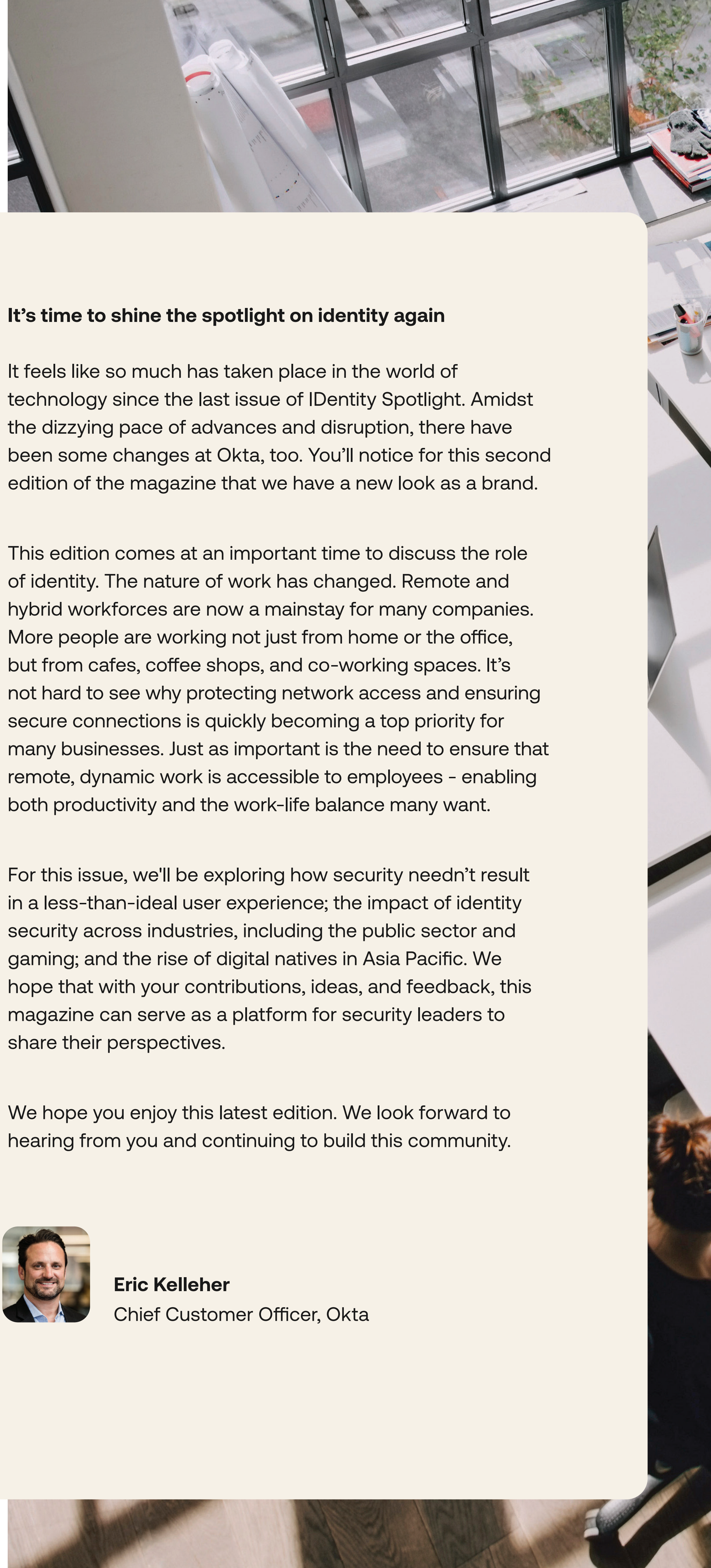
iDentity Spotlight

ISSUE 02
ASIA-PACIFIC

Daniel Hughes
Chief Information Officer
Department for Education,
South Australia

Paul Williamson
Director
Insync Solutions

Creating a secure environment for teachers, students, and technology's potential



It’s time to shine the spotlight on identity again

It feels like so much has taken place in the world of technology since the last issue of IDentity Spotlight. Amidst the dizzying pace of advances and disruption, there have been some changes at Okta, too. You’ll notice for this second edition of the magazine that we have a new look as a brand.

This edition comes at an important time to discuss the role of identity. The nature of work has changed. Remote and hybrid workforces are now a mainstay for many companies. More people are working not just from home or the office, but from cafes, coffee shops, and co-working spaces. It’s not hard to see why protecting network access and ensuring secure connections is quickly becoming a top priority for many businesses. Just as important is the need to ensure that remote, dynamic work is accessible to employees - enabling both productivity and the work-life balance many want.

For this issue, we'll be exploring how security needn’t result in a less-than-ideal user experience; the impact of identity security across industries, including the public sector and gaming; and the rise of digital natives in Asia Pacific. We hope that with your contributions, ideas, and feedback, this magazine can serve as a platform for security leaders to share their perspectives.

We hope you enjoy this latest edition. We look forward to hearing from you and continuing to build this community.

