issue
01
Asia-Pacific

iDentity Spotlight

Brought to you by okta

SCORING A SUPER GOAL STRATEGY FOR BUILDING TRUST IN NEXT-GEN FANS

Rob Pickering
CTO, Australian Football League

PUBLISHER
John Zissimos

EXECUTIVE EDITOR
Celestine Tan

EDITOR IN CHIEF AND MANAGING EDITOR
Jennifer Alejandro

HEAD OF OPERATIONS
Minkyu Chin

HEAD OF SALES DEVELOPMENT
Vivien Chew

APAC EDITORIAL ADVISORS
Molita Coelho
Clare Robson

COUNTRY EDITORS
Kiyomitsu Nakata (Japan)
Bum Jin Cho (South Korea)

DIGITAL MARKETING TEAM
Sarah Alder
Daniel Goodman
Sarah Robertson

WEB MARKETING
Steven Kuy

MARKETING TECHNOLOGY
Paul Guevara

REGIONAL EDITORIAL SUPPORT TEAM
Hollis Scoggin
Cassandra Theocharous
Cherry Lin
Neha Bains
Vivian Wang
Suseri Yaguchi
Keita Ando
Jesse Ambara

APAC VOICES SEGMENT PRODUCER
Rachael Wee

ANZ PARTNERS PROGRAM
Sophie Fielding

REGIONAL PARTNERS PROGRAM
Danielle Adamson

JAPAN PARTNERS PROGRAM
Yuto Senda

REGIONAL STRATEGIC EVENTS
Nicole Reynolds
Lara Smith

PROJECT MANAGEMENT
Simon Hearn
Advait Naik
Balbir Kaur

EDITORIAL
Sofianna Ng
Alycia Lim
Seamus Byrne

CREATIVE & DESIGN
Guilet Libby
Jenn Perng Chong
Ashley Patterson

PUBLISHER'S NOTE

Putting the spotlight on Identity Security

IDentity Spotlight is a publication created to build a community of identity security leaders in APAC; a place to learn, share perspectives and best practices and discover trending insights. Over time, we'll be creating networking chapters in each city, and you are invited to be part of this growing community!

With the launch of the first issue, we turn our attention to hear from the people and organisations who have overcome various challenges in their respective industries. We've had the honour of speaking to Rob Pickering, CTO of the Australian Football League and Ben King, Global VP, Customer Trust, Okta, on the importance of earning users' confidence on their platform by putting their privacy first. We also hear from NTUC Enterprise, Saitama Prefecture and Soul Machines who have shared how the transformation of new-age security infrastructure has helped organisations improve operations and guard against fraudulent attacks.

As we work towards keeping this magazine an open space for security leaders to share their thoughts and perspectives, we welcome new ideas so we can learn from one another. Join us as a contributor by sending us your opinion pieces, or share with us the successes you've had in solving identity security challenges within your organisation. No idea is too big or small, so we urge you to be an active member of this community by sharing your insights.

Finally, we hope you enjoy reading our inaugural issue; available in both digital and hardcopy and we look forward to building an APAC Identity Security Leaders community together.

John Zissimos
Chief Marketing Officer, Okta

CONTENTS

04
COVER STORY

12
IN CONVERSATION

16
OKTA SPOTLIGHT AUSTRALIA

20
OKTA SPOTLIGHT SINGAPORE

AFL CTO Rob Pickering tackles tech transformation in sports

NEW
CRM
for AFL & 7 clubs

NEW
ERP
for 12 clubs

ONE
connected stadium

As CTO of the Australian Football League (AFL), Rob Pickering works alongside some of the oldest and proudest sporting teams in the world, which has taught him what it means to be a team player beyond the world of sports.

The professional organisation behind the unique Australian-rules football sports, the AFL is Australia's most watched and attended sport with its annual grand final being one of the highest attended club championship events in the world. It's fast, it's hard hitting, and it's exciting. But what you may not know is that it increasingly sees technology layered into every aspect of its operations.

