



U.S. General Services Administration
Federal Acquisition Service
Information Technology Category

Zero Trust Architecture Technology Book

Table of Contents

Zero Trust Architecture Introduction	3
Zero Trust Architecture Slip Sheet	12
Zero Trust Architecture White Paper	15
Zero Trust Architecture Use Case	20
How to get Zero Trust Architecture Products and Services	25
Zero Trust Architecture Lessons Learned and Frequently Asked Questions	30
Appendix A - Abbreviations	31

This document is intended to function as a single document or when needed as seven separate documents to meet the various needs of agencies and GSA.

Zero Trust Architecture Introduction

This technology book aims to provide an overview for U.S. federal agencies about Zero Trust Architecture (ZTA). It contains a range of documents, including an executive summary, a white paper, use cases, and information on obtaining ZTA products and services through the U.S. General Services Administration acquisition vehicles.

References to industry partners throughout this document are solely intended to emphasize the available ZTA capabilities and do not constitute any endorsement of any industry partner.

EXECUTIVE SUMMARY

Zero Trust Architecture is a data-centric security model that regards all networks and traffic as potential threats. Rooted in the principle of "trust no one, always verify," ZTA marks a fundamental departure from traditional perimeter-based security approaches. Unlike legacy models that assume trust for users and devices verified at the network perimeter, ZTA ensures that no entity is trusted until its authenticity and authorization are rigorously validated. This architecture introduces an additional layer of security, enabling robust access control to systems and applications while continuously monitoring behaviors to maintain trustworthiness.

ZTA facilitates transitioning from the traditional Trusted Internet Connections (TIC) framework by establishing agency-specific trust zones. These trust zones are defined as discrete computing environments designated for processing, storing, or transmitting information. They adhere to stringent security capabilities required to safeguard the traffic and data within and across these zones. Agency trust levels, categorized as High, Medium, and Low, consist of internal and external zones, Policy Enforcement Points (PEPs), and agency-approved Cloud Service Providers (CSPs).

The Executive Order on [Improving the Nation's Cybersecurity \(EO 14028\)](#), specifically Section 3: Modernizing Federal Government Cybersecurity, underscores the need for decisive measures to modernize cybersecurity practices within the federal government. ZTA adoption is emphasized as a key component of this modernization effort. Supporting this initiative are the Cybersecurity and Infrastructure Security Agency's (CISA) [TIC 3.0 Core Guidance](#), [Cloud Security Technical Reference Architecture \(TRA\)](#), and [Zero Trust Maturity Model \(ZTMM\)](#), which collectively facilitate gradual implementation across five distinct pillars. These frameworks enable incremental advancements toward optimization, addressing the dynamic work environment, evolving technology landscape, and expanding range of cloud services driving the evolution of protections at the "Edge" boundary.

Considerations for Leadership

ZTA is a critical component of an agency's information technology (IT) strategy, serving as a cornerstone for modernizing enterprise solutions and applications. Agencies must identify and prioritize their most essential objectives to achieve effective implementation. Among the pivotal considerations for meeting the 2027 ZTA requirements are the Risk Management Framework (RMF) and the Federal Information Security Management Act (FISMA) requirements. These two elements are interdependent and must be developed in alignment as part of the ZTA roadmap.

One of the most significant challenges agencies currently face in adopting ZTA is acquisition. Existing contracts often lack specific provisions for ZTA, creating additional constraints within the contractual landscape. To overcome these hurdles, agencies must ensure that their ZTA strategy integrates seamlessly with existing domains. The roadmap must prioritize acquisition-based planning.

Engaging agency leadership to raise awareness of the 2027 requirements is essential to drive adoption. Raising leadership awareness includes clearly defining the scope of the enterprise environment—encompassing the inventory of users, enterprise networks, and legacy systems—and emphasizing the security relevance and operational benefits of integrating innovative technologies. By addressing these key areas, agencies can position themselves to effectively implement ZTA as a robust, future-ready security strategies.

Zero Trust Architecture SWOT (Strengths, Weaknesses, Opportunities, and Threats)

Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis or situational analysis is a strategic planning and strategic management technique that an agency can use to identify the strengths, weaknesses, opportunities, and threats when planning a project or initiative.

Strengths:

- **Enhanced Security:** ZTA operates under the assumption that threats may already exist within the network. By verifying every user and device, it significantly reduces the risk of unauthorized access.
- **Adaptability:** Designed for dynamic environments, ZTA scales effectively with an organization's growth and the evolving threat landscape.
- **Granular Access Control:** Organizations can implement granular access controls based on factors such as user identity, device security posture, and contextual attributes.
- **Reduced Attack Surface:** Through network segmentation and strict enforcement of access controls, ZTA minimizes the attack surface, thereby restricting attackers' lateral movement.
- **Compliance Alignment:** ZTA enhances visibility and control over access to sensitive data, supporting organizations in meeting regulatory compliance requirements.

Weaknesses:

- **Complex Implementation:** Implementing ZTA often requires substantial changes to network infrastructure, applications, and security policies, adding complexity to the process.
- **Resource Intensive:** Deployment, management, and continuous monitoring of ZTA demand additional resources.
- **User Experience Impact:** Strict access controls and frequent authentication requirements can adversely affect user experience, potentially leading to productivity challenges.
- **Legacy System Compatibility:** Many legacy systems and applications may lack compatibility with ZTA, necessitating significant effort for integration or replacement.

Opportunities:

- **Innovation in Security Solutions:** ZTA fosters innovation, driving the development of advanced authentication methods, identity management systems, and network segmentation technologies.
- **Cloud Adoption:** With the increasing adoption of cloud-based resources, ZTA provides a robust framework for securing hybrid environments while ensuring consistent security policies.
- **Security Automation:** Integrating ZTA with security automation tools and orchestration platforms streamlines operations and enhances responses to security incidents.
- **Improved Incident Response:** By improving visibility into network traffic and user activities, ZTA facilitates faster detection and resolution of security incidents.

