White paper

Cybersecurity strategies need to evolve

A guide for federal agencies navigating zero trust.

verizon business

Table of contents

Introduction: a challenging security landscape

Hybrid work has redefined cybersecurity's greatest challenge: protecting data and users when the network perimeter is practically everywhere, from homes to coffee shops to traditional offices. For Australian federal government agencies, this uncertainty can create security gaps that can lead to organisational paralysis. Legacy defences, once a part of centralised locations, no longer do the job.

Federal agencies require collaboration with organisations that deliver risk confidence and security strategies that can dynamically follow their users, data and applications that used to be stored in one place. Moving to the cloud has helped provide some options for agencies to move away from old-school physical security infrastructure and take advantage of cloud-native security features that extend the security perimeter beyond the office to the edge of remote work.

With security solutions built on network intelligence, federal agencies can adopt a dynamic posture that can help combat cyber threats and enhance their systems.

Implementing a zero trust architecture (ZTA) allows for robust protections for the users, data, devices, networks and applications regardless of their location. This is especially important for federal agencies as they face an asymmetric assault from legions of bad actors. Eighty-eight percent of Australian IT leaders managing the transition to cloud environments are either already using, currently deploying, or intend to deploy a zero trust security framework.[1]

The remainder of this white paper:

- Defines the core principles of zero trust using industry frameworks
- Provides examples of strategies and methodologies agencies can use to prioritize their ZTA solutions; and
- Describes typical findings and recommendations for Australian government agencies to consider when implementing ZTA solutions

What is zero trust?

Zero trust (ZTA) is a security paradigm designed to protect organisations by establishing, enforcing and continuously analysing least privilege per-request access decisions in information systems. Organisations that implement ZTA require that all users and devices continually prove they are trustworthy. Zero trust embodies the principles of "never trust, always verify," "assume breach" and "verify explicitly."[2] These principles fundamentally transform how agencies secure their systems by requiring continuous authentication and authorisation.

ZTA is the strategy to execute on the zero trust vision. Zero trust architecture is an agency's cybersecurity plan that utilises zero trust concepts to encompass the workflow planning, component relationships and access policies based on a framework of tenets, pillars and capabilities. Tenets describe the principles of zero trust. Pillars logically organise these tenets into functional areas, and the capabilities map solutions to these areas within each pillar.

Tenets: The Australian Cyber Security Centre (ACSC) describes zero trust tenets as a technology agnostic, ideal goal for zero trust adoption. An example of a tenet is "The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture."[3]

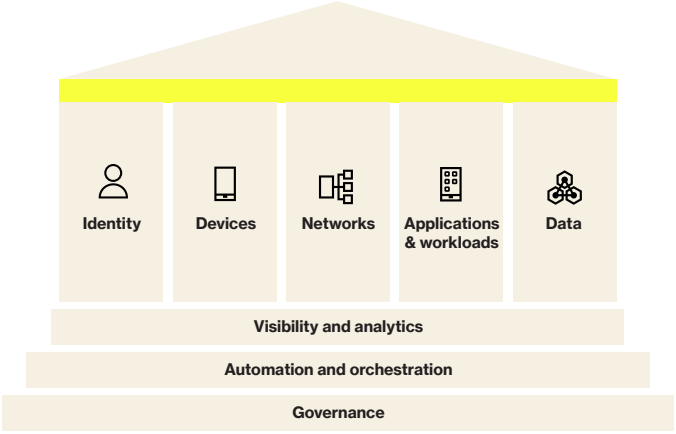
Pillars: logically organises the zero trust tenets into functional areas. For example, the ACSC Zero Trust model includes five zero trust pillars described in Figure 1.

Capabilities: provides a more granular view of the functional capabilities within a pillar, and how that functional capability is used to provide coverage across the pillars. For example, Executing phases to zero trust architecture (pages 7-9) maps zero trust capabilities to the ACSC's zero trust pillars.

Figure 1: ACSC pillars of zero trust[2]

Pillar	Description
Identity	Focuses on the unique attributes that identify users or non-person entities within an organisation. Identity management involves verifying user or entity attempts to access systems using authentication mechanisms and contextual data.
Devices	Involves validating and managing any asset that connects to the network, such as laptops, servers, mobile phones, printers, IoT devices and networking equipment, to ensure it meets acceptable cybersecurity standards.
Networks	Protects communication channels by managing network access dynamically, isolating traffic and encrypting data flows. This includes internal networks, wireless, cellular and other communication pathways.
Applications and workloads	Refers to organisational systems, software, and services running on-premises, in cloud environments or on mobile devices. Organisations must identify these assets and apply appropriate zero trust policies or restrict use of unauthorised applications.
Data	Encompasses structured and unstructured data stored or previously stored across systems, applications, backups and devices. Zero trust practices enforce data categorisation, classification and access control to limit exposure to only those with a legitimate need.