Pickering's work at the AFL incorporates not only the entity's operations but also assisting with the technology for many of the sport's clubs as well as the 60,000 seat Marvel Stadium in the heart of the Melbourne CBD. Managing secure and robust digital infrastructure across everything from public venues to corporate offices can be a varied programme to manage and transform.

He outlines a wide range of large scale changes over the past year – a new CRM for the AFL and seven clubs, a new ERP for twelve clubs, rolling out a new 'Connected Stadium' network and more – all while migrating workloads to public cloud. It's clearly been a non-stop programme of innovation.

"Our key priorities this year are to continue to iterate and build capability on top of these cornerstone investments to deliver maximum value from them," says Pickering. "We're also excited to be rolling out a new customer identity project which aims to remove the different logins across systems and replace them with one login to remove friction for fans so they engage more with the sport they love."

Building trust for the next-gen of fans

As deep as a fan's love can run for their favourite sport and team, Pickering knows that trust in the organisation that runs the game can still be won and lost in the blink of an eye.

"Security and privacy are inextricably linked with trust," he says. "The trust an organisation has from customers, staff and stakeholders takes a long time to build and not long at all to break down. Trust is a key decision point for people to want to work with you, so we see it has tremendous value to the AFL both from a revenue perspective and in maintaining our social licence to operate."

Pickering says that a CTO must look at security through a risk and governance lens, working with the board to understand the security 'risk appetite' and then build controls that match. Then execute flawlessly – something he feels the AFL does better than most thanks to a culture of accountability and ownership that he claims he has not seen anywhere else.

"The AFL's purpose is to progress the game so everyone can share in its heritage and possibilities. When you work here, you're a steward of a game very much embedded in Australian culture – so what you do here matters and how you do it matters even more."

Getting security and trust right as part of driving transformation programmes forward ensures partners and fans alike can feel understood and valued as the sport moves into the future.

Strategies for the win

With some impressive digital evolution at the AFL and excellent results on the scoreboard, what are some key lessons on leading a technology team to victory? Pickering has plenty of advice to share.

- **Investigate options carefully**
  Ensure that small-scale opportunities for improvement are given as much attention as the large-scale transformations that grab the big headlines.

- **Be realistic**
  Analyse your options carefully to maintain the trust of your stakeholders when pitching for the investment you need. While we all want to get our business cases approved, many benefits take a while to arrive and can be difficult to attribute.

- **Get your teams aligned**
  Having everyone aligned toward the success of the transformation means keeping the team top of mind and ensuring they are incentivised to succeed and are ready to operate the new tools once delivered. This means going beyond adding transformation workloads on top of existing commitments. For key roles, investigate backfill to ensure they're able to focus on delivering successfully.

Say no to the MVP

We're not talking Most Valuable Player. Pickering is a big fan of strong investment in DevOps, CI/CD and automated testing capabilities to ensure you don't just ship but move quickly to respond to feedback. But one idea that stands out is his desire to focus on a "minimum lovable product".

> "
> We're excited to be rolling out a new customer identity project which aims to remove the various different logins across systems and replace them with one login – which we think will remove friction for our fans in engaging more with the sport they love.

"Technologists talk about the minimum viable product, but that only works in start-ups and some digital products. No one wants to live a 'viable' life. When teams go through all the pain to adopt a new system it doesn't have to be everything anyone could ever want, but it must be materially better," says Pickering.

Getting to these kinds of 'lovable' results also means choosing the right partners, which Pickering says will truly "make or break" a project. That means more than just providing the right solution, but to also feel you're aligned culturally and have strong communication links so you can speak clearly and honestly to deal with problems before they cause deep impacts.

The future of football

"The future of football is similar to many other sports," says Pickering. "Fans are demanding more access to things they love about the game. More lifestyle information, more behind the scenes access, better game-day experiences in stadiums. Working in sports technology is cool for me because you get to blend the physical and the virtual – bringing to life experiences across in-person and at home."

With that in mind, Pickering sees many opportunities to bring new experiences to life through the latest technologies beyond the game day experience itself. From AR and VR, to NFTs and autonomous retail, exploring every aspect of what tech has to offer is on the table. But it takes time to chart the right course.

