Whitepaper

August 2021

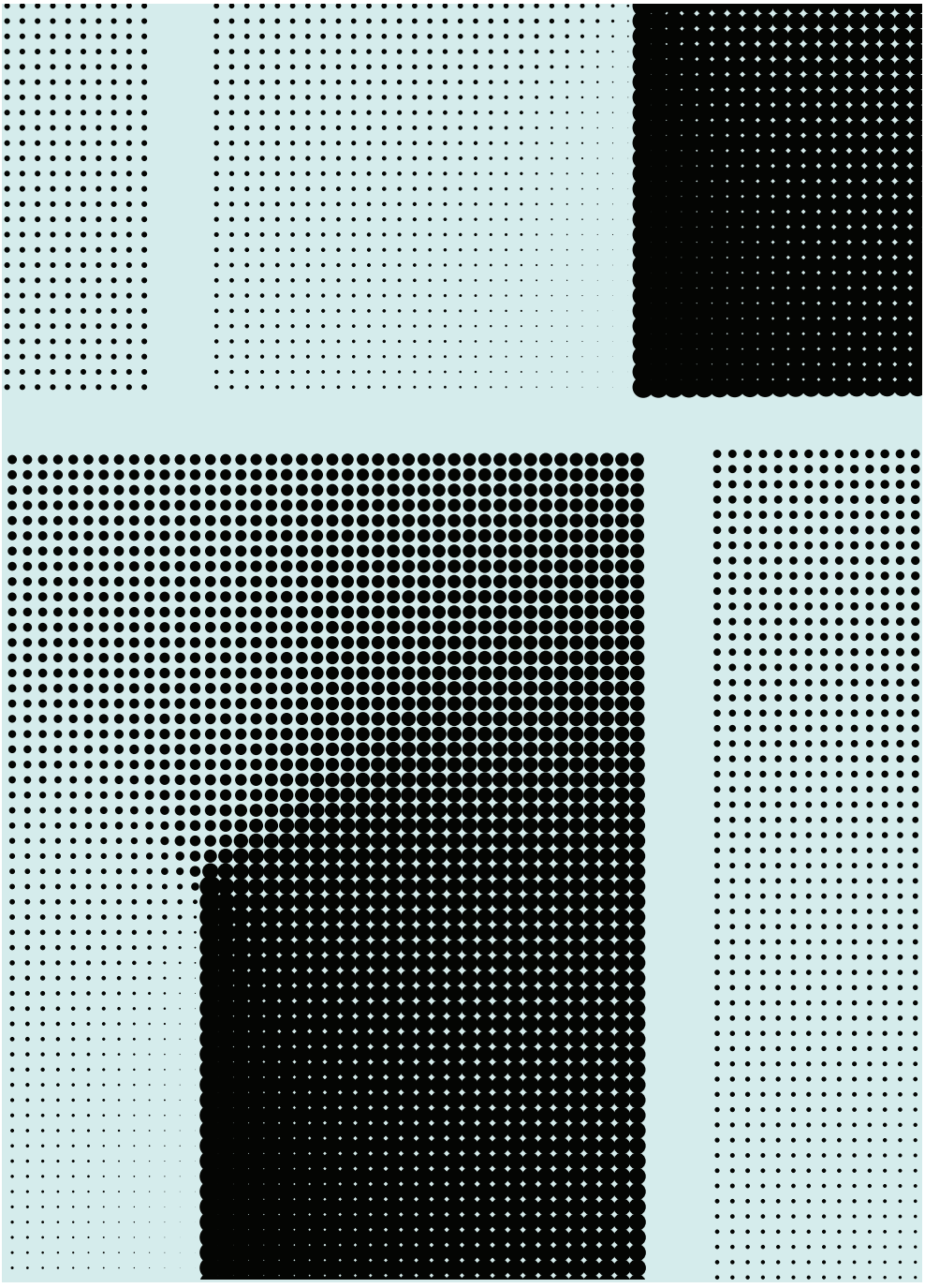
The State of Zero Trust Security in Asia Pacific 2021

Identity and access management maturity in Asia Pacific organisations

Okta Inc.

okta.com

press@okta.com



Contents

Zero Trust Security is here to stay

The Zero Trust Security approach ensures the right people have the right level of access, to the right resources, in the right context, and that access is assessed continuously — all without adding friction for the user.

Since our 2020 report, several market factors drove a surge in Zero Trust Security initiatives. Last year, the scope, scale, and perception of remote work each went through a massive shift. Now, 82% of organisation leaders plan to allow employees to work remotely at least part of the time after the pandemic, and 47% will allow them to permanently work from home full-time[1].

To better secure customers, employees, and businesses as mobile and cloud adoption skyrockets, the vast majority of technology and security leaders have moved past traditional security approaches. Rather than build a perimeter of protection around a "trusted" internal network vs. any "untrusted" external networks, they're adopting the Zero Trust Security frameworks strongly recommended (and in some cases even mandated) by government agencies and industry analysts.

