Australia

White paper

Cybersecurity strategies need to evolve.

A guide for federal agencies navigating Zero Trust.

verizon

Table of contents

Introduction: A challenging security landscape

Over the past 20 years, cybersecurity strategies have primarily focused on protecting the network perimeter in a physically defined space. However, over the course of nearly two years, as the federal workforce retreated home and many traditional offices disappeared, this perimeter has been redefined. Now the network perimeter is everywhere: it's the user's house, a coffee shop, a co-working space or the traditional office. As a result, federal cybersecurity strategies need to evolve as well.

To continue to secure the mission, federal agencies are identifying ways for security to dynamically follow their users, data, and applications since they are no longer anchored to centralized locations protected by static perimeter defense systems. Moving to the cloud has helped provide some options for agencies to move away from aging physical security infrastructure and take advantage of cloud-native security features that extend the security perimeter beyond the centralized office to the edge of remote work.

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. 88% of Australian IT professionals said their organisation is adopting a Zero Trust model, with 28% doing so in the last year alone.[1]

The remainder of this white paper:

- Defines the core principles of the 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 agencies to consider when implementing ZTA solutions.

What is Zero Trust?

Zero Trust is an emerging security paradigm designed to protect agencies by establishing, enforcing, and continuously analyzing least privilege per-request access decisions in information systems. Organizations that implement ZTA require that all users and devices must continually prove they are trustworthy. Zero Trust is the ultimate expression of the philosophy "trust but verify," and it fundamentally changes the way agencies are protected.

ZTA is the strategy to execute on the Zero Trust vision. Zero Trust Architecture is an agency's cybersecurity plan that utilizes Zero Trust concepts to encompass the workflow planning, component relationships, and access policies based on a framework of tenets, pillars, and capabilities. Tenets are used to describe the principles of Zero Trust, pillars logically organize the tenets into functional areas, and the capabilities map solutions to the functional areas in each pillar.

- **Tenets**: The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 describes Zero Trust tenets as a technology agnostic, ideal goal for Zero Trust adoption. An example of a tenet is "The enterprise monitors and measures the integrity and security posture of all owned and associated assets."
- **Pillars**: Logically organizes the Zero Trust tenets into functional areas. For example, the Office of Management and Budget (OMB) Zero Trust model includes eight Zero Trust pillars that are 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, OMB Zero Trust model Figure 2 provides a mapping of Zero Trust capabilities mapped to OMB's Zero Trust capability model.

Figure 1: GSA Pillars of Zero Trust

Pillar	Description
User	Involves focus on user identification, authentication, and access control policies which verify user attempts connecting to the network using dynamic and contextual data analysis.
Device	Performs "system of record" validation of user-controlled and autonomous devices to determine acceptable cybersecurity posture and trustworthiness.
Network	Isolates sensitive resources from being accessed by unauthorized people or things by dynamically defining network access, deploying micro-segmentation techniques, and control network flows while encrypting end-to-end traffic.
Infrastructure	Ensures systems and services within a workload are protected against unintended and unauthorized access, and potential vulnerabilities.
Application	Integrates user, device, and data components to secure access at the application layer. Security wraps each workload and compute container to prevent data collection, unauthorized access or tampering with sensitive applications and services.
Data	Involves focus on securing and enforcing access to data based on the data's categorization and classification to isolate the data from everyone except those that need access.
Visibility and Analytics	Provides insight into user and system behavior analytics by observing real-time communications between all Zero Trust components.
Orchestration and Automation	Automates security and network operational processes across the ZTA by orchestrating functions between similar and disparate security systems and applications.

Source: GSA Zero Trust Buyer's Guide, June 2021, Version 1.0

Figure 2: Zero Trust Architecture Capability Model

Core Pillars

Core Capabilities	User	Device	Network	Infrastructure	Application	Data	Visibility and Analytics	Orchestration & 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 Mgmt	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		

Sources:
- GSA Zero Trust Buyer's Guide, June 2021, Version 1.0
- M-22-09 Federal Zero Trust Strategy document from the Office of Management and Budget
- CISA Zero Trust Maturity Model, June2021 Version 1.0

Industry research indicates a Zero Trust approach is already reducing Australian data breaches (47%) and malware (33%) and uplifting network visibility (37%).[1]

How to begin your Zero Trust journey?