Threats:

- **Sophisticated Cyber Attacks:** As ZTA becomes more prevalent, attackers may devise advanced techniques to bypass its controls, such as exploiting vulnerabilities in authentication mechanisms.
- **Insider Threats:** Despite ZTA's focus on mitigating insider threats, malicious insiders with legitimate credentials remain a significant risk.
- **Misconfiguration Risks:** Errors in ZTA configuration can unintentionally weaken defenses or expose sensitive data.
- **Integration Challenges:** Integrating ZTA with existing security infrastructure and third-party solutions can result in compatibility issues or create security gaps.

OVERVIEW OF ZERO TRUST ARCHITECTURE

ZTA offers agencies a robust framework to continuously authenticate, authorize, and validate all users—whether operating within or outside the network environment—prior to granting access to network applications or data. The maturity level of an agency's ZTA implementation is determined by the extent to which ZTA principles have been effectively applied across its digital environment.

By adopting a ZTA approach, agencies can achieve a comprehensive and resilient cybersecurity defense, mitigating risks and enhancing protection against evolving threats. The progression toward ZTA implementation can be categorized into four distinct maturity levels: Traditional, Initial, Advanced, and Optimal. These levels provide a structured pathway for agencies to enhance their cybersecurity posture and align their strategies with zero-trust principles.

The ZTA Maturity Model serves as a valuable reference for assessing an agency's evolution toward a zero-trust architecture. This model enables organizations to evaluate their current state, identify areas for improvement, and strategically plan their journey toward optimal implementation.

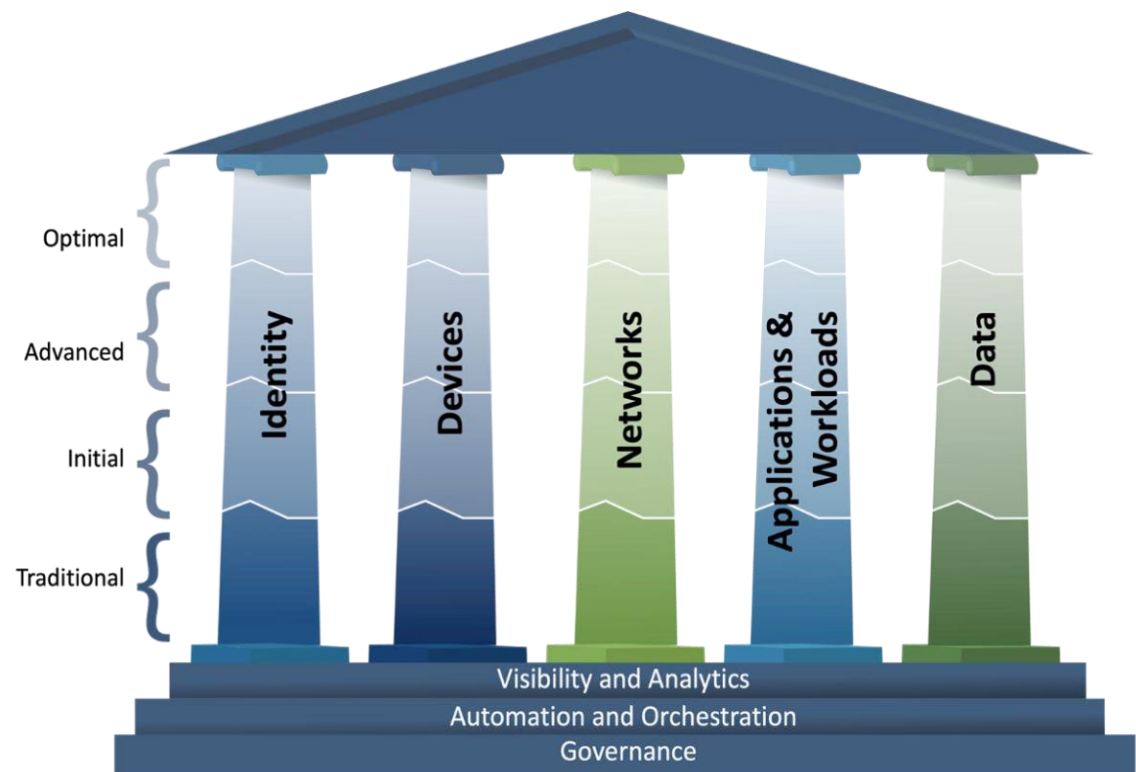







FIGURE 1: ZERO TRUST MATURITY MODEL¹

1 <https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model>

FIGURE 1: ZERO TRUST MATURITY MODEL² (CONTINUED)