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

To learn more about how organisations around the world are approaching Zero Trust Security today and where they're headed over the next 12-18 months, Okta surveyed 700 global security leaders, including 400 in Asia Pacific (APAC), about their initiatives for this third annual report.

[1] Gartner, "**Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time**," July 14, 2020

Top five security takeaways for APAC

APAC organisations prioritise Zero Trust Security the most – but still lag their counterparts in implementation

COVID-19 has accelerated Zero Trust Security as a priority in 77% of APAC organisations. This is slightly higher than EMEA (76%), and North America (74%).

At the same time, APAC organisations were clearly lagging their counterparts in EMEA and North America at the time of the survey – only 13% had already implemented a Zero Trust Security strategy, compared to 20% of organisations each in America and EMEA.

The pandemic is fueling Zero Trust Security prioritisation.

More than three-quarters (78%) of companies around the world say that Zero Trust Security has increased in priority, and nearly 90% are currently working on a Zero Trust Security initiative (up from just 41% a year ago).

Zero Trust Security adoption is on the rise

This year, organisations dramatically accelerated their journey towards identity and access management (IAM) maturity and plan to progress by leaps and bounds by the end of next year. By 2023, 40% of organisations would have implemented context-based access policies; with 29% implementing secure access to APIs – applications categorised under stage 2 of Okta's maturity curve.

Identity is the new perimeter

When asked to rank core Zero Trust Security requirements, the #1 priority was "people" for close to half (44%) of all APAC organisations. Leading companies are adopting strong authentication across resources for employees, customers, partners, contractors, and suppliers, while moving from network-based to more individualised device-based access decisions.

Organisations are upping their security game

As IT and security leaders shift their collective focus beyond quick wins, the most common Zero Trust Security projects organisations are prioritising over the next 12-18 months are those further along the IAM maturity curve. More than a third of all companies are prioritising single sign-on (SSO) and multi-factor authentication (MFA) for external users, context-based access policies, and automated account provisioning and deprovisioning.

Zero Trust Security has Become the Biggest Priority for APAC Business

With the rapid shift to remote working, Zero Trust Security has become a bigger priority for almost all organisations across APAC.

What's more, most companies plan to implement additional Zero Trust Security initiatives within the next 12-18 months, and intend to spend more than they have done before. About 76% in APAC will moderately, or significantly increase their budget on Zero Trust.

However, while all companies agree that Zero Trust Security is important, and intend to invest more, there are clear gaps in the Digital Trust adoption and strategy of organisations across APAC.