Figure 2: Foundation of zero trust[3]



47%

of Australia Pacific and Japan organisations have a defined zero trust initiative, with 35% planning to implement one over the next 6-12 months.[4]

How to begin your zero trust journey?

The Australian Cyber Security Strategy 2023-2030, administered by the Department of Home Affairs, provides federal agencies with a strategic framework and objectives to enhance national cybersecurity resilience, including the adoption of ZTA.

Five Guiding Principles have been developed to shape policy initiatives and drive the adoption of a zero trust culture across federal agencies.[5]

The Guiding Principles are:

- Identify and manage cybersecurity risk at an enterprise level
- Understand accountabilities and responsibilities at all levels
- Know and understand your most critical and sensitive technology assets
- Maintain resiliency through a comprehensive cyber strategy and uplift plans
- Go beyond incident planning

While the Australian Cyber Security Strategy sets clear goals, it allows agencies flexibility to tailor implementation to their specific mission requirements. This adaptability enables agencies to align ZTA adoption with the Australian Cyber Security Centre's (ACSC) Essential Eight framework, which provides prioritised mitigation strategies to address cyber threats effectively.[5,6]

Furthermore, the ACSC Foundations for Modern Defensible Architecture provide a clear baseline of secure design and architectural practices to help agencies prepare for current and emerging cyber threats.[2] Developed to support the adoption of zero trust principles, "never trust, always verify," "assume breach," and "verify explicitly," these Foundations are essential capabilities for advancing zero trust maturity. Implementing them strengthens a defence-in-depth approach, prioritising the protection of critical systems and data to prevent or minimise the impact of cyber incidents on operations.

The ten ACSC Foundations are:

- **Centrally managed enterprise identities:** unifying identity management across users, devices and services
- **High assurance authentication:** ensuring secure, phishing-resistant authentication for all identities
- **Contextual authorisation:** continuously evaluating access based on session context and trust signals
- **Reliable asset inventory:** maintaining visibility and control over all organisational assets
- **Secure endpoints:** hardening, monitoring and managing endpoint security baselines
- **Reduced attack surface:** minimising unnecessary exposure to untrusted networks and services

- **Resilient networks:** designing secure, segmented networks with built-in fault tolerance
- **Secure-by-design software:** adopting secure development and procurement practices
- **Comprehensive assurance & governance:** embedding continuous security assurance into governance
- **Continuous & actionable monitoring:** detecting and responding to threats in real time using high-integrity telemetry

Understanding broader federal government frameworks forms the discovery phase of the zero trust journey. The first zero trust adoption phase is to baseline an agency's current capabilities against an industry-standard framework (i.e., Current Mode Operation). The second phase is defining a desired state of readiness based on near-term incremental improvements (i.e., Interim Mode of Operation). The third phase is to design a long-term roadmap that describes how you will meet the capabilities within the zero trust framework (i.e., Future Mode of Operation).

A summary of the three adoption phases, activities and timelines is shown below. The figures on pages 7–9 illustrate the three phases broken down by the percentage of zero trust capabilities typically covered in each phase.

Phase 1: Current Mode of Operation (CMO).

Complete mapping of the agency's currently implemented solutions to a zero trust capability model to determine what capabilities are currently covered and where there are coverage gaps. The CMO capability mapping exercise typically provides an executive-level overview using colour-coded visualisations that are used to describe the zero trust capabilities that are currently "met," "partially met," and "not met." Typically, the CMO mapping is wrapped up by the two-calendar-month mark.

Phase 2: Interim Mode of Operation (IMO).

Identify at least one IT modernisation initiative that can be completed within the next 12 months and map the new capabilities to be implemented in the zero trust capability model completed during the CMO phase (i.e., show the improvement). For example, agencies migrating from the Trusted Internet Connection 2.0 (TIC 2.0) framework to TIC 3.0 map the new capabilities met by implementing Secure Access Service Edge (SASE) solutions to an updated version of the zero trust capability model.

Phase 3: Future Mode of Operation (FMO).

Define a long-term roadmap that defines the agency's ZTA strategy within a three to five-year timeline. The target completion percentage for ZTA capability coverage should be one hundred percent (100%). This phase typically takes three to six months to complete and is subject to iterative changes with the agency's mission needs and budgetary cycles.

