Zero Trust in the public sector: From concept to capability

OPTUS | THE MANDARIN

Introduction

Public sector cyber breaches used to begin with a complex technical exploit, but today they are just as likely to start with a valid login. This change in attack behaviour demands a new model of security – one that turns traditional notions of trust on their head.

Public sector agencies are particularly attractive targets for cyber criminals. They hold large volumes of highly sensitive personal, financial, and national data, and they operate critical services that citizens and economies depend on. Disruption can have immediate, visible impact, making these organisations high yield targets.

This challenge is compounded by the fact that many agencies operate a mix of modern and legacy systems that form complex operating environments, and are constrained by long technology lifecycles, all of which can increase exposure if not carefully managed.

The technology landscape for public sector agencies has been fundamentally reshaped, transforming not only how services are delivered, but also how they are exploited by attackers.

In a world where cloud services, hybrid workforces, and increasingly complex digital ecosystems are the norm, the attack surface has evolved and grown accordingly.

Attackers today are no longer breaking into networks. They are signing in using valid credentials, then moving across systems to operate undetected inside environments that were designed to trust them.

Traditional security models that prioritise protecting a network perimeter are no longer sufficient, but the requirement to protect sensitive data and systems remains urgent. A new approach is needed – one that sets aside old notions of implicit trust and focuses on identities and permissions rather than devices and locations.

The approach has come to be known as Zero Trust.

Unlike other cyber security models, Zero Trust is not built around a single product or technology. Instead, it is a strategic approach that assumes no user, device, or system should be implicitly trusted, regardless of whether they are inside or outside the network.

Importantly, trust is not just verified at the beginning of a session. It must be continuously earned, with every access request evaluated in real time based on factors such as identity, device posture, behaviour, and context.

Furthermore, access is limited to only what is required, for only as long as it is needed.

In this world of Zero Trust, identity becomes the primary control plane, access is continuously verified, and visibility and monitoring are foundational.

The result? Suspicious activity is detected earlier, contained faster, and prevented from escalating, so public sector organisations can focus on delivering exceptional services with heightened confidence that data and systems are protected to the highest possible standard.

Zero Trust is much more than just a security uplift or a technical intervention. It is an organisation wide transformation that reshapes how services are delivered, how risk is managed, and how trust is established. It directly impacts operating models, application architecture, workforce access, and compliance obligations.

As such, it requires executive ownership, rather than just technical implementation.

Governments around the world are currently moving to adopt Zero Trust. In Australia, the Attorney-General's Department's Protective Security Policy Framework (PSPF) and the Australian Signals Directorate's (ASD) Modern Defensible Architecture (MDA) and Essential Eight cybersecurity maturity model collectively establish the expectation that agencies must evolve toward Zero Trust-aligned architectures.

Similar directives have been issued in countries including the USA, United Kingdom, Singapore, Canada, and across the European Union.

Zero Trust has become the global model for cyber security. The challenge now for public sector organisations is how to adopt it in a way that maintains service continuity, delivers measurable operational value, and minimises implementation risk.

This eBook outlines what Zero Trust means for the public sector in Australia, why it has become a strategic priority, and how leaders can undertake the transition in a structured and achievable way.

Why Zero Trust

Interest in Zero Trust flows from its success at blocking how modern attacks succeed.

Whereas attackers traditionally gained entry via compromised systems, now they do so using stolen credentials or hijacked accounts and then move across systems to find high value targets.

While traditional defensive models were designed to stop the initial intrusion into a network or system, Zero Trust manages trust continuously, limits exposure, and contains damage. It strengthens identity management and enforces least privilege access to reduce the number of systems a successful attacker can reach. User behaviour is also monitored continuously, meaning suspicious actions can be quickly detected and queried.

This effectively counters modern attack methods.

A well-executed Zero Trust strategy delivers:

- Secure and scalable hybrid workforce access.
- Improved visibility across users, devices, and applications.
- Faster detection and response.
- Reduced breach impact through restriction of lateral movement.
- Stronger data protection and compliance alignment.
- Greater operational agility supporting broader digital transformation initiatives.