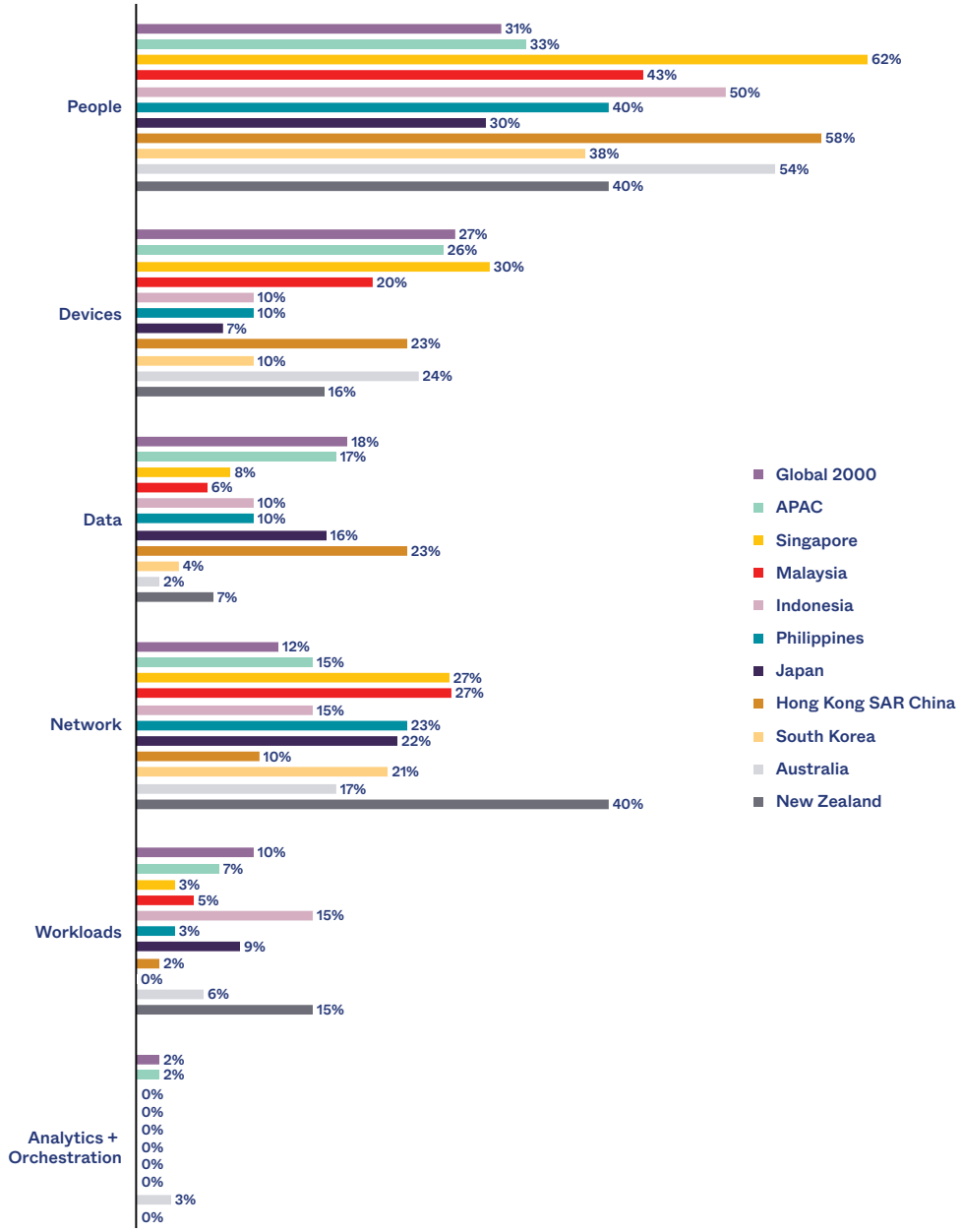
Notable country-level takeaways

- **Australia** has the largest proportion of organisations whose Zero Trust Security strategy has not been affected by COVID-19 and the remote working economy – one-fifth of companies reported that they have not been affected.
- **Japan** especially lags in Zero Trust Security adoption
    - While 82% of organisations in Japan shared that Zero Trust Security has become a greater priority for them, only 68% of organisations indicated that they already have a Zero Trust Security strategy, or are planning to implement one.
        - As many as 32% of organisations declared that they do not have a Zero Trust Security initiative, and do not intend to have one in the coming 12-18 months.
- **New Zealand** organisations have low implementation of Zero Trust Security strategies as well – only 6.7%; although 93.3% plan to implement in the upcoming 12-18 months.
- **Indonesian** and **Philippines** organisations are the most likely to have IAM completely owned by the security department - although the number remains low (15%).
- **Philippines** organisations are the least likely to have existing Zero Trust Security strategies – only 5%; although 95% intend to do so in the upcoming 12-18 months.

Identity: The Cornerstone of Zero Trust

With identity as your company's new perimeter, IAM becomes the central control point across users, devices, data, and their networks. In fact, Gartner recently singled out "identity-first" security as one of the top security and risk trends this year[2], since it provides visibility and control over which users have access to what resources, and minimises risk such as compromised credentials or incorrect provisioning or authentication.

What is the number one Zero Trust Security priority in your organisation?

