2023 survey results, where organizations made it clear they are placing more emphasis on Identity as part of their Zero Trust initiatives than ever before. Globally, more than half of our respondents say that Identity is extremely important to their Zero Trust security strategy — a huge jump over the percentage who said so in 2022, and an increase seen from respondents across all geographic regions, as discussed on the following pages.

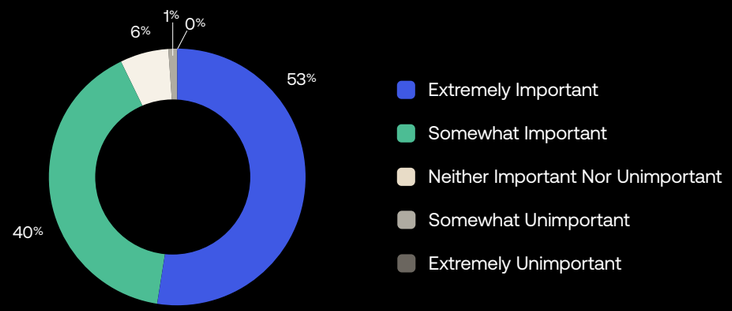
"IT leaders are aligning IAM investments with both security and business goals. Done effectively, IAM creates a secure process for authorization, policy enforcement, provisioning, and deprovisioning that minimizes friction and powers business operations … a potential source of improvements in terms of both security and productivity."

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

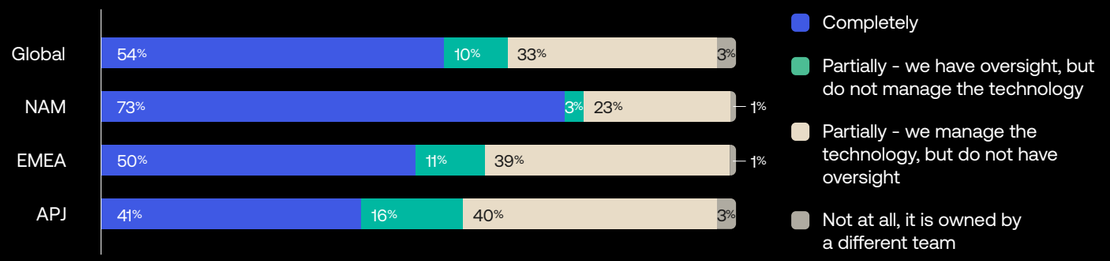
How important is Identity to your overall Zero Trust security strategy?
Regional comparison



How important is Identity to your overall Zero Trust security strategy?
C-suite respondents



To what extent does security own IAM at your organization?
Regional comparison



Note: column totals may not add exactly to 100% due to rounding data labels to whole numbers.

Identity's importance is clear

Identity's critical role in powering Zero Trust initiatives is growing ever clearer. Last year, only 27% of global respondents said Identity was extremely important to their overall Zero Trust security strategy; this year, that number has increased to 51%. By region, North America leads the way, with nearly two-thirds of respondents rating Identity extremely important and nearly one third deeming it somewhat important. The EMEA and APJ regions may still be breaking through some perceptual barriers, with 7% and 8% of respondents respectively declaring Identity neither important nor unimportant; in the APJ region, a few (2%) even called Identity somewhat unimportant or extremely unimportant.

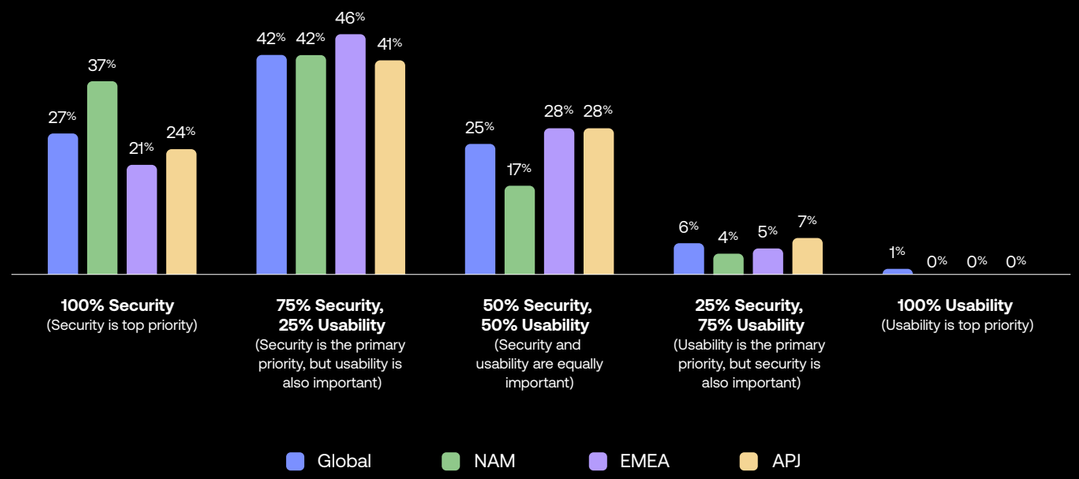
The C-suite chimes in

The vast majority of C-suite respondents continue to prioritize Identity, as they did in last year's report. More than half of our C-suite respondents said this year that Identity was extremely important to a Zero Trust strategy, with another 40% declaring it somewhat important. (Last year, just 26% of C-suite respondents declared Identity mission-critical.) The takeaway: A general understanding of Identity's critical role in modern security has become fairly pervasive now.

IAM responsibility is shifting

One way of understanding companies' fast-evolving approach to security is tracking where IAM control resides within the organizations. Identity used to be largely owned by the IT department, but has increasingly shifted to become a security team responsibility in recent years as Identity-based threats like phishing continue to dominate the threatscape. (Seventy-four percent of breaches last year involved a human element, according to Verizon's 2023 Data Breach Investigations Report.) Security now owns IAM at half the organizations in EMEA; for North America, the number is 73%. Ownership is more dispersed in the APJ region, where just 41% of organizations task security with managing IAM outright, and another 56% of organizations have security either oversee Identity or manage the technology, but not both.

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



Security has generally become a higher priority than usability

The attack surface has expanded dramatically for modern hybrid/multi-cloud corporate networks, leaving organizations increasingly vulnerable to Identity-based threats. As a result, enterprises have shifted their priority balance, sometimes dramatically, in favor of security over usability. Globally, more than two in three companies either say security is the unquestioned top priority or that their current priority balance is three-quarters security, one-quarter usability. This marks a major change from 2021 — in the heart of the pandemic's race to remote work — where usability was the predominant priority. EMEA respondents were the least likely to say security was the top priority (21%), compared to 37% of North American respondents. ■

Workforce Identity maturity

Companies have come to understand the value of Identity management. The trick is putting those ideals into action.

Zero Trust doesn't happen overnight. And as complex initiatives, shifting priorities, and expanding needs all compete for time and resources, organizations can struggle to understand their vulnerabilities and benchmark their progress without clear frameworks in place. Okta's Workforce Identity Maturity Model, detailed below, can help companies contextualize the Identity aspects of their Zero Trust journeys and benchmark their progress. It takes time to move through all the stages, but as organizations begin to leverage Identity-centric security, they start hardening their protection: reducing their attack surface, speeding their response to malicious attacks, reducing IT costs and administrative burdens, and otherwise becoming safer, more efficient, and more agile. On the following pages, we'll quickly review the four stages.

Workforce Identity maturity

The four stages

Stage 1: Fundamental Consolidate and Simplify	• Reduce manual management • Shrink risk surface • Consolidate directories
Stage 2: Scaling Layer Security Controls	• Automate on/offboarding • Improve IT productivity • Reduce admin burden
Stage 3: Advanced Automate and Elevate Experience	• Connect all Identity systems • Automate all admin processes • Deprecate legacy technology
Stage 4: Strategic Optimize and Extend Identity	• Modernize access experience • Eliminate password risk • Expand digital maturity

Stage 1: Fundamental

Consolidate and Simplify

For companies in Stage 1, goals typically include reducing manual management and strengthening defense against Identity-based attacks. Organizations at this stage are trying to move away from manually managing users and apps while hardening their defenses. They often struggle with disconnected, ad-hoc initiatives, unintentionally growing the risk surface and increasing directory sprawl.

High-value Identity initiatives to consider in Stage 1 include: consolidating Identity systems, implementing basic SSO and MFA with role-based access policies, creating a high-availability architecture, adding SLA standards, and developing a comprehensive inventory of on-premises and cloud apps.

Stage 2: Scaling

Layer Security Controls

In Stage 2, companies typically tackle improving IT productivity and reducing administration time and costs. Organizations at this stage may be overly reliant on passwords and invested in manual processes like onboarding and offboarding users. Goals include increasing productivity, easing IT administrator burdens, hardening security posture, and simplifying user access to applications.

Projects to consider in Stage 2 include extending MFA across applications, contractors, and business partners; consolidating security and access controls across cloud and on-prem applications; implementing role-based access control and dynamic access policies; and introducing security and compliance audit and monitoring tools.

Stage 3: Advanced

Automate and Elevate Experience

By Stage 3, organizations are automating any remaining manual processes and connecting all Identity systems under a single, unified management solution. This lets them build efficiency for a dynamic workforce while simultaneously consolidating and deprecating legacy technologies, and helps ensure that all systems are connected and communicating.

Identity projects to consider here include implementing attribute-based and policy-based access control and enforcing least privilege access to APIs, critical infrastructure, and applications. In addition, organizations should look to adopt scheduled user access recertification and implement secure passwordless access to critical infrastructure.

Stage 4: Strategic

Optimize and Extend Identity

In this stage, organizations are protected by interconnected, Identity-backed systems that deliver security and efficiency at scale. They can now safely focus on next-level goals, like delivering modern access experiences and eliminating password-related risks.

In Stage 4, organizations should look to fully adopt and embrace passwordless authentication; deploy fully automated processes for incident prevention, detection, and response; institute risk-based, just-in-time access; and ensure that zero standing privileges remain.

Workforce Identity maturity

Putting Zero Trust initiatives into action

The “never trust, always verify” philosophy of Zero Trust has shifted from theoretical strategy to everyday business reality with lightning speed, as forward-thinking organizations embrace and prioritize Identity initiatives. They’re building new security foundations, starting with extending MFA and SSO to employees and external users as well as for apps, APIs, and other key parts of their network infrastructure. Across all regions, we see a growing number of organizations tackling increasingly complex Identity-based Zero Trust projects — and their progress is encouraging.

Driven by increasingly complex workforces that include full-time employees, contractors, partners, and vendors who all need reliable anytime access, organizations worldwide are making great strides toward establishing strong, Identity-backed Zero Trust security postures.

For example, companies are prioritizing MFA for external users (with 34% of this year’s respondents having the security measure in place) as well as for employees (33%).

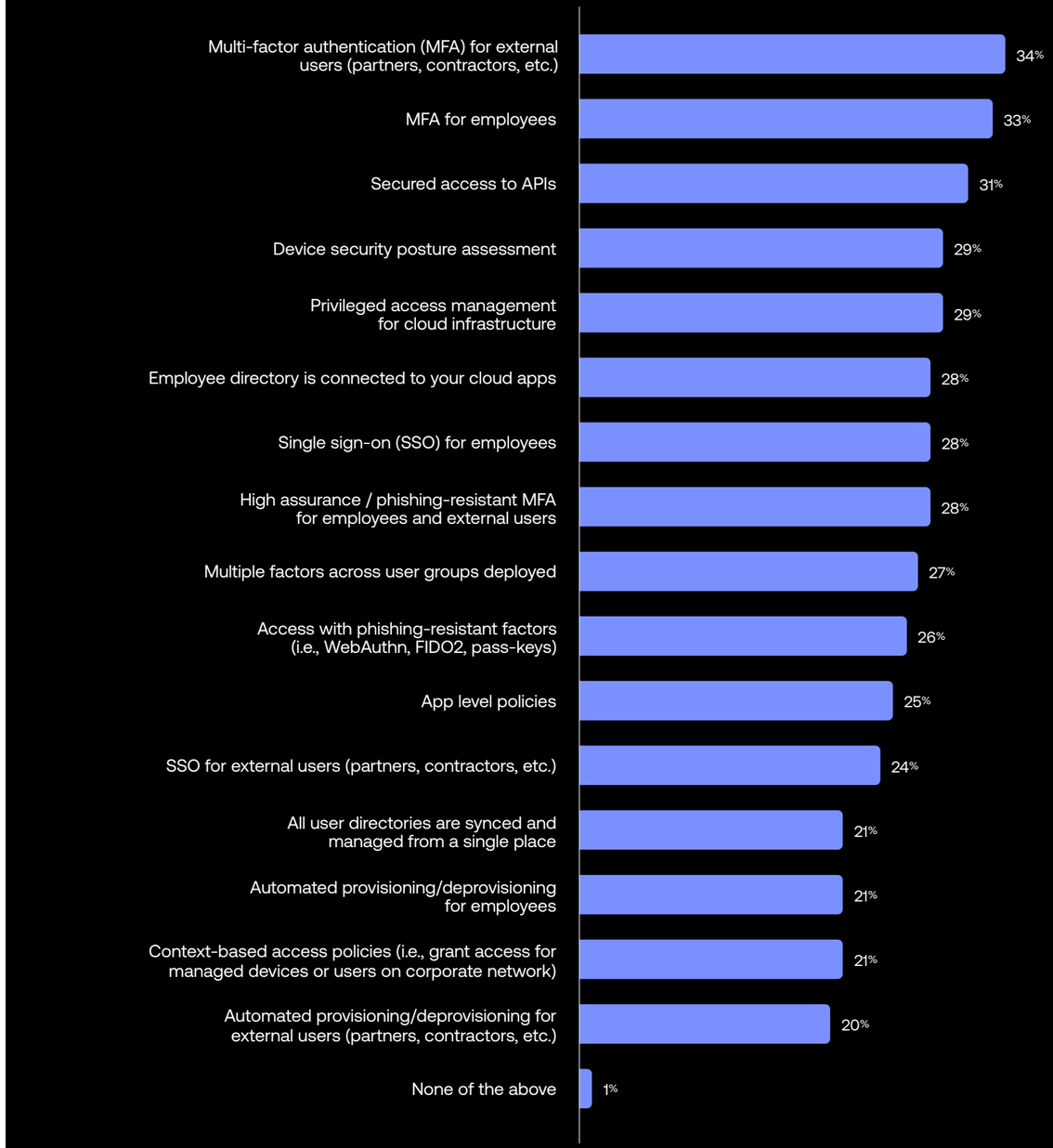
Looking at the data by industry, the top security initiatives that surveyed organizations reported they already have in place this year are:

- **In healthcare:** MFA for external users, MFA for employees, and connecting directories to cloud apps
- **In the public sector:** MFA for external users, secured access to APIs, and MFA for employees
- **In financial services:** MFA for employees, MFA for external users, and privileged access management for cloud infrastructure
- **In software:** MFA for employees, secured access to APIs, and MFA for external users