Core Zero Trust Principles:

Never trust, always verify: No user, device, application, or workload is granted implicit trust. Every interaction must be continuously authenticated, authorised, and validated, based on identity, context, and risk.

Least privilege access: Provide only the minimum level of access that users, devices, and workloads (including automated systems and AI agents) require to perform a specific task, for the shortest time necessary.

Assume breach: Design and operate systems from the assumption that attackers are already present within the environment, and limit their ability to access other systems, escalate privileges, or cause other harm.

Continuous monitoring and validation: Continuously observe, assess, and evaluate users, devices, applications, and activity, to ensure access remains appropriate and secure throughout its duration.

"Zero Trust can lead to a massive improvement in visibility. It takes telemetry from different systems across the network – the devices and the applications themselves – in near real-time and uses that data to make decisions on who should be allowed to connect, and who should not."

Sean Connelly
Architect of U.S. Federal Zero Trust, co-author NIST SP 800-207 & CISA Zero Trust Maturity Model, and Senior Director, Governance, Risk & Compliance at Zscaler

More than a cybersecurity consideration

Effective implementation of Zero Trust requires organisation wide architectural change that impacts business operations, risk appetite, and digital transformation. It is an enterprise transformation that directly impacts business continuity, service delivery, and digital transformation outcomes, and requires executive and board-level ownership.

It reshapes:

- Operating models
- Application architectures
- Workforce access patterns
- Risk appetite and governance

Zero Trust is not a product that can be purchased from a single provider, nor is it a network control or feature. It is a comprehensive architectural approach that covers identity, devices, workloads, networks, data, and monitoring.

"We see Zero Trust fail most often when it's treated as a product decision. For government, it needs to be approached as an architectural, organisation wide transformation that reshapes how identity, access, and trust are designed across the entire environment."

Kavin Arnasalon
Head of Government, Enterprise and Business, Optus

This misunderstanding can generate inconsistent expectations between executives, IT teams, risk managers, and business units. Without a shared understanding, it becomes difficult for organisations to define clear business outcomes, communicate requirements to service providers, or pinpoint gaps in technology and capability.

> **"Zero Trust is not so much about buying more tools. It is about how you can interoperate and get visibility in new ways to gain a better, faster understanding of what is going on across the network."**

Sean Connelly
Architect of U.S. Federal Zero Trust, co-author NIST SP 800-207 & CISA Zero Trust Maturity Model, and Senior Director, Governance, Risk & Compliance at Zscaler

---

Governments around the world are embracing Zero Trust as an effective means of improving cyber defences:

- The United States' Executive Order 14028 directs agencies to modernise their cybersecurity, including progressing toward Zero Trust architecture through reshaping their network environments accordingly.
- The European Union's NIS2 Directive requires member states to implement security and risk management measures that align with Zero Trust principles, including strong access controls, continuous monitoring, and incident detection.
- In the United Kingdom, the National Cyber Security Centre has published guidance designed to assist organisations in adopting Zero Trust principles.
- Canada has adopted Zero Trust architecture as a core principle of its Cyber Security Services Roadmap, outlining a shift toward continuous verification.
- The Singapore Government's Zero Trust Architecture (GovZTA) applies across all government agencies, enforcing principles such as 'never trust, always verify' and continuous access verification.

The Australian Public Sector Zero Trust mandate

The Australian Government is progressively moving toward the adoption of Zero Trust principles as a foundation for modern cybersecurity. This can be characterised as a four-layer approach to implementation: policy, architecture, control, and baseline.