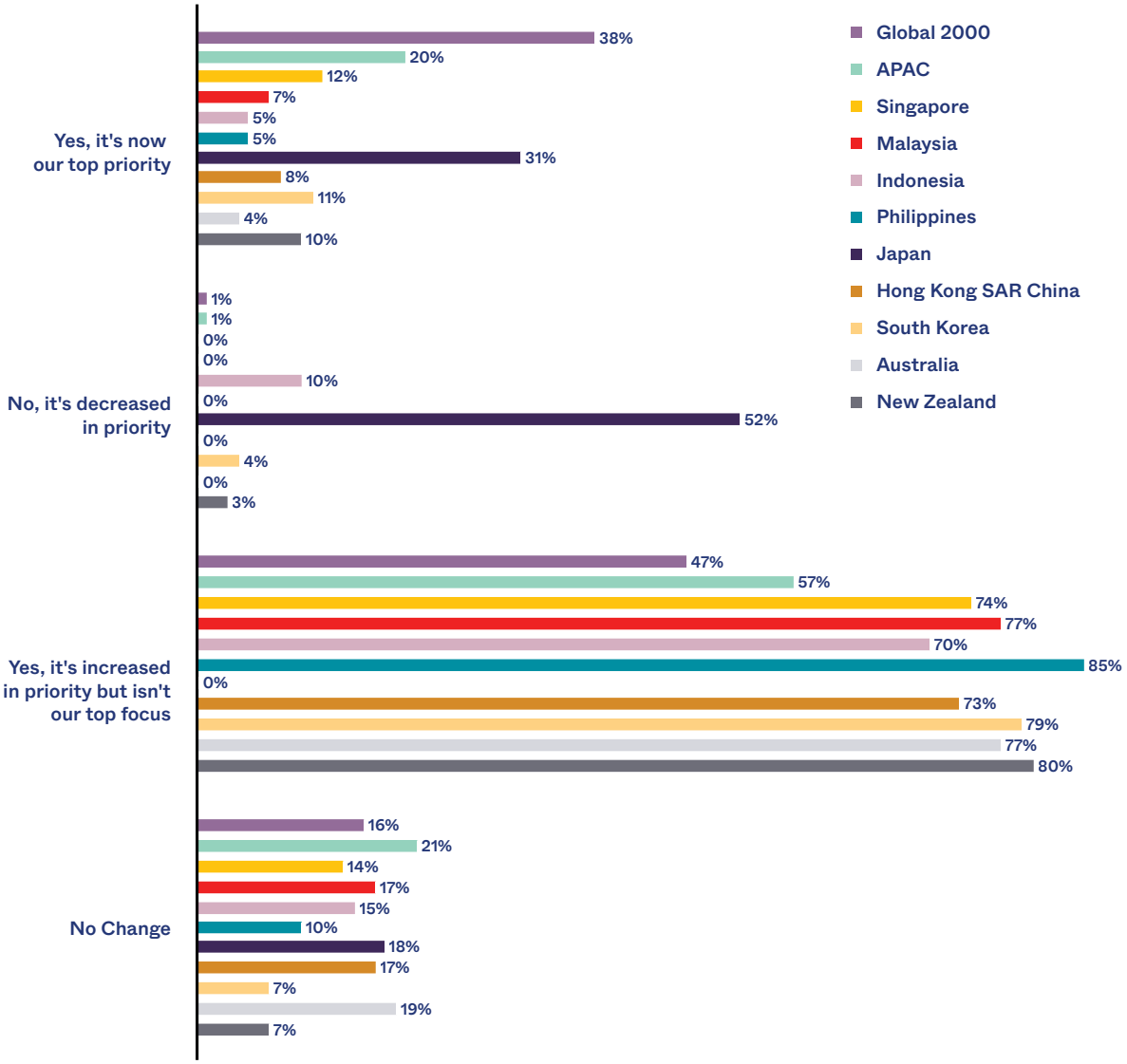


[2] Gartner, "Top Security and Risk Trends for 2021," April 5, 2021

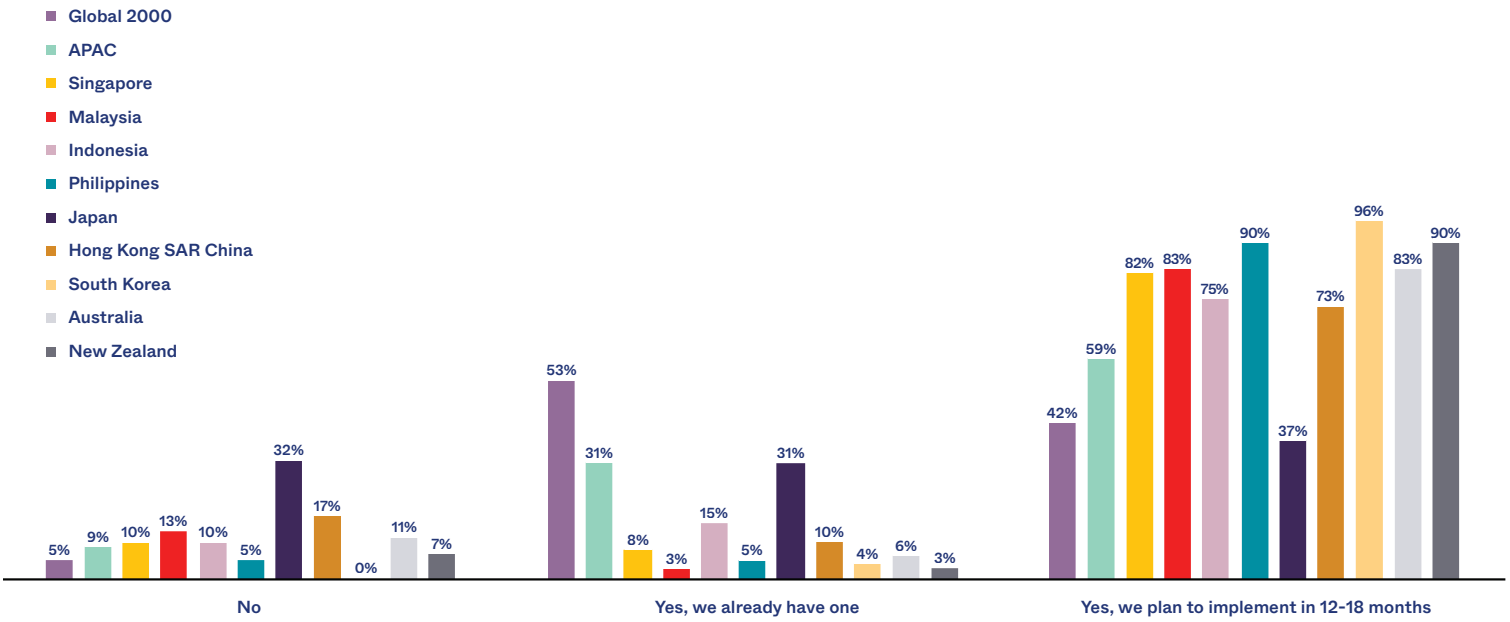
The rise of identity-driven security

In observing how Zero Trust Security and IAM prioritisation have shifted over the last year, it's clear that the pandemic supercharged organisations' move towards Zero Trust Security and many teams were allocated more budget to get there. Across APAC, about 90% said they're working on a Zero Trust Security initiative today or plan to start one in the next 12-18 months. However, in Japan, only 68% of organisations indicated as such – with as many as 32% of organisations declaring that they do not have Zero Trust Security initiative, and do not intend to have one in the upcoming 12-18 months.

Regional comparison: Has COVID-19 and the remote working economy accelerated Zero Trust Security as a priority at your organisation?



Regional comparison: Does your organisation have a defined Zero Trust Security initiative today or that you're planning to start on in the next 12-18 months?

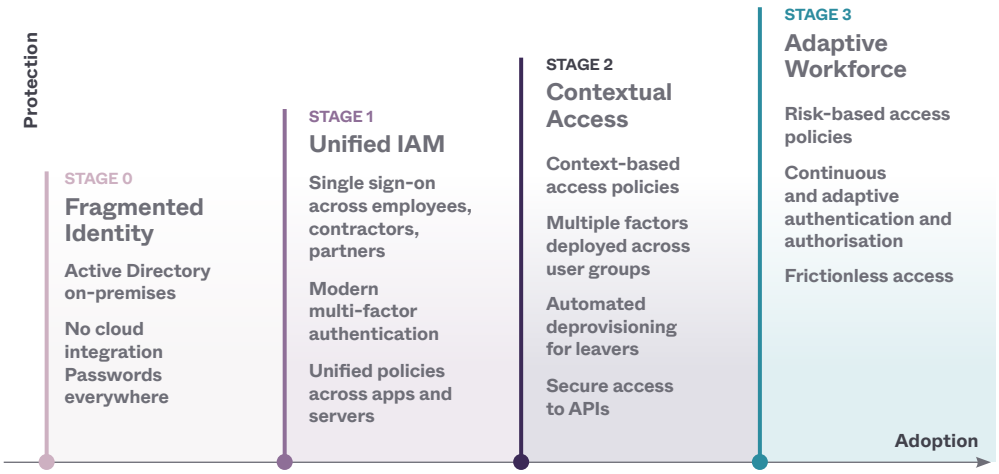


Perhaps unsurprisingly, we found that when the security team has full oversight of IAM at a Global 2000 organisation, they are more likely to already have a defined Zero Trust Security initiative in place — at 70% vs. 53% of companies where security is less involved with IAM.

With only 10% of security teams in APAC having complete ownership over identity management, and 14% of security teams having no oversight at all, a more active involvement of security teams in identity management will be crucial for an organisation's Zero Trust Security.

The Evolution of Zero Trust Security Maturity: 2021

Identity and Access Maturity Curve



Zero Trust Security projects span everything from the types of resources an organisation manages, to which authentication methods they deploy, and more. To this end, Okta's IAM Curve reviews organisations' identity-driven security practices on everything from the type of resources they manage to how they provision and deprovision users. It also explores which authentication methods they deploy, the policies they have in place, and their future business priorities.

The IAM Maturity curve is broken down into the following stages:

During **Stage 0**, an organisation might begin to embrace cloud technologies, but don't yet integrate those solutions with an IAM platform or on-premises resources.