"Every technology leader is bombarded with ideas for tools and technologies they could deploy," says Pickering. "And just maintaining the myriad tools you have at your disposal is a job in itself. How much time do technology leaders spend thinking about things that could redefine a problem and not just solve it? I expect for many of us it's minimal – but it'll need to be more over time as business leaders look to us not just for risk mitigation but as a source of competitive advantage."

Not every CTO lives and breathes what their business puts out into the world, but Pickering does admit he spends a lot of his weekends at AFL games and events. There's no doubt he holds a clear passion for the AFL, its culture and its place in Australian society. Fans can feel confident the tech behind their favourite sport is in safe hands.

PROFILE

Rob Pickering, CTO, AFL

FUN FACTS

Gym-goer, golf and poker player, fur-dad to three rescue pugs Floyd, Betty, and Percy.

RECOMMENDED READING

Principles for Success by Ray Dalio –
I love this book about principles and try to live up to them as much as I can. I'm a big fan of the principle around embracing reality and dealing with it.

Thinking in Bets by Annie Duke –
As a keen poker player, I really learnt a lot from her thoughts on 'resulting' or mistaking good outcomes for good decisions.

INDUSTRY:
OPEN
BANKING

Navigating security in the world of open banking

The financial services industry is often a target for security breaches due to its nature, which manages dollars and cents on a daily basis. This risk has been compounded with open banking at the forefront. Which is why now, more than ever before, FinTechs need to be prepared at all times to protect their assets and their customers.

To get some insights on the security landscape, we speak to Mark Frogoso, who wears multiple hats as Chief Information Security Officer (CISO) of Mynt, and GCash, both leading brand names when it comes to FinTech in the Philippines. With over 16 years of experience, Frogoso is passionate about security in the online world.

Q: What is open banking, and what are the benefits of open banking?

A: The entire concept of open banking revolves around the enablement of customers to own and use their personal data to make better financial services decisions. The benefit of this is that customers have a lot more freedom in deciding how they want to manage their financial portfolio.

Of course, having the freedom of managing this data also means they are more exposed to different risks. Open banking allows customers to share their data using technology like APIs, so that authorised third parties can perform different financial transactions directly. This is why protecting customer privacy is so important in open banking.

Q: What is the level of maturity when it comes to open banking in the region, compared to the rest of the world?

A: Asia Pacific is actually a great hub for open banking, because people are tech savvy. At the same time, there is an underserved market which makes this region the perfect combination for open banking. But when you look at Southeast Asia, the approach is more market driven, instead of a regulatory mandated approach taken by regions outside of Asia.

This affects the level of consumer readiness due to security and privacy considerations. We are creating new financial products and offerings online and expect fast adoption. And all these create the perfect conditions for different risks targeted to organisations and individuals. This is why we are a little slower when it comes to really adopting open banking concepts, but we're catching up.

I believe that regulatory compliance, like having sensible and harmonised regulations in place and detailed specifications for set standards, as well as organisational and market readiness are significant considerations in adopting open banking.

Q: As an IT Security and risk management professional, what are the most common areas that organisations overlook when it comes to security?

A: I think organisations often overlook the most basic things. The first is accountability. This responsibility lies on the board and senior management, and will need to take a top down approach when implementing cybersecurity programmes.

Culture is another aspect that organisations need to focus on to promote security within their organisation. You need to have the right people with the right skill sets and competencies that will help build and implement cybersecurity programmes, but most importantly, employees need to understand their roles and responsibilities in this area and do their part.

Q: What are some of the key questions organisations need to ask themselves before setting up a security infrastructure?

A: Before jumping into setting up a security infrastructure, organisations should first ask themselves if they have the right foundations in place. This means having the senior management of the board implement and drive the cybersecurity programmes, with a clear top-down approach. It cannot start with middle management because everyone needs to be aligned.