Executing phases to zero trust architecture

Phase 1: 1–2 months to complete

Current Mode of Operation (CMO)

Core Pillars

Met Partially met Not met

User	Device	Network	Infrastructure	Application	Data	Visibility and analytics	Orchestration and automation
Access management	Vulnerability management	Zero trust architecture	Cloud workload protection	Web application firewall	Encryption	Device visibility	Policy engine
Authentication	Device security	Software-defined networking	Cloud access security broker	Application security	Data security	Threat intelligence	Policy administrator
User & entity behavior analytics	Device identity	Segmentation	SaaS management platform	Container security	Data spillage	Security information event management	Policy enforcement point
Identity management	Device compliance	Network security	Secure access service edge	Secure access cloud	Information rights management	CDM system	Security policy management
Conditional access	Device authentication	Zero Trust network access		Isolation	Data loss prevention		
Dynamic risk scoring	Device management	Network access control		Any device access	Industry compliance		
	Device inventory	Transport encryption			Integrity		
	Enterprise mobility management	Session protection			Classification		

61%

of global organisations now already have a defined zero trust security initiative in place; another 28% plan to implement one within the next 6–12 months.[5]

Phase 2: 12 months of incremental improvements

Interim Mode of Operation (IMO)

Core Pillars

Met | Partially met | Not met

User	Device	Network	Infrastructure	Application	Data	Visibility and analytics	Orchestration and automation
Access management	Vulnerability management	Zero trust architecture	Cloud workload protection	Web application firewall	Encryption	Device visibility	Policy engine
Authentication	Device security	Software-defined networking	Cloud access security broker	Application security	Data security	Threat intelligence	Policy administrator
User & entity behavior analytics	Device identity	Segmentation	SaaS management platform	Container security	Data spillage	Security information event management	Policy enforcement point
Identity management	Device compliance	Network security	Secure access service edge	Secure access cloud	Information rights management	CDM system	Security policy management
Conditional access	Device authentication	Zero trust network access		Isolation	Data loss prevention		
Dynamic risk scoring	Device management	Network access control		Any device access	Industry compliance		
	Device inventory	Transport encryption			Integrity		
	Enterprise mobility management	Session protection			Classification		

60%

of organisations adopting a zero trust approach see a reduction in data breaches.[6]

Phase 3: 3–5 year roadmap

Future Mode of Operation (FMO)

Core Pillars

Met | Partially met | Not met

User	Device	Network	Infrastructure	Application	Data	Visibility and analytics	Orchestration and automation
Access management	Vulnerability management	Zero trust architecture	Cloud workload protection	Web application firewall	Encryption	Device visibility	Policy engine
Authentication	Device security	Software-defined networking	Cloud access security broker	Application security	Data security	Threat intelligence	Policy administrator
User & entity behavior analytics	Device identity	Segmentation	SaaS management platform	Container security	Data spillage	Security information event management	Policy enforcement point
Identity management	Device compliance	Network security	Secure access service edge	Secure access cloud	Information rights management	CDM system	Security policy management
Conditional access	Device authentication	Zero trust network access		Isolation	Data loss prevention		
Dynamic risk scoring	Device management	Network access control		Any device access	Industry compliance		
	Device inventory	Transport encryption			Integrity		
	Enterprise mobility management	Session protection			Classification		

80%

of global cybersecurity leaders report increasing budgets for zero trust security initiatives compared to the previous year.[6]

Strategies and methods for prioritising zero trust architecture implementations

In the previous section of this white paper, we outlined a three-phased approach with timelines for federal agencies to consider when developing their zero trust strategy. This section builds beyond the phased approach methodology, specifically focusing on actions that can be completed in the two months of Phase 1. This is not meant to be an overwhelming list of actions ranked by priority, these are the easiest to execute, can be executed in parallel and will help shape the agency's priorities with stakeholder input.

Action #1: Map your agency's current solutions to a zero trust capability model.

On one slide, create a colour-coded mapping of your agency's currently implemented solution to a zero trust capability model. You can create your model, or you can use an industry framework like the zero trust capability model derived from the guidance illustrated in Figure 2 of this document. This activity should take no more than a week to complete, and in most cases, can be completed in less than a day. This will become a living document that can be used to prioritise your initiatives and track your progress.

Action #2: Vendors map their solutions to a zero trust capability model.