Eric Kelleher
Chief Customer Officer, Okta

Taking identity-first security to greater heights

To navigate around disruptions triggered by tech advances and the pandemic, many businesses have been gradually adapting their operations. This is especially so in Asia, where the cloud and digital services reign supreme. But amidst the region's economic uncertainty, the market and companies across industries are still poised for sustained growth. In this climate, security and customer experiences are rapidly becoming a top priority for businesses. Zero Trust security, built upon the basis of an identity-first principle, seems to be the path forward.

This is what we are focusing on in our second issue of IDentity Spotlight. Our cover story touches on how businesses can create a seamless customer experience while still keeping their operations secure. We then move on to the impact of identity security on crucial aspects of the business: employees, customers, products, and data. We also delve into how customer identity and access management (CIAM) has become a crucial part of digital strategy for a new generation of digital native businesses—one that also includes the massive esports industry.

We value the opportunity to learn from digital-first leaders like yourselves and relish the chance to discuss these emerging security challenges and trends. After all, it's only with your ideas that we can build a stronger community of professionals, and better empower one another.

We hope you enjoy this issue, and look forward to your continued support of IDentity Spotlight.

Ben Goodman
Senior Vice President & General Manager, APJ, Okta

Authors and Contributors

Publisher
Eric Kelleher

Executive Editor
Ben Goodman

Editor in Chief & Managing Editor
Jennifer Alejandro

Editorial Advisors
Camille Rasmussen
Clare Robson
Jess Bagherpour

Country Editor
Kiyomitsu Nakata (Japan)

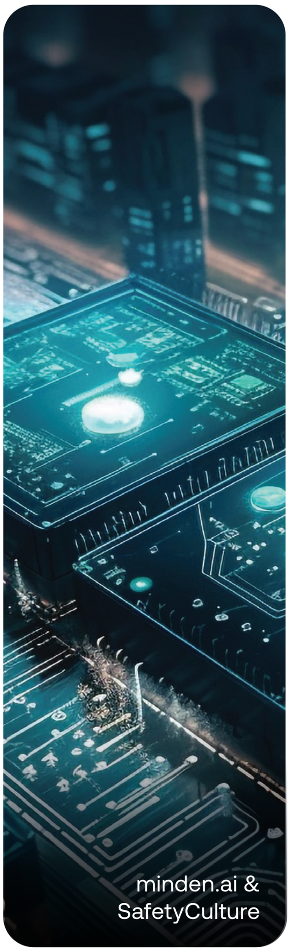
Op-Ed Contributor
Ben King

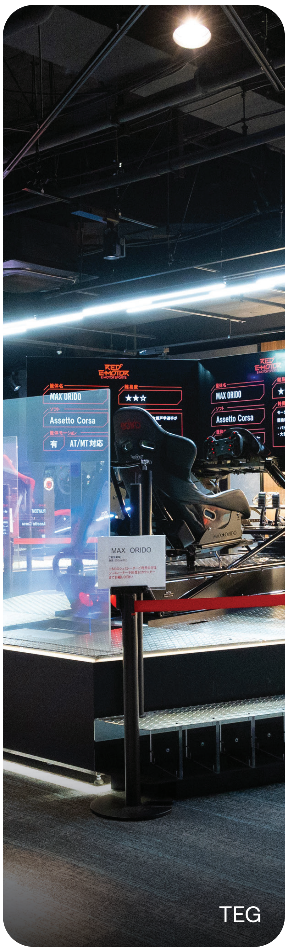
Editorial
Bill Davies
Alycia Lim
Khee Hoon Chan

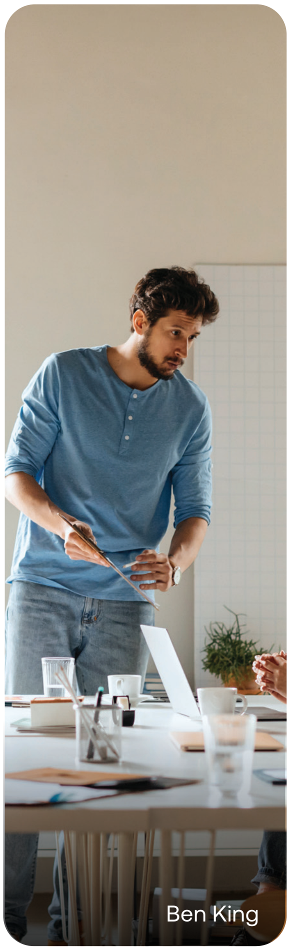
Creative & Design
Guilet Libby
Jenn Perng Chong
Dora Claire David
Vanessa Tan
Camille Iris Sabado

Project Management
Simon Hearn
Advait Naik
Joie Tan
Balbir Kaur

Department for Education, South Australia & Insync Solutions


minden.ai & SafetyCulture


TEG


Ben King

Singpass

Government of South Australia
Department for Education

insync
solutions

Creating a secure environment for teachers and students to harness emerging technology

Technology's impact on the world of education is unquestionable. We're a long way from the days of piles of notebooks, overhead projectors, and chalkboards. These days, technology plays a central role in the design and delivery of curriculum in schools around the world.

Whether it's augmented reality or the hot topic of the moment, generative AI, the emerging use cases for new tech in teaching and administration of education are vast.

But where technology flourishes, security risks often follow. The education sector is no stranger to cyber attacks and data breaches, with high-profile examples in Australia and New Zealand in recent years.