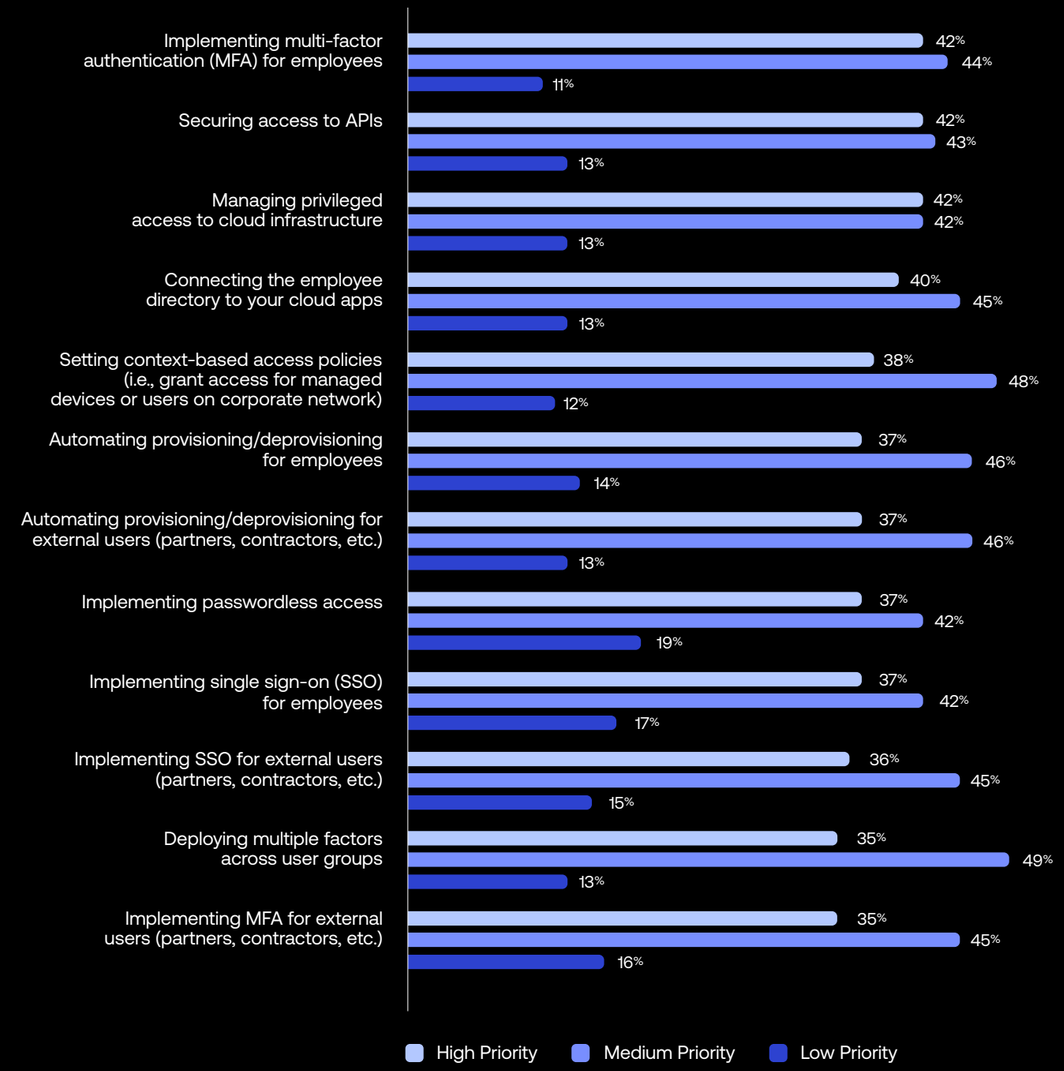
As far as security initiatives still on the drawing board at surveyed companies, this year’s data reveals a fairly even distribution, with the top three planned implementations being managing privileged access to cloud, securing access to APIs, and implementing MFA for employees.

In both 2021 and 2022, providing MFA and SSO for employees topped our respondents’ list of already accomplished security measures, with connecting their employee directories to cloud apps a close third. In 2021, the top priority for the upcoming 12–18 months was providing SSO to external users; in 2022 it was providing privileged access management to cloud infrastructure.

Which of these security initiatives have you already implemented?
All respondents



For these security initiatives, rank the priority level for your organization over the next 12–18 months.
All respondents



Note: column totals may not add exactly to 100% due to rounding data labels to whole numbers.

Workforce Identity maturity

Planning implementations

2021

#1 Single sign-on for external users (57%)

#2 Context-based access policies (43%)

#3 Implementing multi-factor authentication (MFA) for external users like partners and contractors (42%)

2022

#1 Managing privileged access to cloud infrastructure (45%)

#2 Securing access to APIs (41%)

#3 Automating provisioning/deprovisioning for employees (38%)

2023

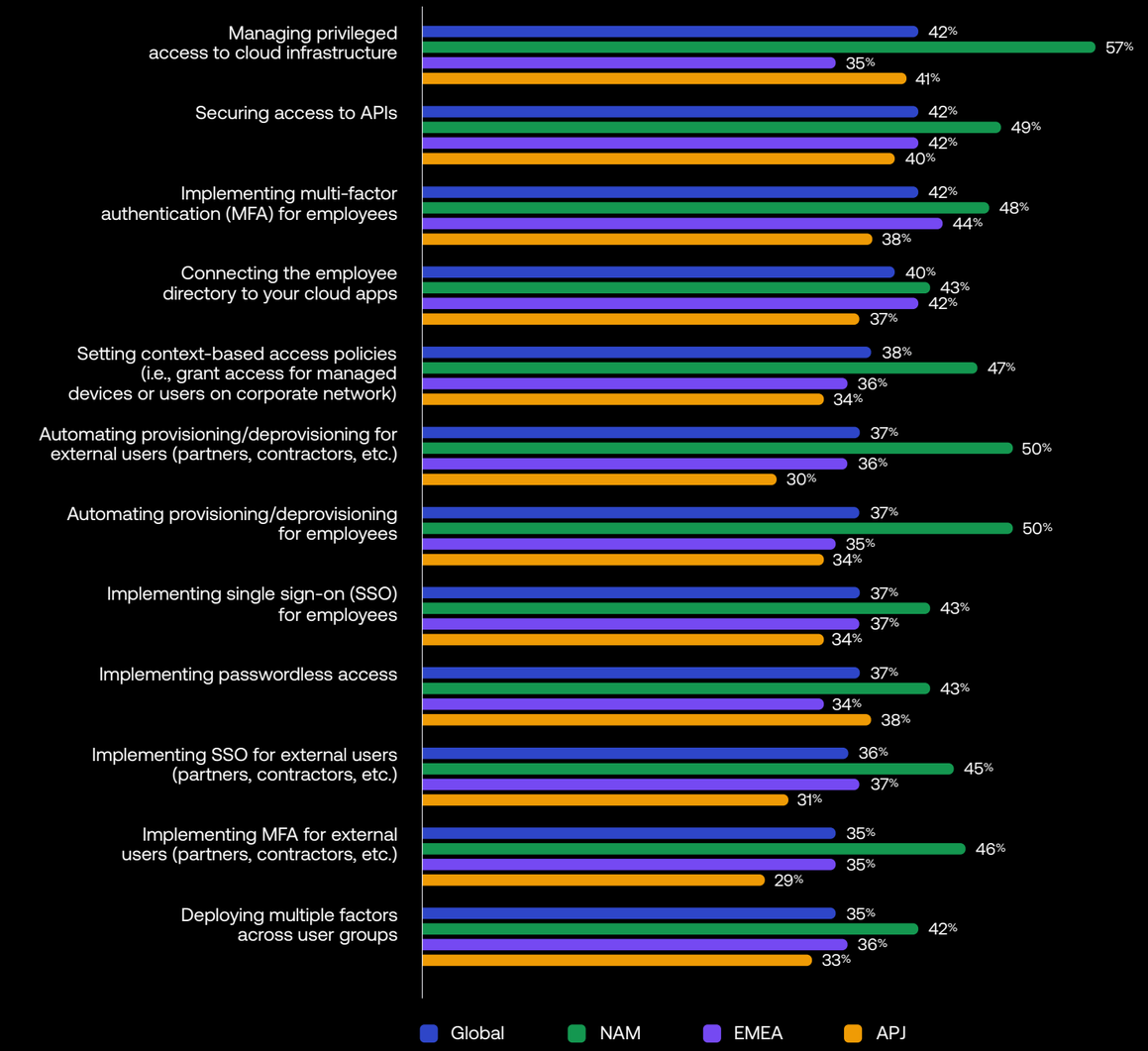
#1 Managing privileged access to cloud infrastructure (42%)

#2 Securing access to APIs (42%)

#3 Implementing multi-factor authentication (MFA) for employees (42%)

Each year, we ask our survey respondents to list the Zero Trust solutions they're planning to implement over the next year to year and a half. Looking at the top three global responses year by year, we can see some interesting trend lines. In 2021, companies were most concerned with setting up external users with SSO and MFA and tightening access policies. As these implementations have fallen into place for many organizations, the focus has shifted to securing privileged access to cloud and access to APIs, as well as automating provisioning/deprovisioning for employees (last year) and implementing MFA for employees (this year).

Which of these security initiatives is a high priority for your organization in the next 12–18 months? (Chart includes only "high priority" responses.)
Regional comparison



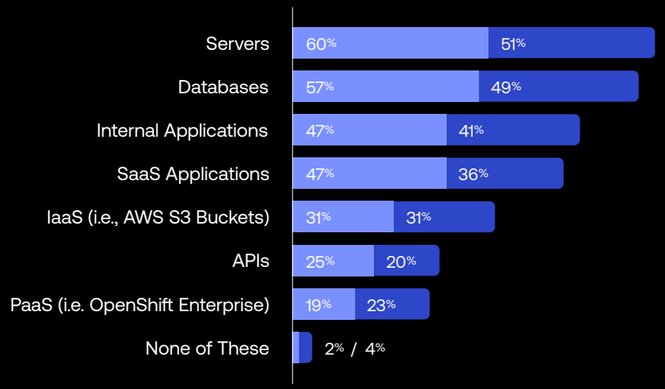
North American companies place a higher priority on security initiatives

Taking a deeper dive into this year's data, we can see regional variations start to emerge. Respondents were most likely to assign security initiatives of all types a high priority in North America, where managing privileged access to cloud and automating provisioning/deprovisioning led the way in terms of specific planned security initiatives. In EMEA, the highest priority initiatives were implementing MFA for employees, securing access to APIs, and connecting the employee directory to cloud apps. Companies in the APJ region were a bit less likely to identify initiatives as high priority, on average, but produced a balanced set of planning concerns, with managing privileged access to cloud infrastructure and securing access to APIs at the top, followed closely by implementing MFA for employees, implementing passwordless access, and connecting employee directories to cloud apps.

Workforce Identity maturity

Protecting authentication

Which classes of resources have you already extended MFA/SSO to, and which classes of resources are you planning to extend them to in the next 12–18 months?
All respondents



Note: column totals may add to more than 100% due to respondents who select both responses.

Servers and databases are most likely resources to get MFA/SSO protection

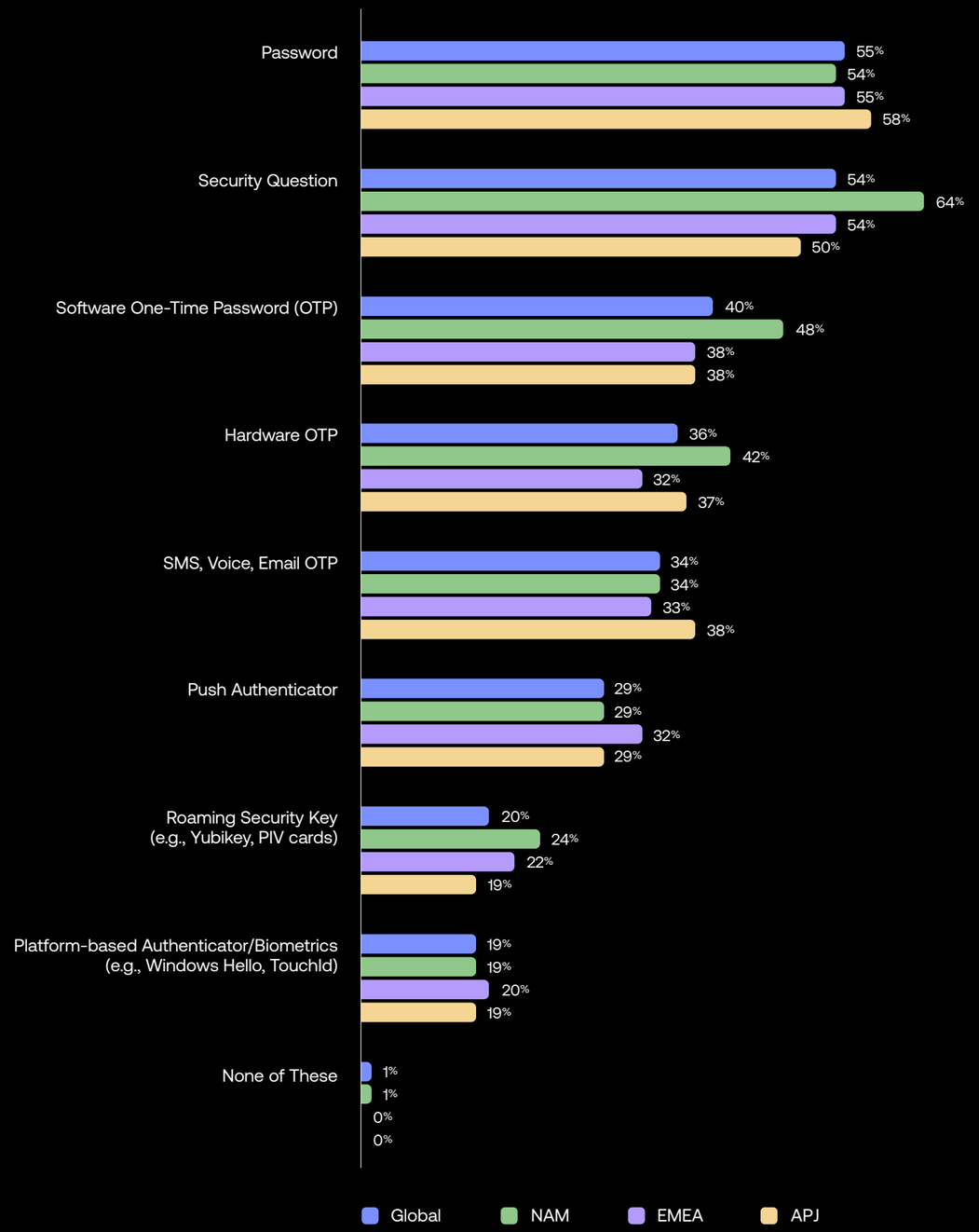
Last year's report saw an emphasis on extending MFA and SSO to internal applications and software as a service (SaaS) apps. This year, the emphasis has shifted to core network components: Three out of five (60%) respondents report already using MFA and/or SSO for servers, and databases are gaining new Identity-backed protection as well, with 57% of respondents having already extended MFA and/or SSO to them. From a regional perspective, there were no meaningful differences among regions: Servers, databases, and apps (internal and SaaS) were the top classes named by companies in the North America, EMEA, and APJ regions, both in terms of where they've already extended MFA/SSO and where they plan to extend these protections next.

