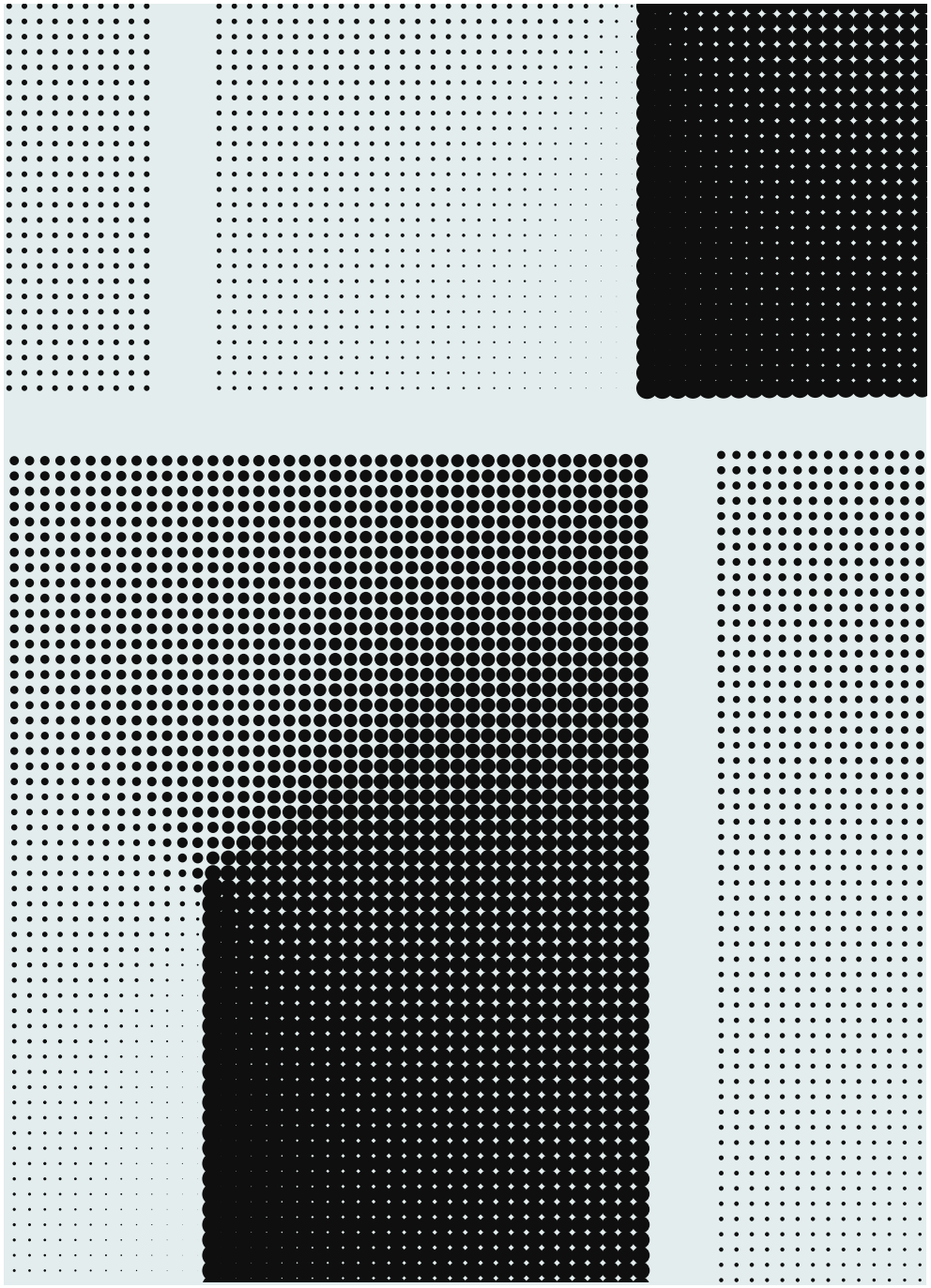
WHITEPAPER
Asia Pacific
August 2022

The State of Zero Trust Security in Asia Pacific 2022

Identity and Access Management maturity in Asia Pacific organisations

Okta Inc.
okta.com
info_apac@okta.com



okta

Contents

Why Zero Trust Is Essential, Now

Research has shown that the philosophy of Zero Trust security — "never trust; always verify" — has struck a chord. It took decades for organisations to move past the basic castle-and-moat security mindset and to accept that, in a cloud-based world, there is no perimeter to defend, and intruders are always on our networks.