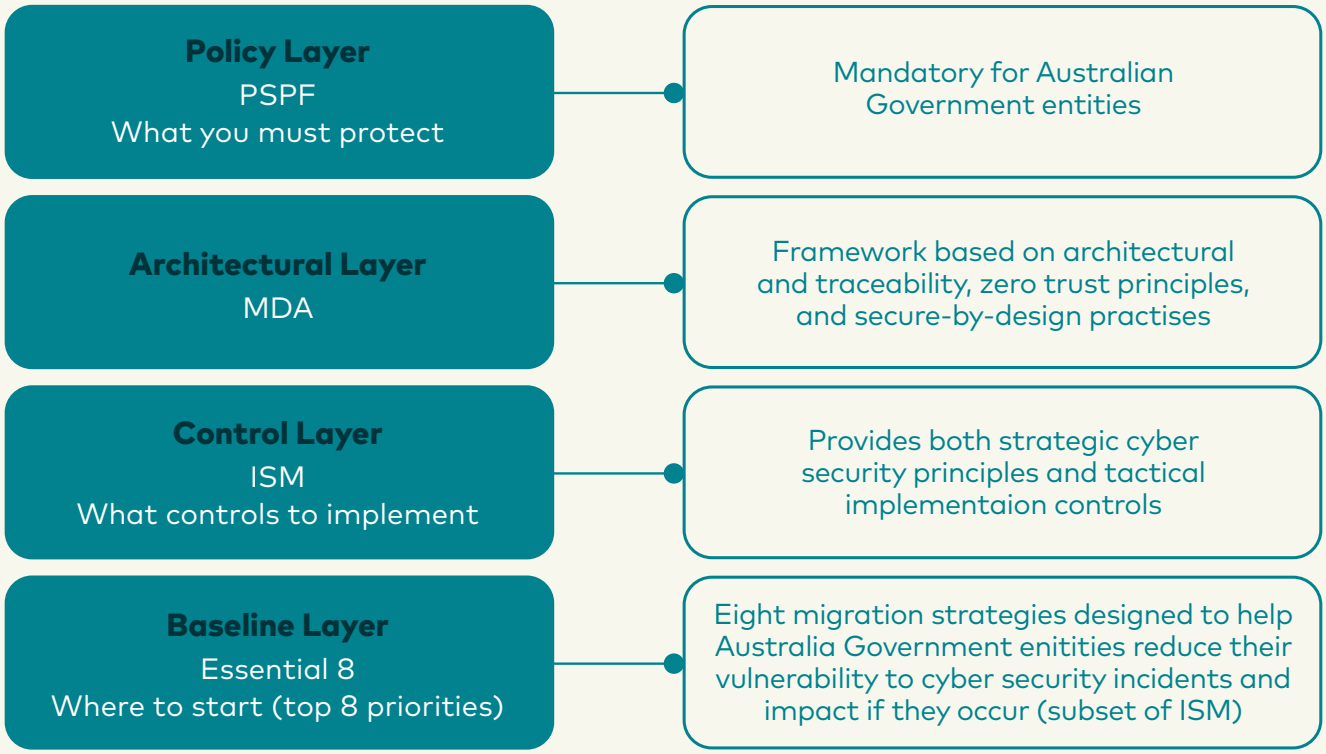
The 2025 Protective Security Policy Framework (PSPF), issued by the Attorney-General's Department, sets mandatory requirements for non-corporate Commonwealth entities, reinforcing security practices that align closely with Zero Trust principles. This is the **Zero Trust Policy Layer**.

The Australian Signals Directorate's (ASD) *Foundations for a Modern Defensible Architecture* (MDA) provides guidance to help organisations plan and prepare for the adoption of technologies aligned with Zero Trust principles, and how to translate policy requirements into modern operating environments. This is the **Zero Trust Architectural Layer**.

The ASD's Information Security Manual provides strategic cyber security principles and detailed implementation controls and serves as the control framework that operationalises and validates the architecture. This is the **Zero Trust Control Layer**.

The ASD Essential 8 maturity model provides mitigation strategies designed to help Australian government entities reduce their vulnerability to cyber security incidents and the impact of incidents when they occur. This is the **Zero Trust Baseline Layer**.

These four layers form a policy-to-architecture continuum, from obligation to execution.



The directive to embrace Zero Trust in the Australian public sector is increasingly visible at the state government level.

The 2026-2028 NSW Government Cyber Security Strategy describes Zero Trust principles as a critical requirement for achieving success when improving cyber resilience, with significant focus given to the need to strengthen identity capabilities.

