Adopting Zero Trust Security: An APAC Perspective

Okta Inc.
100 First Street
San Francisco, CA 94105

info@okta.com
1-888-722-7871

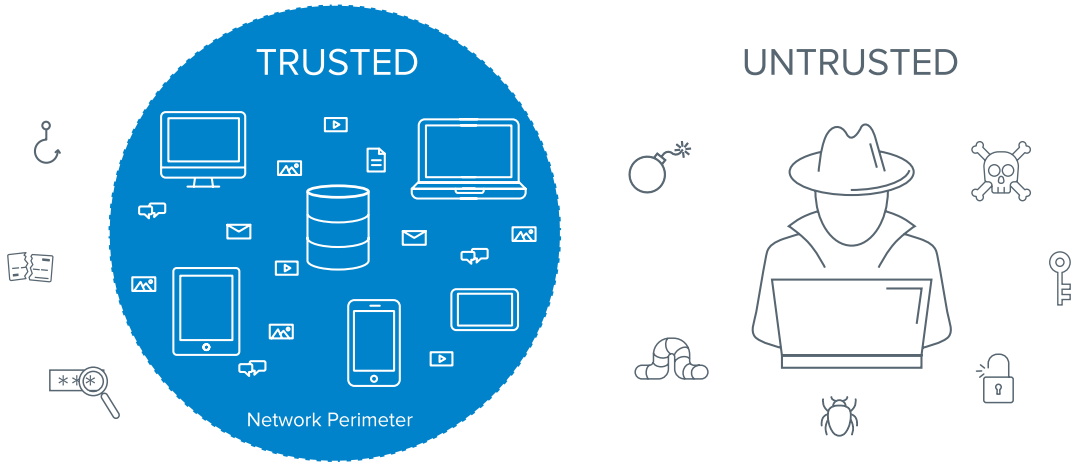
Introduction

The Zero Trust security framework can be summarised in four words: never trust, always verify. In today's mobile and cloud-driven world, traditional, network perimeter-oriented approaches to security aren't enough. Instead, companies need to securely enable access for various users—such as employees, partners, contractors, and even customers—regardless of their location, device, or network.

As the business and threat landscapes continue to evolve, global brands are adopting Zero Trust approaches to security. In many geographies, it's only just starting to pick up. The Asia-Pacific (APAC) region, for instance, is still largely in the early stages of adoption—especially as regulations like open banking drive the need to rethink secure access from apps to APIs.

Embarking on a Zero Trust journey

Zero Trust as a term has received a lot of recognition and hype in security communities, in particular over the last couple of years. While specific approaches can vary from vendor to vendor, what it represents is a shift in the security mindset: as organisations adopt cloud and mobile technologies, traditional, firewall-based approaches to security no longer make sense. In this world, modern security means ensuring the right people have the right level of access, to the right resources, in the right context, and that access is assessed continuously—without adding friction for the user. By employing a Zero Trust framework, organisations are able to abandon the concept that they have a "trusted" internal network and an "untrusted" external network, and instead treating all users with the same level of scrutiny.



In recent years, we've seen enterprises across North America address their security concerns by embracing this modern, Zero Trust model for security. As markets throughout APAC and EMEA increasingly follow suit, it's important that organisations understand the identity landscape they're operating in:

Zero Trust lives across various existing frameworks. The term 'Zero Trust' first emerged in a 2009 framework developed by Forrester Research, which argued that all network traffic should be seen as untrusted. Since then, the rise of cloud and mobile has served as a catalyst for evolving Forrester's original Zero Trust model. Gartner's 2017 Continuous Adaptive Risk and Trust Assessment (CARTA) framework echoed Forrester's Zero Trust framework with an added focus on not just authenticating and authorizing access at the front gate, but doing it continuously throughout the user's experience through an adaptive, risk-based

assessment to identify potential threats. Google's BeyondCorp research was published in 2014 and today serves as the marquee example of Zero Trust done right at massive scale. Most recently, the U.S. National Institute of Standards and Technology (NIST) launched their Zero Trust cybersecurity framework in 2019 as Special Publication 800-207, which recommended considerations for U.S. government agencies.