But today, boardrooms all over the world are embracing the security framework of Zero Trust, which has quickly evolved from quirky buzzword to strategic differentiator to business imperative.

"Zero Trust is an information security model that denies access to applications and data by default," according to Forrester's 2022 definition. "Zero Trust advocates these three core principles: All entities are untrusted by default; least privilege access is enforced; and comprehensive security monitoring is implemented."

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

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

Since the release of Okta's 2021 State of Zero Trust Security report last year, the percentage of APAC companies with a defined Zero Trust initiative already underway increased —from 31% to 50%. Overall, 96% of APAC respondents have a defined Zero Trust security initiative in play or in plan for 2022.

> The percentage of APAC companies with a defined Zero Trust initiative already underway increased from 31% in 2021 to 50% in 2022

For the fourth annual State of Zero Trust report, Okta surveyed 700 security leaders across the globe, including 200 from Asia Pacific, to assess where they are on the journey toward a complete Zero Trust security posture.

We asked about the specific initiatives they have in place already and how they're planning to prioritise these over the near and long term.

We explored the priorities that matter for Zero Trust initiatives, using the Zero Trust framework popularised by Forrester and CISA.

Not surprisingly, Data, Network, and Devices continue to rank as the highest priorities among surveyed organisations, though this may shift over time, with the People category gradually increasing in stature as organisations come to terms with an evolving security perimeter that places less emphasis on the network and more emphasis on the user. Identity is a powerful force multiplier for Zero Trust security initiatives, as explored in detail.

As this year's report makes clear, this mindset is essentially universal now: Nearly all APAC organisations surveyed have either already started a Zero Trust initiative or have definitive plans to start one in the coming months.

Top three security strategy takeaways for APAC

1. Zero Trust isn't just a buzzword anymore

The adoption of a Zero Trust mentality has become the default security paradigm for organisations all over the world, and most of these already have initiatives in place and are actively looking for specific solutions to accelerate their journey to Zero Trust.

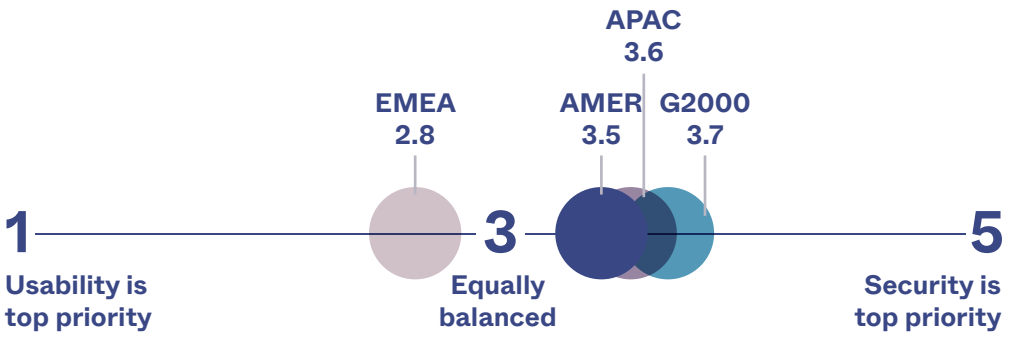
These aren't just plans: The speed at which organisations at large have been putting this philosophy into action is astounding. In 2021, 31% of APAC organisations reported they had a Zero Trust initiative already in place; this year that number has increased, to almost 50%.

Although this growth in adoption is impressive, APAC Zero Trust adoption lags the global average (55%) and illustrates a slower rate of adoption (18% YoY growth in APAC) compared to the global average (31% YoY growth globally) and other regions like EMEA and North America.

Security concerns are an increasingly strong motivator: Organisations have struggled to balance competing security and usability concerns for a long time, and while usability concerns have taken precedence in recent years, the scales have tipped this year, and security projects on average represent a slightly higher priority for surveyed organisations.

In contrast with global trends, it's interesting to note that APAC respondents prioritise security (75%) over usability (25%).

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



What's also noteworthy is that APAC organisations show strong growth in Zero Trust adoption — but still lag their global counterparts.