Some examples include:

- Having the commitment from the board and executive leaders. Build successful and comprehensive security programmes and capabilities, and provide the appropriate support and commitment.
- Have a technologist, business-focused, transformational, and visionary CISO. CISOs need to improve not just on being a technologist

but more on the business side as well. The need to develop some of the soft skills is important to drive change within the organisation. In addition to preparing the business and organisation for its future growth, CISOs need to prepare for the future by continuously evolving and challenging the status quo and think of the future of security given the evolving regulatory and threat landscape, and technology advancements.

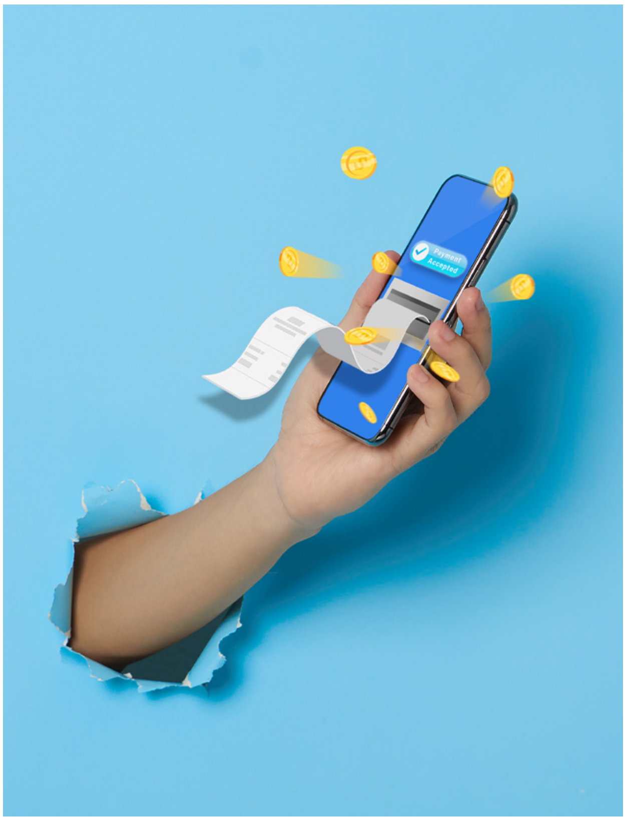
- Ensure regulatory compliance. Compliance to regulatory requirements is always challenging, but effective security leaders must ensure compliance is met to advance their security efforts and projects.
- Mature IT operations and governance processes. Look within the organisation and ensure that internal governance and IT processes are in place as it will have a direct impact on the downstream security processes.
- Have a human as security control. Humans may be your weakest link, but they can also be your strongest ally and security control.

Also, it's important to understand what your organisation already has in place, and have a clear measure of success. This is so that you're not just implementing something for the sake of implementing it, but to ensure it is done correctly and effectively.

Q: We know that security, particularly in the banking and finance industry is key. But how important is zero trust, and do you think FinTechs are keeping up to date with customer expectations?

A: Security is key not just for the financial services industry, but across all industries and sectors. But while the same risks are applicable to traditional banking, open banking expands the risk because access to other financial institutions through the third party entity.

Because cybersecurity is borderless, even the most secure company or organisation can be at risk if they're employing a third party with weak security. Essentially, you're only as secure as your weakest link. In open finance and open data, if an individual has authorised and given consent for a third party to access their information from different financial institutions, that means that an account takeover (threat actor who has access to someone's account) would have access to the same information.



This is why we need to implement robust access control (authorisation, authentication) and back-end checks so that we can immediately identify when something is out of the norm.

It's critical that FinTechs start implementing zero trust now, and I believe many FinTechs are still building that trust in the ecosystem. Because of the evolving threat landscape, there is still a lot that needs to be done to improve the way we do zero trust and security in general. Being adaptable and agile in adopting zero trust is also going to be more crucial as we introduce new technologies like AI and ML, even quantum computing in the near future.

Q: What are some practical things that people can do to keep their personal accounts secure?

A: The first thing is of course to be mindful and aware of the security risks that are out there. Keep your accounts safe by ensuring your passwords and online identities are protected.

Secondly, secure the devices that you use on a day to day basis. If you have a workstation or laptop you use daily, even your mobile device, make sure you keep them locked.