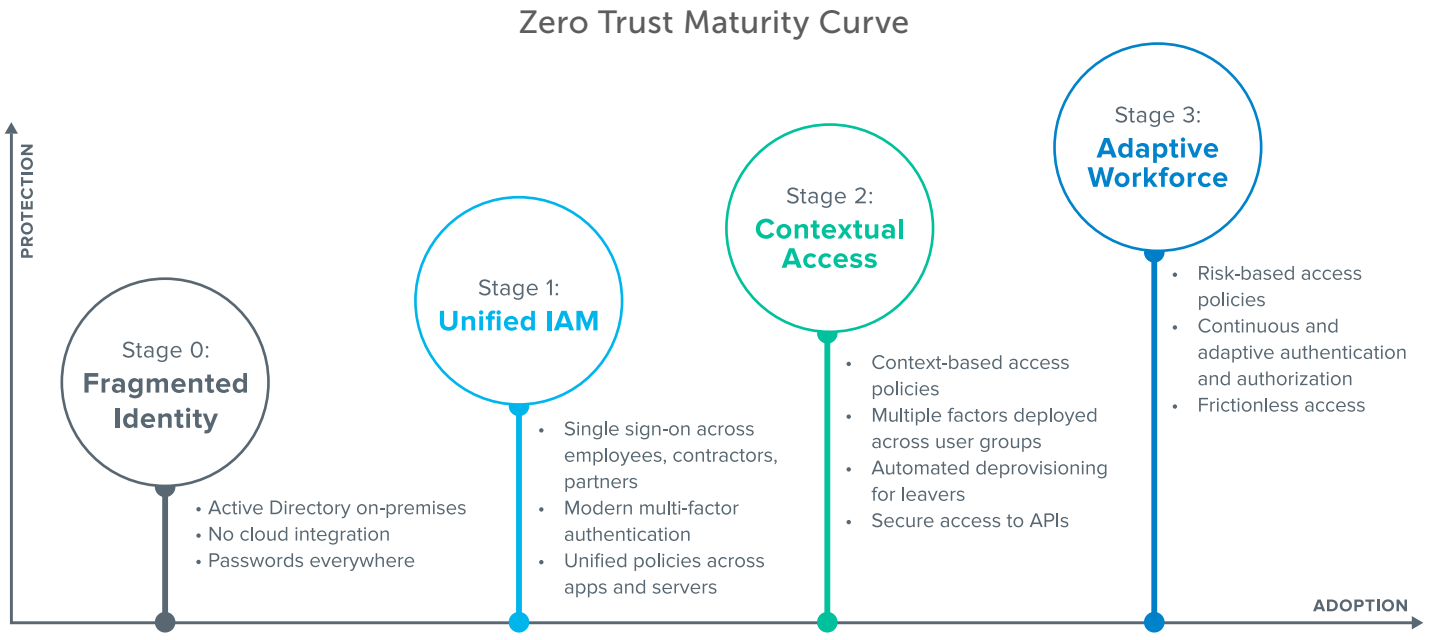
There are multiple solutions. The unifying theme to all of these models is that they offer guidelines and best practices for organisations to guard against modern cyber threats—and there is no single product or solution that will be a silver bullet to protect against everything. Instead, they each provide paths for organisations to be strategic and intentional with their security and ensure they have the right solutions in place for the business.

Start your Zero Trust journey with identity

The journey to Zero Trust security isn't the same for everyone, but many organisations find that the best place to begin is by implementing identity and access management (IAM) solutions to serve as the core technology:

> ### Start with identity and device security
>
> **We consistently find that enterprises have the earliest and rapidest success if they focus on improving identity management and device security. These two core components of the Zero Trust eXtended (ZTX) ecosystem drive rapid risk reduction and build confidence with executives that the organization can realize security benefits from its Zero Trust program quickly.**
>
> - A Practical Guide To A Zero Trust Implementation, Chase Cunningham, Forrester Research, 15 January 2020

Okta developed the Identity and Access Management Maturity Curve to help organisations understand where they are on the Zero Trust path and what their next steps should be. We also polled security leaders across Australia and New Zealand on their current IAM projects to see how far they had progressed on their Zero Trust journeys.



