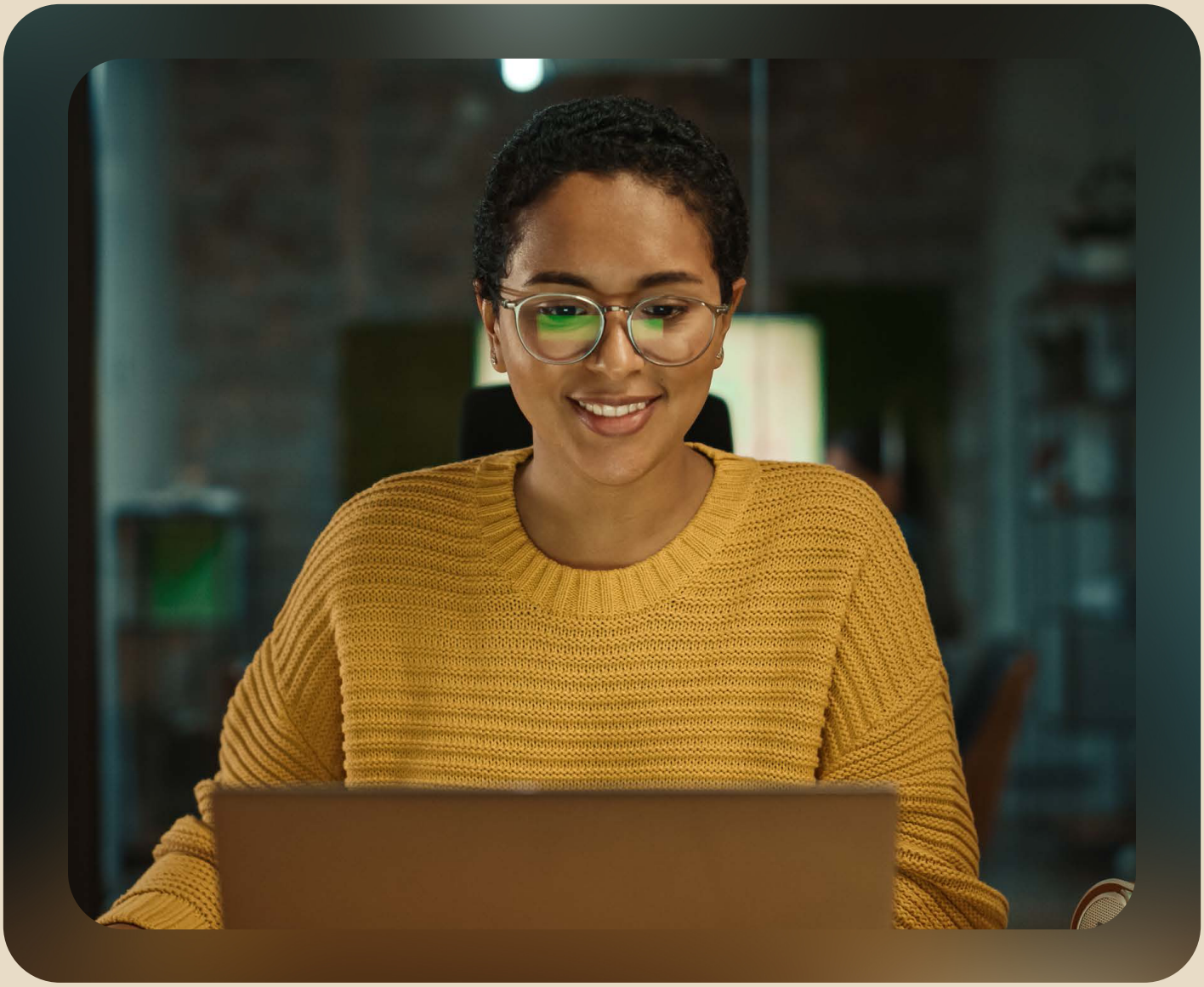
2023

A Public Sector Guide
for External Services

Leveraging Identity



okta

Contents

Introduction

Government and education organisations today are tasked with providing a vast number of services to the Australian people – a core principle of which is to ensure those services reach the right people, and that the data provided by residents or staff is safe from malicious actors. Whether government-to-consumer (G2C), government-to-government (G2G), or government-to-business (G2B) and education business models alike, ensuring all external-facing Identity services are secure and user-friendly can bolster trust, fight fraud, and much more.