Finally, I would advise people to install at least one security software (e.g. anti-malware programme) on their personal devices to protect themselves from any malicious software that may come through the internet.

Bringing cyber risk conversations to the boardroom: a step-by-step guide

The cyber threat landscape has become more sophisticated in recent years, and organisations need to stay on their toes by ensuring they have the right processes in place. Here's a short guide on how CISOs can bring up conversations around cyber risk in the boardroom, without sounding any alarm bells.

By **Ben King**
Global VP,
Customer Trust, Okta

STEP
01

Establishing cyber risk appetite

A vital first step to effective risk management is determining an organisation's appetite for risk. However, not everyone in the boardroom is familiar with the cyber landscape their organisation operates in. This is where CISOs need to step in to educate board members and provide them with the necessary information. With everyone on a level playing field, they can come to a consensus on what they are trying to protect, why they are protecting it and from whom. Only with an agreed and documented risk appetite statement can we measure current maturity, gaps and risk in any meaningful way.

STEP
02

A scaled approach to managing risk

Once the organisation's risk appetite is determined, start building a strategy by looking at these key areas:

- **Situational Awareness**
  What are the current and emerging threats? Then find out the relevance of these threats for your industry and specific organisation. What drives these risk factors, and how is your organisation reacting to them?
- **Security Incidents**
  Review recent security incidents for the board's awareness in the reporting period – how did the organisation respond? Was the root cause addressed and resolved or was it merely mitigated, and how?
- **Security Capability**
  Measure and communicate maturity assessment of your existing security capability. The best way to do this is to compare it either against industry frameworks, or against industry peers, and see where your organisation stands.
- **Communicate a clear strategy and execution plan**
  Be clear on what the plan is and take into consideration longer term implications for the organisation. The execution plan should also be airtight so that everyone in the boardroom has a clear picture on what needs to be done.

STEP
03

Explaining the importance of cyber risk assessment strategies

Upon establishing a strategy and plan, CISOs need to communicate the business value of risk management in a way that is understood by members of the board, such as by illustrating the potential repercussions of any breach. What is the impact to the company's business and its reputation? What is the impact on revenue and share price, as well as on other stakeholders such as employees, customers, and regulatory bodies?

Roleplays and tabletop exercises are a good way to bring across these potential impacts in a realistic way. This is also a good way to assess the company's crisis preparedness.

STEP
04

Bridging the risk gap effectively

With the growing number of cyber risks, companies need to be mindful of where to invest limited resources to mitigate potential security threats. Some metrics that can help in assessing the effectiveness of existing risk management and security measures include:

- The number of security incidents per reporting period, time taken to identify these incidents, and time taken to remediate them
- Patching cadence of primary operating systems or applications
- Awareness measures such as phishing simulation and reporting
- Third Party Risk Management measures including supply chain vulnerabilities and critical supplier risk assessments
- Recovery metrics covering business continuity and disaster recovery planning and testing

In addition to relying on in-house capabilities, CISOs can also consider deploying best-of-breed solutions that are already available on the market, which are already secure, scaled for growth, cloud-native, and future-ready. This will ensure they free up precious talent and manpower resources to work on more high level, value-added functions within the organisation.