Stronger authenticators are closing the gap on passwords

Passwords remain the stubborn standard for authentication, despite their low assurance, and are still used at more than half of our respondents' organizations, across all regions. Security questions (a similarly low-assurance factor) are the second-most often used, globally and in EMEA and APJ, while they've taken the top spot in North America. Overall, organizations are still using low-assurance factors at a high rate (these factors also include hardware OTP and SMS/Voice/Email OTPs), even though they can be compromised relatively easily by cybercriminals.

Medium-assurance factors like physical token OTPs and push authenticators are in use at fewer organizations (36% and 29%, respectively), and just 19% of organizations are using high-assurance factors like platform-based authenticators and biometrics. We expect to see MFA continue its march to the mainstream, while increasing regulations will likely push industries like financial services and the public sector toward passwordless and other high-assurance phishing-resistant authentication factors.

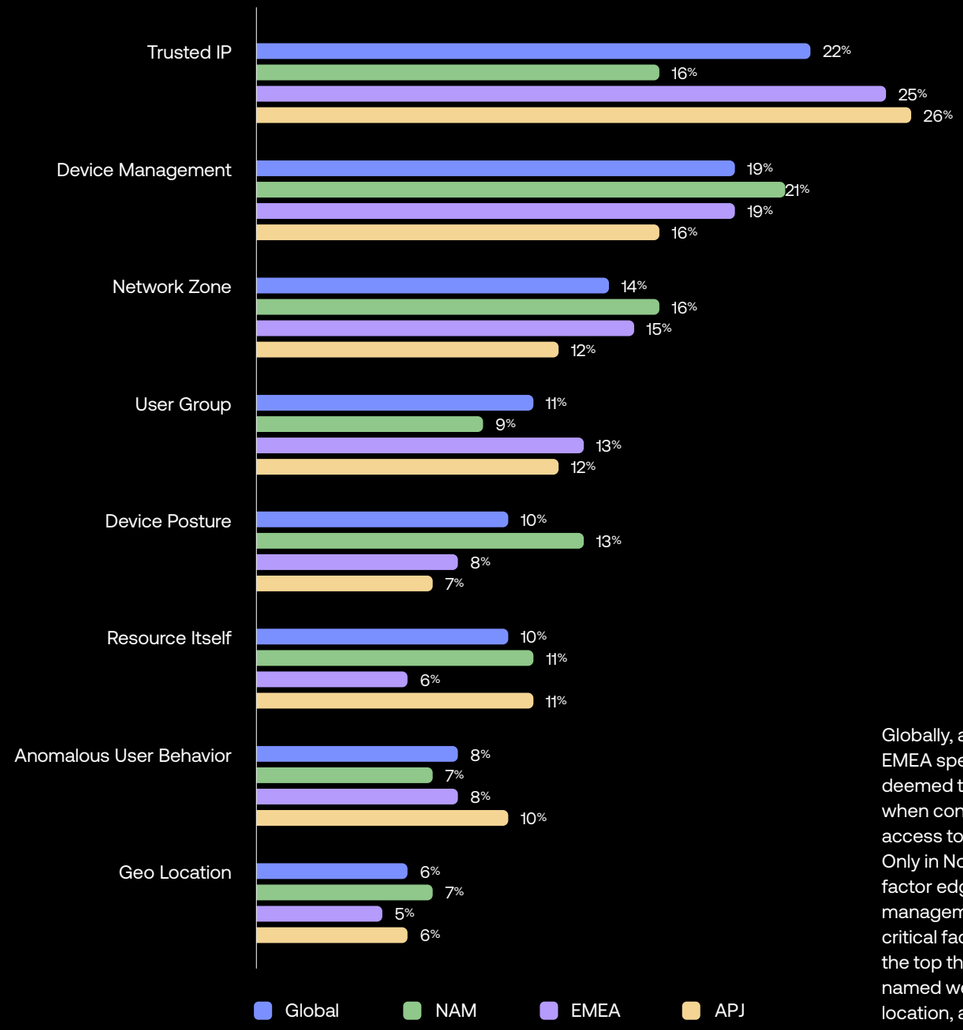
Select the authentication factors that your organization uses to verify internal and external users.
Regional comparison



Workforce Identity maturity

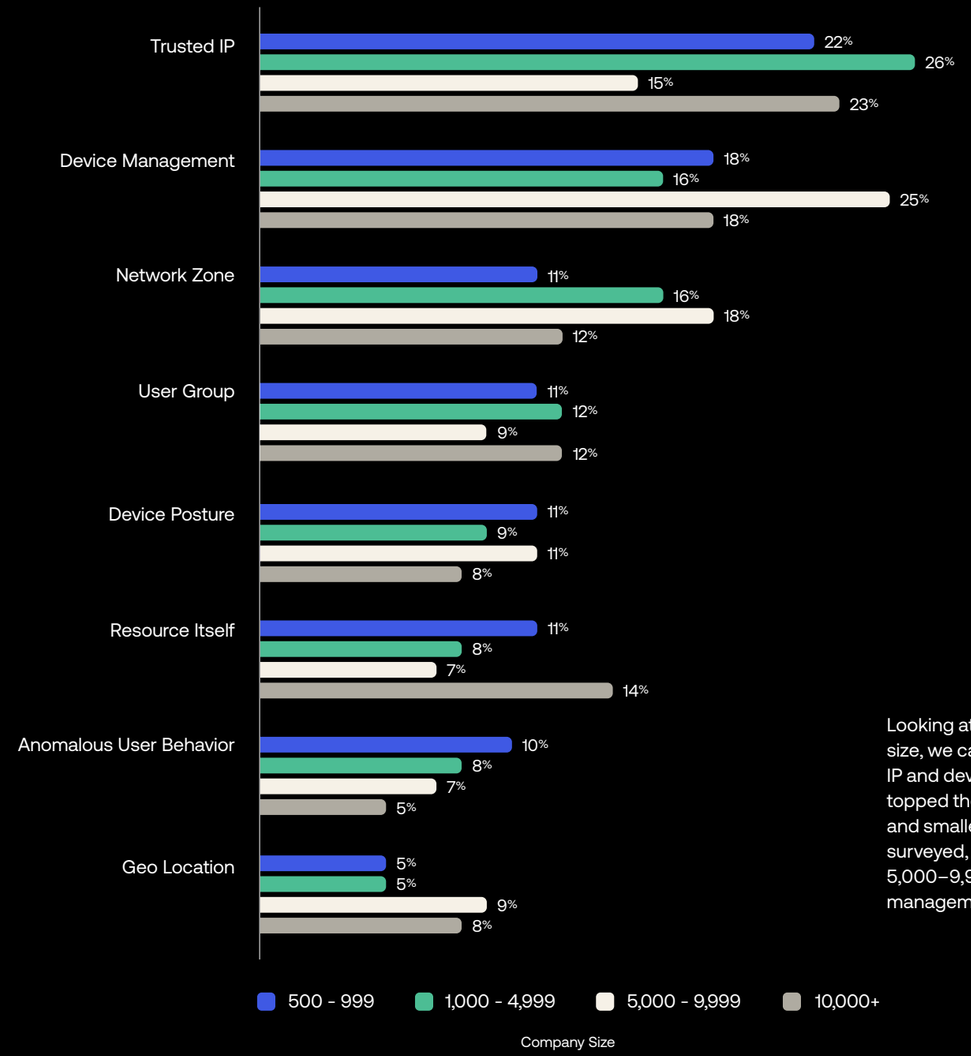
Approving access to internal resources

What are the most critical factors when controlling and approving access to your internal resources?
Regional comparison



Globally, as well as in APJ and EMEA specifically, trusted IP was deemed the most critical factor when controlling and approving access to internal resources. Only in North America was this factor edged out, by device management (the second-most-critical factor globally). Last year the top three critical factors named were device trust, geo location, and trusted IP.

What are the most critical factors when controlling and approving access to your internal resources?
By company size



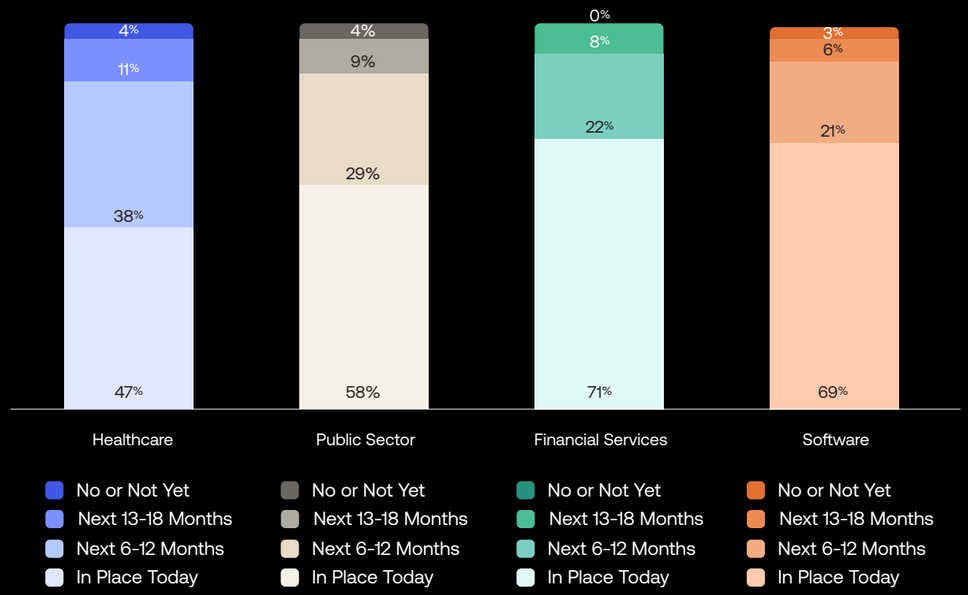
Looking at the data by company size, we can see that trusted IP and device management topped the list for the largest and smallest companies we surveyed, while those between 5,000–9,999 deemed device management more critical. ■

Zero Trust progress by industry

A deeper dive into the details for key industry verticals

The journey to Zero Trust varies greatly from industry to industry, as do company priorities and practices. With this year's survey, we again focused on the data for four key industries: healthcare, the public sector, financial services, and software. The first three are especially highly regulated, and therefore have additional incentives to invest in Zero Trust security initiatives to keep their ecosystems secure and compliant. Taken as a whole, all four industries seem to be ahead of where they were last year, but are still finding their way to leveraging true Zero Trust security.

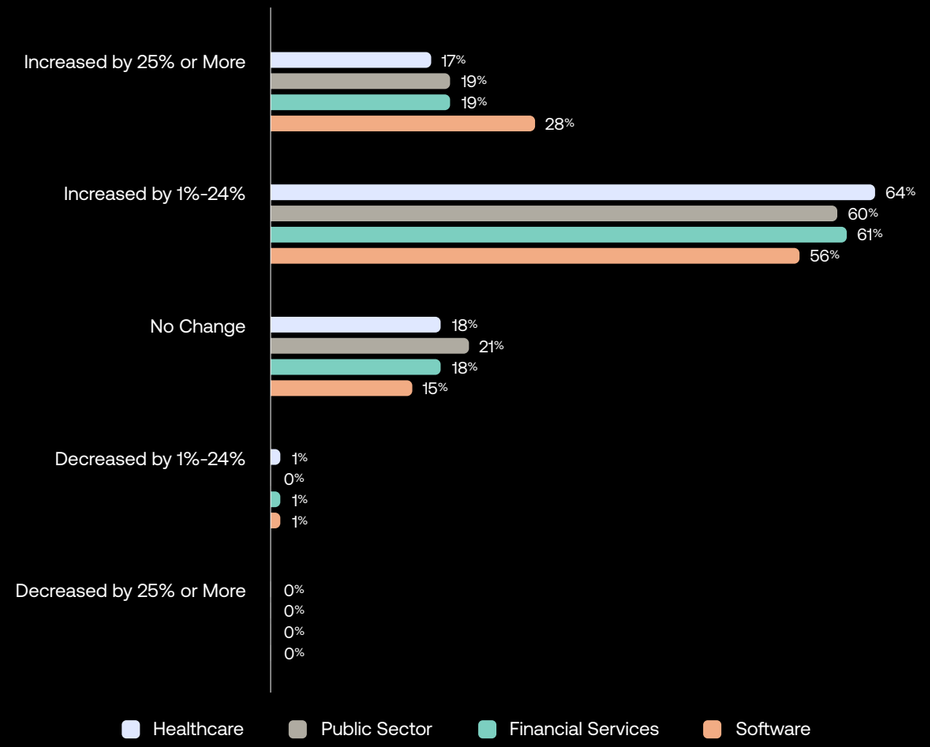
Does your organization have a defined Zero Trust security initiative today, or that you're planning to start on in the next 12–18 months?
Comparison by industry



Financial services and software lead all sectors in Zero Trust adoption

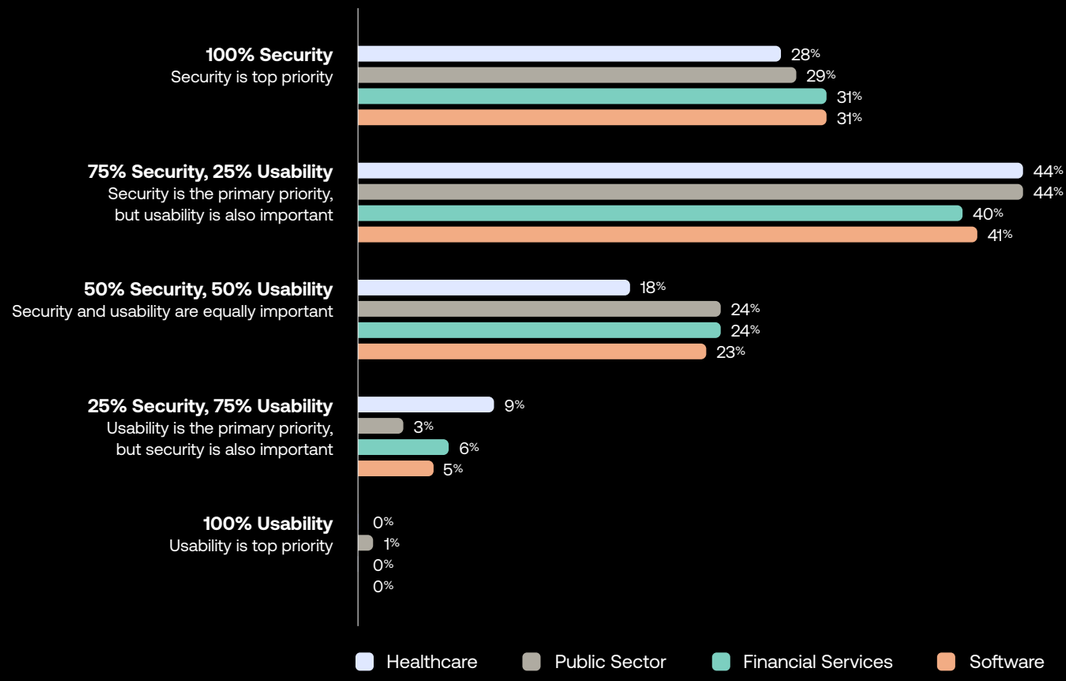
Across industries, this year's survey reveals a clear dedication to Zero Trust. No more than 4% of respondents in any of our four target sectors selected "no Zero Trust initiative in place and none planned for the following 18 months." Companies in financial services and software are more likely to have an initiative in place today (at 71% and 68%, respectively), with healthcare and the public sector only a little ways behind, as we'll detail on the following pages.