The education environment is also a complex one, where users range from young children to time-poor teachers and backroom staff, with potentially rebellious teenagers thrown into the mix. And all of them need their identity and access to systems managed securely and correctly.

The department covers

900

schools, preschools, and childcare centres across the region

So what could stand in the way of technology's full potential being harnessed in the classroom and beyond? How can educational bodies move forward with confidence, stability, and flexibility? And does the need to keep these environments secure stifle innovation and negatively impact the user experience?

Delivering world-leading education in South Australia

The Department for Education in South Australia delivers school education throughout this geographically diverse state. In total, the department covers over 900 schools, preschools, and childcare centres.

Daniel Hughes, the Department's Chief Information Officer, believes that technology plays a key role in helping open up pathways and opportunities for students to immerse themselves in technology that exists today, but also emerging technologies that will be part of future job pathways.

But for all this progress to be possible, the organisation needs to be set up for success. As Hughes puts it, "We need to make sure the right digital foundations are in place. Without those, it's hard to have conversations with schools and preschools about how they use technology to achieve better outcomes."

Simplifying the lives of teachers

Working with Insync Solutions, the Department for Education deployed Okta single sign-on across their entire organisation and school network, transforming the experience for students, teachers, operations, and corporate-level staff.

When Hughes and the team from Insync sat with teachers to understand their technology experience, it became clear that some changes needed to be made. One teacher reported having to try to log in as many as 15 times before she could begin teaching the class. It's delays like this that can really add up over the school day and eat up valuable time that could be spent giving students a world-leading education.

20%

reduction in frontline service desk volume

Some teachers were having to log in as many as

15x

> "One of the biggest challenges we faced was scale. This led us to a hub and spoke model, providing seamless authentication and access to applications to provide the same experience for everybody—whether you're a metropolitan school or a regional school in a very remote area."
>
> - Paul Williamson
> Director, Insync Solutions

The changes made became even more important during the COVID-19 pandemic, when students needed to access learning and the right resources from anywhere. This period produced some important lessons for Hughes. "Technology changes have always been difficult in a large system such as ours," said Hughes. "However, what we learnt from the pandemic is that we can be more agile, adaptable, and flexible when we consider significant technology change."

Exploring future and emerging tech with confidence

With stronger foundations in place, what does the future hold for the department and its technology?

“One of the challenges I've currently got as a Chief Information Officer is understanding how we can immerse emerging technologies into the classroom context,” said Hughes.

Moving to single sign-on has given him peace of mind moving forward into these new technological frontiers, helping them empower schools to get the most out of innovation.

> “Schools, by their nature, are innovative and creative, and we want to promote and support that. To know that we've got the right security parameters in play means that we've got a heightened level of confidence as we adopt new approaches going forward.”
>
> - Daniel Hughes
> Chief Information Officer, Department for Education, South Australia

Experimenting with AI

A lot of the wider discussion around generative AI and education has focused on the potential for negative outcomes, like students using it for their essays and homework and trying to avoid detection. But harnessed properly and controlled correctly in the education environment, the potential benefits of this emerging technology are huge.

It's something the Department for Education is already working at. They're experimenting with generative AI products to see how these can enhance learning for students and teachers, but doing so with student safety first and foremost.

Moving into these exciting spaces with the right foundations in place is key to success. "We have a Chief Executive and a Minister who are very supportive of the use of generative AI within the classroom," Hughes said. "So we're looking for ways to start delivering these platforms in meaningful ways for our students. However, it's important to know that we can enable it for certain cohorts of students and enable it systematically. We certainly never had that agility and flexibility before."

Does enhanced security mean increased complexity for the Department for Education? Hughes admits he could see where such a preconception would come from. “Traditionally, enhanced security has often tripped over innovation, especially when it failed to put the user first.”

But having been on this journey, Hughes' perspective has changed. “Following what we’ve learned in the last few years, heightened security controls have resulted in simplicity for us and a better user experience.”

minden.ai

SafetyCulture

Digital Native Businesses: pioneering the digital landscape securely with CIAM

From food delivery to cryptocurrency, digital native businesses (DNBs) have grown exponentially over the past decade, driving economic growth and creating new jobs. According to International Data Corporation, DNBs are companies that use cloud-native technologies and leverage data and AI across all aspects of their business. To keep that data secure, customer identity and access management (CIAM) becomes a natural and necessary part of the architecture. In fact, CIAM is critical to the success of DNBs as it allows them to provide seamless and secure customer experiences while meeting compliance requirements.

33%

of DNBs consider themselves 'extremely knowledgeable' when it comes to understanding CIAM*

73%

of DNBs in the APJ market consider CIAM to be a critical part of their overall digital strategy*

New Okta research conducted with Kantar, we found that in the Asia Pacific and Japan (APJ) region, about a third of DNBs consider themselves ‘extremely knowledgeable’ when it comes to understanding CIAM. Furthermore, 73 percent of the DNBs in the APJ market consider CIAM to be a critical part of their overall digital strategy. As cybercrime and data breaches become increasingly common, these figures reveal that organisations are headed in the right direction.