Supporting digital first readiness in APAC with Customer Identity

By **Linus Lai**,
Chief Analyst ANZ,
IDC

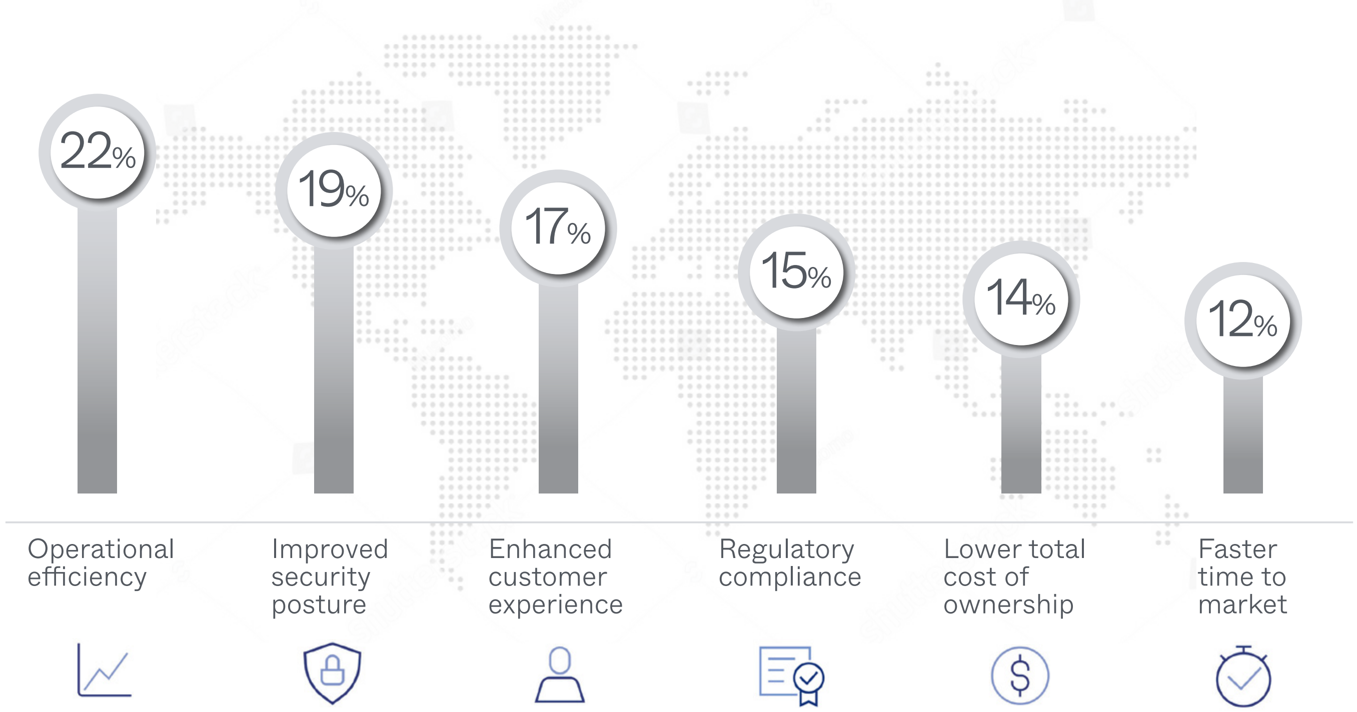
As businesses evolve with technology, organisations have begun to adopt digital-first strategies. Being digital-first is a mindset. It's how leaders think about their end-to-end operating model as a digital business, and can look very different across industries.

As these organisations reimagine ways to improve efficiencies, productivity, and stakeholder experiences across every touchpoint in a digital world, security becomes a recurring theme. Therefore, it is important to look at Customer Identity and Access Management (CIAM) to help manage the challenges around identity, operational efficiencies and as a way to improve security.

In a recent research we conducted, we found that 74% of enterprises already place CIAM among their top priorities as a digital-first organisation. We also asked organisations to share their top three business benefits after investing in CIAM. Here are the findings:

Customer/consumer identity and access management benefits

What are the top 3 business benefits that your organisation has achieved (or is expecting to achieve) by investing in customer identity and access management solutions?



Source: IDC's Asia Pacific Customer Identity and Access Management Survey, sponsored by Okta, April 2022

CIAM platforms are cloud-delivered, which means the same capabilities offered to enterprises are now able to be delivered to smaller businesses. Regardless of size, businesses can benefit from the advanced capabilities and managed services, removing the complexities behind running these platforms.

From helping organisations get their digital apps and services to market faster to improving user adoption, conversion, and engagement, all while reducing risks, learn more about the role of CIAM and how it can support digital first organisations in APAC by scanning the QR code below:

soul machines™

Humanising AI interactions with secure cloud-based global innovation

Movie lovers around the world have been dazzled by the work of Mark Sagar. From King Kong to Avatar and Rise of the Planet of the Apes, his work on Hollywood blockbusters has won Oscars.