	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	 <ul style="list-style-type: none"> Continuous validation and risk analysis Enterprise-wide identity integration Tailored, as-needed automated access 	 <ul style="list-style-type: none"> Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections Resource access depends on real-time device risk analytics 	 <ul style="list-style-type: none"> Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience Configurations evolve to meet application profile needs Integrates best practices for cryptographic agility 	 <ul style="list-style-type: none"> Applications available over public networks with continuously authorized access Protections against sophisticated attacks in all workflows Immutable workloads with security testing integrated throughout lifecycle 	 <ul style="list-style-type: none"> Continuous data inventorying Automated data categorization and labeling enterprise-wide Optimized data availability DLP exfil blocking Dynamic access controls Encrypts data in use
	Visibility and Analytics		Automation and Orchestration		Governance
Advanced	<ul style="list-style-type: none"> Phishing-resistant MFA Consolidation and secure integration of identity stores Automated identity risk assessments Need/session-based access 	<ul style="list-style-type: none"> Most physical and virtual assets are tracked Enforced compliance implemented with integrated threat protections Initial resource access depends on device posture 	<ul style="list-style-type: none"> Expanded isolation and resilience mechanisms Configurations adapt based on automated risk-aware application profile assessments Encrypts applicable network traffic and manages issuance and rotation of keys 	<ul style="list-style-type: none"> Most mission critical applications available over public networks to authorized users Protections integrated in all application workflows with context-based access controls Coordinated teams for development, security, and operations 	<ul style="list-style-type: none"> Automated data inventory with tracking Consistent, tiered, targeted categorization and labeling Redundant, highly available data stores Static DLP Automated context-based access Encrypts data at rest
	Visibility and Analytics		Automation and Orchestration		Governance
Initial	<ul style="list-style-type: none"> MFA with passwords Self-managed and hosted identity stores Manual identity risk assessments Access expires with automated review 	<ul style="list-style-type: none"> All physical assets tracked Limited device-based access control and compliance enforcement Some protections delivered via automation 	<ul style="list-style-type: none"> Initial isolation of critical workloads Network capabilities manage availability demands for more applications Dynamic configurations for some portions of the network Encrypt more traffic and formalize key management policies 	<ul style="list-style-type: none"> Some mission critical workflows have integrated protections and are accessible over public networks to authorized users Formal code deployment mechanisms through CI/CD pipelines Static and dynamic security testing prior to deployment 	<ul style="list-style-type: none"> Limited automation to inventory data and control access Begin to implement a strategy for data categorization Some highly available data stores Encrypts data in transit Initial centralized key management policies
	Visibility and Analytics		Automation and Orchestration		Governance
Traditional	<ul style="list-style-type: none"> Passwords or MFA On-premises identity stores Limited identity risk assessments Permanent access with periodic review 	<ul style="list-style-type: none"> Manually tracking device inventory Limited compliance visibility No device criteria for resource access Manual deployment of threat protections to some devices 	<ul style="list-style-type: none"> Large perimeter/macro-segmentation Limited resilience and manually managed rulesets and configurations Minimal traffic encryption with ad hoc key management 	<ul style="list-style-type: none"> Mission critical applications accessible via private networks Protections have minimal workflow integration Ad hoc development, testing, and production environments 	<ul style="list-style-type: none"> Manually inventory and categorize data On-prem data stores Static access controls Minimal encryption of data at rest and in transit with ad hoc key management
	Visibility and Analytics		Automation and Orchestration		Governance

2

² <https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model>

Zero Trust Architecture Description

ZTA establishes a comprehensive framework by incorporating the interconnected relationships of its five foundational pillars—Identity, Devices, Networks, Applications & Workloads, and Data—and three cross-cutting capabilities: Visibility & Analytics, Automation and Orchestration, and Governance. Together, this structured approach empowers agencies to enhance and modernize their cybersecurity defenses through the following capabilities:

- **Authentication and Trustworthiness:** Continuously authenticate, monitor, and validate user identities to ensure trustworthiness.
- **Device and Endpoint Management:** Identify, monitor, and manage devices and endpoints within the network environment.
- **Access and Data Flow Control:** Implement robust controls to manage access and regulate data flows across networks.
- **Application Security:** Secure and accredit applications within the technology stack to ensure comprehensive protection.
- **Automation of Security Processes:** Automate security monitoring processes and establish interoperability among tools within information systems.
- **Real-Time Behavioral Analysis:** Analyze user behavior and other data to monitor real-time activities and proactively strengthen network defenses.
- **IPv6 Integration:** Support and enable IPv6 technologies and addressing to align with evolving technological standards.

Zero Trust Architecture Definition

ZTA represents an enterprise-wide cybersecurity strategy that leverages zero trust principles while integrating component relationships, workflow planning, and access policies. A zero-trust enterprise encompasses the physical and virtual network infrastructure, along with operational policies, that collectively emerge as the outcome of a well-executed ZTA plan.

In planning and implementing ZTA, agencies must anticipate and address potential challenges, including:

- Accommodating complex and hybrid environments.
- Managing a diverse array of tools and technologies.
- Transitioning from legacy systems.
- Identifying and addressing security gaps.
- Navigating cost constraints.
- Balancing security measures with performance requirements.
- Shifting organizational mindsets and culture.
- Managing the diverse scope of devices in use.
- Overcoming modernization limitations and constraints.

Zero Trust Network Access (ZTNA) serves as one of the five core components of Secure Access Service Edge (SASE), which is built upon a cloud-native

Security Service Edge (SSE) model. At its foundation, SASE provides comprehensive, cloud-based cybersecurity and network solutions, extending the capabilities established through secure web gateways over the last decade.

SASE ensures clean, secure, and compliant internet access while delivering a seamless user experience for all individuals, irrespective of device, operating system, network type, or geographic location. By utilizing a cloud-based proxy architecture, SASE delivers these benefits consistently and efficiently.

A SASE framework combines a software-defined wide area network (SD-WAN) or similar WAN solutions with multiple advanced security capabilities, including:

- Cloud Access Security Brokers (CASB),
- Cloud Service Web Gateways,
- Firewall as a Service (FWaaS)

EXECUTIVE BRIEF

Organizations operate within an ever-evolving threat landscape characterized by increasingly sophisticated cyberattacks. Traditional security models that relied heavily on perimeter-based defenses are no longer adequate to address these challenges. ZTA presents a robust and comprehensive alternative by recognizing that threats can originate both inside and outside the network. This paradigm enforces stringent identity verification for every user and device attempting to access resources, thereby significantly reducing the risk of unauthorized access and security breaches.

Zero Trust represents a transformative approach to modern cybersecurity, redefining the protection of data, networks, and information systems. Through the application of ZTA principles, all users and devices—whether internal or external to the network—are rigorously authorized and authenticated before access to data, assets, applications, or services is granted. This ensures a heightened level of security and reinforces the resilience of organizational systems against emerging threats.