Having CIAM solutions implemented within the backend architecture is key as it acts as the virtual “front door,” keeping data safe while providing easy access to websites and applications. While businesses know the importance of implementing a CIAM solution, choosing the right one for the business can be challenging.

**Source: The Future is CIAM: insights from 200 APJ leaders. Research from Okta, 2023.*

Build vs buy: making the right choice for your business

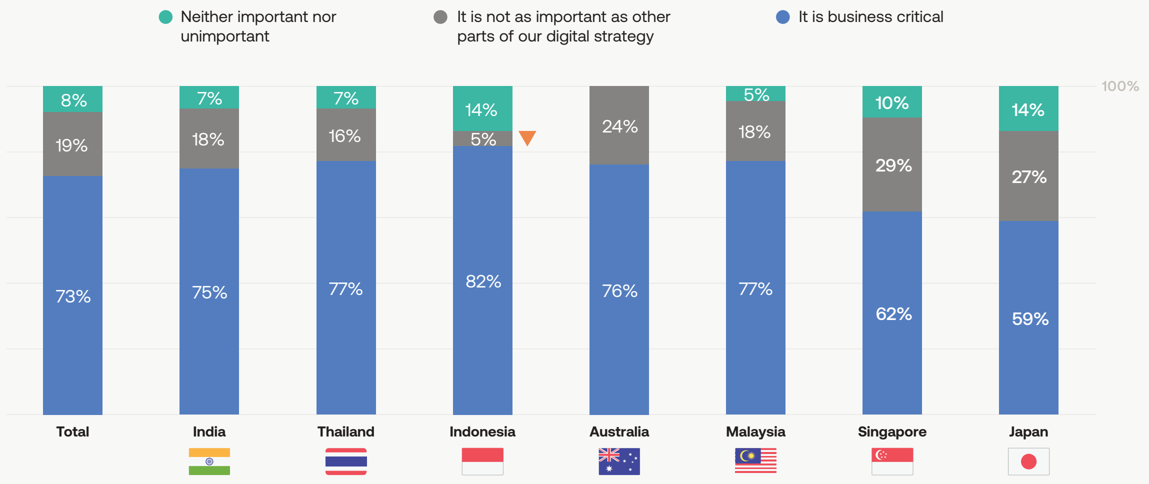
A majority of digital native businesses in APJ have in-house CIAM solutions. Businesses often choose to build rather than buy because of data privacy concerns and a desire for complete control and ownership of the solution. The remaining 34 percent of organisations surveyed in the Kantar report say they use an off-the-shelf solution, citing high scalability and reliability as their key reason. What holds organisations back from exploring SaaS-based solutions is often migration complexity, followed by cost.

While in-house solutions give organisations greater control and ownership, having an external application can actually be more cost effective in the long run. CIAM platforms are also built with security as a core tenet, and because they have a deeper level of expertise they're able to identify any issues and resolve them quickly.

For many businesses, gathering customer information securely is crucial to their success. One such example is minden.ai, a Singaporean enterprise known for the development of the yuu App. yuu is a loyalty coalition programme that rewards consumers every time they make a transaction. From the get-go, the organisation chose to deploy Okta for its longstanding reputation in Identity. With the goal of a big bang launch, there was no room for error, so the team chose to leverage Okta's expertise in ensuring that all of its stakeholders were able to access the app securely.

When it came to cost, minden.ai took a long-term view, and looked at opportunity cost instead of the total cost of ownership for the implementation of an external security solution. By having experts in the field manage its security and compliance side of the business, engineers were freed up to do more innovative work that would build other revenue-generating solutions.

Importance of CIAM as part of overall digital strategy



Base: All respondents (n=218). India (n=44), Thailand (n=44), Indonesia (n=44), Australia (n=21), Malaysia (n=22), Singapore (n=21), Japan (n=22)
Q2. How important is having a customer identity (CIAM) solution as part of your overall digital strategy?

▲/ ▼ = Significantly higher/ lower than rest of market

Source: The Future is CIAM: Insights from 200 APJ leaders. Research from Okta, 2023.

Supporting scalability, reliably

One of the benefits of entrusting your organisation's identity management solution to a third party is the flexibility it enables. Every business wants to scale quickly, but being able to do so while ensuring the best level of security for customers can be challenging, particularly in a space that's always transforming.

For SafetyCulture, a SaaS company in Australia that helps organisations around the world keep people in the workplace safe, providing a connected experience with ease of access was key. Being a digitally native business that is constantly evolving, moving to a third-party CIAM solution made sense, as they could let their in-house developers focus on innovation, rather than spending time on the nitty-gritty of an in-house security solution.

> "On some things, it's just better to go with specialists, rather than generalists. That way, we can focus on solving problems for our customers."
>
> - James Simpson
> Chief Technology Officer, SafetyCulture

Having an in-house security solution means constantly keeping up and anticipating what the next developments are. By freeing up the mental space and workload from its engineers, SafetyCulture could focus their attention on building and innovating new solutions for their customers instead–scaling up with expansion into new markets while maintaining a seamless experience, no matter where in the world their customers are.

Choosing the right CIAM solution for DNBs

It’s undeniable that CIAM is critical to the success of any digital business, particularly digital native businesses that come with the promise of flexibility and growth. So, finding the most suitable solution that provides seamless and secure customer experiences while meeting compliance requirements is key.