The US. Presidential Executive Order (EO) 14028, Improving the Nation's Cybersecurity issued in May 2021 provides federal agencies with directives and timelines; however, it doesn't prescribe the implementation methodology. The lack of prescriptive instructions is not a shortcoming of the EO; it's an opportunity for agencies to tailor the execution to their mission needs.

The first phase to Zero Trust adoption is to baseline an agency's current capabilities against an industry standard framework (i.e., Current Mode Operation). The second phase is to define 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 the desired state of completeness toward meeting all of the capabilities within the Zero Trust framework (i.e. Future Mode of Operation).

A summary of the three adoption phases, activities, and timelines are enumerated below. The figures on pages 7–9 provide an illustration of 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 a 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 color coded visualizations that is used to describe the Zero Trust capabilities that are currently "Met," "Partially Met," and "Not Met." The timeline required to complete the CMO mapping typically does not exceed two calendar months.

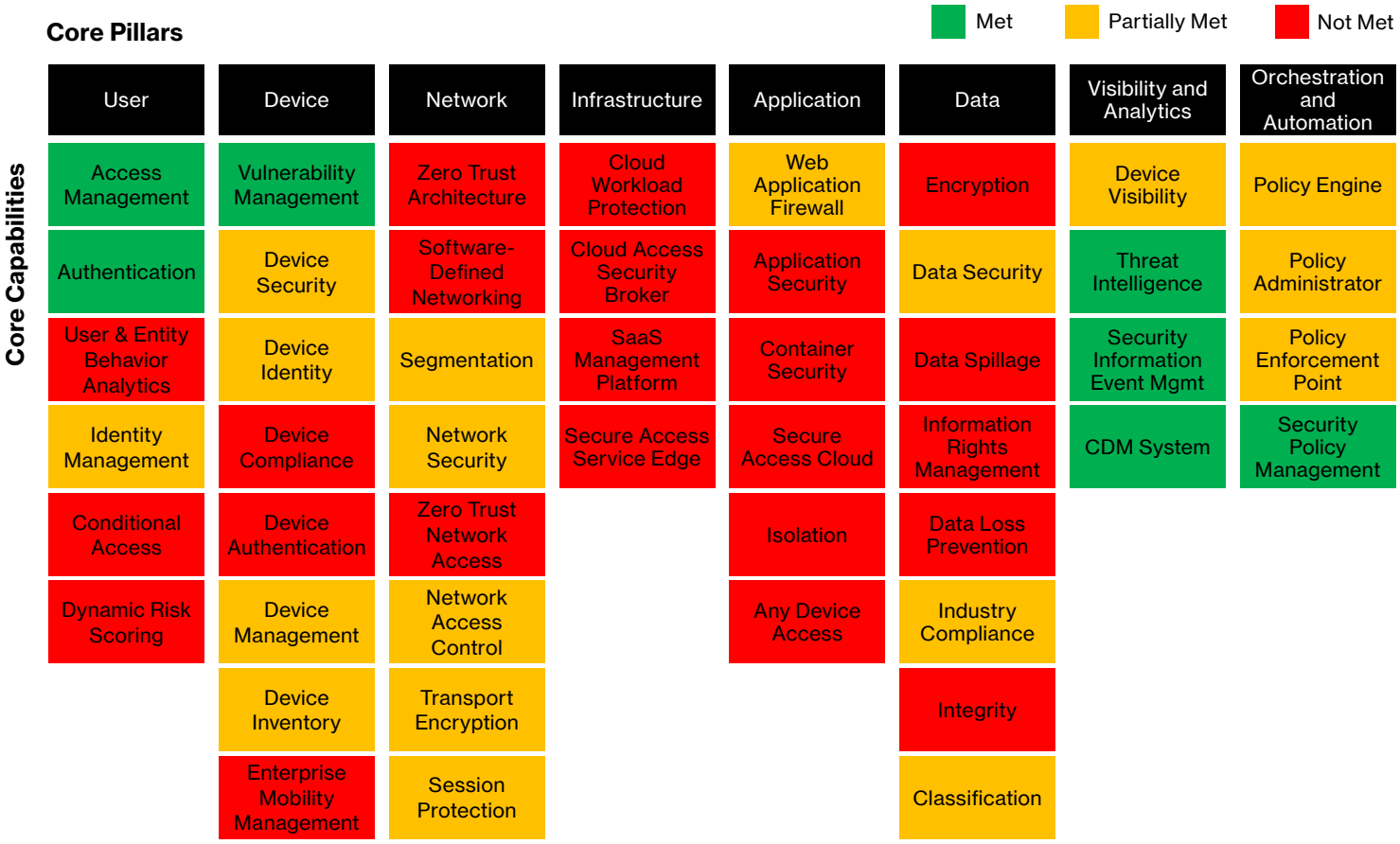
Phase 2: Interim Mode of Operation (IMO) – Identify at least one IT modernization initiative that can be completed within the next 12 months and map the new capabilities to be implemented the Zero Trust capability model completed during the CMO phase. (i.e. show the improvement) For example, agencies 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 3-5 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)