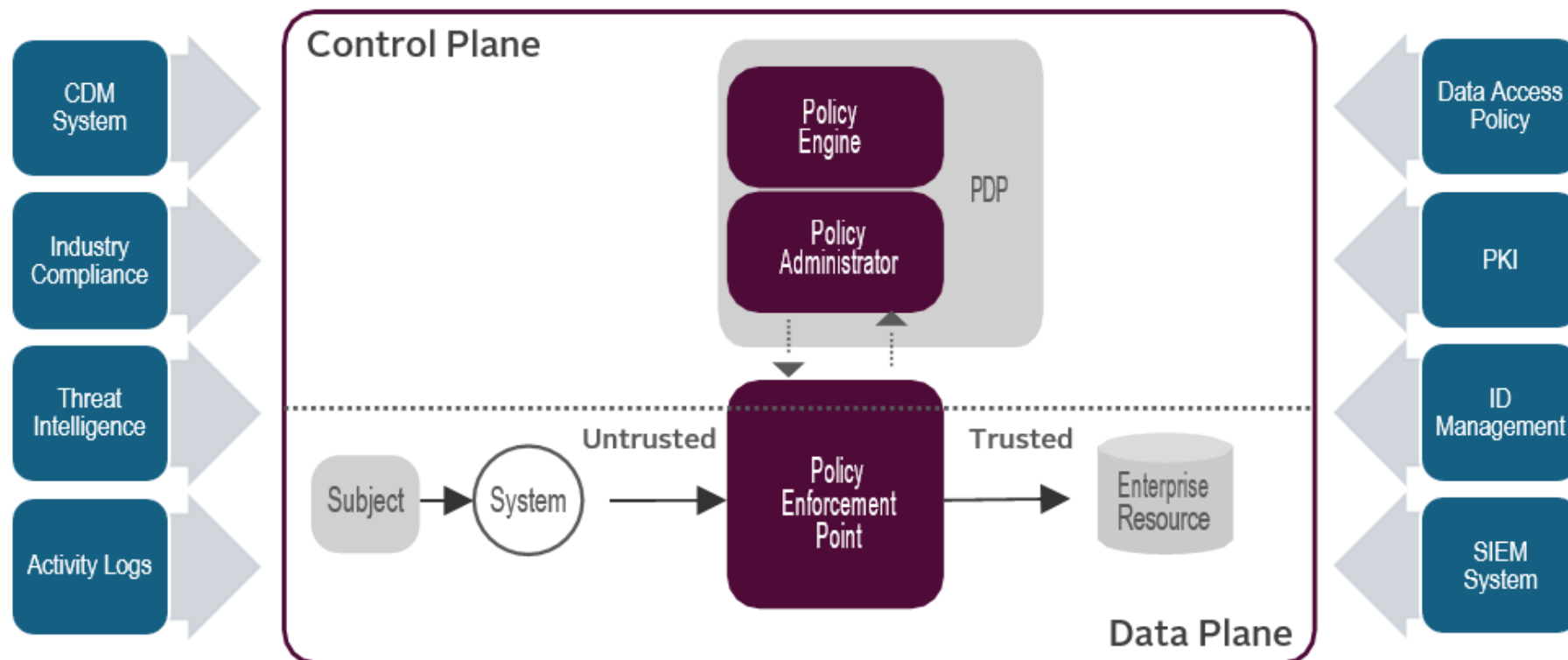
Zero Trust Architecture Framework

The ZTA framework employs robust mechanisms such as strong authentication, advanced access management, and network segmentation to safeguard against both cyber and insider threats. This framework represents a departure from traditional perimeter-based security models and focusing on protection at the access point level.

The accompanying diagram illustrates how ZTA incorporates fundamental principles outlined in the NIST 800-207 Zero Trust Framework. These principles include:

- **Continuous Verification:** Ensuring the ongoing authentication and validation of users and devices.
- **Limited Impact Radius:** Minimizing the potential scope of damage in the event of a breach by segmenting networks and resources.
- **Automated Collection and Response:** Leveraging automation to collect data, analyze threats, and respond effectively in real-time.

FIGURE 2: NIST 800-207 ZERO TRUST FRAMEWORK³



Key Concepts and Technologies within Zero Trust

- **Zero Trust Access:** A core concept within the Zero Trust framework, embracing the principle of "never trust, always verify" to ensure strict access control to agency resources.
- **Zero Trust Network Access (ZTNA):** A security posture that leverages an array of technologies and functions to provide secure access to internal applications for remote users, promoting the adoption of a Zero Trust Security Model.
- **Zero Trust Application Access:** A Zero Trust model that employs predefined access controls to evaluate and manage requests for access to an agency's applications.
- **Security Service Edge (SSE):** A critical security component that protects access to web, cloud services, and private applications. Its capabilities include access control, threat protection, data security, security monitoring, and acceptable-use control, implemented through both network-based and API-based integrations.

- **Software-Defined Perimeter (SDP):** An access control approach wherein connected devices are only aware of the resources (e.g., applications, servers) to which they are directly connected, thereby enhancing security.
- **Secure Access Service Edge (SASE):** Zero Trust principles are a key component of SASE, which protects IT environments by verifying user identities before granting access and establishing secure access boundaries around applications. SASE combines a software-defined wide area network (SD-WAN) or similar technologies with multiple security features, including cloud access security brokers, secure web gateways, and firewalls as a service.
- **Edge Computing:** A distributed computing paradigm that processes, analyzes, and stores data near its point of generation within the network. Zero Trust principles specifically address the access control aspects within edge computing environments, ensuring secure access to distributed resources.