From providing services to the Australian public to engaging with business customers and mission partners, public sector organisations support a wide range of external interactions. Too often, individuals and business partners must struggle through multiple Identity systems in order to engage with government. That erodes the end-user experience and impedes an agency's ability to meet its mission. Federal agencies, state and local governments, and higher education alike: All must provide a secure and seamless Identity experience for their external stakeholders.

“Whether we are talking about the government’s customer as the Australian public, another government agency, or a business partner, people want to avoid retelling the same information and want to avoid getting stuck in a digital queue while confirming their Identity,” said Patrick Chu, federal civilian director for Okta, the leading independent Identity partner trusted by government organisations and educational institutions to provide secure connections between people and technology.

While it’s vital that staff be able to access applications and information without hassle, secure access with a seamless experience has never been reserved for just the workforce. The external Identity journey is vital to ensuring smooth interactions for those outside an organisation who need access to services or information. And this is more important now than ever, given that customer service has emerged as a priority at the highest levels.

$25.6b

Growth from 2022–2027
The global Identity and Access Management market is expected to grow from $13.4 billion in 2022 to $25.6 billion by 2027.

With the global Identity and Access Management market expected to grow from $13.4 billion in 2022 to $25.6 billion by 2027[1], there's growing awareness of the key role Identity plays, not only in enabling seamless service delivery, but also in securing IT systems and data. The Digital Economy Strategy (DES)[2], for example, makes it clear that strong digital Identity solutions, including those applied to public-facing systems, are foundational to security.

[1] https://www.marketsandmarkets.com/Market-Reports/identity-access- management-iam-market-1168. html?gclid=EAIaIQobChMIzO3iI7KO_gIVtcmUCR3e7wk5EAAYAyAAEgJ3Z PD_BwE

[2] https://apo.org.au/sites/default/files/resource-files/2021-05/apo-nid312247.pdf

An Urgent Need

There's an urgency to the Identity situation in the public sector. Many agencies and universities still depend on legacy custom-built customer Identity solutions. Often these have been implemented without considering security features such as Multi-Factor Authentication, threat detection, or reporting.

As technology continues to dominate interactions with government, IT teams are finding it increasingly difficult to manage access on an app- by-app and customer-by-customer basis. For example, when a university has different Identity tools for managing student applications, submitting student aid, and applying for student work, things quickly become unwieldy.

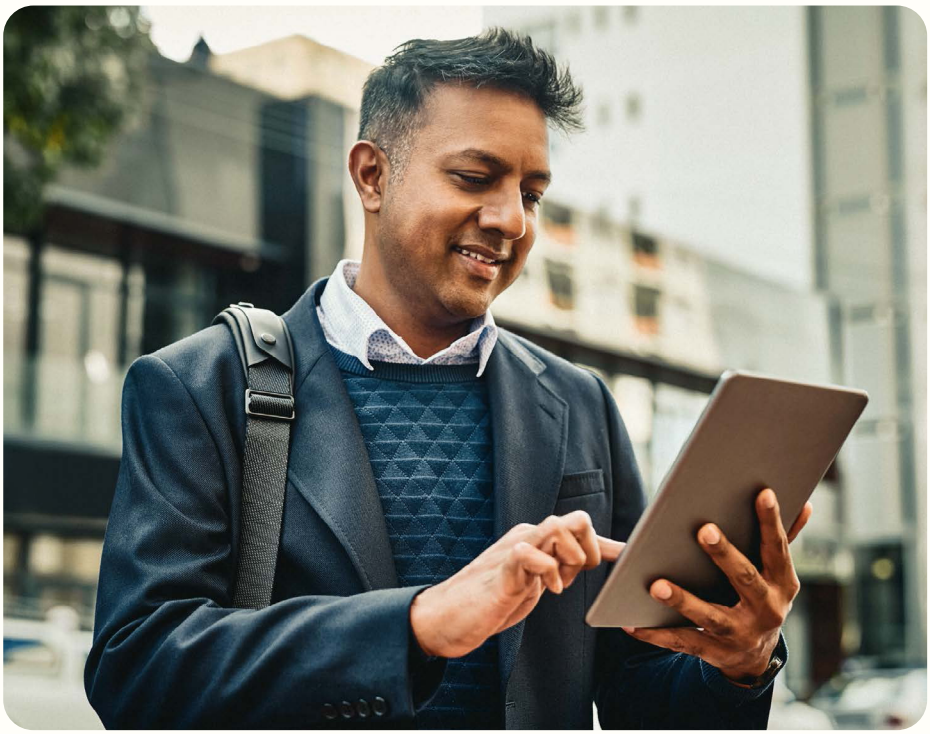
There's also the user experience to consider. As government seeks to serve every member of the Australian public – from business owners to members of the military to those seeking benefits services and beyond – agencies need intuitive logins that are accessible even to less tech-savvy users.