Stage 0

Fragmented identity

Many organisations begin their Zero Trust journeys with a variety of on-premises and cloud applications that are not integrated together or with on-premises directories such as Active Directory—and that's true for Australian and New Zealand organisations as well, with the majority of organisations in this stage. As a result, IT is forced to manage disparate identities across a number of systems as well as the many applications and services used without IT awareness. For the user, this also means numerous (and, most likely, unsecure) passwords. Without visibility and ownership over these fragmented identities, IT and security teams are left with potentially large windows for attackers to exploit access into individual systems.

Stage 1

Unified identity and access management (IAM)

The first step to resolving the security gaps left open by many fragmented identities is consolidating under one IAM system, across both on-premises and cloud applications—a functionality offered by Okta Access Gateway. This Stage 1 consolidation, via single sign-on (SSO), is critical to managing access and should apply to any user that needs access to a service, including the full extended enterprise of employees, contractors, and partners—no small feat. We see many Australian and New Zealand organisations prioritising SSO implementations over the next year, with 52% of businesses planning to start on these projects in the next 12-18 months.

Layering a second factor of authentication to that centralized identity access point further helps to mitigate attacks targeting credentials. Additionally, unifying access policies across applications as well as servers, a critical part of IT infrastructure, is key to bringing IAM together into one secure, manageable place for IT.

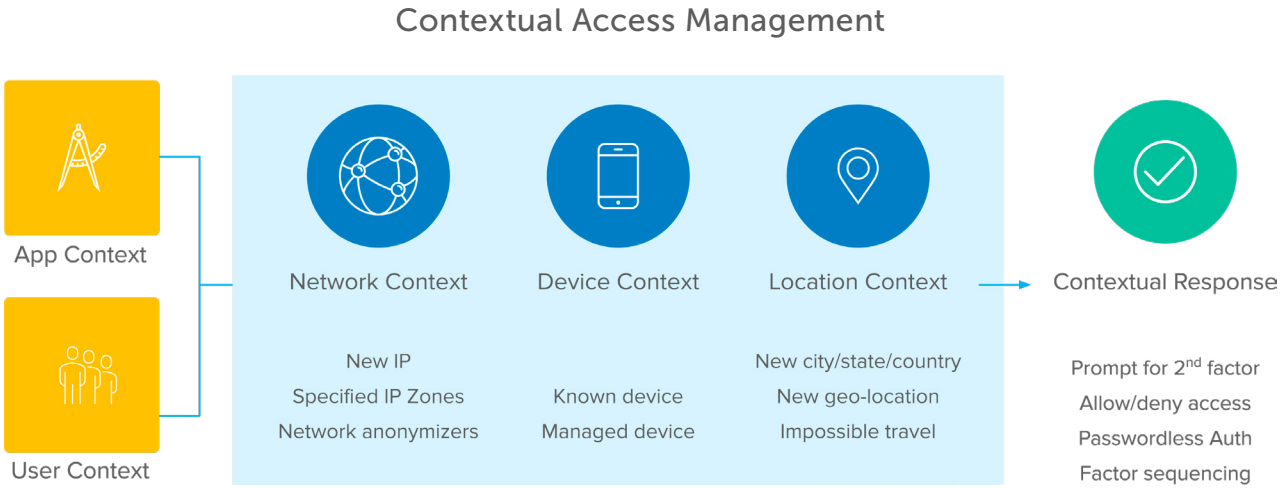
> **With hundreds of thousands of employees worldwide, Hitachi needed a modern solution to centralise its identity and access management, enabling new technology and scalable provisioning. With Okta, Hitachi has replaced legacy systems, consolidated access experiences, and streamlined technology adoption cycles.** See how.

Stage 2

Contextual access

Once IT has unified IAM, the next stage in Zero Trust security is layering in context-based access policies. This means gathering rich signals about the user's context (i.e. who are they? Are they in a risky user group?), application context (i.e., which application the user is trying to access), device context, location and network, and applying access policies based on that information. For example, a policy could be set to allow seamless access to managed devices from the corporate network, but unmanaged devices logging in from new locations would be prompted for multi-factor authentication (MFA). Organisations can also employ multiple factors across user groups to step up authentication based on an understanding of those authentication attempts. Examples might include low-risk users without smartphones using one-time passcodes, or high-value targets using hard tokens and a cryptographic handshake to securely authenticate to a service.