Applications & Examples

The integration of security measures across the operating environment and the network layer, as facilitated by a Secure Access Service Edge (SASE) framework, provides a comprehensive approach to modern cybersecurity. The following components highlight the core aspects of this solution:

- **Access Control:** Safeguard applications containing sensitive data by enforcing least-privilege access policies. These policies verify identity and other contextual signals for every request or connection, ensuring robust protection.
- **Outbound Filtering:** Enhance security for users and devices connecting to the internet by implementing protections that filter and log Domain Name Service (DNS) queries, Hypertext Transfer Protocol (HTTP) requests, and network-level traffic.
- **Traffic Analysis:** Analyze data stored within cloud-based applications to identify potential violations of IT policies, misconfigurations, or instances of data mishandling, thereby maintaining compliance and integrity.
- **Data Protection:** Conduct thorough scanning of data within the environment or exiting to external destinations. Identify non-compliant data storage practices, even within trusted tools, and enforce stricter access controls where necessary.
- **User Experience:** Continuously monitor and optimize the user experience for tools and applications, whether hosted internally or in the cloud, to ensure seamless and efficient operation while maintaining security.

Assessing Providers

Assessing security providers requires a comprehensive approach that emphasizes alignment with federal guidelines and regulatory requirements. Agencies must evaluate providers based on their adherence to supply chain security best practices, ensuring robust safeguards are in place to protect against vulnerabilities within the supply chain. Collaboration and information sharing play a pivotal role, enabling seamless integration and fostering transparency among stakeholders. By prioritizing solutions that meet industry-wide standards and address emerging challenges, agencies can ensure both compliance and operational effectiveness. This strategic focus not only strengthens individual organizations but also contributes to broader industry impact, reinforcing the resilience of critical infrastructure.

Value and use

ZTA represents a pivotal advancement in modern cybersecurity by adopting a risk-based approach to identity and access control. It emphasizes adaptive segmentation, ensuring resources are isolated and protected based on context and risk levels. Through continuous monitoring and proactive security measures, ZTA fosters an enhanced security posture, effectively mitigating vulnerabilities and safeguarding against evolving threats. By embedding these principles, organizations can maintain robust defenses, protect sensitive data, and ensure compliance with stringent security standards in an increasingly dynamic threat landscape.

Lifecycle Stage

ZTA is increasingly recognized as a critical component of the modern enterprise operational environment, reflecting its vital role in addressing contemporary cybersecurity challenges. As organizations evolve their security postures, ZTA adoption has shifted from being an emerging concept to becoming a foundational element of enterprise cybersecurity strategies. Its lifecycle has progressed to widespread implementation across industries as organizations prioritize robust identity verification, access management, and continuous monitoring to safeguard their critical assets. This growing acceptance highlights ZTA's adaptability and effectiveness in mitigating risks within dynamic and complex digital landscapes.

Market Signals

Enterprises will have transitioned away from overburdened Virtual Private Networks (VPNs), while 80% of new digital business applications will be accessed using Zero Trust Access methodologies. This reflects a significant shift toward modernized, secure access frameworks.

Key signals driving this evolution include:

- **Increased Interest in Zero Trust:** Organizations are increasingly recognizing the value of Zero Trust as a critical cybersecurity approach.
- **U.S. Government Commitment:** Federal initiatives are advancing Zero Trust principles, setting a standard for secure operations.
- **Global Adoption Trends:** Other nations are following a similar path by embracing Zero Trust frameworks in their cybersecurity strategies.
- **Streamlined Implementation:** Advances in technology have simplified, automated, and accelerated the implementation of ZTA, making it more accessible to organizations.
- **Vendor Collaboration:** Partnerships among leading technology providers are yielding effective results, further enabling the successful deployment of Zero Trust solutions.

GSA IS HERE TO HELP

If you would like more information on the topics covered in this paper, please reach out to your designated GSA representative at <https://gsa.gov/nspsupport> or call 855-482-4348 to get in touch. GSA has multiple offerings for products, services, and solutions to support your planning, implementation, and continued support of the components of your ZTA.

Zero Trust Architecture Brief

Zero Trust Architecture (ZTA) is a security framework founded on the principle of “trust no one, always verify,” representing a transformative departure from traditional perimeter-based security models. Unlike legacy approaches that assume trust for users and devices verified at the network perimeter, ZTA ensures that no entity is trusted without thorough verification. This model incorporates an additional layer of security to manage access to systems and applications, while continuous behavioral monitoring reinforces ongoing trustworthiness and strengthens the overall security posture.

ZTA is structured around five foundational pillars: Identity, Devices, Networks, Applications & Workloads, and Data. Additionally, it incorporates three cross-cutting capabilities: Visibility & Analytics, Automation and Orchestration, and Governance.

Comprehensive guidance on ZTA implementation is available through resources such as the Cybersecurity and Infrastructure Security Agency (CISA) [Trusted Internet Connections \(TIC\) 3.0 Core Guidance](#) and the [Cloud Security Technical Reference Architecture](#) documents. Further insights are also provided in publications under the Enterprise Infrastructure Solutions (EIS) ZTA solution sets.

The General Services Administration's (GSA) EIS industry partners play a key role in assisting agencies with the planning and implementation of ZTA solutions. These efforts align with the objectives outlined in [Executive Order 14028, Improving the Nation's Cybersecurity](#) [Section 3 (a–c)], which emphasizes the modernization of cybersecurity practices to strengthen national security.

The Enterprise Infrastructure Solutions (EIS) ZTA solution sets are designed to align with key federal guidelines and standards, including:

- [National Institute of Standards and Technology \(NIST\) Special Publication \(SP\) 800-207](#): Providing a comprehensive description of Zero Trust Architecture principles and frameworks.
- [Cybersecurity and Infrastructure Security Agency \(CISA\) Zero Trust Maturity Model \(ZTMM\)](#): Offering enhanced clarity to support continued modernization efforts within dynamic and evolving operational environments.
- [Office of Management and Budget \(OMB\) Memorandum M-19-26](#): Updating the Trusted Internet Connections (TIC) Initiative to reflect contemporary security needs and practices.