The Queensland Cyber Security Strategy 2025–2027 brings a similar focus to the requirement to build cyber resilience, taking a policy and governance-led approach to uplifting assurance with a commitment to adopting Zero Trust 'to strengthen preparedness, defences and cyber teams' capability'.

Also, the South Australian Cyber Security Strategy 2025-2031 highlights the need for Zero Trust principles such as secure-by-design, in alignment with its mission to make South Australia a cyber-resilient state.

In Victoria, the Victorian Auditor-General's Office has explicitly referenced Zero Trust as a modern security model, particularly in the context of securing server infrastructure, within a broader government posture that continues to emphasise baseline controls such as the Australian Cyber Security Centre Essential Eight.

CASE STUDY

Implementing Zero Trust in the US public sector

The scale of change required by Zero Trust means adoption must be deliberate and carefully planned, supported by a clear articulation of both its benefits and its rationale.

Sean Connelly gained firsthand experience of the need for clarity and alignment when he was tasked with introducing Zero Trust into US Federal Government agencies.

As the Zero Trust Initiative Director at the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), Connelly co-authored its defining standards (NIST SP 800-207 on Zero Trust Architecture), as well as the CISA Zero Trust Maturity Model, and spent 11 years at CISA translating federal cybersecurity policy into operational practice.

During his time at CISA, Connelly and his colleagues defined four key states for describing an agency's Zero Trust maturity:

1 Traditional	Security is perimeter-based, with implicit trust granted once inside the network. Controls are fragmented across domains, visibility is limited, and responses are largely manual, making it difficult to detect threats that exploit trusted access.
2 Initial	Organisations introduce core Zero Trust capabilities such as MFA, basic device checks, and early segmentation. Telemetry is collected but not fully integrated, and policies remain relatively static, resulting in uneven implementation.
3 Advanced	Zero Trust principles are embedded across the environment, with context-aware access decisions based on identity, device, and risk. Integrated telemetry improves visibility while automation strengthens detection and response.
4 Optimal	Security becomes fully dynamic and continuously verified across all users, devices, and data. Security is embedded as an enabling capability across the organisation with unified controls, real-time analytics, and high levels of automation.

CASE STUDY

Connelly said the pathway to effective Zero Trust adoption always began with extensive consultation with stakeholders within individual agencies. This first step from Traditional to Initial was often the hardest.

"We had a memo and an executive order signed by the President, and still we had to go agency-by-agency and talk to them about what it meant to adopt a more modern identity platform," Connelly said. "The challenging discussions involved how the organisation needed to change.

"It can be easier to just focus on the new technology, but success comes down to clarifying how the organisation itself needs to shift to align with the new technology."

This need for effective communication continued long after the agency had taken its first steps.

"The agencies that were more successful were the ones that had weekly meetings with different stakeholders and system owners," Connelly said. "They explained what Zero Trust was going to mean on a tactical level – what the shift was going to be, and how it was going to impact them. Ultimately, they needed to see how security was going to enable their mission in ways that were not possible before.

"None of that was about the technology – it was the people-side that mattered."

Connelly said the transition to Zero Trust could be made more challenging by the requirement to demonstrate the returns gained from the effort expended. He said it was important to set aside traditional key performance indicators, such as reductions in cost, in favour of understanding how the change benefitted the process owners.

This required clear articulation of how embedding security across every aspect of the agency's operations would strengthen delivery

CASE STUDY

and build confidence in transformation initiatives such as cloud migrations and the adoption of AI-supported systems.

"Most traditional environments rely on static policy, fragmented controls, or legacy procedures," Connelly said. "The challenge when adopting AI is whether these architectures can support continuous, near real-time decision making."

In addition, the introduction of Zero Trust also provided the foundations by which an agency could make greater use of AI within its own security programs.

"We know attackers are using AI to move faster and adapt in near real-time," Connelly said. "On the defensive side, AI brings the capability to compress the time between signals and decisions."