Whether you choose to build your own or buy a third-party solution, weigh the overall pros and cons with the long-term big picture in mind to drive secure and sustainable growth.

TEG

Identity Security & Authentication in esports: A case study on TEG

From virtual reality (VR) to the metaverse, the advent of new, emerging technologies is changing the face of the booming esports industry. No longer are esports arenas confined to physical locations, with online spaces increasingly becoming an attractive destination for both participants and spectators. Then there are new innovations in Web3 that are transforming the value of digital tokens found within games. This trend, however, also follows a shift in the security and computing demands for today's esports businesses. More is now at stake when it comes to protecting and authenticating users.

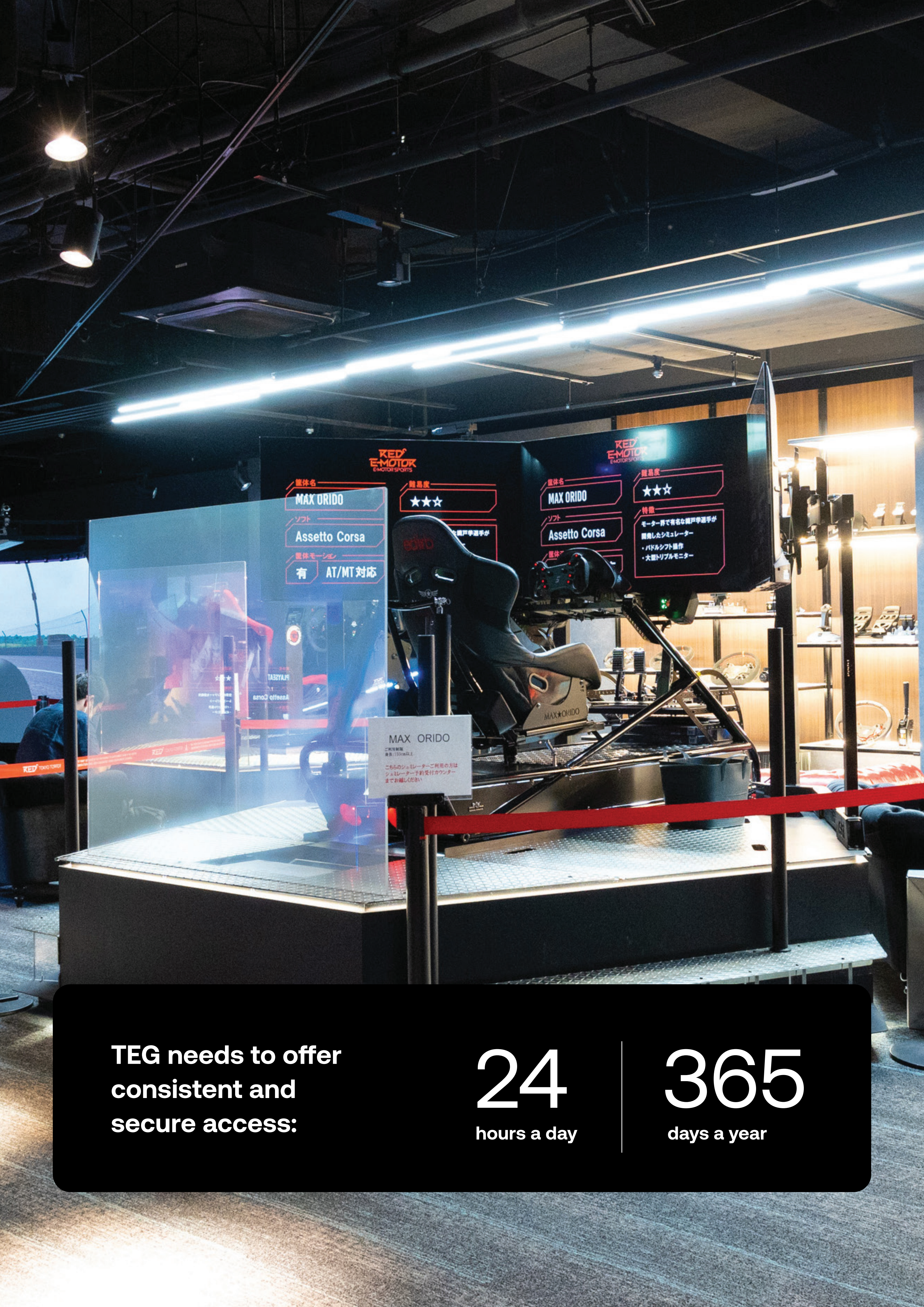
As more and more games integrate blockchain for play-to-earn models, decentralised identity solutions are coming into play. The landscape is vast, and as players try to navigate this new world, the gaming industry is finding ways to safeguard players and their identities.

One example of a gaming company that specialises in the development of esports theme parks is TEG. TEG opened the largest esports park in Japan, known as RED° Tokyo Tower, which boasts a vast area of around 5,600 square meters, and over 20 types of attractions, such as VR games, a stadium and a streaming studio. To visit RED°, customers have to purchase admission tickets, and the digital division of TEG has decided to introduce Okta Customer Identity Cloud (Okta CIC) for authenticating their purchases.