EIS serves as an ideal contract vehicle for agencies to plan, implement, and operationally support the logical components required for effective ZTA deployment. This alignment ensures a seamless and compliant pathway for achieving Zero Trust goals.

HOW TO GET IT

ZTA is not a standalone service to be purchased but a strategic concept implemented through the services procured by an organization. Enterprise Infrastructure Solutions (EIS) services, such as Software-Defined Wide Area Network Service (SDWANS), Managed Security Services (MSS), Managed Network Services (MNS), Managed Mobility Services (MMS), and cloud services (Infrastructure as a Service [IaaS], Platform as a Service [PaaS], and Software as a Service [SaaS]), offer the logical components and operational support necessary for ZTA deployment.

For additional guidance, the GSA provides a comprehensive white paper on ZTA. Agencies can also leverage other GSA contract vehicles, such as the Multiple Award Schedule (MAS) and Governmentwide Acquisition Contracts (GWACs), to support integrated or managed ZTA solutions effectively.

To further assist agencies, GSA has published the [Zero Trust Architecture Buyer's Guide](#), a valuable resource for planning and executing ZTA strategies in alignment with organizational objectives.

BUSINESS VALUE

The foundational tenets of ZTA, as outlined in NIST SP 800-207, play a critical role in identifying and mitigating cybersecurity risks.

Adopting ZTA enables agencies to harness the benefits of cloud computing and shared services while enhancing security and potentially reducing overall costs. Additionally, implementing ZTA elements improves user experiences by providing direct access to the internet and cloud resources. This approach optimizes data-access traffic patterns and mitigates the risk of network bottlenecks.

EIS industry partners are well-equipped to support agencies in the planning, implementation, and ongoing operational support of the logical components required for ZTA solutions. Through EIS-managed service offerings, agencies can effectively advance their Zero Trust initiatives.

Furthermore, Software-Defined Wide Area Networking (SD-WAN) pricing models demonstrate significant cost efficiencies in network management. By leveraging centralized control and orchestration, agencies can achieve lower total operational costs while maintaining a robust security posture.

RECOMMENDATIONS

Agencies are encouraged to integrate Zero Trust Architecture as part of their comprehensive modernization and virtualization strategies. This should include alignment with key components such as Software-Defined Wide Area Networking (SD-WAN), Trusted Internet Connections (TIC) 3.0, and Internet Protocol version 6 (IPv6). The implementation approach must consider the agency's unique security posture and risk tolerance to ensure an effective and tailored ZTA strategy.

Engage with your GSA Solutions Broker to leverage GSA resources for evaluating your current architecture. This includes identifying opportunities for modernization and obtaining solicitation guidance to utilize GSA tools, products, and services effectively.

Agencies should review the Cybersecurity and Infrastructure Security Agency (CISA) [Zero Trust Maturity Model \(ZTMM\)](#) as well as the [NIST SP 800-207 framework](#) for a comprehensive understanding of ZTA.

Ensure that ZTA solutions address the five distinct pillars outlined by CISA: Identity, Devices, Networks, Applications & Workloads, and Data. Agencies should assess their current ZTA maturity level—categorized as Traditional, Initial, Advanced, and Optimal—and plan strategies for progression.

Additionally, agencies should reference CISA's [Program Guidebook](#), [Reference Architecture](#), [Security Capabilities Catalog](#), [Use Case Handbook](#), and [Overlay Handbook](#). These resources provide valuable insights into protecting operational environments while aligning with risk management strategies and the security considerations defined within TIC use cases.

EIS SERVICES ENABLING ZTA

The following EIS services can be integrated to create comprehensive ZTA solution sets:

- **Software-Defined Wide Area Network Service (SDWANS):** Implement managed or co-managed SD-WANS as an “overlay” to support the logical components of ZTA and several TIC 3.0 Use Cases. Utilize multiple “underlay” transport options, such as Internet Protocol Service (IPS), broadband internet, and mobile wireless, to enhance availability.
- **Managed Security Services (MSS):** Access comprehensive cybersecurity solutions, including Cloud Access Security Brokers (CASB), Identity and Access Management, Endpoint Management, Secure Web Gateway, and TIC services.

- **Managed Network Services (MNS):** Gain support for network planning, design, implementation, maintenance, operations, and customer service to strengthen network infrastructure.
- **Cloud Services:** Utilize FedRAMP-authorized cloud-based solutions, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), to enhance security and operational efficiency.
- **Managed Mobility Services (MMS):** Effectively manage mobile devices, wireless networks, and other mobile computing services to ensure secure access across diverse environments.
- **Service-Related Equipment (SRE):** Deploy the necessary equipment to fully implement EIS services within ZTA frameworks.
- **Service-Related Labor (SRL):** While EIS network services include all SRL required for implementation, agencies may incorporate additional labor into task orders to support specific EIS services.

Examples of EIS Service Combinations Supporting ZTA Components:

1. **TIC 3.0 Branch Office, Remote User, and Cloud Use Case Solutions:** Enhance productivity and improve user experiences by ensuring secure, optimized access to the internet, cloud service providers, and internal agency resources.
2. **Secure Access Service Edge (SASE):** Adopt a network architecture that integrates VPN and SD-WAN capabilities with cloud-native security features, such as secure web gateways, CASB, firewalls, and zero-trust network access.
3. **Cloud Access Security Broker (CASB):** Leverage cloud-hosted software that acts as a policy enforcement point between users and cloud service providers to maintain secure access control.

HOW CAN GSA HELP?