2. There's no silver bullet for enterprise security

Zero Trust is a solid guiding principle, but getting there is a complex proposition, requiring multiple deeply integrated best-of-breed solutions working seamlessly together. Every company has a different starting situation, different resources, and different priorities, leading to unique journeys to reach the same destination — true Zero Trust security.

3. Identity is the key to making Zero Trust a reality

For all their differences, organisations around the world have come to realise that identity is critical for a successful security and Zero Trust strategy. Companies are working overtime to secure the new perimeter—identity—as part of their Zero Trust initiatives. And the specific IAM strategies they're advancing to support those initiatives can be expressed in five distinct phases, as detailed in the report.

The overwhelming majority of APAC respondents said that identity was important to their overall Zero Trust security strategy.

Identity-driven security is hitting its stride in APAC

Given that the pandemic has spurred a remote-working mindset, the identity-driven security endemic to the broad theme of Zero Trust Security has become a bigger priority for almost all organisations across APAC.

In last year's report, about 76% of respondents in APAC said they would moderately, or significantly increase their budget on Zero Trust.This year's report shows that the latest respondents are largely true to form. When asked how their Zero Trust budgets have changed in the past 12 months, 82% reported a moderate increase in budgetary spend.

According to the data, in APAC the top 3 challenges when it comes to implementing a Zero Trust security initiative are talent and skills shortage (31%), lack of stakeholder buy-in (18%) and lack of awareness for the solution (18%).

At a glance: key takeaways for APAC respondents

Almost half (49%) of APAC organisations have a Zero Trust Strategy in place today. While there is still a long way to go, this trajectory shows progress, compared to last year where APAC adoption was at 31%.

- The year-on-year growth of Zero Trust adoption in APAC (18%) is significantly slower than the global average (31%)
- 83% of APAC respondents say Identity is important to their Zero Trust security strategy, but only 15% think Identity is business critical
- More than half of all APAC organisations prioritise security over usability
- APAC has the lowest adoption of passwordless access globally, with only 0.5% already implemented and only 10% planning to implement in the next 18 months
- The top 3 challenges within APAC to implement Zero Trust initiatives are: 1. Skill shortage. 2. Awareness of Zero Trust. 3. Stakeholder Buy-in.
- 96% of APAC respondents have a defined Zero Trust security initiative in play or in plan in 2022

Identity: the core of Zero Trust solutions

Even though each organisation's Zero Trust journey is unique, there is a growing consensus among global organisational thinking that an identity-first approach to Zero Trust is not only paramount, but essential.

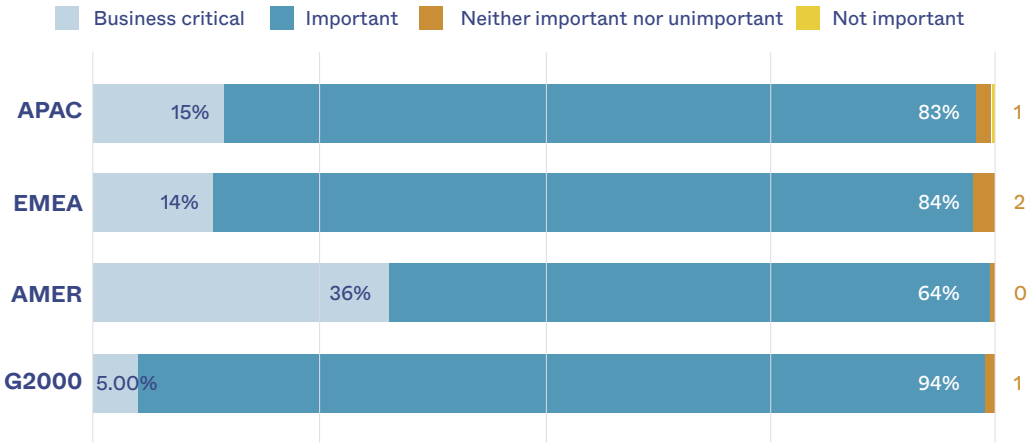
As such, this allows organisations to fully leverage identity and access management (IAM), by integrating it with other critical security solutions, into a powerful central control point for intelligently governing access among users, devices, data, and networks.