Furthermore, if a user leaves or changes roles within an organisation, automated provisioning ensures the user has access only to the tools they need to do their work—or, in the case of a departure, automatically revokes all access, mitigating the risk of orphaned accounts or latent access after a departure. Finally, these rich access controls should be extended to all technologies used by the workforce, including secure access to APIs. While Australian and New Zealand organisations are primarily focused on Stage 1 projects overall, we see a heavy focus on extending access controls to API security in this region, as well as in Europe.



Stage 3

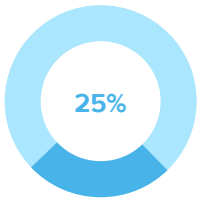
Adaptive workforce

The final stage of Zero Trust implementation extends organisations' focus on authenticating and authorising access. This means authentication no longer occurs just at the front gate, but continuously throughout the user's experience through an adaptive, risk-based assessment to identify potential threats. This first looks like adding an intelligent, risk-based engine to the contextual responses from Stage 2, going beyond the discrete policies set in the prior stage. IT can as a result set risk tolerance and allow the risk scoring based on those contextual signals to determine the riskiness of a particular authentication event, and prompt for a second factor based on that insight. That trust is also no longer absolute: this adaptive authentication is continuously monitored for a change in one of those signals, re-prompting for authentication and authorisation verification should an aspect of that user's context change. Finally, while security is increased through these intelligent, risk-based access controls, the experience for the end user is ultimately simplified—allowing for frictionless access and, in cases where IT has set a policy to allow for it, passwordless authentication.

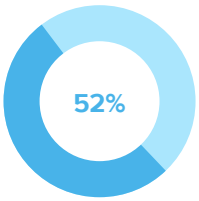
In Australia and New Zealand, most polled companies fall into Stage 0 or Stage 1 of the maturity curve. Here's a closer look at the Zero Trust strategies these organisations are implementing—and how the Okta Identity Cloud sets them up for success.

Zero Trust in APAC by the numbers

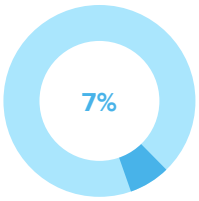
Within a Zero Trust framework, a modern SSO solution can help secure the login process, reducing the risks from weak passwords while streamlining access to applications. This is rapidly becoming a priority:



25%
of organisations have implemented SSO for employees



52%
plan to adopt it in the next 18 months



But they can still do more.
Only 7%
have extended SSO to external users

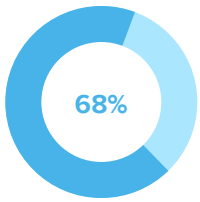
For instance, a centralised meta-directory allows companies to seamlessly connect their user store with all their on-prem and cloud applications, and set specific, granular access policies for users, groups, and devices.

MFA is also critical for a Zero Trust strategy. An adaptive MFA solution is context-aware, meaning that it automatically flags unfamiliar authorisation requests by screening for the user's network, device, and location. If any of these are not recognised, the user can be prompted to provide additional credentials.

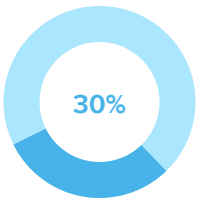
Number of IT leaders adopting MFA for their employees

Finally, the rich access controls afforded by a comprehensive security stack should be extended to all technologies used by the workforce, including APIs.

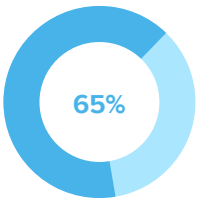
Though there is still a long way to go before APAC fully adopts the Zero Trust framework, several Australian and New Zealand organisations have already made progress with these solutions:



68%
have extended SSO to SaaS applications



30%
have secure access controls for APIs

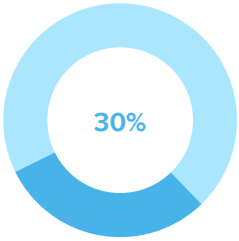


65%
plans to extend SSO to their servers

21st Century Fox overhauled its perimeter-based security practices with Zero Trust architecture in order to securely manage its traffic from 30,000 employees, 50,000 contractors, and 1.8 billion subscribers.
See how they did it.