If you would like more information on the topics covered in this paper, please reach out to your designated GSA representative at <https://gsa.gov/nspsupport> or call 855-482-4348 to get in touch. GSA has multiple offerings for products, services, and solutions to support your planning, implementation, and continued support of the components of your ZTA.

Zero Trust Architecture White Paper

INTRODUCTION

Zero Trust Architecture is a modern security framework founded on the principle of “trust no one, always verify.” This approach represents a fundamental shift away from traditional perimeter-based security models. Unlike legacy approaches that rely on trusting users and devices verified at the network perimeter, ZTA ensures that no entity is trusted until its identity and access privileges are rigorously validated.

By implementing an additional layer of security, ZTA strengthens access control to systems and applications, mitigating potential vulnerabilities. Furthermore, it incorporates continuous monitoring of user and device behaviors to ensure sustained trustworthiness, thus offering a robust defense against evolving cyber threats.

ZTA is built on the fundamental principle of assuming a breach. It adopts a proactive security posture to address potential threats and minimize the impact of breaches should they occur. By implementing a least-privileged access approach, ZTA ensures that entities are granted only the minimum access rights necessary to perform their specific functions, significantly reducing vulnerabilities.

Key Benefits of ZTA Implementation:

- **Proactive Data Loss Prevention:** Protects sensitive information by addressing risks before data exposure occurs.
- **Faster Incident Response:** Enhances the speed and efficiency of responses to security incidents, reducing downtime and mitigating damage.
- **Reduced Overhead Costs:** Streamlines security processes, lowering operational expenses associated with managing complex security frameworks.
- **Improved Compliance and Regulatory Adherence:** Strengthens alignment with regulatory standards and compliance requirements through robust access and monitoring controls.

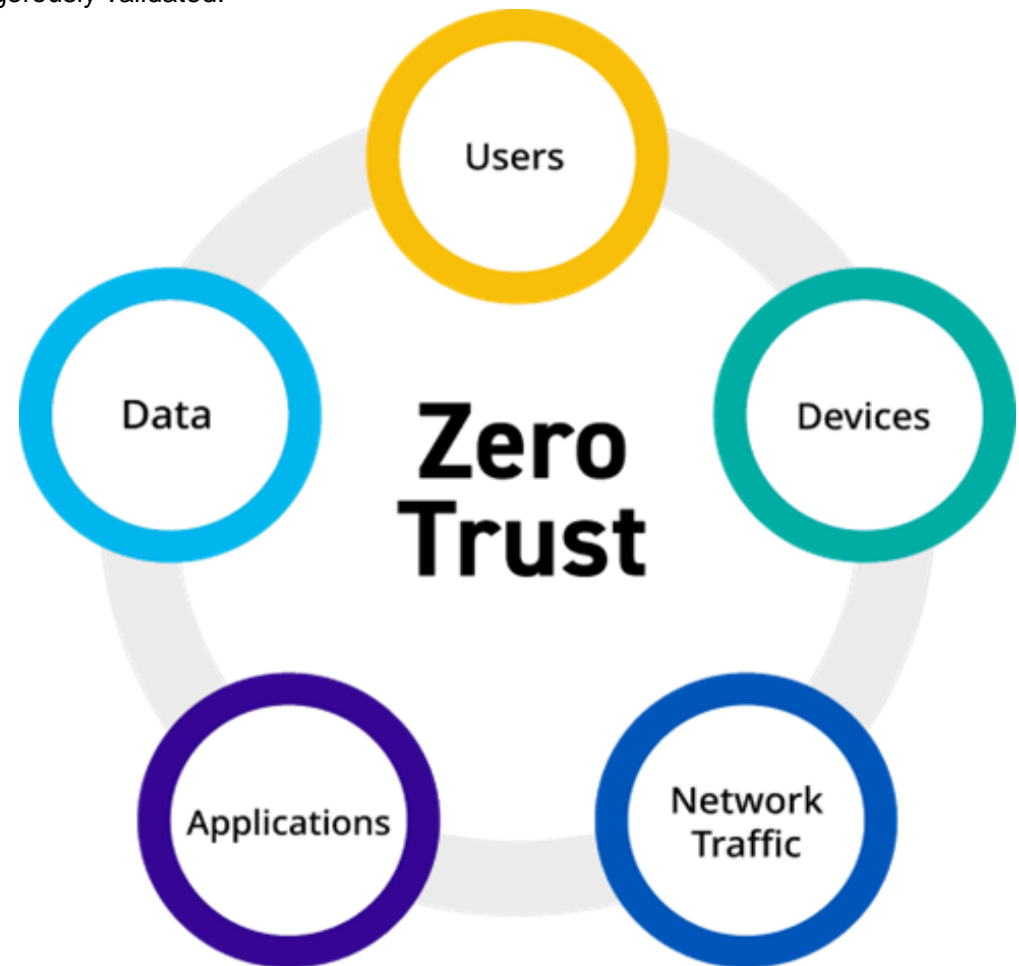


FIGURE 1: ZERO TRUST SECURITY⁴

⁴ <https://finevpn.org/glossary/zero-trust-security/>

FEDERAL GUIDANCE AND EFFORTS SUPPORTING ZERO TRUST

The federal government has increasingly embraced cloud services as a cornerstone of Information Technology (IT) modernization strategies. As-a-Service offerings have revolutionized enterprise environments by shifting operations off-premise and into the cloud. Federal initiatives have been instrumental in supporting adoption and advancing cybersecurity frameworks, including ZTA.