Importantly, the first interaction most public sector organisations have with the Australian public is via log-in services. When those services are complicated and threat-prone, many of these impressions start out on the wrong foot.

At a time when trust in government is already at record-low levels, it erodes public trust even further when government agencies fail to provide simple, effective login and Identity management services. At present, only 45% of Australians say they trust government to do the right thing (-7 points year-on-year) – and failure to act now will only compound the problem going forward.[3]

Technology is becoming ever more pervasive. That means the systems supporting the customer experience must be adaptable enough to accommodate emerging and perhaps unforeseen future interactions.

With cloud-based systems, government can take a new approach to Identity, taking advantage of scalable, future-ready tools, like Single Sign-on – tools that allow agencies for example to personalise external engagements. Such an approach would reduce the administrative burden that threatens to overwhelm IT teams and would deliver the kind of seamless interactions that the Australian public, students, and other key external stakeholders want and expect.



[3] https://www.pewresearch.org/politics/2022/06/06/public-trust-in- government-1958-2022/

Identity at the Federal Level

The Challenge

Legacy Identity approaches make it complicated and time-consuming for the Australian public to engage with government.

Individuals looking to access services may find themselves providing the same information multiple times to multiple government agencies or even within a single agency. They may run into a range of authentication and authorisation experiences, all of which add time and complexity to their interactions.

There are government-to-government Identity issues as well. Agencies are tasked to deliver inter-governmental support, such as the proper distribution of data or access to needed systems.

Businesses turn to government economic and financial data as well for regulatory guidance and procurement opportunities. These interactions with government can become problematic, especially when legacy Identity systems make it difficult to access these resources and information.

All these hurdles generate frustration on the part of stakeholders. Moreover, the inability to gain smooth and easy access interrupts an agency's ability to deliver important services on behalf of the Australian people. "If they can't avoid providing these bad experiences, the government risks falling short on their mission delivery," Chu said.

The Goal

As stated in The Digital Economy Strategy (DES), Australian Government is pushing for the nation to become a world-leading digital economy and society by 2030. The DES works in tandem with the Digital Government Strategy, with a focus on 100% digital delivery of government services to simplify the digital experience for Australians anywhere, anytime, and on any device.

To enable this transition, The Federal Government is continuing to develop a single online credential that enables individuals and businesses to prove who they are via the Australian Government Identity System (myGovID). The Digital Identity System will enable more secure and convenient engagement with government services, and in future, the private sector.

Data privacy is also a key priority pushing forward. To maintain the trust of the Australian people and safeguard their valuable information from cyber threats, the public sector must adhere to evolving security legislation and standards. This includes strict compliance with key regulations such as the Privacy Act, the SOCI Act, and The Australian Signals Directorate's (ASD) Essential Eight Maturity Model that prioritises a set of mitigation strategies such as Multi-Factor Authentication to mitigate known cybersecurity risks.

For agencies that serve other agencies and those that interact with business partners, "the goal is to facilitate information exchange in a secure and seamless manner," Chu said. In doing so, agencies position themselves for future success. "When an agency can provide access to critical resources from anywhere in the world, while also validating who has access to what, they can better operationalize how they run support which could ultimately lead to more staff and funding."

"When an agency can provide access to critical resources from anywhere in the world, while also validating who has access to what, they can better operationalise how they run support which could ultimately lead to more staff and funding."

Patrick Chu
Director, Federal Civilian, Okta

Identity in action: Heal transforms healthcare with Okta

The Challenge

Sometimes, changing an industry in a radical way has to do with going back to a simpler age, when people connected on a more basic, human level, without the layers of bureaucracy and technology that exist today.

For Heal, that was certainly the case. The company was started in 2014 by a doctor-technology entrepreneur couple who decided there had to be a better way for young families to deal with healthcare emergencies.