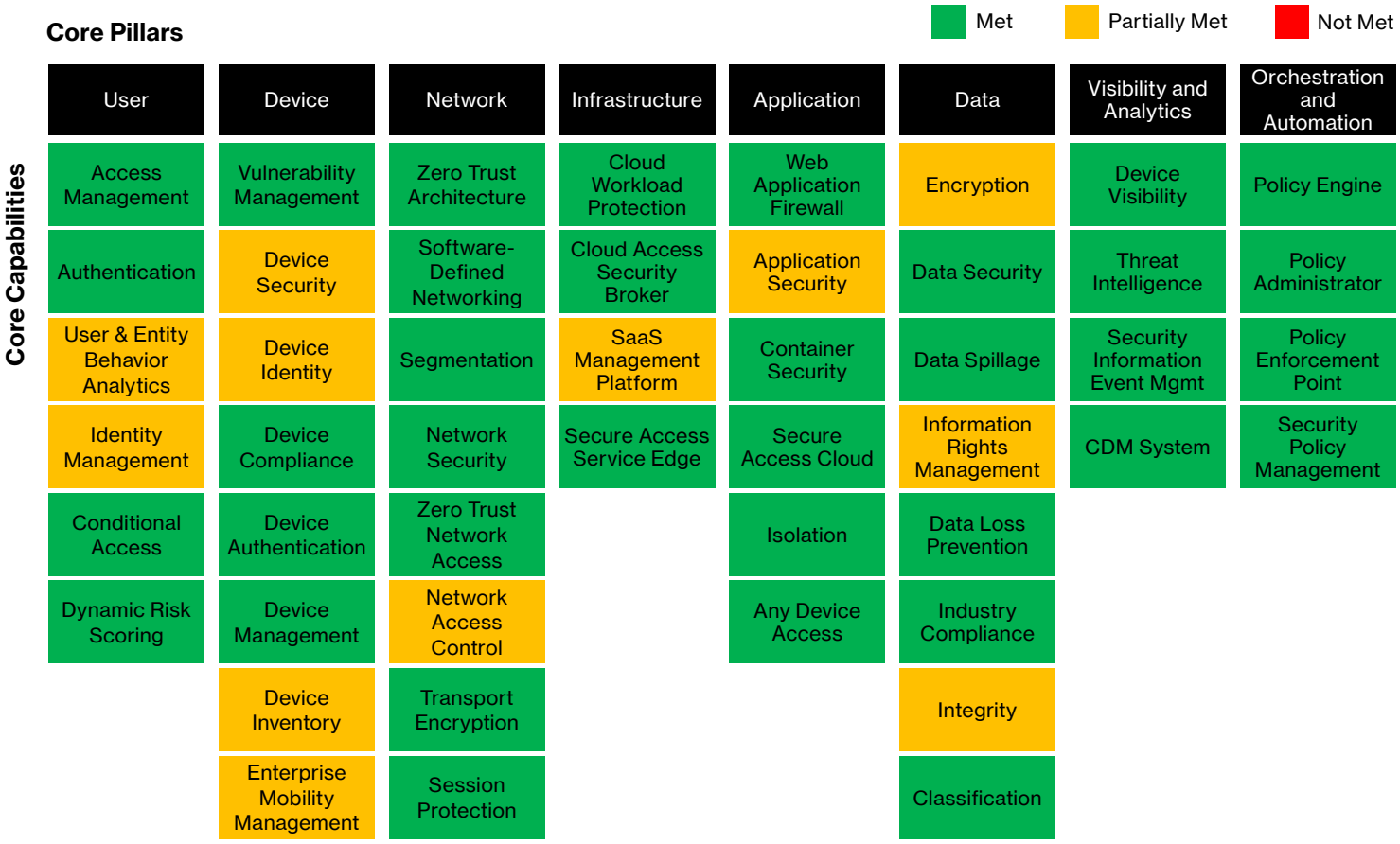


72% of organisations around the world have implemented Zero Trust, or plan to.[2]

Executing phases to Zero Trust architecture

Phase 2: 12 months of incremental improvements

Interim Mode of Operation (IMO)