Research found that 80% of global organisations say identity is important to their overall Zero Trust security strategy, and an additional 19% go so far as to call identity business critical. That's a full 99% of organisations naming identity as a major factor in their Zero Trust strategy. Among CISOs and other members of the C-suite specifically, 26% deem identity business critical (among the 98% who say it's important). No wonder Gartner recently singled out "identity system defence" as one of the 7 Top Trends for Security in 2022.

APAC respondents rated the importance of identity to their overall Zero Trust security strategy at 83%. Furthermore, 14% said it was critical to their business.

83% of APAC respondents say Identity is important to their Zero Trust security strategy

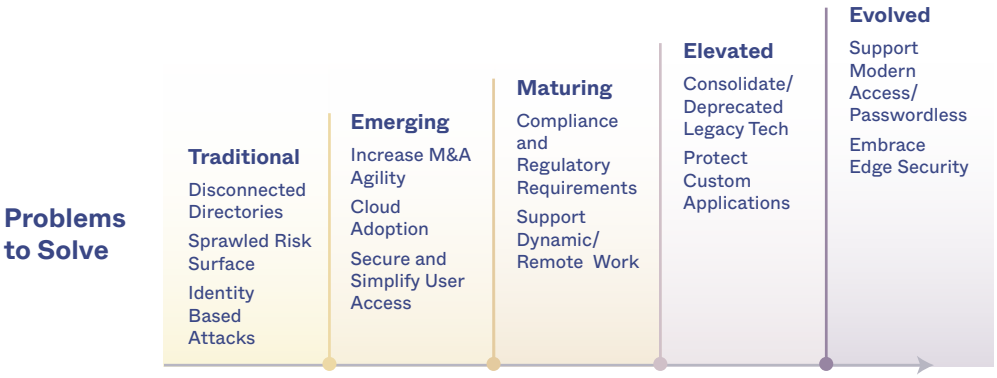
Regional Comparison: How important is identity to your overall Zero Trust security strategy?



Also in this year's survey, it was discovered that security teams are more likely to fully own IAM technologies in their security projects at Forbes Global 2000 companies than at smaller companies, although more security teams worldwide are providing at least partial oversight of IAM. However, in APAC and North America the number is almost unchanged.

Furthermore, the shift toward security is more pronounced in APAC and North America, with the EMEA region reporting a more balanced prioritisation between the two. Why is the balance tipping towards security? Companies that have now firmly established remote and hybrid work practices are already leveraging pandemic-era investments in usability and may be catching up on some security debt.

Identity Adoption Model for Zero Trust Initiatives



The Five Phases of Zero Trust Maturity

When it comes to Zero Trust, companies are putting their money where their mouth is: Most organisations have at least begun their journey to Zero Trust security, starting with critical identity initiatives.

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

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

Phase 1: Traditional

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

The report shows that within the next 18 months, nearly 100% of respondents in companies worldwide and in Global 2000 companies plan to complete the identity projects in Phase 1. Extending MFA for employees is the most adopted identity project across the board, and within the next 18 months, 100% of respondents from all regions plan to have adopted MFA for employees as part of their overall identity strategy.

In APAC, extending MFA for employees (76%) is the most adopted identity project and within the next 18 months, 100% of respondents from all regions plan to have adopted this identity project as part of their overall identity. Fewer respondents in APAC have indicated their company's directory is connected to cloud apps (68%), but they plan to advance towards completion of this identity project within the next 18 months.

> In APAC, extending MFA for employees (76%) is the most adopted identity project

Fewer respondents have indicated their company's directory is already connected to cloud apps, but many may still be in the process of cloud migration; they generally plan to advance towards completion of this identity project within the next 18 months.

Phase 2: Emerging

In the Emerging phase, organisations are typically attempting to correlate activity across disparate systems, resulting from changes like increased adoption of cloud apps and/or from M&A activity, that create a greater need to simplify user access.

To evaluate progress in Phase 2, respondents were asked whether their organisations are deploying MFA for external users, including their business partners and contractors, and if they've added single sign-on (SSO) for employees. In APAC, results showed that 39% of organisations have already implemented MFA for external users, with a further 27% to be implemented in the next 12-18 months. Even more compelling, 70% of businesses have already implemented SSO for employees with a further 30% to be implemented in the next 12-18 months.