To enable this patient-focused care, the Heal team developed a mobile platform they dubbed “On Call,” which connects patients and doctors, and helps patients avoid emergency rooms and long wait times. The company also adopted best-of-breed tools for medical providers to view and record patient records, keep track of supplies, and deal with paperwork.

From a data privacy standpoint, however, healthcare is increasingly complicated. “It goes way beyond securing personal identifying information,” says Rish Tandon, the company’s CTO. “We have to ensure that, when it comes to our patients, their records are completely safe. Identity plays a very important role in that.”

The Solution

Initially, when the team built On Call, they used an in-house identity solution. “We very quickly realised that we would not be able to keep up with the needs we had in terms of securing patients’ identities, and also be able to do things like single sign-on with partners,” says Tandon.

After evaluating their options, the team built the app using Stormpath APIs. Then, in 2017, Stormpath and Okta joined forces. “We had a good outcome with Stormpath,” says Tandon, “and in our tests, we saw that we were getting the same outcomes with Okta. It didn’t make any sense for us to go to a different provider.”

The team worked closely with Okta to export data from the Stormpath database into the Okta environment. “We were able to recreate every single role that we had in the Stormpath realm, inside the Okta realm,” he says. “It was one of the most seamless vendor transitions I have ever seen.”

In about two weeks, the team moved all their account data into Okta to manage user registration, sign-on, and forgotten passwords. Okta protects the APIs that connect On Call to Heal partners as well, managing delegated authorisation and access for them.

State and Local Government

In state and local government, effective Identity solutions are key to supporting interactions with residents and delivering vital services. When people go online to look up real estate tax information, renew a driver's license, or pay a government fee, they want that interaction to be seamless and stress-free.

The Challenge

Historically, the process of applying for or renewing benefits or engaging with other functions of state government, such as licensing and permits, "has been time-consuming, confusing, and complicated," said Erika Messerschmidt, senior manager of solutions engineering for Okta.

Government-to-government transactions, as well as engagements with the business community, have likewise been plagued by manual, paper-based processes. And recent circumstances have made a difficult situation worse.

"For example, states continue to struggle with pandemic backlogs due to the intense burdens on Unemployment Insurance (UI) systems," Messerschmidt said. That pressure, in turn, has been exacerbated by an uptick in fraud exploits aimed at state and local governments. "Using the Identity of another person and using fake Identity information are two fraud schemes that contributed to the fraud and breakdown of federal-state relief programs," Messerschmidt adds.

"Using the Identity of another person and using fake Identity information are two fraud schemes that contributed to the fraud and breakdown of federal-state relief programs."

Erika Messerschmidt
Senior Manager of Solutions Engineering, Okta

On the upside, these trends have generated momentum around state and local Identity efforts.

"Recent federal initiatives and legislation have established the risk of getting Identity verification wrong and are responding with strategy and funding to support stronger preventative steps," Messerschmidt said. "There's now a collective effort across government to modernise efforts and improve service delivery to benefit the intended person."

The Goal

When the Australian public interacts with state and local government, they expect a level of ease and intuitiveness that's at least on par with what they encounter in their digital private-sector engagements.

“That is always in the back of the mind for most government officials,” Messerschmidt noted. “State and local governments are working through complex bureaucratic structures that can slow down the development and deployment of digital services,” she said – but that does not excuse them from the responsibility of elevating that end-user experience.

Trust in government is low, and it’s vital that state and local authorities have in place Identity systems that deliver a seamless experience while still ensuring the safety of personal information. Individuals want it, and the businesses that interact with government increasingly are demanding it.

“To deliver the frictionless, seamless, and most importantly secure experience desired, you’ll want a central view of identities to easily manage user access and without the need for multiple usernames or passwords,” Messerschmidt said.