Connelly said that as agencies progressed through the four stages of maturity, perceptions of security shifted from a technical constraint to a business enabler, and from an exercise in risk avoidance to becoming a means of building confidence and resilience.

"Trust will no longer look as binary – 'on' and 'off'," Connelly said. "Confidence is a spectrum, based on an awareness of what needs to happen and what shouldn't happen."

The path to Zero Trust in Australia

While there is generally strong awareness of Zero Trust across the Australian public sector, translating that understanding into integrated architectures and sequenced transformation programs with measurable outcomes remains a challenge. This can lead to fragmented implementations that fail to deliver Zero Trust's full security and operational benefits.

Other challenges include:

- Lack of visibility across assets and environments.
- Constraints imposed by legacy architectures.
- Resistance arising from fear of operational disruption.

> **"As the organisation moves to this more modern platform, seams or gaps between the old and new platforms can be exposed. Those gaps are what adversaries look for - especially in the old systems which may not be receiving as much attention as before."**

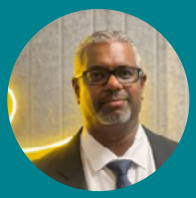
Sean Connelly
Architect of U.S. Federal Zero Trust, co-author NIST SP 800-207 & CISA Zero Trust Maturity Model, and Senior Director, Governance, Risk & Compliance at Zscaler

"The visibility challenge: One of the key technical barriers to implementing Zero Trust is achieving sufficient visibility across an organisation's environment. Many organisations may struggle to confidently identify all applications, data flows, machine identities, and interservice transactions operating within their networks. Factors such as legacy systems, shadow IT, mergers and acquisitions, and decentralised development can further exacerbate these gaps.

Effective Zero Trust policies require a clear understanding of the relationships between identities, assets, and transactions. Without comprehensive visibility, organisations cannot confidently enforce access controls or assess risk, limiting Zero Trust readiness. In addition, segmentation requires knowledge of which systems communicate and why, while behavioural analytics rely on accurate baselines of normal activity.

The ASD's Foundations for a Modern Defensible Architecture (MDA) highlights this requirement through its emphasis on maintaining a reliable application and asset inventory (Foundation 4), which underpins the design of effective policies and the enforcement of least-privilege access.

Centralised telemetry and continuous monitoring can provide clearer insight into users, systems, and risks, enabling faster, more informed operational and security decisions."



Kavin Arnasalon
Head of Government, Enterprise and Business, Optus

Zero Trust succeeds when delivered as a long term architectural program, implemented as a staged, risk managed transformation rather than a series of discrete technology deployments or compliance responses.

Successful implementations are defined by three factors: sequencing, integration, and alignment with the business:

- **Sequencing:** Capabilities are implemented in a deliberate order, prioritising high-risk and high-value areas first. Foundational elements such as identity, visibility, and access control are established early, ensuring that subsequent investments build on a stable and effective security base.
- **Integration:** Security capabilities are designed to work together. Identity, endpoint, network, and monitoring controls are integrated to provide unified visibility and enable consistent, context-aware access decisions to be made across the environment.
- **Business alignment:** Zero Trust initiatives are closely aligned to organisational priorities, service delivery needs, and risk appetite. This ensures that security measures support operational outcomes and that investments are clearly linked to measurable business value.

While Zero Trust encompasses a wide range of capabilities, its core principles provide a clear path for staged implementation. Rather than attempting wholesale change, organisations should build capability progressively, focusing on measurable outcomes at each step:

- Anchor on identity as the control plane.
- Establish visibility across users, devices, and applications.
- Prioritise high-risk and high-value use cases.
- Deliver in phased increments aligned to business outcomes.

For Australian public sector agencies, the ASD's Foundations for a Modern Defensible Architecture (MDA) provides a practical framework to guide this journey. It establishes a Zero Trust-aligned foundation that supports outcome-driven transformation over tool-led implementation. Agencies should align to the MDA as their architectural reference point, adopt secure-by-design principles, and implement change through staged, risk managed programs that remain tightly linked to business objectives:

- Identity and Access Management (IAM) and Multi Factor Authentication (MFA).
- Endpoint security and posture assessment.
- Network and application segmentation.
- Secure connectivity (e.g., ZTNA/SASE).
- Continuous monitoring, analytics, and validation.