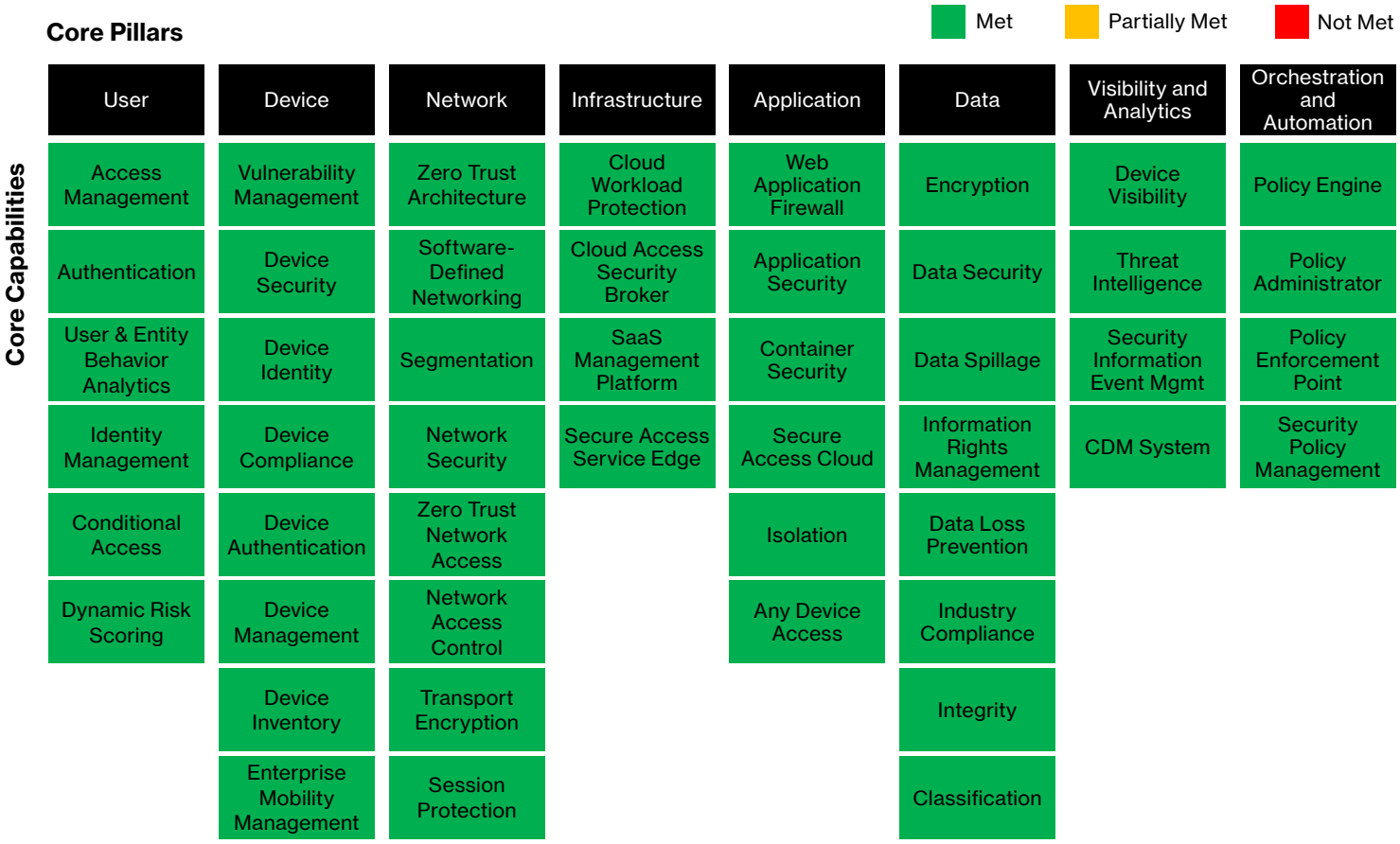


60% **Zero Trust adoption is growing per annum.[3]**

Executing phases to Zero Trust architecture

Phase 3: 3–5 year roadmap

Future Mode of Operation (FMO)



62% **of organisations are now familiar with Zero Trust design.[4]**

Strategies and methods for prioritizing Zero Trust architecture implementations

In the previous section of this white paper we outlined a three phased approach with timelines for agencies to consider when developing their Zero Trust strategy. This section builds off of the phased approach methodology, specifically focusing on actions that can be completed in the two-month period of Phase 1. This is not meant to be a comprehensive set of actions enumerated 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 agencies current solutions to a Zero Trust Capability Model

On one slide, create a color-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 OMB's guidance illustrated in Figure 2 of this document. Color the capabilities you meet green, amber for partially met, and red for not met. 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 prioritize your initiatives and track your progress.

Action #2 – Have your vendors to 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 there's a common understanding of terminology. 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 you identify if their solutions can fill gaps in your environment.

Zero Trust strategy actions are simple to execute, can be executed in parallel, and will help shape agency priorities with stakeholder input.

Strategies and methods for prioritizing Zero Trust architecture implementations

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