Ask your vendors to map their solutions to the same zero trust capability model framework used in Action #1, and have them present it to you. Include the definitions of the Pillars and Capabilities as an appendix to the slide deck to ensure the terminology makes sense. This activity should take your vendors a week or less to complete, and no more than one hour to present and discuss. This activity will help you understand the vendors' capabilities, what integrations their solutions have with other vendors and more importantly, help identify if their solutions can patch the pain points in your current environment.

Action #3: Create use cases describing how your agency connects to applications hosted in the cloud and on-premises.

In slide format, develop the top five use cases that describe how agency users securely connect to applications hosted with Australian IRAP Authorised Cloud Service Providers (CSP) and applications hosted on-premise. The use case slides should read from left to right, and describe in five steps or fewer how end-user devices securely connect to applications. If you need guidance on developing the use cases, you can start by using government-provided guidance (e.g., TIC 3.0 use cases) and/or contact your vendors to help you develop them. These use cases should take less than a week to complete and will help you define a more granular mapping of your ZTA capabilities when completing the mapping exercises from Action #1 and Action #2.

Action #4: Validate the accuracy of your Configuration Management Database (CMDB).

Obtain an electronic copy from the System of Record (SOR) used to track the inventory of your assets (e.g., CMDB). Zero trust solutions generate dynamic risk scores using a variety of data about users, devices and applications; you'll need to continuously validate the accuracy of your assets to improve the trust scoring algorithms that protect your agency. Do not make this a complex exercise; time-box this activity to one-week intervals and track your progress by reporting on the accuracy of your inventory by one metric: the percentage accuracy of your CMDB. It's not uncommon for agency CMDBs to be around 60% accurate when this activity starts. You should set a realistic target for accuracy, for example, 95% within 12 months.

Action #5: Obtain the Net Book Value (NBV) of your pre-existing assets displaced by cloud-native solutions.

In spreadsheet format, create a list of the hardware appliances that can be displaced by software-based, cloud-native, Australian IRAP Authorised Cloud Service Providers (CSP). Have a chat with stakeholders from your finance team to determine the NBV of these assets and, consequently, their financial value. If your agency depreciates the value of an IT asset over five years, the asset's NBV is $0 after five years. You can begin this activity by using an in-flight cloud initiative, or you can start by evaluating a new initiative like Secure Access Service Edge (SASE) solutions. For example, SASE solutions typically displace many hardware-based appliances (e.g., Virtual Private Network (VPN), Secure Web Gateway (SWG), etc.).

Conclusion

With new guidance available, agencies are ready to start on their journey to implementing a Zero Trust Architecture in their organisation. While it may seem daunting to overhaul legacy systems and reimagine cybersecurity frameworks, a variety of resources are on hand to support.

One recommendation to get started is adopting solutions like SASE, which is a cloud-native, software-based solution that merges software-defined wide area network (SD-WAN) capabilities with other features that maintain zero trust principles. SASE is a cloud-based solution that is designed to provide secure access to an organisation's end users who could be working from laptops anywhere. With solutions that encompass zero trust concepts, agencies can better monitor who is on their systems and secure their networks.

By mapping out an agency's current security posture and how they are using either the existing tools in their environment or adding new tools, it will help establish the foundations of a successful zero trust implementation. The zero trust security model helps reimagine how agencies apply security access across their network and focuses on better defending the system.

With solutions that encompass zero trust concepts, agencies can better monitor who is on their systems and secure their networks.

Learn more

To learn more about how to help enhance security for your operations, contact your Verizon Business Account Representative.

Email apaccontactus@verizon.com.
Visit verizon.com/business/en-au/contact-us/

1. Zscaler: "The State of Zero Trust Transformation, 2023." https://info.zscaler.com/resources-industry-reports-state-of-zero-trust-transformation-2023
2. Australian Cyber Security Centre: "Foundations for modern defensible architecture." https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/modern-defensible-architecture/foundations-modern-defensible-architecture
3. Australian Cyber Security Centre: "Gateway security guidance package: Gateway technology guides," https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/gateway-hardening/gateway-security-guidance-package-gateway-technology-guides
4. Okta: "The State of Zero Trust Security 2023." https://www.okta.com/sites/default/files/2023-09/SOZT_Report.pdf
5. Department of Home Affairs: "Guiding Principles to embed a Zero Trust Culture." https://www.homeaffairs.gov.au/cyber-security-subsite/files/consultation-paper-guiding-principles-to-embed-zero-trust-culture.pdf
6. IBM: "Cost of a Data Breach Report 2024." https://www.ibm.com/reports/data-breach