Building the business case

The business case for Zero Trust cannot be framed as a security uplift alone. It must be defined in terms of risk reduction, operational value, and its role in enabling organisational resilience. For Australian public sector agencies, this means recognising security not as a cost centre, but as a core capability that underpins service delivery, regulatory compliance, and public trust.

Specifically, this means:

Lower probability and impact of breaches:
By enforcing least-privilege access and continuous verification, Zero Trust reduces the likelihood of unauthorised access and limits lateral movement, containing incidents before they escalate into large-scale breaches.

Reduced complexity and legacy cost overheads:
Modernising identity, access, and network architectures helps simplify fragmented environments, reduces reliance on legacy infrastructure, and lowers the long term cost of maintaining overlapping or outdated controls.

Improved compliance alignment:
Zero Trust supports alignment with Australian frameworks such as the PSPF and the ASD ISM and Essential Eight, making it easier to demonstrate compliance and meet audit and assurance requirements.

Increased workforce productivity and flexibility:
Secure, identity-based access enables staff to work effectively across locations and devices without compromising security, supporting hybrid work models and improving user experience.

Ultimately Zero Trust creates a secure baseline for adopting cloud services, data sharing initiatives, and emerging technologies such as AI, ensuring innovation does not outpace security.

"The true return isn't about how much this new system is saving in terms of compute or load or how many people are using it. The true impact is in terms of outcomes getting processed faster. But that is not always something that can easily be measured. You need a different way to look at some of these system changes beyond operating expenses and resource allocation, to look at the mission itself, and how it is being met in a new, better way than it was before."

Sean Connelly
Architect of U.S. Federal Zero Trust, co-author NIST SP 800-207 & CISA Zero Trust Maturity Model, and Senior Director, Governance, Risk & Compliance at Zscaler

Partnering for Zero Trust success

Few public sector agencies possess the skills and experience to bring Zero Trust to life. For this reason, it is critical that they select a partner with both the skills and experience needed.

This partner should bring:

- Deep architectural expertise aligned to ASD's Foundations for a Modern Defensible Architecture (MDA).
- Proven ability to integrate across complex environments.
- Local delivery capability and sovereign alignment.
- End-to-end capability to design, implement, and operate.

Optus and Zscaler are partnering to help Australian public sector agencies deliver Zero Trust as a structured, outcome-driven transformation. Zscaler provides a cloud-native, identity-led Zero Trust platform, while Optus delivers the underlying network and security layer, providing enhanced visibility and faster time to resolution. This is supported by Optus' architectural leadership, integration capability, and local operational experience, enabling Zero Trust to be delivered at scale across Australian government environments. This reduces architectural complexity, supports phased and risk managed implementation, and aligns closely with Australian Government security frameworks.

"Zero Trust delivers the most value for government when it is approached as an architectural program rather than a technology deployment. Our role at Optus is to help agencies translate policy intent into secure, practical designs."

Kavin Arnasalon
Head of Government, Enterprise and Business, Optus

This partnership enables agencies to strengthen resilience, maintain service continuity, and build trust while accelerating digital transformation.

Conclusion

As threats increasingly exploit identities rather than network boundaries, continuous verification and least-privilege access are essential. This means Zero Trust is now a foundational requirement for cyber security across the Australian public sector, reflected in frameworks such as the Protective Security Policy Framework and the ASD's Modern Defensible Architecture and the Essential Eight.

When implemented effectively, Zero Trust strengthens security while enabling resilience, compliance, and modern service delivery.

Successfully adopting Zero Trust requires a staged, organisation wide approach supported by strong leadership and clear alignment to policy and architecture, and the backing of experienced partners.

Ultimately, Zero Trust is not just a technical uplift, but a strategic capability that allows Australian government agencies to operate securely and confidently in an increasingly complex digital environment.

OPTUS | THE MANDARIN