But Mark is also the CEO and founder of New Zealand AI company Soul Machines, bringing ultra-realistic “digital people’’ into everyday life. He and his team are creating a “new AI interface” for human-machine relations for everything from finance to education and beyond – designed to interact naturally, intelligently, and emotively.

As Soul Machines has grown, it needed to expand its circle of Auckland researchers into a global network of business strategists, digital artists, marketers, salespeople, scientists and more. To do that, Soul Machines required a world-class identity management solution to protect its groundbreaking intellectual property while enabling frictionless collaboration wherever its staff may be.

In seeking a workforce identity solution, Soul Machines wanted more than a platform that simply “ticked the security and compliance boxes.” It wanted to run under a holistic workforce identity solution; one that empowers people through free-flowing inspiration exchange with security baked in. After canvassing solutions, Soul Machines found only Okta Identity Cloud, in collaboration with Auth0, shared this vision of identity empowerment.

“We needed a true empowerment and automation tool enabling innovative minds to get where they need to go faster,” says Sam Brightheart, Director of Information Technology, Soul Machines. “Seamless app integration, confidential information exchange, automated access control... these enable our global team to work in the most proactive, collaborative manner possible. With Okta and Auth0 joining forces, we can also look forward to more options and flexibility to innovate.”

The benefits of the migration were undeniable. From requiring a day or more to onboard a staffer, it now takes Soul Machines less than 40 minutes to set up a worker with all permissions. Deprovisioning is even simpler, with access denied in just a few clicks. Powerful workflow automations enable seamless creative engagement across teams while maintaining the highest degree of confidentiality. Previously, the company relied on email trails for tracking.

“We felt we needed a paper trail for permissions to confidential resources,” recalls Brightheart. “That became a strain on the top levels of management, and on top of that it wasn’t secure.”

Today, Soul Machine enjoys both efficiency and security with automated role-based access control. Looking towards the future, the company plans to free up even more creative processes by moving to other feature sets, and shift beyond identity management to viewing Okta and Auth0 as tools that empower the workforce, and in turn the business.

> “
>
> Seamless app integration, confidential information exchange, automated access control... these enable our global team to work in the most proactive, collaborative manner possible. With Okta and Auth0 joining forces, we can also look forward to more options and flexibility to innovate.

彩の国 埼玉県
Saitama Prefecture

Bringing Saitama employees and citizens into the future with digitised administrative operations

> “We will break away from the administrative office work of paper culture, realize a new next-generation work style, and work by digitisation.

Located north of Tokyo in the Kanto Plain, Saitama Prefecture is a region looking toward new work styles and lifestyles to encourage growth. The region is the fifth largest in Japan by population, but with a slightly ageing population. As such, it aims to encourage younger arrivals and renew Saitama Prefecture through digital transformation.

In March 2021, the Saitama Prefecture Digital Transformation Promotion Plan (or DX Promotion Plan) got underway and in January 2022 the DX Vision Roadmap set in place KPIs to realize the vision for the future of Saitama Prefecture.

One key aspect of the roadmap was a new Administrative Office Vision, that states: “We will break away from the administrative office work of paper culture, realise a new next-generation work style, and work by digitisation.”

To enable this new digitised administration environment and enable greater teleworking opportunities, Saitama Prefecture needed to introduce a range of cloud services and IDaaS to give its workers the infrastructure and secure access it needed to bring this all to life.

Through its digitisation planning process, Saitama Prefecture chose Box for its cloud file management system, DocuWorks for paperless support software, and Zoom as its communication system for telework. These core tools needed to be accessible for the 12,000 prefectural office employees, and it was Okta Identity Cloud that was chosen as the IDaaS authentication platform.

The installation work was carried out in four months from July to October 2021, and by mid-November the service was put into service across the organisation. With IDaaS in place, the Saitama Prefecture team has a simple and secure authentication system in place that providers single sign-in and multi-factor authentication that can easily serve for any additional digital services the prefecture may add in future.