Authentication, however, was not the only objective that TEG wanted to achieve. The company didn't just want to create a system where fans could purchase admission tickets online. What it envisioned was a platform where creators and fans could meet online. With only a single login, people could not only gain entrance to the park, but also seamlessly access all services provided by RED° with a single sign-on. This would include access to additional web services, the ability to buy special event tickets, and access to the RED° online store.

But creating an individual authentication software for every service can take up a lot of development time and cost. Doing this can also increase the security risks associated with using each service, while impairing their usability for customers.

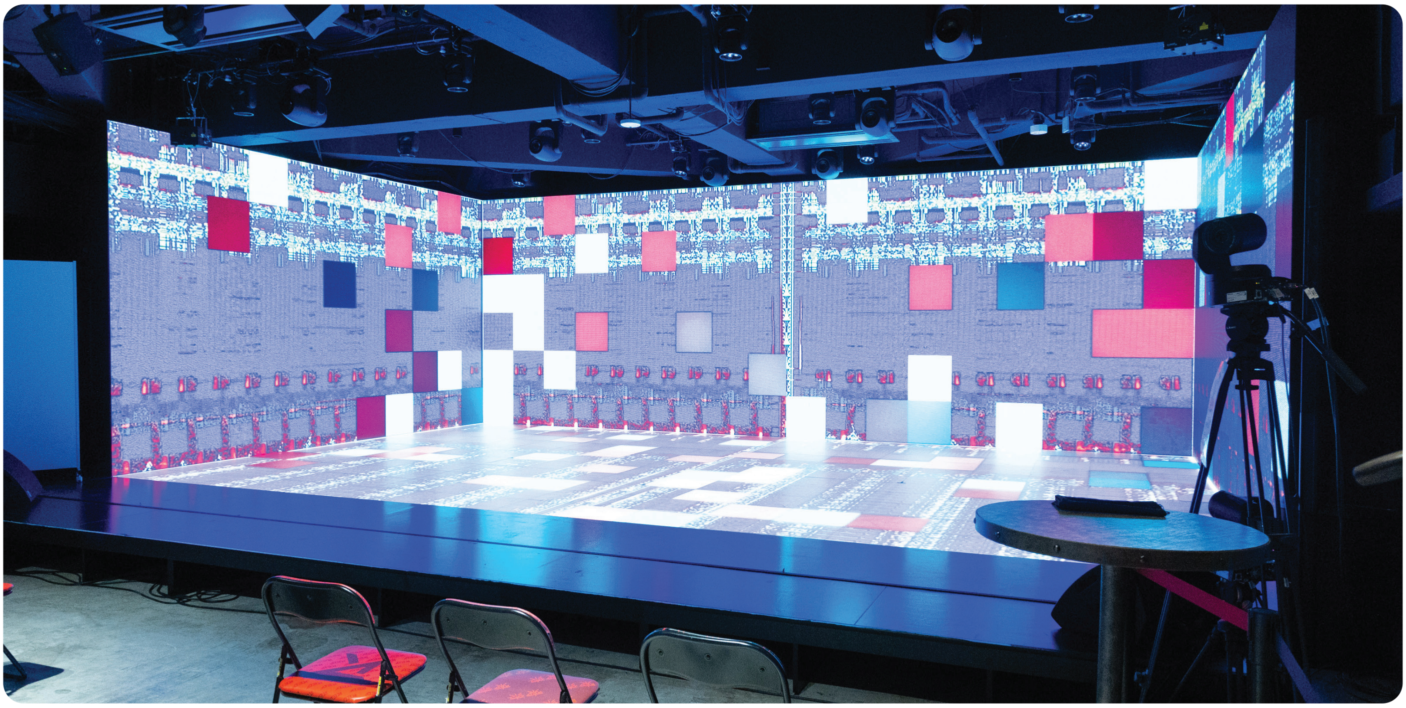
TEG sought a solution that could address three particular issues for its digital platform. Firstly, RED° and other TEG services are deployed 24 hours a day, 365 days a year. At the same time, given that TEG operates in the entertainment field, momentary peaks in demand are to be expected. As a result, the authentication platform had to be reliable enough to withstand high workloads.



TEG needs to offer consistent and secure access:

24 hours a day

365 days a year



Secondly, TEG planned to deploy additional services in the future, so the solution needed tobe easily integrated with these services. And finally, comprehensive support is vital to TEG, since a priority is to introduce these features quickly and efficiently. Okta offered essential access to the technical support and documentation that TEG needed and continuous support when the authentication platform was in operation.

Given that TEG only had a short period of time to implement the authentication features needed for its services, the company decided to implement Okta CIC across its infrastructure. Okta CIC was easy to implement, since it is in line with authentication standards such as OAuth and Open ID. The language in the technical documents was easy to understand, so developing on Okta CIC became quite intuitive for the TEG digital division.

For TEG, it was important that the authentication platform it used could impose strict security requirements to prevent leaks of confidential data, while still applying security patches frequently. With Okta, the company was able to leave all the security updates to the team, knowing that they were operating at the highest security level. Since deploying Okta CIC, the services remain largely problem-free even half a year later, with the digital division able to operate with the Okta CIC platform even under the most stressful of environments.