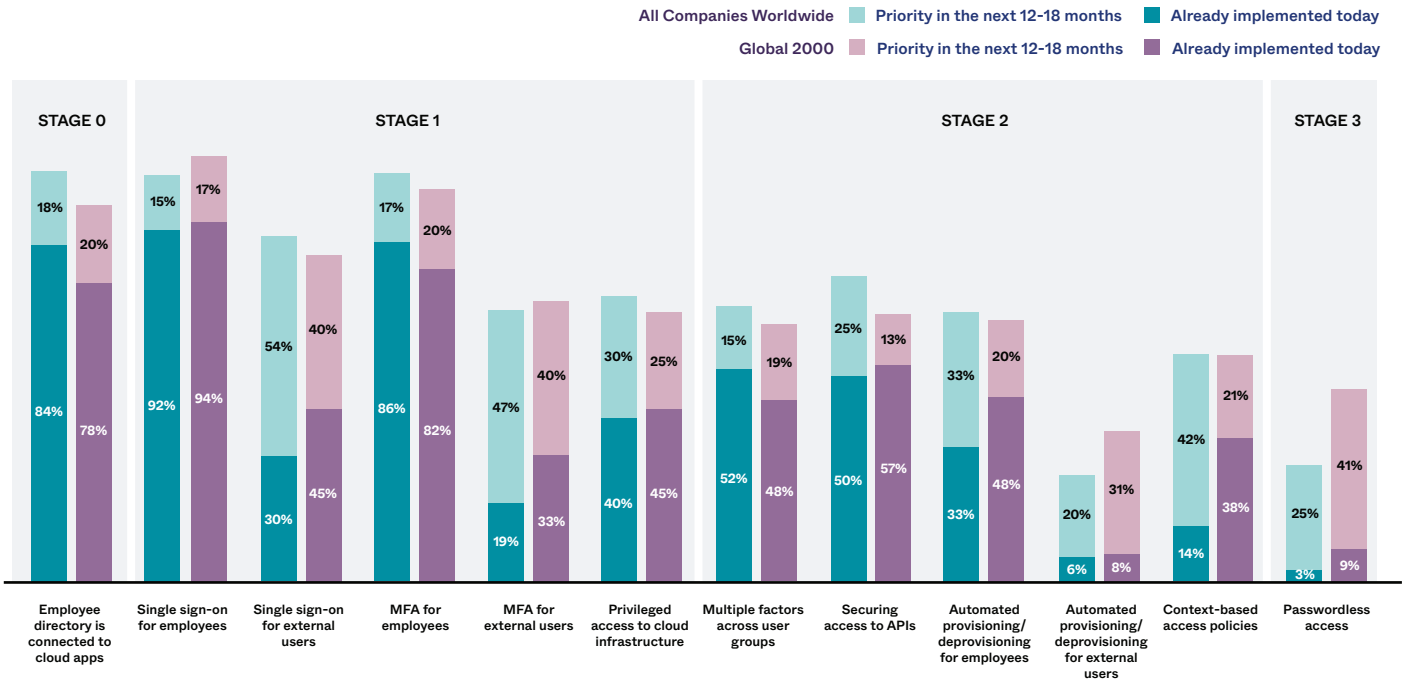
At **Stage 1**, teams start wrapping their arms around a unified IAM ecosystem and eliminating poor password hygiene by implementing single sign-on (SSO) and multi-factor authentication (MFA) for employees to access key resources.

Moving into **Stage 2**, businesses adopt additional security best practices by extending access controls to other resources such as their APIs, and also using rich context and diverse factors to better inform authentication decisions.

Once companies reach **Stage 3**, they've successfully adopted a full risk-based authentication approach to Zero Trust, including passwordless and continuous access solutions.

Unlike last year, when the majority of the companies we surveyed were still focused on Stage 0 or Stage 1 projects, this year all 100% of respondents expected to be firmly in Stage 1 by 2022. By 2023 40% of organisations within APAC would have implemented context-based access policies; with 29% implementing secure access to APIs – applications categorised under Stage 2 of Okta's maturity curve.

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



Promisingly, within APAC, Stage 1 implementations such as single sign-on for employees (implemented at 84% of organisations) and multi-factor authentications (84%) have already been implemented across most organisations. Implementation for several Stage 2 strategies and solutions have been healthy as well, including secure access to APIs (35%). While only 3% of organisations have context-based access policies, 40% intend to implement it within the next 12-18 months.

That said, there are areas currently being neglected by organisations in APAC. For one, no organisations had implemented passwordless access, and only 10% intend to do so within the next two years.