How has your organization's budget for security initiatives around the adoption of a Zero Trust strategy changed (if at all) in the past 12 months?
Comparison by industry



Despite macroeconomic pressures forcing cost-cutting elsewhere, organizations across all four of our focus industries are still putting their money where their mouth is: investing in Zero Trust security initiatives. Around four out of five organizations we surveyed, across all four industries, saw an increase in budgets over the past year for security initiatives, while almost no surveyed organizations in any industry saw their security budgets decrease.

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



The key takeaway from this top-heavy, security-centric chart is unmistakable; data breaches occur nearly five times a day now (according to The Identity Theft Resource Center's 2022 Data Breach Report), and in this climate, usability is taking a backseat to security. Respondents across all four of our key industries were most likely to report that they're placing 75% of their emphasis on security and 25% on usability; the second most likely response, for each, was that security is their top priority outright. Minimizing friction for employees and contractors remains important, but in highly regulated industries, the risk of providing a suboptimal user experience doesn't outweigh the risk of a security or compliance breach.

Zero Trust progress by industry

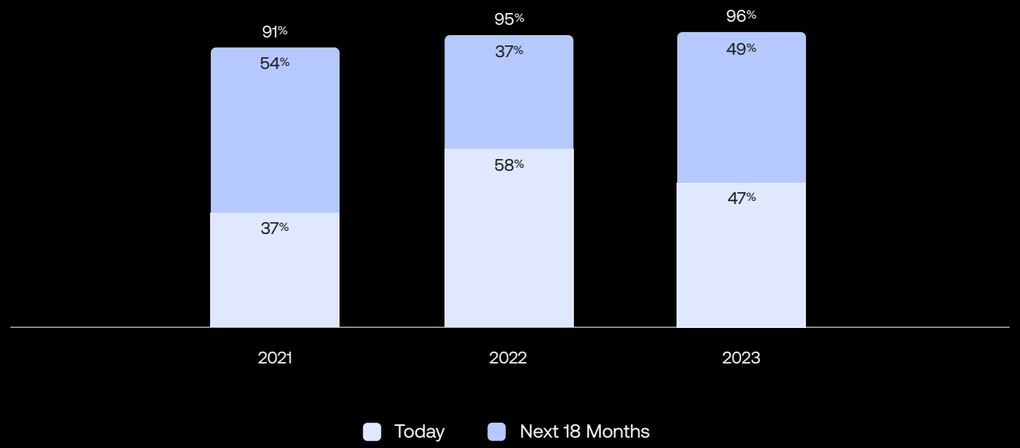
Healthcare

The healthcare sector can sometimes be less quick to move, but organizations here are continuing to make progress on Zero Trust planning and execution. The majority of healthcare respondents either have a Zero Trust initiative in place or plan to in the not-too-distant future. And though many in the sector still struggle to evolve away from risky lower-assurance authentication factors, these organizations are by and large recognizing the importance of Identity and embracing MFA and SSO for internal and external users, as well as for databases and other resources.

Zero Trust definition and planning phases close in on 100%

Over the past three years, we've seen the healthcare industry's interest in Zero Trust initiatives wax and wane, but not by much. All but 4% of healthcare organizations surveyed this year either have a Zero Trust initiative in place now or are planning one in the next 18 months. And the total number of healthcare organizations either with an initiative in place or in their near-future plans has been inching closer to 100% each year. (Fewer organizations this year than last report having an initiative in place already, possibly due to a 2022 decrease in IT spending, reported by The Wall Street Journal, that may be reversing now). In the aggregate, we expect that more healthcare organizations will put their Zero Trust initiatives into action, while those that have one already will further progress those initiatives.

Does your organization have a defined Zero Trust security initiative today or that you're planning to start in the next 18 months?
Healthcare year-by-year comparison

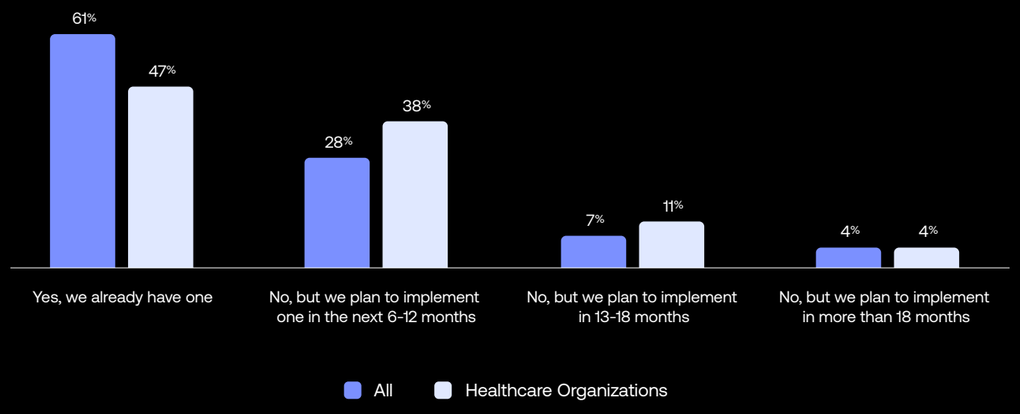


Healthcare lags slightly behind the average, but has plans to catch up

Measuring healthcare's performance against global organizations' performance, we see that fewer healthcare organizations currently have a Zero Trust initiative in place relative to the global average. However, these companies are working overtime to catch up, and far outpace global organizations when it comes to plans for the next 6–12 months — 38% of healthcare organizations plan an implementation in that timeframe, vs. just 28% for global organizations.

When we asked how important Identity is to their Zero Trust security strategy, more than nine out of 10 healthcare respondents said that Identity was either very important or somewhat important. This is perhaps no surprise, given the highly sensitive personally identifiable information that's so critical to protect for companies in the healthcare sector (and such a focus of their regulators).

Does your organization have a defined Zero Trust security initiative today or that you're planning to start in the coming months?
Healthcare vs. all respondents

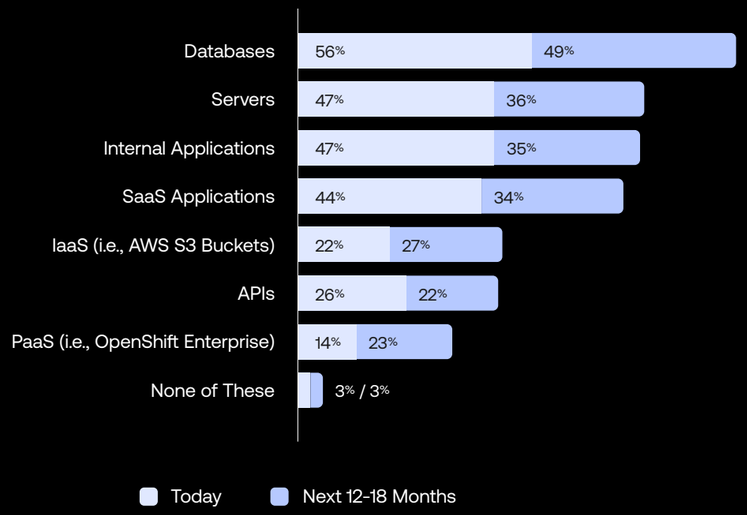


Which of the following initiatives has your organization already implemented, or do you plan to implement within the next 12–18 months?
Healthcare

MFA and directory connection are top healthcare initiatives

MFA for employees and for external users are perennially among the most popular initiatives for healthcare organizations, and this year's no exception. Connecting employee directories to cloud apps rounds out the top three responses in terms of security initiatives that have already been implemented. More than a third of organizations already have MFA in place for employees at surveyed healthcare organizations, and in terms of future planning, adding MFA for employees tops the list, at 52%. Other initiatives like SSO and automated provisioning were lower planning priorities for healthcare organizations this year.

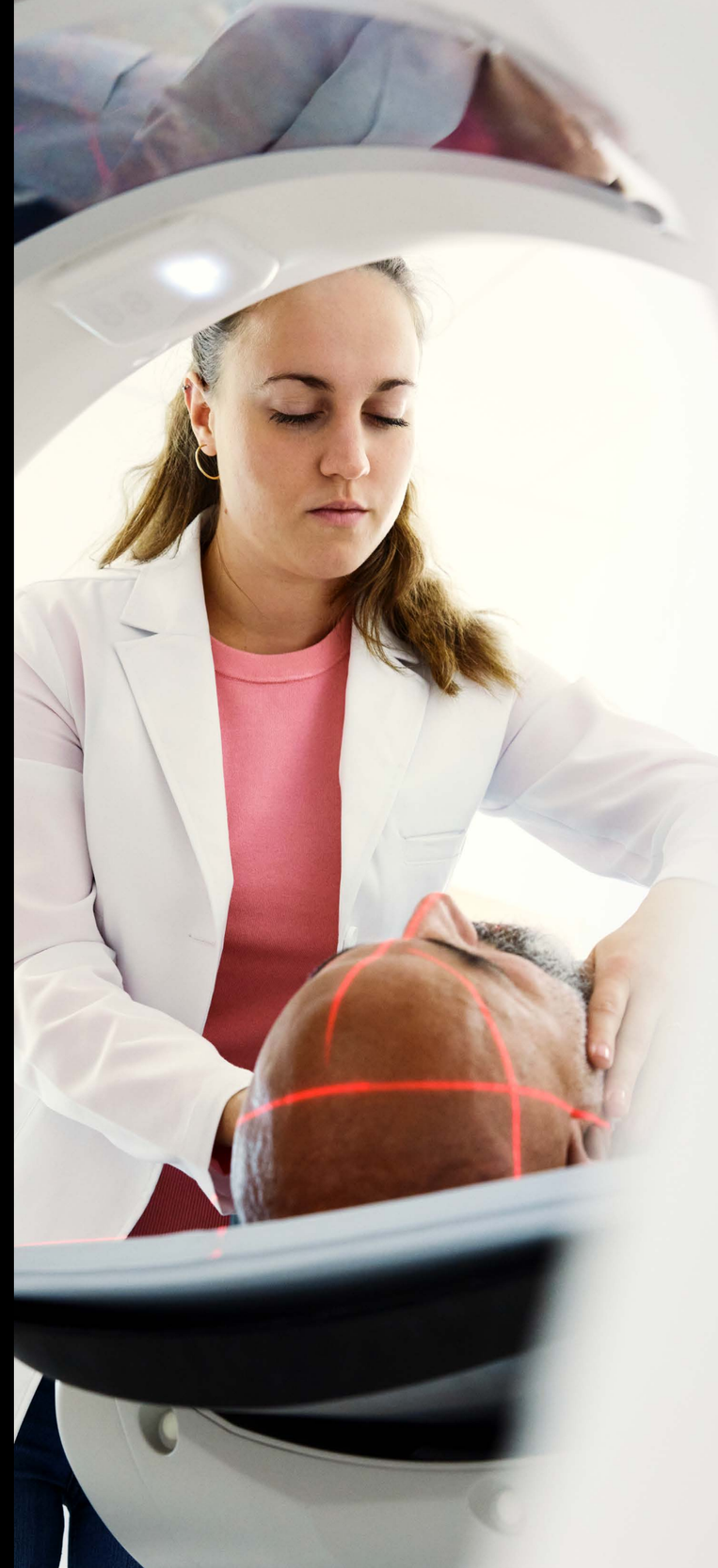
Which classes of resources have you already extended SSO and/or MFA to, and which do you plan to in the next 12–18 months?
Healthcare

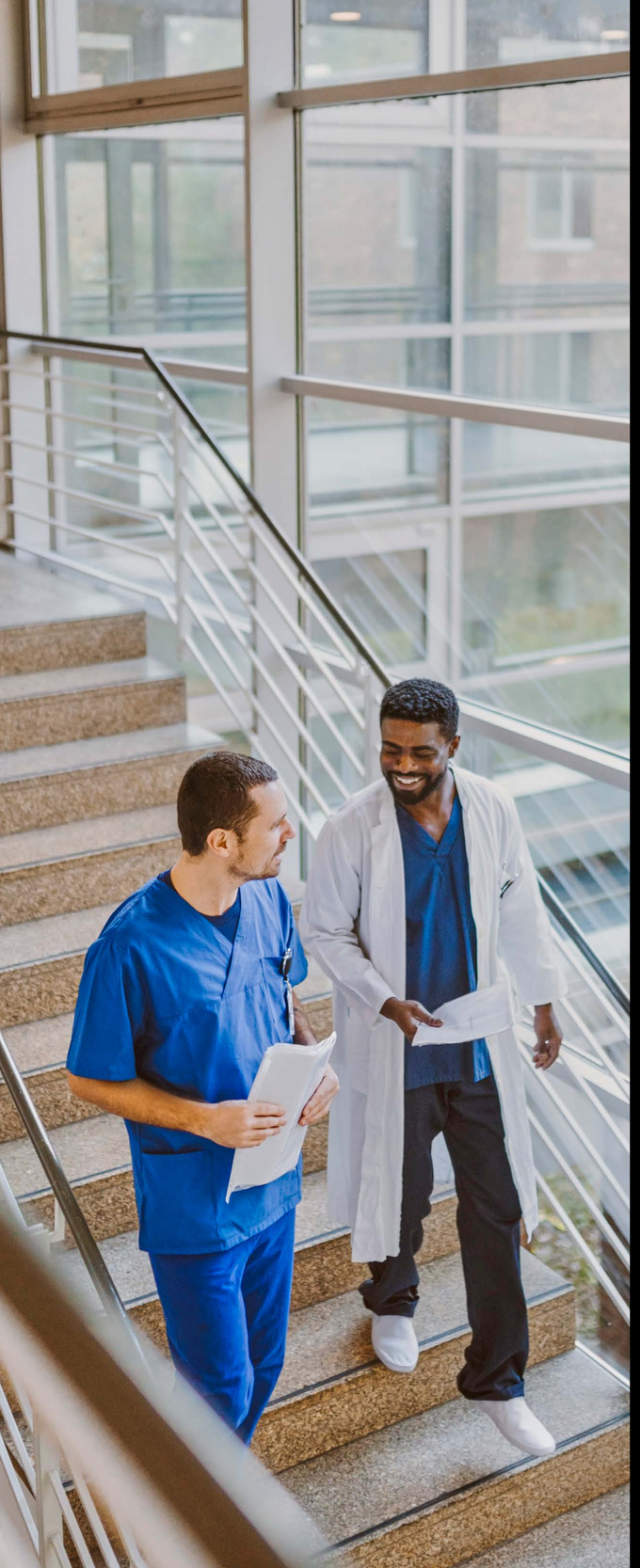


Databases, servers, and apps top the SSO/MFA protection list

Healthcare organizations are most likely to have extended SSO and/or MFA protection to databases, which can contain private, sensitive patient information that represents a high-value target for cybercriminals. But extending SSO/MFA to servers and internal and SaaS apps isn't far behind, in terms of current adoption and future planning for organizations in this sector.