In slide format, develop the top five use cases that describe how agency users securely connect to applications hosted with FedRAMP, NIST 800-53 or Australian IRAP Authorized 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 less 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 a 12 month period.

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, FedRAMP, NIST 800-53 or Australian IRAP Authorized Cloud Service Providers (CSP). Partner with stakeholders from your finance team to determine the NBV of these assets to determine their financial value. If your agency depreciates the value of an IT asset over a period of five years, the assets NBV is $0 dollars 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 organization. While it may seem daunting to overhaul legacy systems and reimagine cybersecurity frameworks, there are many resources to look to for 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 ensures end users, who are now working remotely, can securely connect to the agency's network. With solutions that encompass Zero Trust concepts, agencies are able to 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 are able to better monitor who is on their systems and secure their networks.

verizon

1. Australia leads APAC in adoption of zero trust; Technology Decisions; Dylan Bushell-Embling; Wednesday, 27 October, 2021.
2. Jump Cloud – top zero trust security stats https://jumpcloud.com/blog/top-zero-trust-security-stats
3. Forcepoint industry analyst report – 2022 Gartner market guide for Zero Trust Network Access https://www.forcepoint.com/resources/industry-analyst-reports/2022-gartner-market-guide-zero-trust-network-access
4. Statista – security solutions familiarity by region https://www.statista.com/statistics/1238257/it-security-solutions-familiarity-by-region/