As Australia, New Zealand, and other Asian regions explore open banking, organisations have a unique opportunity to interact with users, offer financial products and services, and collect related data. But to do so, they'll need to comply with high standards and stringent regulations.

API security will be key to this process. The Bank of New Zealand (BNZ) has released its own open banking-compliant API for developers to test, but these developers must first meet many complex requirements. Companies that can prove they adhere to a Zero Trust model—particularly with their API security—will have an advantage in this transforming financial space.

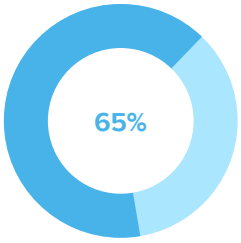


In the next 12-18 months,
30%
of organisations plan
to secure API access with SSO

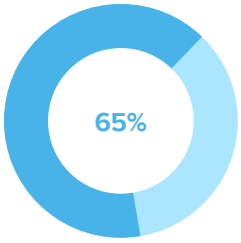
Beyond SSO, implementing API gateways keeps your systems safe from malicious data, improper requests, and denial of service attacks. At the same time, an API access management solution allows security teams to centrally control policies and log access requests, with complete standards-compliant OAuth 2.0 API Authorisation for granting fine-grained permissions—strengthening authentication and access management.

Challenges to Zero Trust in APAC

Though progress is being made in Zero Trust, there are still barriers that Australian and New Zealand organisations need to overcome:



65%
are concerned about the high costs of Zero Trust implementation

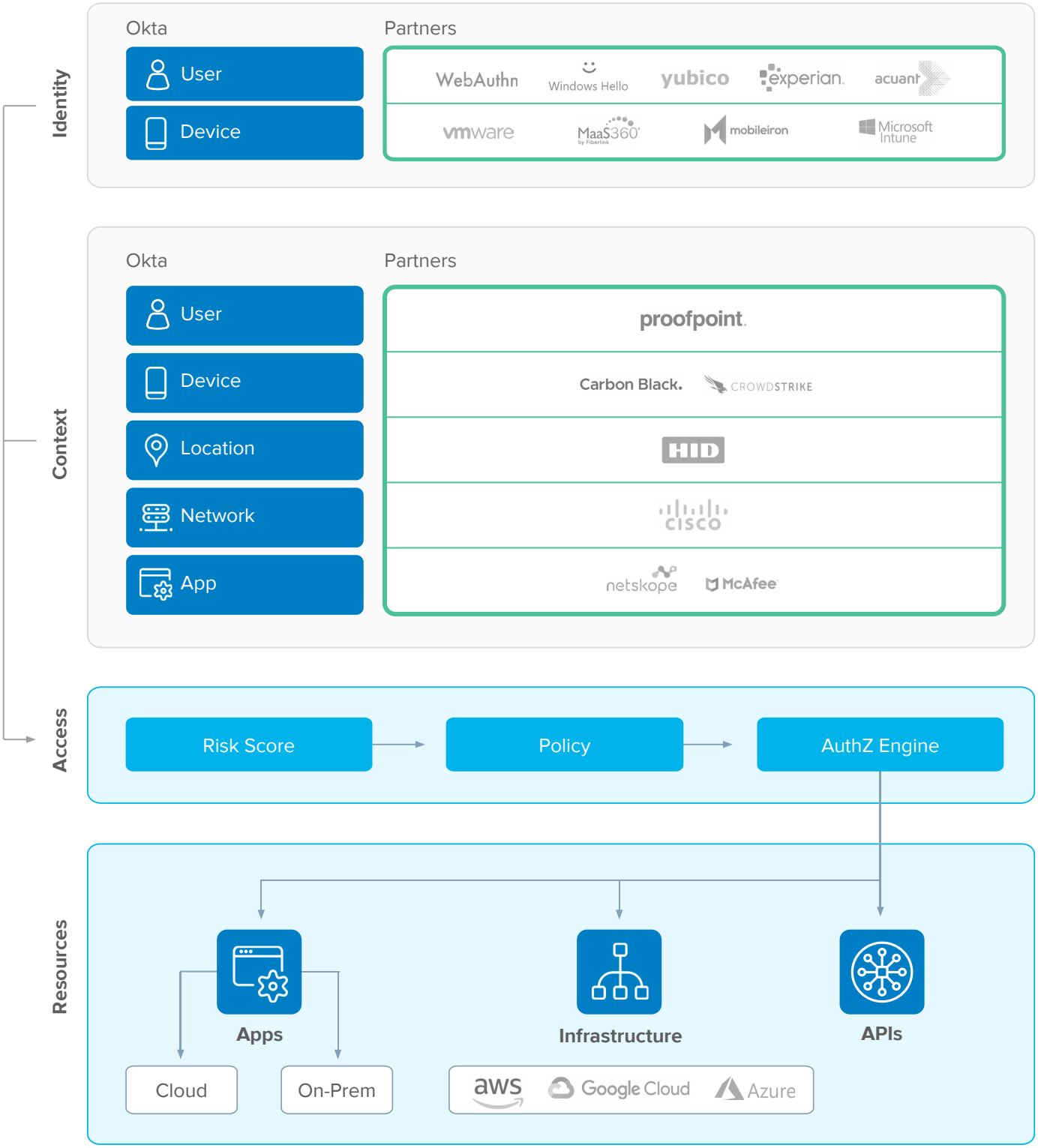


65%
are concerned about recruiting and retaining top IT talent to handle it

To mitigate these challenges, it's important to remember that Zero Trust doesn't mean completely restarting your security stack. It means rethinking its core components and revisiting how you're using your existing technology.

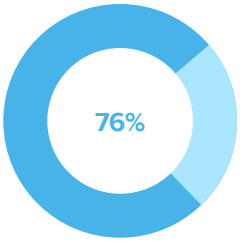
Zero Trust identity integrations

Thousands of organisations use Okta to unify their user identities through our suite of security products. But beyond delivering identity as the foundation for Zero Trust, Okta also integrates deeply across other security solutions. The Okta Integration Network covers all components of the extended Zero Trust ecosystem through partnerships with various solutions.



With a single integration, organisations can obtain a wide perspective on the threat landscape and protect themselves with a suite of best-of-breed cyber security solutions.

In a cyber threat landscape where it can be difficult to pinpoint who is behind an attack, security information and event management (SIEM) solutions that help monitor user activity are vital. This has become a priority in Australia and New Zealand.



In the next 12-18 months,

76%

of organisations plan to integrate identity with a SIEM solution

Okta's vast partnership network allows our customers to access these SIEM capabilities alongside other valuable authentication data that can be crucial in understanding how users are engaging with your systems.

Today's organisations start with identity and look to Okta as the beginning of their Zero Trust journeys, using the Okta Identity Cloud as the core of their next-generation identity and access strategy—and ensuring that only the right people have access to the right information, at the right time. That way, they'll be able to protect their business and people as they scale to meet the demands of today's mobile and cloud-centric ecosystem.

How far are you in your Zero Trust journey?

Find out where your organisation sits on the maturity curve with our free Identity and Zero Trust Assessment Tool.

About Okta

Okta is the leader in managing and securing identities for thousands of customers and millions of people. We take a comprehensive approach to security that spans our hiring practices, the architecture and development of the software that powers Okta, and the data center strategies and operations that enable the company to deliver a world-class service. In addition to product innovation and an award-winning customer support approach, Okta's solution is backed by a world-class cybersecurity team that works around the clock to provide the most secure platform for their users and the information they are entrusted. We employ state of the art encryption key management to secure customer data. Protection of customer data is audited in accordance with GDPR, FedRAMP and NIST 800-53, HIPAA, and ISO 27001 requirements. The company protects user information for global organizations such as ENGIE, Eurostar, Scottish Gas Networks, and News Corp, as well as some of the most highly regulated, complex companies, including American Express, U.S. Department of Justice, and Nasdaq.

To Learn more please visit www.okta.com/education