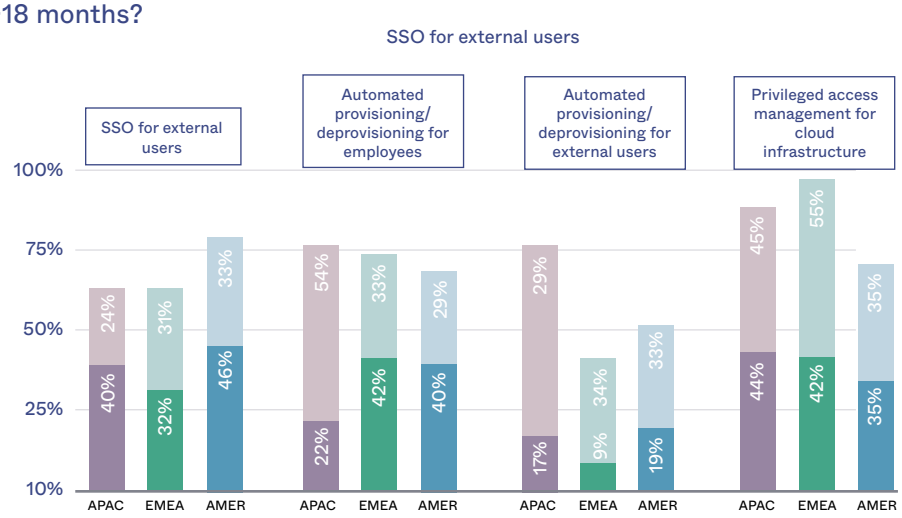
More and more companies are relying not just on remote employees, but on contractors, volunteers, suppliers, and other non-full-time employee partners. These individuals represent a growing security threat for organisations and extending MFA to these external users is a major focus for all regions, to help keep resources accessible yet safe.

Phase 3: Maturing

The report found that maturing organisations have complex challenges like increased compliance and regulatory requirements, a hybrid infrastructure, and the need to support a large, busy, dynamic, partly or mostly remote workforce. Meeting these challenges means extending and expanding their IAM efforts beyond their employees and legacy network to accommodate increasing external users and an expanding cloud or multi-cloud infrastructure.

Respondents from companies in APAC will be placing a lot of emphasis on automating the provisioning and deprovisioning of employees and working on privileged access for cloud infrastructure in the coming 18 months - going from 22% to 76% adoption and from 43.5% to 88% (more than double) adoption respectively.

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



Phase 4: Elevated

Organisations farther along the maturity curve have conquered the basics of identity based Zero Trust and have the tools and processes in place to tackle ever more complex identity challenges.

All Global 2000 companies surveyed plan to complete identity projects, including deploying multiple factors across user groups (44% already implemented for APAC) and securing access to APIs (46% already implemented for APAC), over the next 12-18 months.

At least half of these companies plan to have completed all identity projects in phase 4 during that same timeframe, with an emphasis on context-based access policies like how well a device is trusted at the time the user is trying to gain access, the location of the access attempt, the user and/or resource itself, and other critical inputs.

Phase 5: Evolved

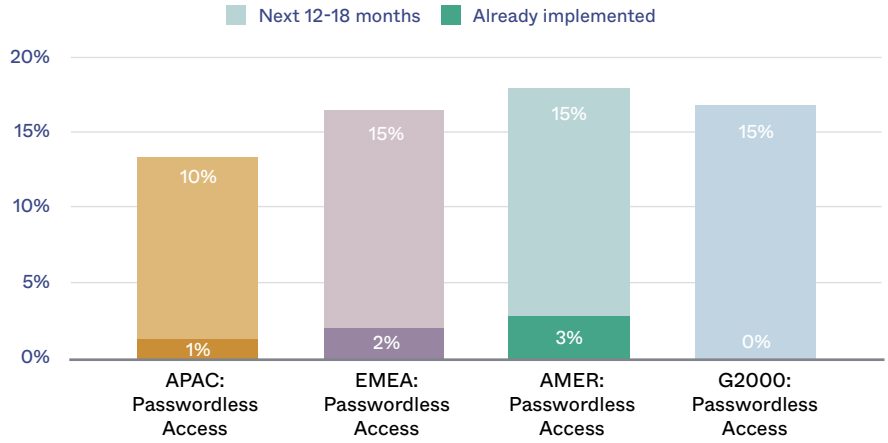
It was found that organisations in the Evolved phase have already shifted operations to cloud-based platforms like AWS, and they're focused on automation and adopting edge security.