Note: column totals may add to more than 100% due to respondents who select both responses.

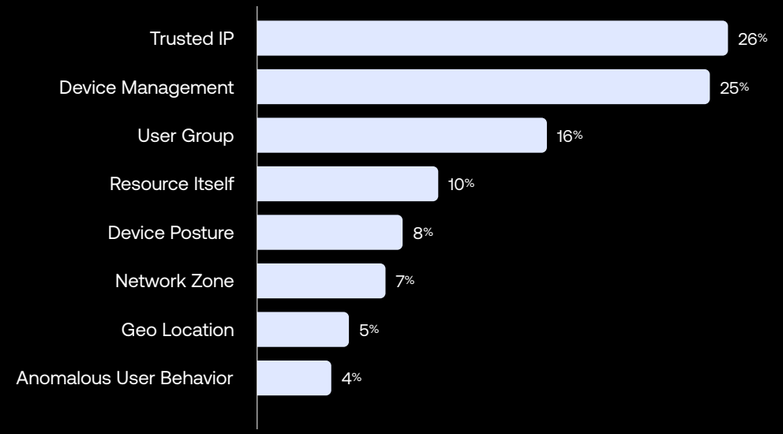




Trusted IP and device management deemed top access control factors

More than half of all healthcare organizations responding to our survey consider either trusted IP or device management the top factor when controlling and approving access to internal resources, which is in line with the top two choices of global respondents. User group and the resource itself were next in line as top factors for controlling and approving access.

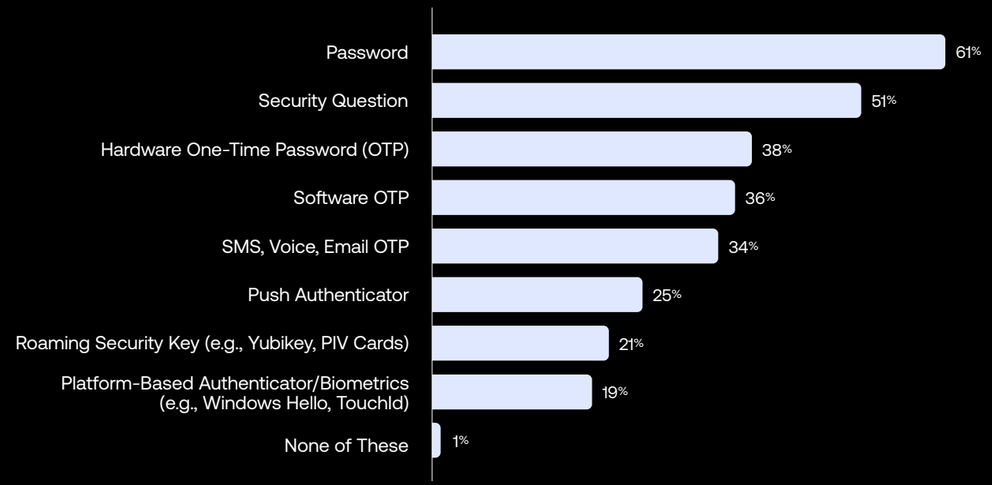
Rank the most critical factor when controlling and approving access to your internal resources.
Healthcare



Password and security questions are healthcare's top auth factors

Passwords are still the leading authentication factor for healthcare organizations, with 61% of respondents citing their use, so the passwordless future is still a ways off for this sector. Security questions are a close second, in use at more than half of all healthcare companies surveyed. One-time passwords (OTP) — in hardware, software, and SMS/voice/email varieties — are in a virtual tie for third, with platform-based authenticators and biometrics least often reported as top authentication factors for this sector.

Select the authentication factors that your organization currently uses to verify internal and external users.
Healthcare



Zero Trust progress by industry

Public sector

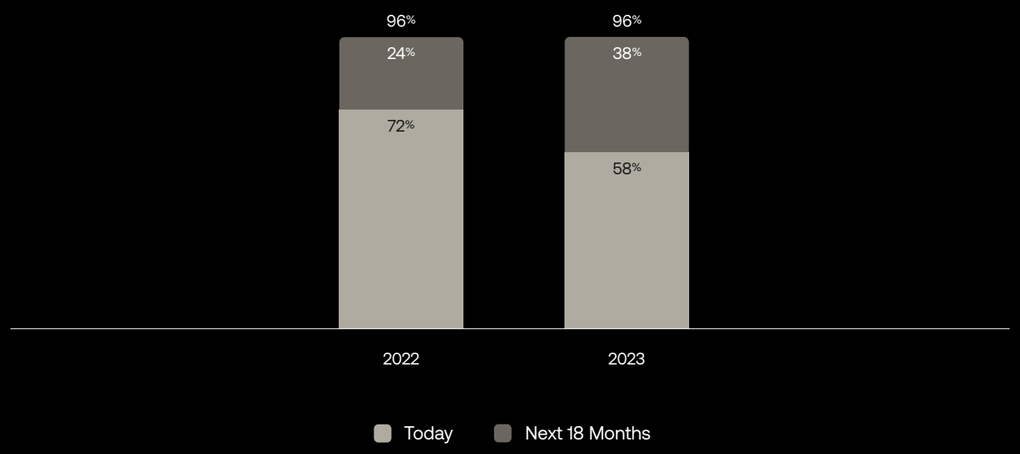
There may be no industry under greater pressure to shore up their security with Zero Trust than the global public sector. In North America, for example, the U.S. Federal Zero Trust Strategy now explicitly requires all federal agencies to meet specific cybersecurity standards and objectives by September 2024 to reinforce the government's defenses against increasingly sophisticated and persistent threat campaigns. And that's hardly the only U.S. governmental guidance: Consider, too, the National Cybersecurity Strategy and the Department of Defense's Zero Trust Strategy and Roadmap.

This year, we surveyed public sector organizations in North America, EMEA, and APJ regions. (For this report, public sector organizations do not include state or local organizations.) Our survey results revealed that 58% of the organizations in this sector already have a Zero Trust initiative in place, and another 38% plan to get one off the ground shortly. These organizations are using SSO and/or MFA to safeguard their most important resources, and embracing strong boundaries to keep their infrastructure and assets safe.

Nearly all public sector organizations have Zero Trust initiatives in the works

Public sector organizations are holding steady in their commitment to Zero Trust. From 2022 to 2023, the overall number of public sector organizations that either already have a Zero Trust initiative in place or that plan to start one soon has held steady at 96%. Among last year's surveyed public sector organizations, a full 72% had Zero Trust initiatives in place. But it's worth noting that last year's public sector respondents were almost all (86%) from North America. This year, we widened the scope: Only 31% of surveyed public sector companies this year were from North America, and in this wider sampling just 58% report already having a Zero Trust initiative in place, though another 38% have definitive plans to start their initiatives soon.

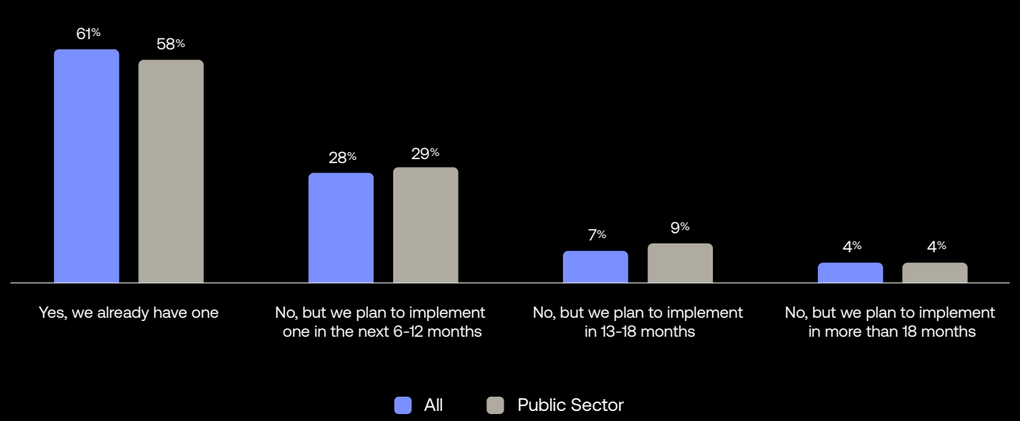
Does your organization have a defined Zero Trust security initiative today or that you're planning to start in the next 18 months?
Public sector year-by-year comparison



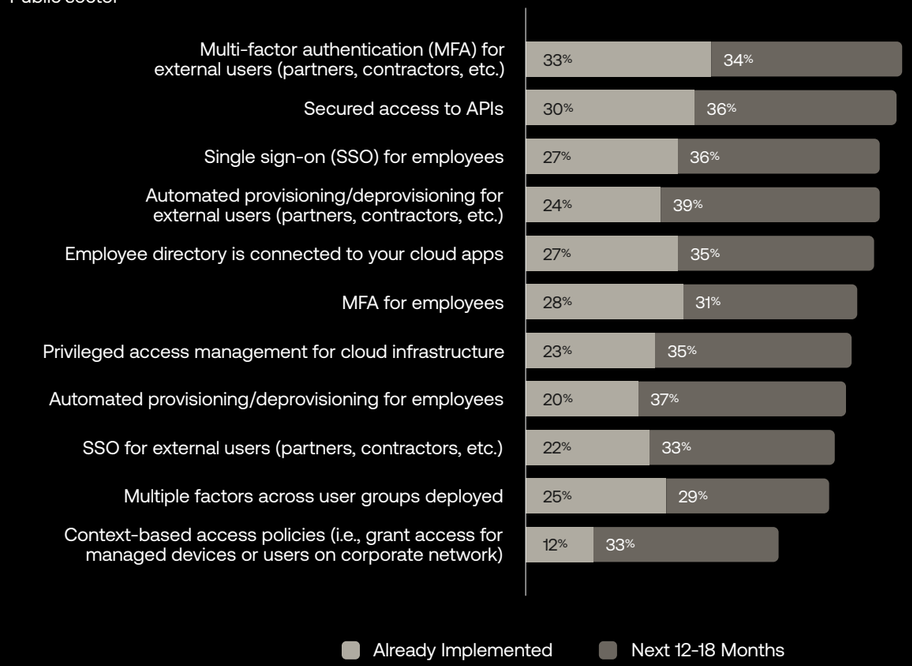
Public sector organizations lag behind on initiatives, but outpace on planning

This year's surveyed public sector organizations are almost on pace with the global average when it comes to already having a Zero Trust security initiative in place: 61% of all companies have such a program, while 58% of organizations in the public sector do. However, nearly one-third of public sector organizations plan to begin an initiative within the next 6–12 months — in many cases, as a response to government mandates — slightly outpacing the global average.

Does your organization have a defined Zero Trust security initiative today or that you're planning to start in the coming months?
Public sector vs. all respondents



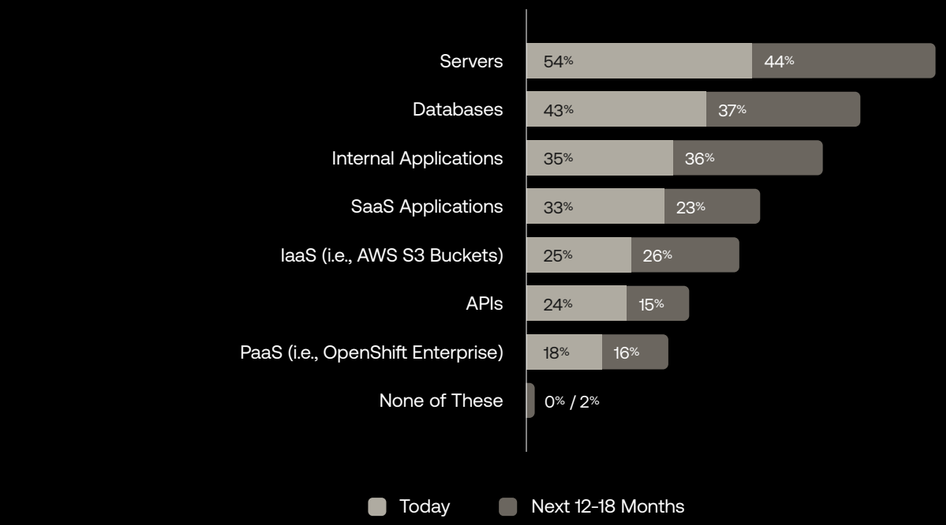
Which of the following initiatives has your organization already implemented, or do you plan to implement within the next 12–18 months?
Public sector



MFA for external users, and securing API access top public sector initiatives

Government entities around the world rely on a wide array of internationally based contractors and external partners, so it's no surprise applying MFA for external users (including partners and third-party vendors) and securing API access are the leading initiatives for public sector organizations, at 33% and 30% of surveyed organizations, respectively. Another 34% of public sector organizations plan to extend MFA to these external users within the next 12–18 months. Implementing SSO for employees and automated provisioning/deprovisioning for external users take the next spots in terms of priority for today's public sector organizations.