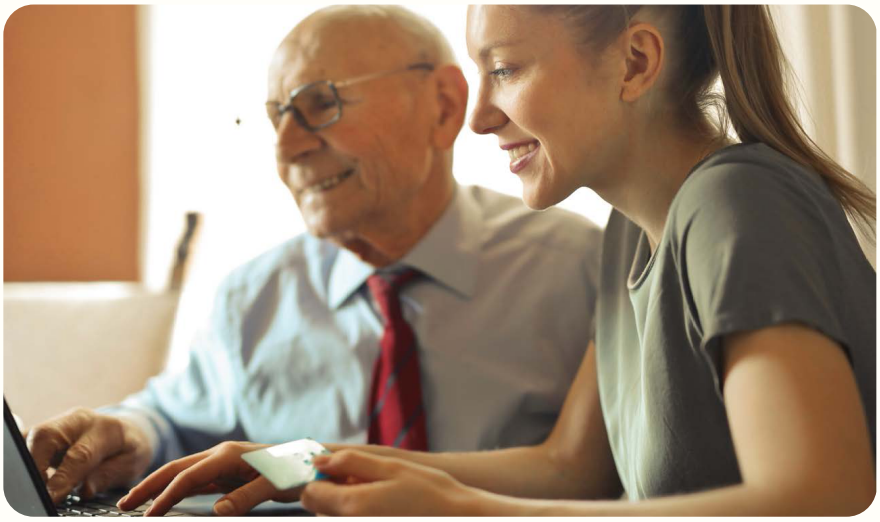
Identity in action: City of Greater Dandenong Council fast tracks results for resident satisfaction

The Challenge

The City of Greater Dandenong Council faced a situation familiar to many government organisations.

Each of its 50 business units operated under IT different systems and processes – creating a complex, siloed infrastructure that prevented IT teams from delivering seamless access to its services while keeping project costs to a minimum.

To enable the frictionless experiences residents demanded, and to enable greater transparency across its network, the council turned to Okta for a solution.



The Solution

The introduction of Okta offered a simplified and cost-effective dashboard option with a 'resident first' design approach. Rate payers could have as many as six usernames and passwords to interact with the Council - Okta's Single Sign On (SSO) dropped that to just one.

Okta's design also leveraged existing systems, rather than reinventing the wheel. This resulted in a one-month implementation, versus a standard comprehensive portal option which takes longer.

The total cost of Okta implementation also amounted to just $150,000 – a considerable reduction on the $2 million it would have cost for the council to build the solution from scratch.

Today, 180,000 residents now have seamless access to Council services for greatly improved experience with local government.

Education

When it comes to Identity and Access Management (IAM), education faces a unique situation.

The Challenge

In the education sector, it's important to provide all users with a secure and seamless digital experience. That gets complicated when users must interface with multiple systems, often encountering varied authentication protocols. They might, for example, have to use different credentials to access learning modules, academic records, tuition and payment information, and other campus resources.

In their interactions with outside scholars and other academic institutions, schools are seeking to facilitate seamless collaboration while also addressing the security concerns that arise with present workaround solutions. And in their engagements with the business community, colleges may be looking to coordinate more efficiently with employers in order to support high job-placement rates. Commercial partnerships and other ties that can help to strengthen the institution's reputation may be held up by outdated security practices.

The intrinsic openness of the campus environment inevitably complicates efforts around Identity. Schools want to promote a free and open exchange of ideas and, in the digital age, that means they must facilitate access to key data and applications.

"Universities and Technical and Further Education (TAFE) institutions accept many visiting students, faculty, and staff for various reasons," Messerschmidt said. "At the very least, these visitors will need Wi-Fi access, and they will likely need readily available access to other systems as well, whether in pursuit of research projects or other academic objectives."

Higher Education

Too often, “these visitors may need a separate username and password to access systems, or they could potentially ‘borrow’ credentials from another student or faculty member,” Messerschmidt said – a common workaround that jeopardises security.

The Goal

In modernising the approach to Identity, many schools will be looking to ease the burden of IT staff, who may be spending untold hours provisioning and managing identities under current legacy solutions. They’re looking to free up time and talent to devote to higher-order technology needs.

All this becomes even more urgent as schools adapt their operations to the needs of the post-pandemic era.

“Administrators, more specifically CISOs and CIOs, strive to create a seamless learning experience, especially in the current hybrid learning environment,” Messerschmidt said. “A student’s location should most definitely be taken into consideration, but they should be able to use their ‘home’ credentials versus creating multiple accounts.”

“Administrators, more specifically CISOs and CIOs, strive to create a seamless learning experience, especially in the current hybrid learning environment.”

Erika Messerschmidt
Senior Manager of Solutions Engineering, Okta

Identity in action: delivering world-class education in South Australia

The Challenge

The Department for Education for South Australia is a state government department delivering school education throughout this geographically diverse state. In total, the department covers over 900 schools, pre-schools, and childcare centres.