Here, the focus shifts from implementing the core Zero Trust projects highlighted in earlier phases to optimising user lifecycle management, applying security access control to servers, and implementing passwordless access using high assurance factors, such as factor sequencing, biometric-based logins through WebAuthn, and U2F security keys.

Encouragingly, the report found that respondents from all regions plan to ramp up adoption of passwordless access. This is especially positive considering that more than half of all data breaches today involve weak or stolen credentials, with credential abuse responsible for much of the increasing incidence of ransomware and other identity-based attacks.

APAC has the lowest adoption of passwordless access globally, with only 0.5% already implemented and only 10% planning to implement in the next 18 months

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



Zero Trust Progress by Industry Vertical

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

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

Key Vertical: Healthcare

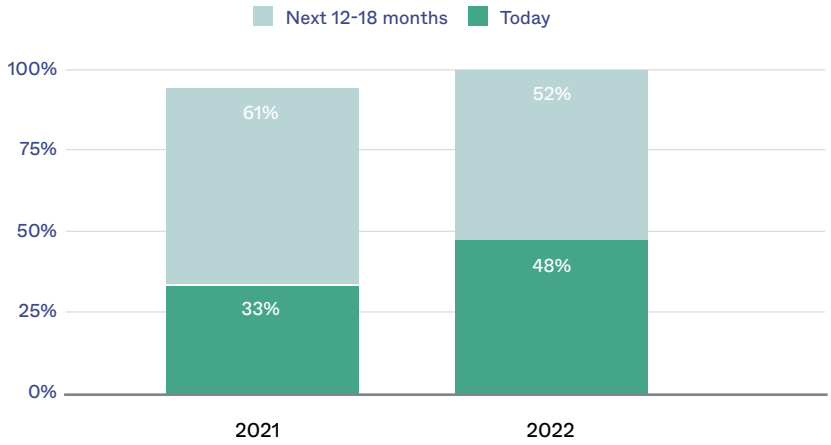
The last holdouts in the healthcare sector are getting their Zero Trust adoption plans in place: The number of healthcare respondents who either have a Zero Trust initiative in play or are planning to start over the next 12-18 months has climbed from 91% in 2021 to 96% in 2022. An impressive 58% of respondents in healthcare have already begun implementing their Zero Trust initiatives, representing a 20-percentage point increase over the 37% who'd begun by the time of last year's report.

Encouragingly, 88% of APAC respondents in healthcare recorded a moderate increase in Zero Trust budgets in the previous 12 months, with 63% of the same pool of respondents prioritising security over usability.

88% of the APAC healthcare industry either already have a Zero Trust initiative in place or intend to have one within the next 6-12 months, continuing the momentum for execution in the short term – and reflecting the perceived vulnerability of the sector to malicious attacks.

Key Vertical: Financial Services

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



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

94% of financial services organisations across APAC prioritise security over usability, and more than 88% of the same pool of respondents recorded a moderate increase in Zero Trust budgets in the previous 12 months.

Most of the definitional work to get Zero Trust initiatives in the works for financial services organisations is already happening. FinServ organisations may be slightly behind in their Zero Trust maturity relative to some other sectors today, but have active, specific plans to make significant strides to catch up in the near term.

Key Vertical: Software

In last year's report, the software industry lagged significantly behind the other target industries we surveyed. But also in that report, software company respondents promised they would make significant strides in Zero Trust security initiatives over the ensuing 12-18 months. In 2021, just 9% of software organisations surveyed had a defined Zero Trust initiative already in place, but another 79% planned to start one.

And they came through with flying colours. This year, the number of software organisations in APAC with an initiative underway climbed all the way to 50%, and with another 45% planning to get a defined initiative in place over the next 18 months, a full 95% of software companies in APAC have at least begun their journeys. We've seen the same quick uptake in Zero Trust adoption: Software companies intend to move quickly. The speed at which they're defining their Zero Trust strategies has increased, and they generally expect to implement a Zero Trust initiative in the next 6-12 months.

Key Vertical: Government

While government organisations globally may appear to be ahead of their peers in their adoption of Zero Trust initiatives, this is not reflected in APAC, with less than half the respondents in the region's government sector having a Zero Trust security initiative in place.