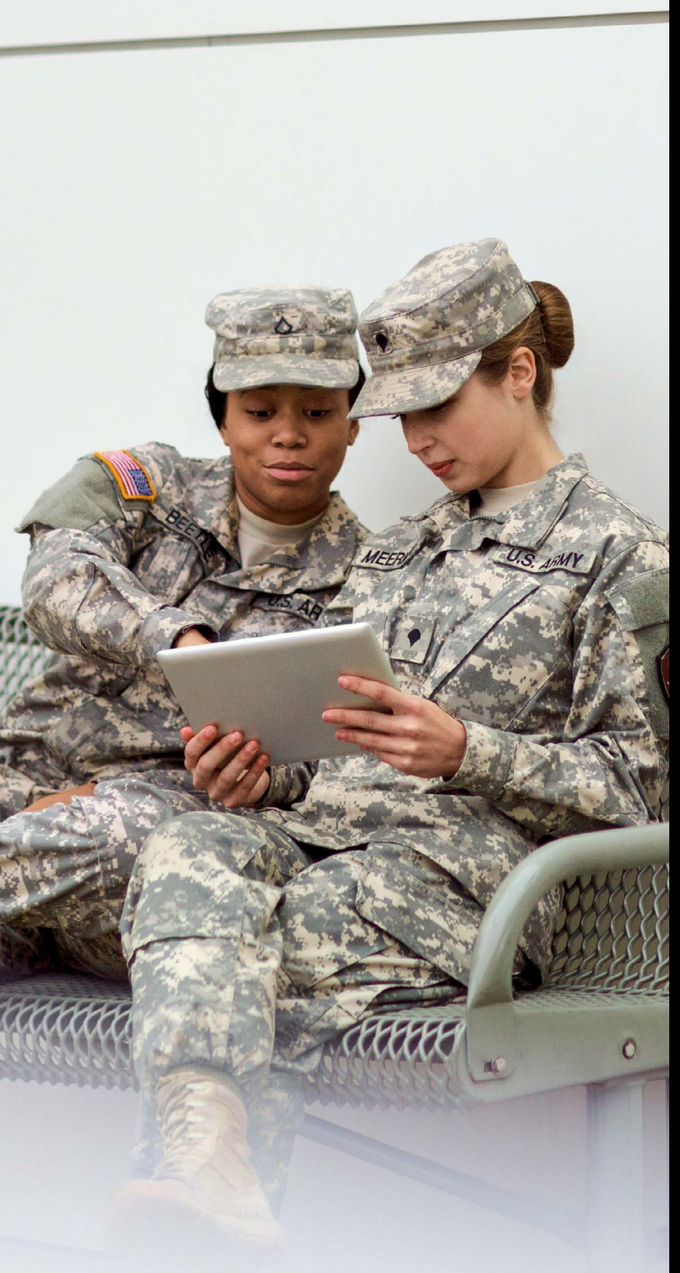
Which classes of resources have you already extended SSO and/or MFA to, and which do you plan to in the next 12–18 months?
Public sector



Note: column totals may add to more than 100% due to respondents who select both responses.

SSO/MFA protection extended first to servers and databases

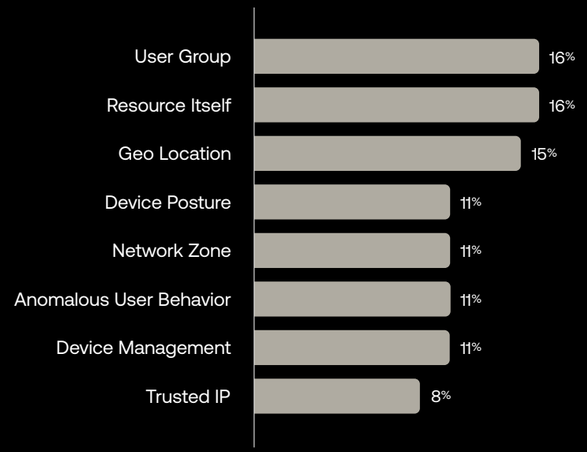
Servers and databases rule the day for the public sector when it comes to SSO and MFA protection. More than half of surveyed organizations in this sector have already applied SSO and/or MFA protection to servers, and 43% have applied one or both to databases. Internal apps and SaaS apps come in right behind these, with each in place already at about a third of organizations, followed by IaaS, APIs, and PaaS.



“User Group” and “Resource” most critical factors for resource access

Public sector organizations are especially careful about protecting their digital assets from unwelcome eyes. The factors that top their list for controlling and approving access to internal resources starts with user groups, the resource itself, and geo location, followed by a virtual tie for most of the other factors listed.

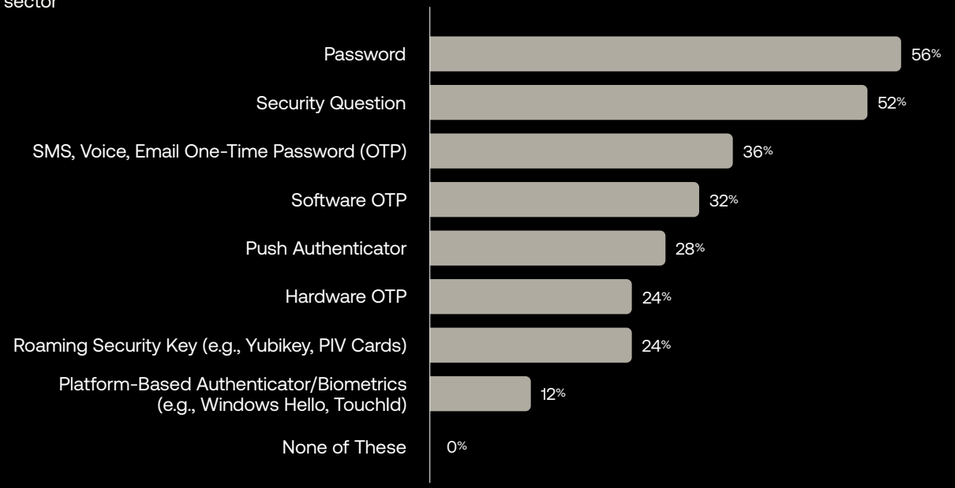
Rank the most critical factor when controlling and approving access to your internal resources.
Public sector



“Password” and “Security Question” still lead the pack for verifying users

Lower-assurance authorization factors still lead the pack in the public sector, as elsewhere in this report, with passwords and security questions cited by more respondents than any other factors. Change is in the air, however, as higher-assurance factors like software and hardware OTP, as well as SMS/voice/email OTP, gain popularity. (The ephemeral nature of OTP factors makes them inherently safer than storable, hackable passwords and security questions.) ■

Select the authentication factors that your organization currently uses to verify internal and external users.
Public sector



Zero Trust progress by industry

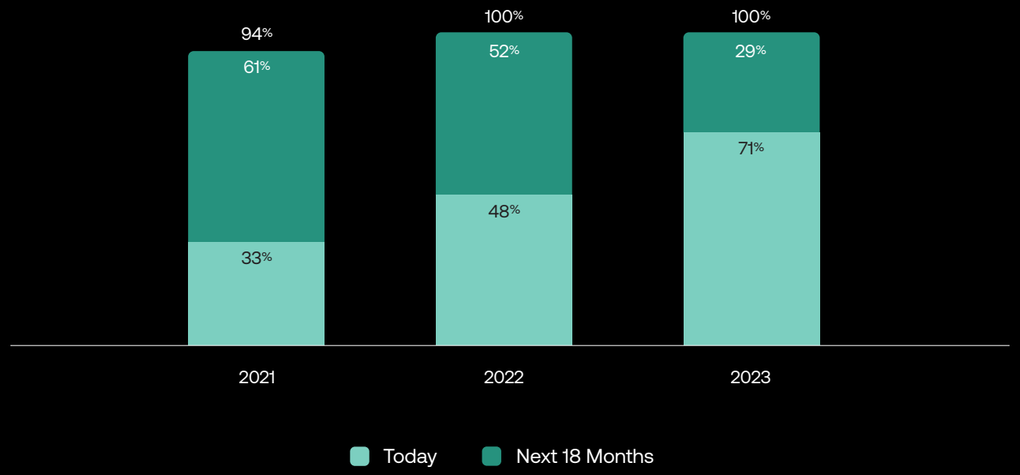
Financial services

Financial services organizations are prime targets for cyberattacks and have been hit especially hard by security breaches over the past few years. At least 79 U.S. financial services companies reported data breaches affecting 1,000 or more consumers in 2022, with the biggest breaches each affecting millions of consumers. Zero Trust gives these organizations a clear path forward toward securing their vital systems and customer data. Today, more than two-thirds of all financial services organizations have a Zero Trust initiative in place, and most of the remaining third have an initiative in the works.

Seven of 10 FinServ companies have a Zero Trust initiative in place today

Security breaches can be incredibly costly: an average of $4.45M per breach, according to IBM's Cost of a Data Breach 2023 report. So it's no coincidence that more and more financial services organizations each year are putting Zero Trust initiatives in place. In 2021, just one-third of respondents in this sector reported having a defined Zero Trust initiative, and in 2022 that number jumped to nearly half of financial services respondents. This year, a full 71% of the financial services organizations in our survey report having an active Zero Trust initiative in place. That's an impressive three-year growth curve.

Does your organization have a defined Zero Trust security initiative today or that you're planning to start in the next 18 months?
Financial services year-by-year comparison

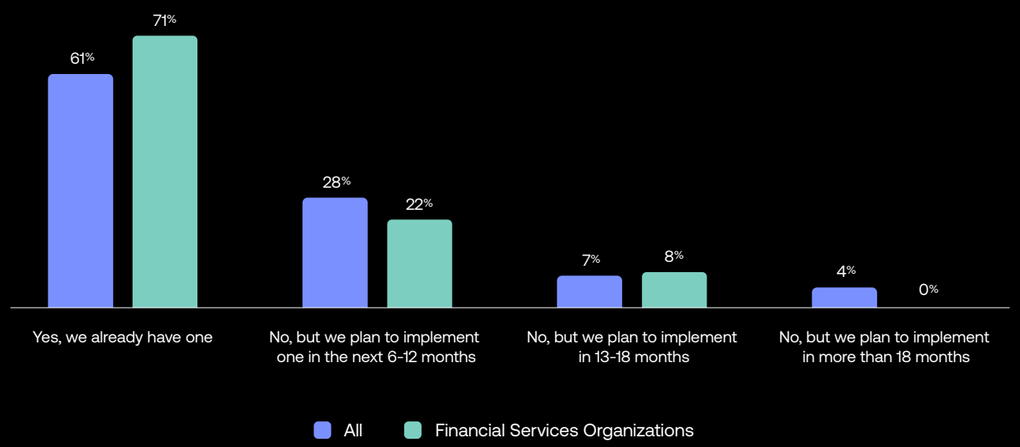


Financial services lead the pack in bringing Zero Trust initiatives to life

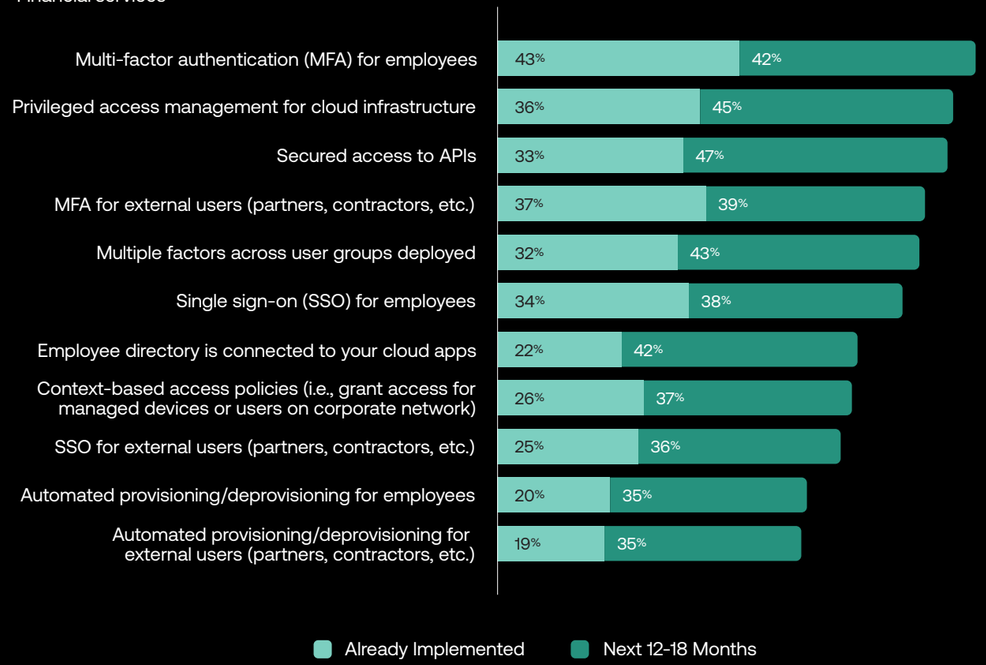
More than two-thirds of financial services organizations have a defined Zero Trust initiative underway already, and another 22% and 8% plan to do so within the next 12 and 18 months, respectively. This sector is outpacing the global average for initiatives already in play, and all surveyed FinServ organizations said they either already had a Zero Trust initiative in place or planned to implement one within an 18-month window.

When it comes to Identity's value to Zero Trust, the financial services sector is fully onboard. More than 90% of this industry's respondents said that Identity is either extremely or somewhat important to their Zero Trust strategy, with nearly half calling it extremely important. Only about 2% deemed it unimportant or extremely unimportant.

Does your organization have a defined Zero Trust security initiative today or that you're planning to start in the coming months?
Financial services vs. all respondents



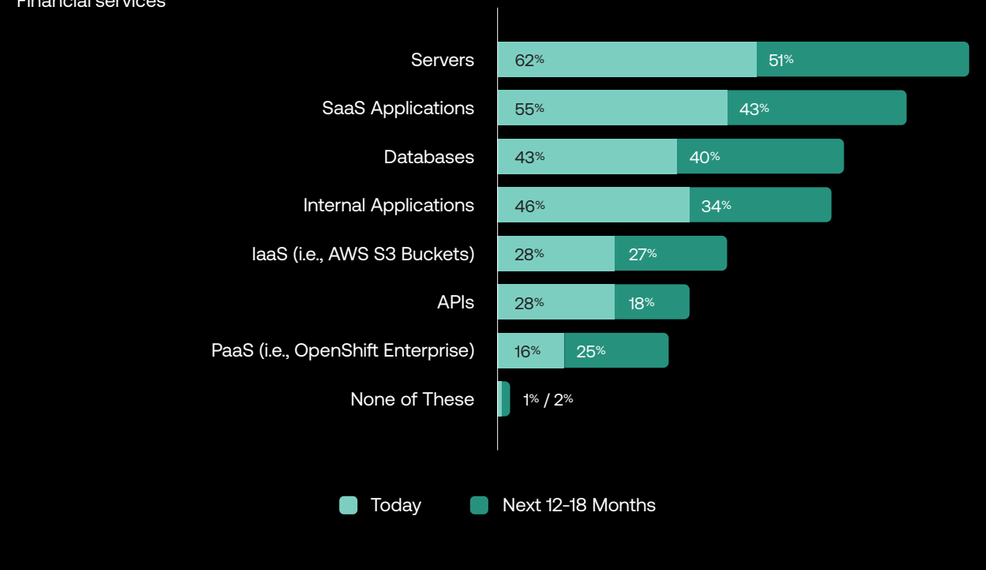
Which of the following initiatives has your organization already implemented, or do you plan to implement within the next 12–18 months?
Financial services



Top initiatives for FinServ: MFA, privileged access management

MFA for employees is the leading Zero Trust initiative for financial services organizations this year, with 43% of respondents having already implemented this security feature and another 42% planning to implement it in the next 12–18 months. Privileged access management for the cloud is the implementation cited next most often, at 36% of companies, and 33% of companies report having secured access to APIs. Lower priorities for this sector include SSO for external users and automated provisioning and deprovisioning.