TEG is currently working on launching Red Token, a next-generation cryptocurrency, which will be connected to and used in conjunction with RED°. As TEG plugs into the business of the metaverse, robust and reliable security will not only be playing a greater role for the company, but eventually the esports landscape at large.

Ben King
Vice President,
Customer Trust, Okta

Getting into Phishing-Resistant Authentication with Ben King

Most CISOs and IT teams are familiar with multifactor authentication (MFA), as it is a commonly used defense strategy against cyber threats. But what about phishing-resistant authentication? We speak to Ben King, Vice President, Customer Trust at Okta, who shares with us more about what phishing-resistant authentication is, how it differs from MFA, and why it should be a part of every cybersecurity checklist.

What is phishing-resistant authentication? How is it different from two-factor authentication or MFA?

MFA limits credential-based attacks, and offers detection opportunities when an attack is attempted. Over time, however, adversaries have adapted their attacks in an effort to bypass traditional MFA protection as its use has become more prevalent. A common scenario is an Adversary-in-the-Middle (AiTM) attack where a user is directed to a fake phishing site that is configured as a reverse proxy server. These sites can pass legitimate credentials and MFA challenges back and forth between a target and a legitimate web application. If the target authenticates via this proxy, the adversary can access passwords and a valid authenticated session.

To maintain security, experts are championing phishing-resistant authentication. This is a mechanism where the authenticator is cryptographically bound to the domain, such that it can determine the legitimacy of a request upon use. This defends a user against just about any phishing attack by ensuring the MFA challenge only works for the address/domain the user intended to access. Examples of phishing-resistant authentication available in the market today include FIDO2 WebAuthn, Okta Verify FastPass, and Smart Cards.

What are the key challenges that organisations face today and how will phishing-resistant authentication play a role in protecting against evolving threats and attacks?

Phishing attacks lead to credential compromise for the target and unauthorised access to a target's account. This access can be abused in many ways, from stealing confidential data like corporate IP and customer details to business email compromise and other forms of fraud. Generally, people are a vulnerable and attractive target for criminals, and a well-crafted phish can fool even the most skeptical user. By using phishing-resistant authentication to stop these attacks early in the kill chain, organisations greatly decrease the risk they face from these attacks, allowing them to focus time and resources in better places.

What types of industries will benefit most from phishing-resistant authentication?

History has shown any industry where users regularly use email is under threat from phishing attacks. Criminals can and will take advantage of anyone they can, from students and healthcare workers to bankers and government officials.

What are some of the key benefits of implementing phishing-resistant authentication?

There are a multitude of benefits when implementing phishing-resistant authentication. It helps security teams remove a major risk which is a root cause of illegitimate access and many attacks. As a result, there will be fewer occurrences of users resetting passwords, a reduction in account takeover activity, and therefore a reduction in required follow-up or remediation, and as a whole, there will be less risk of business email compromise or data extortion scenarios. All of these benefit stakeholders at every level.

This doesn't mean security teams have less to do in their day job; it simply means they can focus on more important tasks, and areas that add real value to the organisations they support.

Where do you see phishing-resistant authentication fitting into the larger security strategy of an organisation?

Security strategy for any organisation already includes identity security as a foundational component, and this has only become more apparent with the popularity of Zero Trust security frameworks in recent years. This covers the security of users and the access they have, to the data, applications, infrastructure, and resources they need to access. A user's identity is where access, data flows, and transactions all begin, and so is a fundamental control point for every organisation.

Just as using an additional (MFA) factor is a simple uplift from a traditional username and password at login, the uplift to phishing-resistant authentication is a little different in terms of user experience. Complementing a possession factor (such as FastPass) with a fingerprint or facial recognition (to verify user presence) has been shown to decrease verification time and improve user experience compared to passwords, while also delivering a more robust security outcome.

As corporations, individuals, and governments take steps to build and demonstrate trust to operate more effectively, how do you see Okta as an enabler?

Building trust requires significant time and effort, but losing it can happen in an instant. Security and transparency have become table stakes to operate and compete in a digital world in which workplace and consumer norms have shifted. The expectation of security comes not just from legislators and regulators, but from the supply chain, from partners, customers, and end users, and is consistently reported on by the media.

As the global leader in identity security, Okta offers an independent identity platform, enabling out-of-the-box integration to a network of over 7,500 technology partners. This identity service is available to organisations to protect and support their user base.

What do you think are the biggest challenges and opportunities for phishing-resistant authentication in the future, and how is Okta addressing them?

The biggest challenge facing the uptake of phishing-resistant authentication is the change-resistant mentality of many towards technology and user experience. Many fail to clearly see the risk to themselves and their organisations until the damage has been done, at which point it's too late.

The opportunity, of course, is to secure ourselves, our communities, and our organisations, while improving useability and providing amazing and seamless digital journeys for end users—before falling victim to a preventable attack.

The internet is talking a lot about generative AI. How do you think generative AI will impact cybersecurity and how should organisations remain vigilant in this changing landscape?