The similarities among government respondents globally can be seen in their plans to make significant strides across the maturity curve. Specifically, their plans amount to nearly doubling progress against six of the 12 identity projects on the curve, prioritising initiatives like deploying MFA for employees and to user groups.

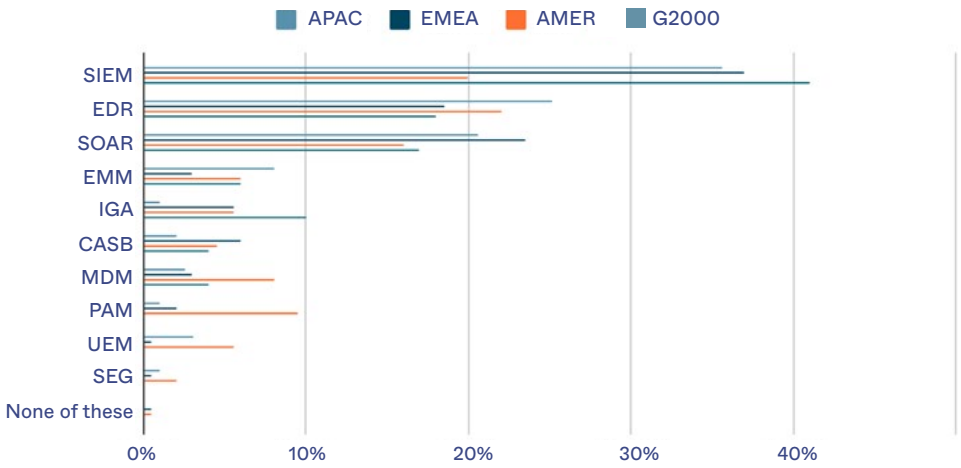
Today's Identity-First Security Ecosystem

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

The report states that the Zero Trust defense an organisation establishes is simply more effective and more efficient if it can integrate its IAM solution across the entire security architecture — including security information and event management (SIEM), security orchestration, automation and response (SOAR), enterprise mobility management (EMM) for endpoint protection, mobile device management (MDM), cloud access security brokers (CASB), and privileged access management (PAM). Coordinating IAM with SIEM can help organisations intelligently triage potential security events, for example; integrating IAM with SOAR can enable better-informed automated security responses and integrating IAM with EDR can use identity to centrally correlate independent data points that together indicate an attack is in progress.

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

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



The Promises (And Challenges) Of Zero Trust, and what lies ahead

The latest report found that many global organisations have made significant progress in their Zero Trust initiatives since last year, but they still face several sobering challenges, like making significant investments to help their teams implement new technology.

When we asked security leaders their top challenges to implementing specific Zero Trust initiatives, talent/skills shortage was at the top of the list for APAC organisations, emphasised by technology gaps.

So, what lies ahead for the development of Zero Trust?

Considering the talent/skill shortage faced around the world, organisations need to find solutions that help them progress along their Zero Trust journeys without creating the need for additional budgets, headcount, or training resources. And these solutions need to be easier and quicker to deploy, and able to scale as organisations grow and advance Zero Trust strategies. Stakeholder buy-in concerns could result from security departments not having full ownership over their IAM solutions, and possibly other security-related solutions in their environments. Other departments less invested in Zero Trust initiatives may be reluctant to reallocate resources to such efforts.

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

Survey Methodology

Commissioned by Okta, Pulse Q&A conducted a survey of 700 director-and-above security decision makers at global organisations, across many industries. Decision makers were defined as people responsible for making technology purchasing decisions, from which our survey partner Pulse collected responses in early 2022.

Industry data focused on four industry verticals (healthcare, financial services, software and government) and three geographical regions as well as the companies in the Forbes Global 2000. Asia Pacific, including Japan, comprised 29% of respondents. The security leaders surveyed were VPs, directors, or C-level executives, and the report authors used percentages within each segment to normalise. In terms of APAC-specific data, 8% comprised government and 26% comprised C-level respondents.

Respondents hailed from organisations with at least 500 staff. In line with last year's report, about 40% of the respondents worked with companies with more than 10,000 headcounts.

About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organisations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organisations everywhere, giving them the confidence to reach their full potential. More than 15,800 organisations, including JetBlue, Nordstrom, Siemens, Slack, Takeda, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers. For more information, go to **okta.com/au**