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



Note: column totals may add to more than 100% due to respondents who select both responses.

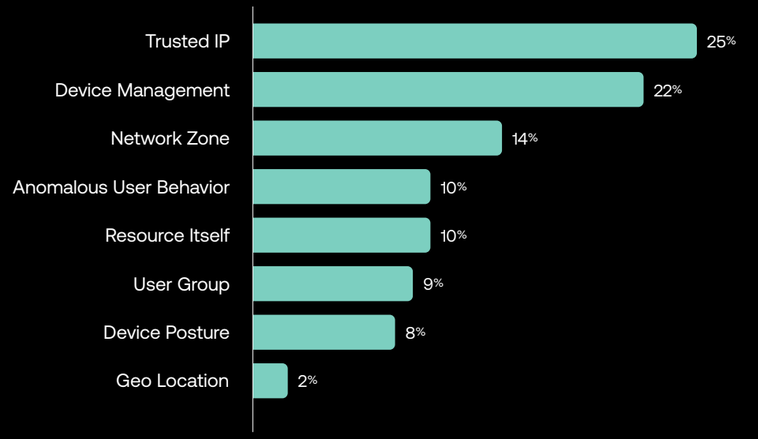
SSO and/or MFA applied most to servers, SaaS applications

Financial services organizations are keeping a close eye on their servers, with 62% already protecting access to them with SSO and/or MFA, and 51% planning to extend such coverage in the near future. (Respondents could choose both options.) SaaS apps, databases, and internal apps round out the top resources to which financial services organizations are applying (or planning to apply) these Identity measures.

Trusted IP and device management are top access approval factors

When it comes to controlling and approving access to internal resources, financial services organizations really want to know where you are and what device you're using. One in four surveyed named trusted IP their top access approval factor, and another 22% chose device management as their top factor. Network zone, anomalous user behavior, and resource itself followed, with geo location a standout as the least-chosen factor.

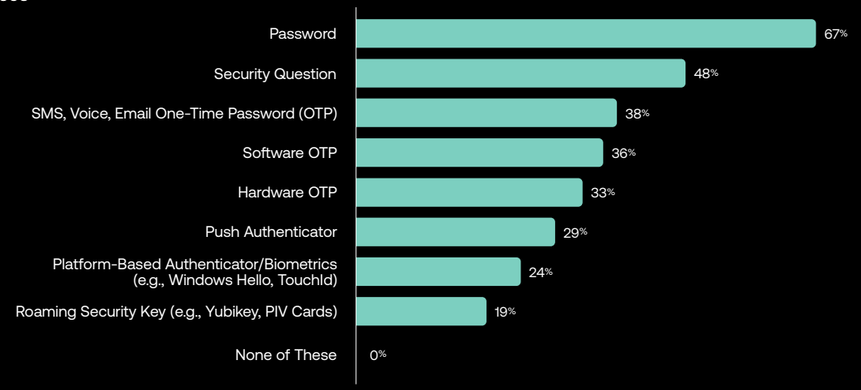
Rank the most critical factor when controlling and approving access to your internal resources.
Financial services



FinServ's top authentication factors: Passwords, security questions

The password still reigns supreme as the top authentication factor for financial services organizations, with fully two-thirds of respondents citing passwords as an authentication factor currently in use. Knowledge-based security questions were the second most common, at 48%, and OTP options each were cited by about a third of FinServ respondents.

Select the authentication factors that your organization currently uses to verify internal and external users.
Financial services



Zero Trust progress by industry

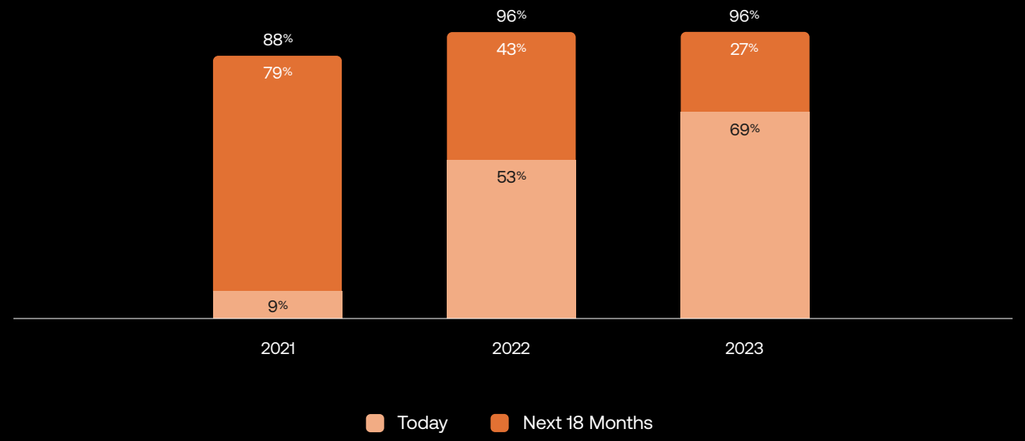
Software

In previous years, software has sometimes lagged behind our other target industries. But the sector's been making up ground steadily and progressing their Zero Trust security initiatives, outpacing the average even though they lack the extra incentives of the more highly regulated key industries we focus on elsewhere in this report. In particular, software companies are doing a better job of evolving their authentication methodology, relying more on higher-assurance authentication factors than the other focus industries in this year's survey.

Two-thirds of companies in this sector have Zero Trust initiatives

Software organizations are quickly catching up with their peers in the journey to Zero Trust. Whereas our 2021 report showed that fewer than one in 10 software respondents had current Zero Trust initiatives in place, that number today is almost 70%, with nearly all the remaining respondents saying they are planning to start one in the near future. Just 4% of software companies surveyed don't have a Zero Trust initiative in place and don't plan to put one in place over the next 18 months.

Does your organization have a defined Zero Trust security initiative today or that you're planning to start in the next 18 months?
Software year-by-year comparison

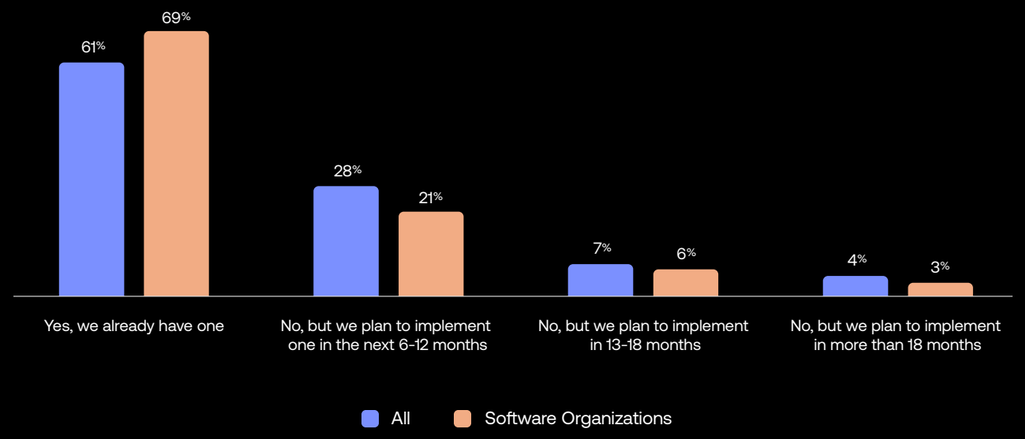


Software companies outpace their peers in ZT initiative rollouts

Software organizations are outperforming the global average when it comes to having a defined Zero Trust security initiative in place, with 69% compared to a global 61% across all respondents. The holdouts plan to start their initiatives either in the next 6–12 months (21%), 13–18 months (6%) or more than 18 months (3%).

No industry in our survey better understands Identity's value to Zero Trust than the software sector. Asked how important Identity is to their Zero Trust security strategy, more than nine out of 10 software respondents say Identity is either extremely important (54%) or somewhat important (37%), and fewer than 1% of respondents say Identity is somewhat unimportant.

Does your organization have a defined Zero Trust security initiative today or that you're planning to start in the coming months?
Software vs. all respondents

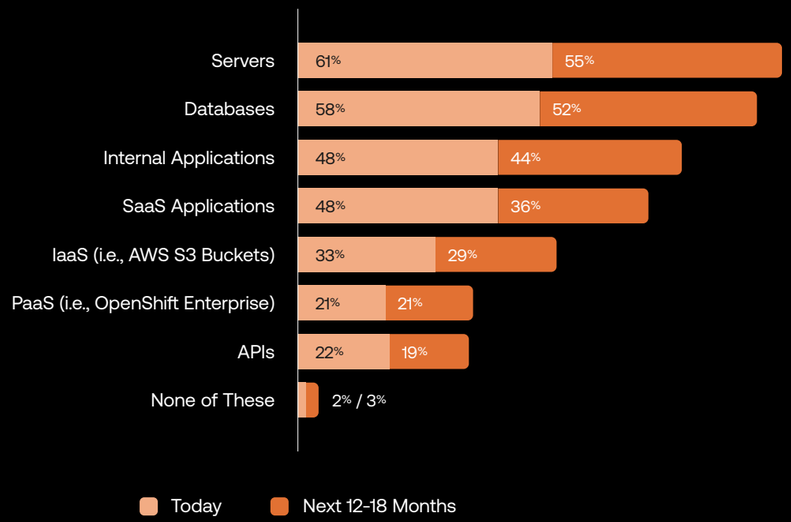


Which of the following initiatives has your organization already implemented, or do you plan to implement within the next 12–18 months?
Software

Top initiatives in software: MFA for employees and API security

MFA for employees and secure access to APIs are equally important to the software organizations we surveyed. In each of those categories, 34% of respondents said they already had an initiative in place, and more than two in five software companies plan to implement one or both of those in the next 12–18 months. MFA for external users came in next, at 32%, in terms of security initiatives that have already been implemented by companies in this sector.

Which classes of resources have you already extended SSO and/or MFA to, and which do you plan to in the next 12–18 months?
Software



Note: column totals may add to more than 100% due to respondents who select both responses.

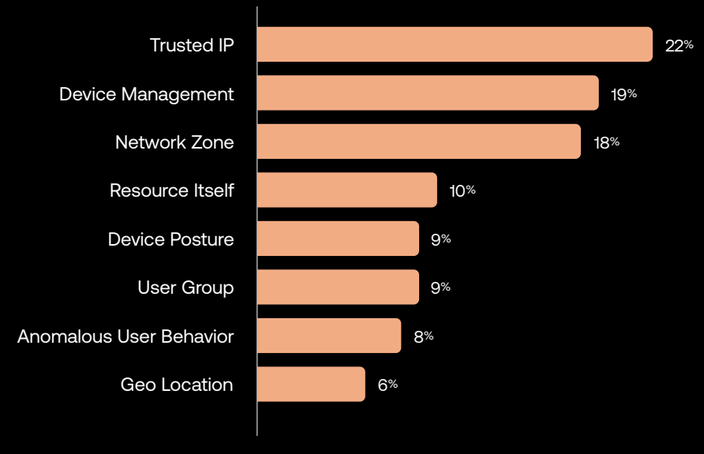
Top resources for SSO/MFA extension: Servers, databases

This year, software organizations were all about protecting access to their servers (61%) and databases (58%) by extending single sign-on (SSO) and/or multi-factor authentication (MFA) to them. An additional 48% of those surveyed indicated that internal apps are currently protected by SSO and/or MFA, and the same percentage say they've protected SaaS resources with SSO and/or MFA.

Top factors for resource access: Trusted IP, device management

When controlling access to internal resources, 22% of software companies consider trusted IP their top factor and another 19% consider device management their top factor, with network zone (18%) rounding out the top three. About one in 10 cited individual resources (such as sensitive systems) as their top factor, while 9% chose device posture or user group. Geo location was the factor least likely to be chosen as the top factor by software companies surveyed.

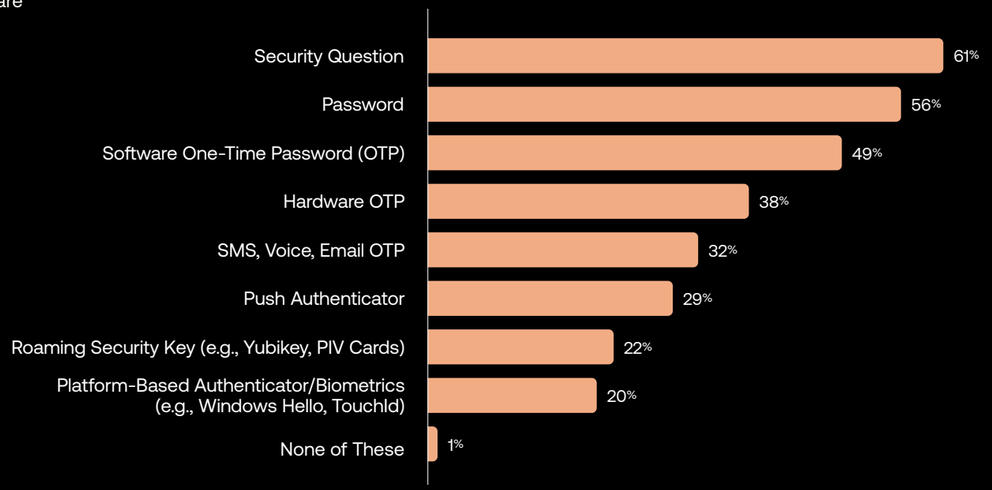
Rank the most critical factor when controlling and approving access to your internal resources.
Software



Security questions pass passwords as software orgs' No. 1 auth factor

The software sector is the only focus industry in our report for which risky, insecure passwords are not the most common authentication factor. Passwords are still up there in the number two spot — still in use at 56% of respondent companies — but the rise of security questions to the number one spot (cited by 61% of surveyed software organizations) indicates that in this sector, at least, passwords may at last be losing ground. To be clear, security questions and passwords are both low-assurance factors best replaced by higher-assurance factors like OTP, which are gaining popularity.