Conversations about AI, machine learning, neural networks and large language models are not new, despite the marketing and media frenzy kicked off by the innovative experience Open AI has showcased with ChatGPT. That said, I see a variety of scenarios in which generative AI will impact the cybersecurity threat landscape, and this list will only increase.

- Phishing is a concern, and the use of better tools will enable better emails to be crafted in less time than ever before. The old indicators of a phish, perhaps poor spelling or grammar, may cease to appear.
- Deepfakes, including synthetic video and audio, will likewise only improve in their realism. In recent months, we've seen disinformation images showing Boris Johnson being arrested and Donald Trump in a prison uniform. Uses for this technology to enable fraud or manipulate public opinion abound.
- Generative AI is being probed by researchers to circumvent ethical controls, including demonstrations where online tools generate functioning malware.

- Finally, my largest immediate concern is the poor understanding of what happens to data input to an online service. It is likely that data is stored, perhaps poorly secured, and by nature AI tools learn from data input and may repeat elements of it by way of answering another user's requests. We've already seen examples of this, where corporate IP or personal information has been potentially exposed and is irrevocable.

At the speed technology progresses, cybersecurity measures are a full-time job. As new cybersecurity measures get implemented, cybercriminals are already planning their next move. To be truly secure, organisations should work with the latest technologies and partners to ensure a future-proof platform.

singpass

Okta integrates with Singapore's national digital ID system

The integration with Singpass will let Okta customers authenticate consumers using Singapore's national digital ID system and is expected to expand the company's reach in regulated industries.

Article authored by Aaron Tan, originally published by Computer Weekly

Okta has integrated its customer identity and access management (CIAM) service with Singpass, enabling organisations to provide consumers with access to digital services using Singapore's national digital ID system.

First launched in 2003 as an identity service for users to access e-government services using a single set of credentials, Singpass has since expanded its capabilities to enable users to digitally sign documents, look up contributions to their Central Provident Fund accounts, and access digital equivalents of their driving licence and identity card, among others.

Leveraging application programming interfaces (APIs), the service is also being used by private sector organisations such as banks and financial services firms to facilitate account applications and other transactions.

With the integration between Okta and Singpass, a complimentary service for Okta customers, such organisations will be able to leverage the infrastructure that has been built around citizen services to authenticate consumers for private sector services, said Ben Goodman, Okta's Senior Vice-President and General Manager of Asia-Pacific.

Singpass has a user base of more than

4.2M

users

“The Okta-Singpass integration is really around bringing the best of government services to private sector digital services and enabling a more trusted way of authenticating and accelerating customer onboarding and engagement, with a greater level of safety and control around identity management,” he told *Computer Weekly.*

Besides authenticating consumers with Singpass, Okta customers can also take advantage of other benefits of CIAM, such as step-up authentication, fraud analytics, as well as capabilities to prevent credential stuffing. Goodman said this will enrich the value of the Okta platform for existing customers and enable the company to reach out to new customers in regulated industries.

Anil Panicker, Okta’s senior manager for solutions engineering in Asia-Pacific, said the company has developed capabilities to support the Singpass integration. These include support for OpenID Connect to facilitate authorisation code flows as well as additional layers of security through signatures and encryption, alleviating the overheads that organisations may bear when they do their own integrations with Singpass.

NTUC Enterprise, a social enterprise with a footprint in healthcare, insurance and retail, among other areas, is one of the early beneficiaries of Okta’s integration with Singpass.

“As an organisation that has tested the Singpass solution with millions of users over the past year, we are delighted to report positive outcomes, in particular, improved user experience and increased customer satisfaction,” said Winson Lim, Head of Digital Product Development at NE Digital, the data, digital and technology arm of NTUC Enterprise.

A Government Technology Agency spokesperson told *Computer Weekly* that the agency, at the request of relying parties, also works with other reputable CIAM platforms with a strong security posture to integrate with Singpass and bring value to citizens and businesses. “Relying parties will still need to onboard with us, which we will determine on a use case basis,” she said.

Serving

97%

of Singapore citizens and Permanent Residents aged 15 and above

It facilitates approximately

300M

personal and corporate transactions every year

A relying party is an entity that relies on the credentials and authentication mechanisms provided by an ID system, typically to process a transaction or grant access to information or a system.

Besides Singpass, Okta is also involved in other digital identity initiatives, including those run by the private sector. In Indonesia, for example, it is working with PrivyID, a digital trust provider, to deliver credential management services for 47 million consumers, said Goodman.

> "The solution's robust security features also give us greater assurance that we are interacting with authentic parties."
>
> - Winson Lim
> Head of Digital Product Development, NE Digital

"We are also doing a lot of work with various government agencies in Australia around digital identities, authentication and providing frictionless experiences around their platforms," he said.

Thank you

Thank you to all the contributors who have made this magazine possible.

It is our goal to make this publication a substantial source of news and information for leaders in Identity Security across APAC.

Join the IDentity Spotlight APAC community as a contributor by submitting your story ideas, essays, and opinion articles.

To reach out to the editorial team to share industry news, career movements, identity security transformation projects or simply to provide feedback, write to us at **IdentitySpotlight@okta.com**

This magazine is printed on 100% recycled material as part of OKTA's sustainability initiative.