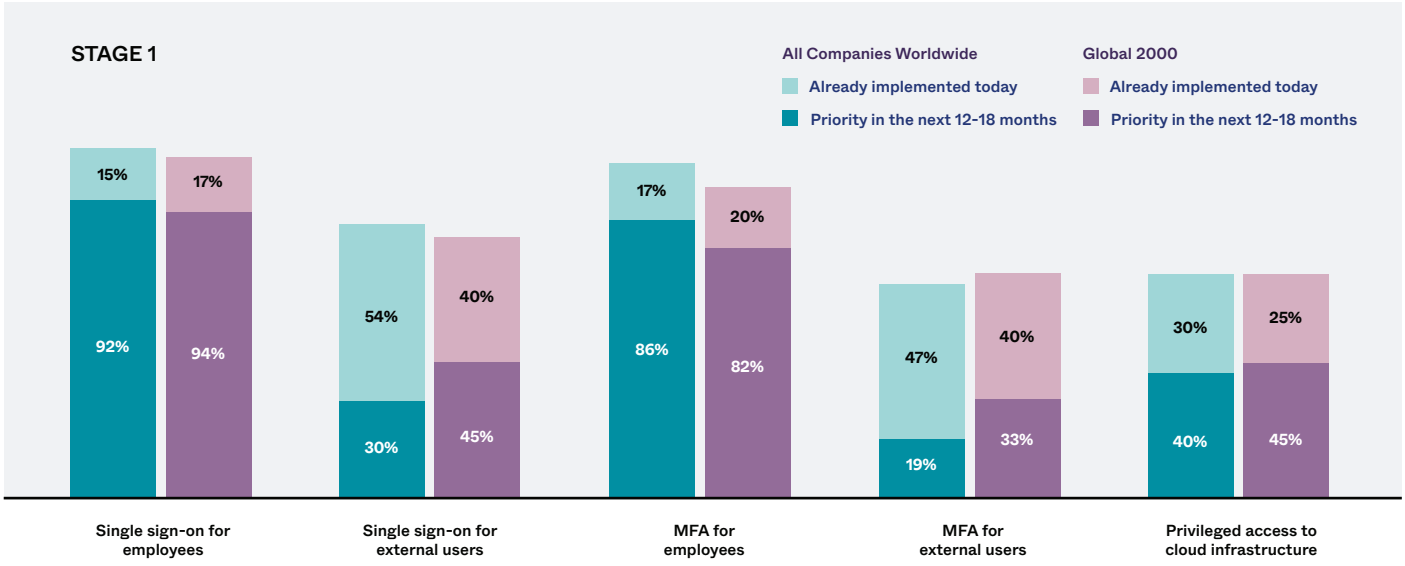
Stage 1 adoption will exceed 67% of APAC companies by 2023

Stage 1: Unified IAM

By adding multiple layers of security to their authentication mechanisms, Stage 1 organisations are finding effective ways to give the right people access to the right resources, with minimal friction.

At least two of the five projects in Stage 1 have been adopted by more than 84% of companies today, with 70% of Global 2000 companies expected to have implemented all five projects by 2023. However, none of companies in APAC anticipate that they would have implemented all five projects within the same timeframe (by 2023).

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



For the next 2 years, companies in APAC are prioritising tasks that secure access to external users like partners, contractors and suppliers. About 17% of companies in the region expects to kick off SSO projects, and 40% and 25% will pursue MFA projects.

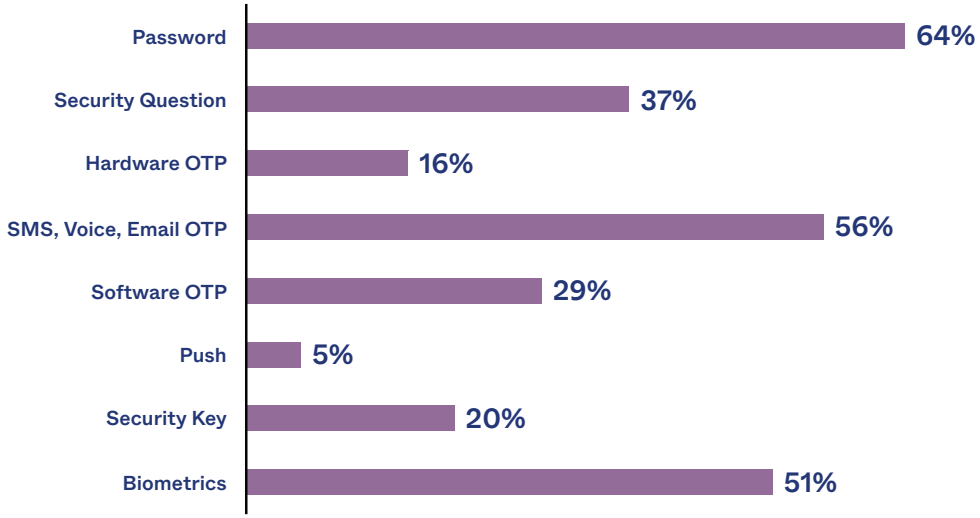
Stage 2: Contextual access

To evaluate Stage 2, we asked respondents whether their organisations deploy safeguards such as multiple factors across user groups and secure access to APIs.

In APAC, four out of these five Stage 2 projects will have been implemented by nearly half of companies by 2023. Over this same timeframe, two of these projects (securing access to APIs and automating provisioning/deprovisioning) are expected to reach >70% adoption amongst APAC organisations.

Security factors

Security factors currently implemented by organisations in Asia Pacific



Impressively, 49% of global companies say they use biometrics, a high assurance factor. That said, the majority of companies still rely on low assurance factors, such as passwords and security questions that can be stolen through social engineering (at 89% and 63% adoption respectively).