Select the authentication factors that your organization currently uses to verify internal and external users.
Software



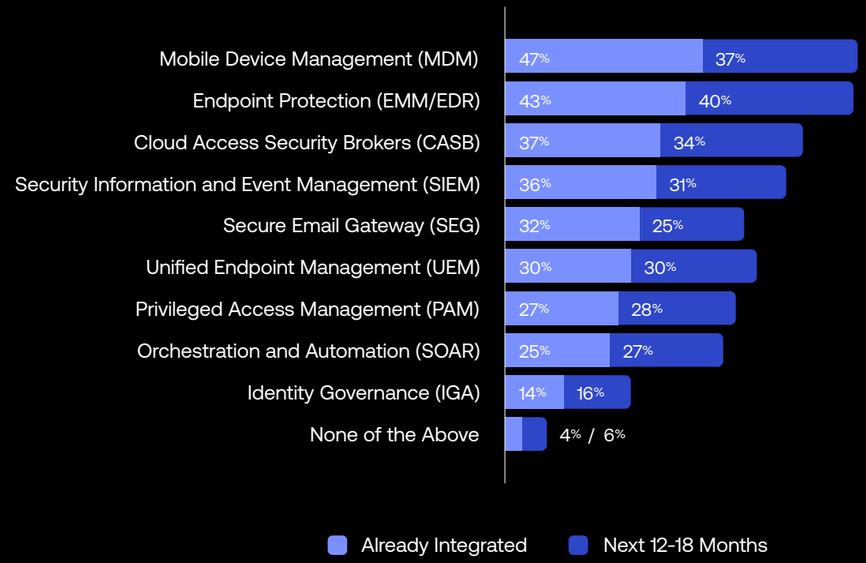
Identity-driven security

The evolving enterprise ecosystem

If Identity is the new security perimeter, then that puts Identity management squarely at the center of security strategy. Hybrid/multi-cloud organizations today have to ensure their IAM solution works hand-in-hand with security systems so security teams can keep external and internal threats at bay without impeding the efficiency of their authenticated workforce. In other words, building a true Zero Trust ecosystem means integrating Identity management tools with security stacks.

We asked security and IT leaders which tools they'd already integrated with their IAM systems and which they planned to integrate in the near future. Those results have changed a bit from last year, where security information and event management (SIEM) led the way. Today, mobile device management (MDM) is the most widely integrated system, according to our survey respondents, and SIEM, MDM, and endpoint protection are the top three "most important" systems to prioritize integrating directly with an IAM solution.

Which of the following have you integrated with your ID and access solution, and which do you plan to implement within the next 12–18 months?
All respondents



Top IAM integration solution in 2023: Mobile device management

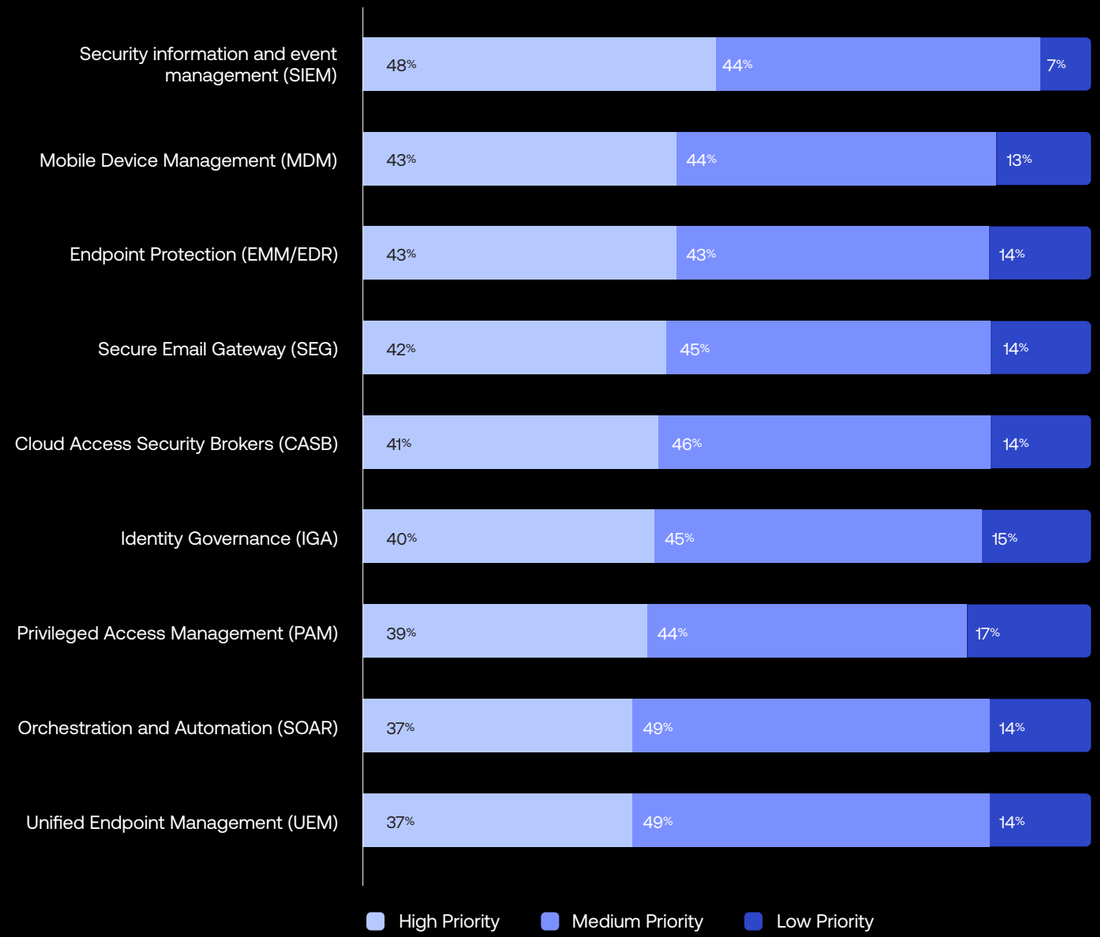
Mobile device management squeaks in as the most common IAM integration in this year's results after a long, steady rise (it was No. 7 in 2021 and No. 4 last year). In 2021, 11% of respondents had integrated MDM with IAM solutions; today, that number is 47%, with another 37% planning to do so over the next 12–18 months. The industry continues to put a strong emphasis on integrations that provide high-value security monitoring and protection tools and reliable endpoint management.

The top concerns by region:

- NAM: mobile device management, CASB, and endpoint protection
- EMEA: SIEM, secure email gateway, and unified endpoint management
- APJ: mobile device management, SIEM, SOAR, and endpoint protection

These IAM integrations can work together to simplify governance and safely enable policy-based access controls, fine-grained authorization, and other intuitive automations for forward-thinking organizations.

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



Prioritization of IAM integrations shows SIEM, MDM, and endpoints in the lead

Asked to assign high, medium, or low priority to the potential IAM integrations above, global respondents were most likely to choose SIEM as a high priority, at 48%, followed by MDM and endpoint protection, at 43% each. Integrations for SOAR and UEM were more likely to be ranked a medium priority, while no category was ranked a low priority by more than 17%. ■

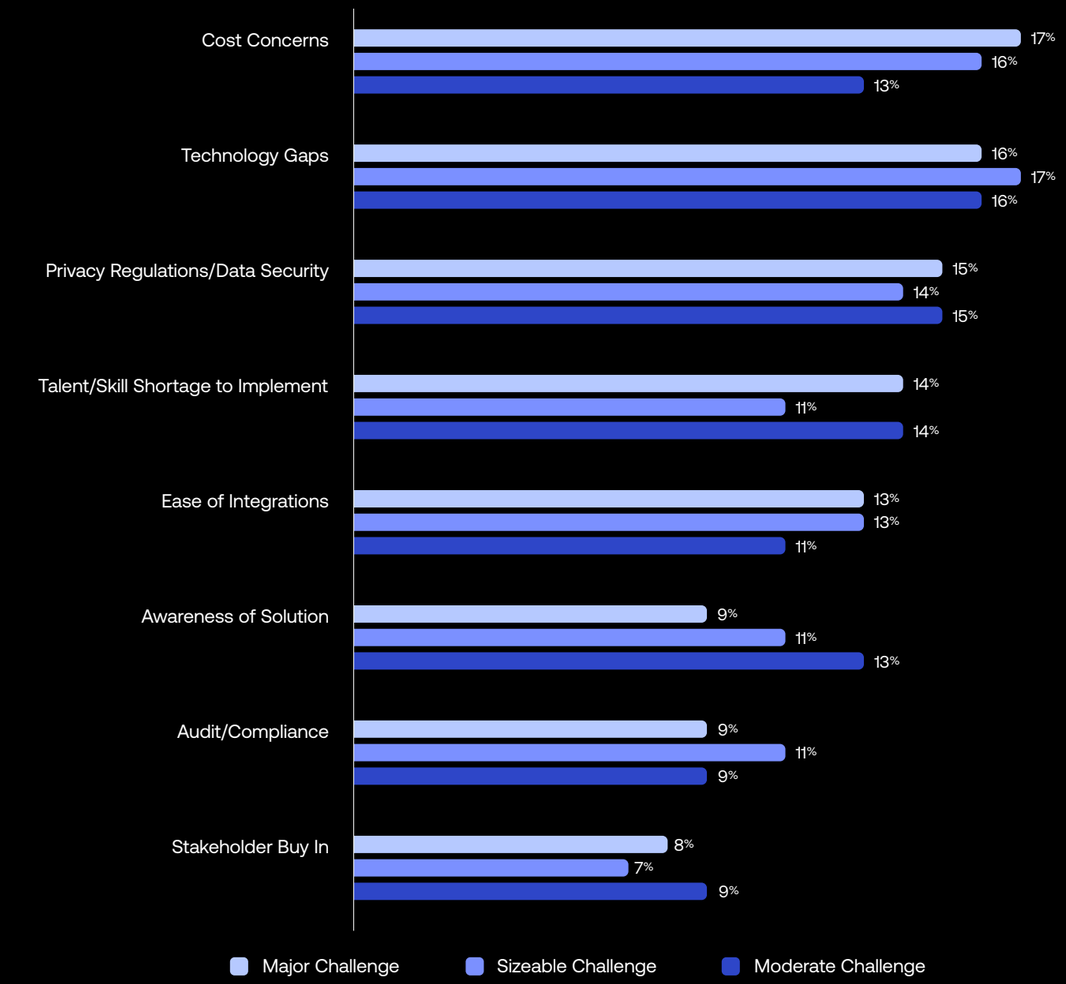
Note: column totals may not add exactly to 100% due to rounding data labels to whole numbers.

The long road to Zero Trust

Companies are overcoming systemic hurdles and launching mission-critical Zero Trust initiatives.

Zero Trust is the only way to properly secure a modern hybrid/multi-cloud enterprise, allowing organizations to confidently automate access and provisioning for global teams while mitigating internal and external threats. The philosophy is now well understood, and for the vast majority of organizations of every size, in every sector, and in every region, the plans are in place or underway. But without the right software, partners, and processes, it can be challenging to put these principles into action and fully leverage the promise of Zero Trust. Organizations around the world continue to struggle with a range of security-related issues including cost concerns, technology gaps, skills shortages, and more, as this year's data illuminates.

Top three challenges to adopting a Zero Trust solution:



Top challenges to Zero Trust adoption this year: Cost concerns and technology

This year, respondents cited cost concerns, technology gaps, and privacy regulations/data security most often as their top challenges to enacting Zero Trust security initiatives. The rise of privacy regulations is new this year, but cost has been a recurrent challenge. In 2021, cost concerns were the second most often cited top challenge (the No. 1 challenge cited was talent/skill shortage; No. 3 was technology gaps). And in 2022, cost concerns came in third after issues with talent/skill shortage and stakeholder buy-in. This year, issues with talent/skill shortage remain relatively high, but issues around stakeholder buy-in have diminished—perhaps as trusted experts have validated Zero Trust principles.

Looking at this year's data by job title, the overall trends shift a bit: For the CxOs Okta surveyed, privacy regulations and talent shortage were top of mind; for the VPs we surveyed, their top issues were ease of integration and privacy regulations, and for directors, their top concerns were audit compliance and ease of integration.

The long road to Zero Trust

What lies ahead for Zero Trust

Every organization's Zero Trust journey is different. For companies trying to modernize and stay ahead of fast-evolving security threats, deploying such a complex strategic initiative can be a significant, years-long challenge. Nonetheless, we're seeing organizations steadily activating their plans, increasing their budgets for Zero Trust initiatives despite uncertain economic times, and making real progress toward hardening cloud security.

To get to true Zero Trust, organizations need to address data security and privacy concerns (including regulatory guidelines) while keeping their workforces humming along productively. Companies need solutions that integrate easily and quickly into their existing tech stacks and ecosystems to extract the greatest possible value from their investments. And they need to address ongoing challenges like the frustratingly persistent skills/talent gap.

Fortunately, getting stakeholder buy-in seems to be growing easier, and the benefits of strong Identity management are becoming more clear. Many business leaders now recognize that the value of Zero Trust extends beyond security: It's also a strategic business driver that improves the workforce and customer experience, unlocks meaningful collaboration for hybrid teams, and underpins the smooth, secure experiences that grow customer trust and revenue.

Securing the new Identity perimeter is perhaps the most critical challenge facing enterprises today. But successfully getting to true, Identity-backed Zero Trust allows an organization to fully leverage the power of the cloud, opening up new opportunities for agility, innovation, and business growth.

The long road to Zero Trust

Review of our key takeaways

- **Zero Trust has shifted quickly from a plan of action to business as usual.**

  Zero Trust — yesterday's stretch goal — is today's operational reality. The majority of organizations have already deployed a Zero Trust initiative and are already leveraging it to stay secure and competitive. Organizations that haven't, by and large, have a defined plan on their schedule and in the works.

- **Identity is now widely understood to be mission critical for Zero Trust strategy.**

  For today's nimble, hybrid/multi-cloud enterprises, Identity is the new perimeter — and strong Identity management is a fundamental strategy for organizational success that gives enterprises a safe path to scale confidently.

- **Zero Trust budgets are still rising, stubbornly resisting market forces.**

  Outside attacks and insider threats are not taking a break for bad economic times, and neither can security budgets — companies are staying focused on hardening their defenses through Identity-based security initiatives.

- **Companies trying to adopt Zero Trust still face some uphill battles.**

  Designing, scheduling, and implementing a Zero Trust security strategy is a complex initiative involving many stakeholders, and the path to success is unique to each organization, with privacy regulations, technology gaps, cost concerns, and other factors all adding to the challenge.

Want to find out more, including how to benchmark where your organization ranks on Okta's Workforce Identity Maturity Model? Here's help.

About Okta

Okta is the world's Identity company. As the leading independent Identity partner, we free everyone to safely use any technology — anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.

Disclaimer

This document and any recommendations about your security practices are not legal, security, or business advice. This document is intended for general informational purposes only and may not reflect the most current security and legal developments nor all relevant security or legal issues. You are responsible for obtaining legal, security, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein. Okta is not liable to you for any loss or damages that may result from your implementation of the recommendations in this document.

okta

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