“This is our first experience of shifting to the cloud on such a large scale and we needed to ensure access to our various cloud services was safely secured,” said Masaomi Ueda, from the Administration and Digital Reform Division of the Ministry of Economy and Finance for Saitama Prefecture.

Ueda saw that the management requirements of their older on-premises solution required much more maintenance for the technology team. Today, new digital services are updated regularly with minimal burden on the prefecture’s small team.

Across the various services, each can be assigned different security levels to suit the requirements of the platform, despite some legacy systems remaining on-prem. The promotion of DX in Saitama Prefecture is a medium to long term initiative that has seen great strides in its realisation for the prefecture and its citizens, businesses, and government. While the development of a truly digital infrastructure within the agency has just begun, having the right foundations in place means more advanced solutions can be implemented in the future.

NTUC Enterprise: Securely building a single customer view for its brands

NTUC Enterprise touches life in Singapore in myriad ways. From FairPrice Group supermarkets and eateries, to NTUC First Campus preschools, NTUC Health eldercare and clinics, the company features a suite of 10 social enterprises offering products and services for inter-generational families.

Since 2020, NTUC Enterprise has undergone a broad digital transformation, spearheaded by NE Digital. Seeking to streamline communications and form a better understanding of NTUC Enterprise's customers, they quickly ran into a serious challenge: separate customer accounts for each social enterprise's service, preventing the organisation from building a unified, holistic view of its customers.

To move forward, NTUC Enterprise needed an identity solution that would migrate all of this scattered data into a single profile for each customer, all while adhering to Singapore's Personal Data Protection Act (PDPA).

"I might have an account with NTUC FairPrice, one with NTUC LearningHub, and another with NTUC Health," says Winson Lim, Head of Digital Product Development at NE Digital. "Even if I just need to change my address, I would need to have multiple contact points to update my profile. We also saw we don't have a single location to identify if someone is a very valuable customer and we want to treat them like a VIP. The existing in-house identity solution did not have the capability to do that linkage."

Winson's goal was to build this single customer view. Using Auth0's API, the NE Digital team had the capability to connect across various vendors, regardless of different authentication systems. With 1.2 million users migrating from the legacy systems, NTUC Enterprise opted for automatic migration. Impressively, the whole process to "go live" for FairPrice took just two months, and NTUC Enterprise was able to customise the process with Auth0's rules.

"Without Auth0, building our own identity solution would require a team of five to six people, and could cost us over half a million dollars," says Winson, noting many other benefits that alleviate other security monitoring pressures. The SDKs for simple integration into apps and web services are also a huge saving on operational demands.

NTUC Enterprise wanted to take advantage of cloud features to unite their workforce and customers but always had to ensure all changes would abide regulations. PDPA places strong rules around how a Singaporean resident's personal data is used and stored, making it very difficult to operate via public cloud servers outside the country. But this was easily solved with a private cloud.

Since NTUC Enterprise implemented Auth0, the average resolution time for customer support tickets has dropped from four days to one. Today, NTUC Enterprise is focused on delivering more value to its customers by uniting each of them under a single identity.

> “
>
> Without Auth0, buliding our own identity solution would require a team of five to six people, and could cost us over half a million dollars.

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 by subscribing to the magazine and qualify as a contributor to submit your story ideas, essays and opinion articles. You can also get invited to exclusive Identity Security Leaders networking events in your city. Scan the below QR code and be a subscriber today.

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**

Discover how Okta can help your business today

Take your innovation to the next level with leading identity and access management for your customers and employees

AUTHENTICATION
Up and running with 7,000+ pre-built integrations

AUTHORISATION
Rapid application development with API gateways

LIFECYCLE MANAGEMENT
Save time with 120+ pre-built SCIM integrations

USER MANAGEMENT
Pre-build workflows for effortless user management

ADAPTIVE MFA
Delight users with One-Touch Authentication

okta

15min	12+	3x
to embed Auth0 into your apps	SDKs in the languages you work in	lower cost than the legacy customer IAM

Consistently Named a Leader by Top Industry Analysts

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