Stage 3: Adaptive workforce

To progress to the next Stage of Zero Trust Security, organisations can embrace passwordless access using high assurance factors.

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

This year, APAC businesses expect to shift from minimal adoption of passwordless access to 29%.

A Best-in-Class Zero Trust Security Ecosystem

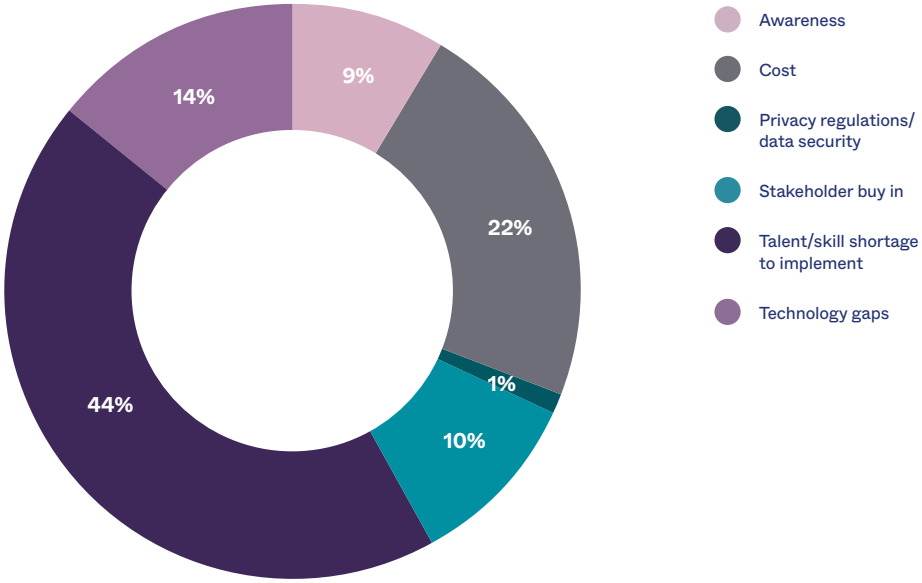
No single solution automates all of the Zero Trust Security recommendations promoted by Forrester, NIST, and others. A critical best practice in any industry is to leverage identity as a foundational technology across the security stack. Integrating your entire security architecture — including security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

With this in mind, we asked security leaders what other tools they have integrated or plan to integrate with their IAM system, and found that the most common integrations in place today were EP and CASB — at 80% and 69% of companies. The majority of companies selected SIEM as the single most important security integration.

What's Next for Zero Trust?

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

Top challenges APAC organisations face in implementing a Zero Trust Security model:



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

In the months and years ahead, there's also room for Zero Trust Security to connect to Customer Identity and Access Management (CIAM), as consumers become more cyber savvy and greater amounts of data gets stored in the cloud.

Businesses handle vast volumes of sensitive financial and personal data from customers. Inadequate controls in CIAM processes and technology can lead to breaches, involuntary data exposure, and non-compliance issues.

Ultimately, it is organisations' ability to prevent incidents like account takeovers and customer information theft, and provide a frictionless experience, will help them gain trust with today's consumers.

The Way Forward for Zero Trust Security

When it comes to implementing Zero Trust Security, there is no silver bullet. At the same time, the digital nature of our modern economy means that security threats will only intensify, so no business can afford to stand still.

To this end, there are several ways you can make inroads with identity-driven security:

- Recognise that people are the new perimeter, and adopt strong authentication across all your services, everywhere.
- Centralise your identity and access control across the enterprise so you can more easily manage risk.
- Reduce risk by reviewing the IAM maturity curve, determining where your organisation is, and finding some immediate wins to quickly advance your position through an identity-first approach to Zero Trust.
- Extend your security ecosystem by integrating key tools with your IAM solution, thus enabling holistic security visibility and collaboration.
- Consider even more advanced methods such as adopting passwordless authentication and context-based access policies, as well as shifting beyond protecting employee accounts to also securing access for partner accounts.

Check out **Okta's Zero Trust Security assessment tool** for a prescriptive roadmap to putting Zero Trust Security identity and access controls in place. Our assessment will review your practices surrounding everything from the type of resources you manage, to how your IT department provisions and deprovisions users, which authentication methods you deploy, and your future business priorities. We'll determine your current maturity and offer actionable recommendations on where you can go from here.

Survey methodology

Commissioned by Okta, Pulse Q&A conducted a survey of 300 director and above security decision makers at APAC companies across multiple industries. In Japan, Rakuten Insight conducted a survey with 100 security decision makers. Decision makers were defined as someone responsible for making technology purchasing decisions, and Pulse collected responses in early 2021.

Respondents hailed from organisations with at least 500 staff. About 40% of the respondents worked with companies with more than 10,000 headcount. Key industries covered include finance, banking and insurance, healthcare and social assistance, software, and others.

About Okta

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