Daniel Hughes, the Department's Chief Information Officer, believes that technology has a key role to help "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 needed to be set up for success. As Daniel puts it, "we need to make sure the right digital foundations are in place, without those it's hard then to have conversations with schools and preschools around how they then use technology to achieve better outcomes."

The Solution

When Daniel and the team from Okta partner, Insync Solutions, sat with teachers to understand their technology experience, it became clear that some changes needed to be made. One teacher reported having to try and 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-class education.

Working with Okta partner, Insync Solutions, they deployed Single Sign-On across their entire organisation and school network, transforming the experience for students, teachers, operations and corporate-level staff all at once.

According to Paul Williamson, Director at Insync Solutions, "one of the biggest challenges we faced was the scale. This led us to a hub and spoke model, providing seamless authentication and access to applications to provide that same experience for everybody, it doesn't matter if you're a Metropolitan School or a regional school in a very remote area."

Since implementing Okta, The Department for Education for South Australia has seen a 20% reduction in frontline service desk volume and gained back hours of lost teaching time every week.

Looking Ahead

$3.1b

The Australian Institute of Criminology estimates that identity crime carries an economic impact of more than $3.1b annually.

With rising expectations around customer experience, and a growing cybersecurity threat, Identity is a front-and-centre concern in the public sector. “Nearly every organisation today needs a way to have visibility and control into who has access to what,” according to the Identity Defined Security Alliance.[4]

Going forward, public sector entities will need to find robust solutions to Identity for both workforce as well as public and community users.

There is undoubtedly a strong economic motivation at play. According to The Australian Institute of Criminology, Identity crime carries a staggering financial impact, exceeding $3.1 billion annually. This substantial figure highlights the immense profitability of this industry for cybercriminals, underscoring the need for robust measures to combat such activities.[5]

Government and higher education need to look to the future of Identity in order to support their digital transformation efforts. Legacy solutions haven’t been able to keep pace with the transition to the cloud: They don’t scale well, nor do they integrate with cloud systems to support a seamless user experience.

What does a modernised Identity solution look like? It needs to deliver:

- **A cloud-based approach to external-facing Identity:** The adaptability of a cloud-based solution allows developers to quickly deploy new or updated tools, such as social authentication, so that they reach the public more quickly.
- **A centralised approach to access management:** By bringing all access points and administrative decisions under one roof, a modernised solution eases the burden on administrators, freeing up valuable IT talent for higher-level tasks.
- **Comprehensive access policies based on criteria like user profiles and group memberships**, including requirements to recognise and control segmented access rights for different scenarios. With automation technology, policy engines can deliver stronger Identity hygiene: If a student changes a department, for example, or a staff member audits a course, those permissions are updated accordingly.
- **Ability to apply additional security based on contextual access management:** This allows administrators to manage Identity more finely, looking at what app is being accessed, authentication attempts, location of access, time of access, the strength of the password, anomalies in user behavior, devices being used, IP addresses, impossible travel scenarios, and more.

[4] https://www.idsalliance.org/ modernizing-identity-governance/

[5] https://www.smh.com.au/technology/how-global-organisations-are-combatting-identity-fraud-20230505-p5d5zu.html

A leader in customer Identity, Okta helps government and education organisations of all levels, delivering robust solutions in support of public sector organisations. Its solution include:

- **Universal Directory:** Enables organisations to manage data from multiple sources, granting access that's filtered and published to those with the proper security permission to access it.
- **Okta Verify:** A Multi-Factor Authentication app that makes it less likely that someone pretending to be the user can gain access to the account.
- **Adaptive MFA:** Protects Identity and access to data wherever your users go and wherever your data lives.
- **API Access Management:** Allows you to secure your APIs with Custom Authorisation Servers, custom scopes, claims, policies, and rules to determine who can access API resources, regardless of the API gateway.

Learn more about how Okta can help ensure Identity and access management is seamless and secure for your external services!

Continue here

About Okta

Okta is the leading independent Identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 16,400 organizations, including JetBlue, Nordstrom, Siemens, Slack, Takeda, and Teach for America, trust Okta to help protect the identities of their workforces and customers. To learn more visit okta.com/au/

okta

Australia Headquarters
80 Pacific Hwy
North Sydney NSW 2060
(02) 8318 7677