Key efforts driving cloud integration and ZTA implementation include:

- **Federal Risk and Authorization Management Program (FedRAMP):** Provides a standardized approach to authorization, security assessment, and continuous monitoring for cloud-based technologies, including Unified-Communications-as-a-Service (UCaaS) solutions.
- **Cloud Smart Strategy:** Launched in 2018, this initiative aims to modernize federal agencies' IT infrastructure and accelerate the adoption of cloud-based technologies to improve efficiency and security.
- **Trusted Internet Connections (TIC) 3.0:** The Cybersecurity and Infrastructure Security Agency (CISA) released the TIC 3.0 Security Capabilities Catalog (Version 2), driving security standards and leveraging advancements in technology as agencies adopt mobile and cloud environments.
- **National Security Agency (NSA) Cybersecurity Technical Report** Released in June 2021, this report outlines secure deployment of Unified Communications/Voice and Video over IP systems and references protections for cloud connectivity during migration efforts.
- **Presidential Executive Order 14028 and Government Accountability Office (GAO) Report:** In response to increasing cyber threats, the GAO published the [Cybersecurity Implementation of Executive Order Requirements Is Essential to Address Key Actions \(GAO-24-106343\)](#) in April 2024. This paper reviews progress in implementing 115 provisions and 55 leadership and oversight requirements established by the executive order.

THE ZERO TRUST LIFECYCLE PHASES

1. **Emerging Phase:** ZTA emerges as a critical outcome of the TIC initiative, focusing on safeguarding agency data, information, and systems at the point of access. The legacy TIC solutions, which relied on perimeter-based security approaches, imposed limitations on agencies' ability to securely leverage innovative technologies and cloud services.
2. **Research and Development Phase:** ZTA solutions continuously evolve, expanding to include partnerships with edge and network security services, as well as shared or cloud-based offerings, ensuring alignment with modern technology advancements.
3. **Early Solutions Phase:** This stage necessitates a transformation in agency business models and partnerships with providers to adopt a broader architectural approach. It emphasizes considerations for cloud-based solutions and supports remote workers.
4. **Initial Adoption Phase:** During this phase, agencies incorporate ZTA into their modernization objectives, employing a systematic implementation strategy that highlights its benefits to leadership and stakeholders.

FIGURE 2: ZERO TRUST LIFECYCLE PHASES



5. **Private Sector Experiments Phase:** For-profit organizations begin integrating ZTA technologies into their systems, though these implementations are not yet widely adopted across industries.
6. **Government Experiments Phase:** Federal, state, local, and tribal governments explore ZTA technologies as part of their service delivery and operational frameworks, testing their efficacy and applicability.
7. **Broad Acceptance Phase:** ZTA achieves widespread acceptance with buy-in at the highest organizational levels, enabling a formalized, integrated security strategy across all layers of the operating environment. Proven ZTA capabilities enhance visibility, monitoring, reporting, and rapid recovery from breaches through IT-integrated security practices.
8. **Decline Phase:** ZTA reduces reliance on Virtual Private Networks (VPNs) and infrastructure bandwidth by facilitating secure access to systems and data beyond the traditional network perimeter.
9. **End-of-Sale Phase:** To maintain competitiveness, vendors must demonstrate the capability to deliver ZTA solutions through single or multi-provider approaches.
10. **End-of-Life Phase:** While ZTA continues to evolve, its lifecycle reflects ongoing advancements in security technologies and implementation practices.
11. **Additional Application Paths:** ZTA emerges as a core component of Secure Access Service Edge (SASE), seamlessly integrating network and security functions in a cloud-based environment. Agency policies are updated to support advancements in segmentation, cloud/shared platforms, and artificial intelligence (AI) technologies.

ZERO TRUST ARCHITECTURE MIGRATION

The National Institute of Standards and Technology (NIST) provides a structured framework for migrating to Zero Trust Architecture. Agencies and organizations can follow these critical steps to ensure a seamless and effective transition:

1. **Identify Actors on the Enterprise:** Assess and catalog all individuals, devices, and entities interacting within the enterprise to understand the scope of access and security requirements.
2. **Identify Assets Owned by the Enterprise:** Compile a detailed inventory of assets, including data, applications, and systems, to establish a foundation for managing and securing resources.
3. **Identify Key Processes and Evaluate Risks Associated with Execution:** Analyze essential business processes and assess associated risks to determine vulnerabilities and prioritize mitigation efforts.
4. **Formulate Policies for the ZTA Candidate:** Develop comprehensive policies tailored to the specific needs of the ZTA model, ensuring alignment with organizational objectives and security goals.
5. **Identify Candidate Solutions:** Evaluate potential tools, technologies, and services that meet ZTA requirements and address identified risks effectively.
6. **Initial Deployment and Monitoring:** Implement the selected ZTA solutions and conduct continuous monitoring to validate functionality, assess effectiveness, and identify areas for improvement.

CONSIDERATIONS FOR AGENCIES

Agencies should account for the following critical considerations to ensure the successful implementation and integration of ZTA within their operations:

- **Engagement with Leadership:** Maintain ongoing dialogue with leadership at all stages of implementation—before, during, and after deployment—to secure buy-in and foster alignment.
- **Frequent Communication and Transparency:** Conduct regular Q&A sessions and provide comprehensive FAQs to address potential concerns and enhance understanding.
- **Integration with Existing Security Requirements:** Align ZTA initiatives with other established security frameworks, such as the Federal Information Security Modernization Act (FISMA) and guidance from the Cybersecurity and Infrastructure Security Agency (CISA).
- **Unified Approach:** Ensure seamless collaboration across Operations, Engineering, Identity Management, and Information Security teams to create a cohesive strategy.
- **Preserve Critical Elements:** Avoid compromising on fundamental components essential to achieving the intended security outcomes.
- **Embrace Auditing:** Foster a culture of transparency by welcoming audits to identify areas for improvement and ensure ongoing compliance.
- **Select Capable Partners:** Collaborate with vendors or partners capable of effectively integrating, inspecting, and supporting ZTA solutions.
- **Leverage Federated Services:** Draw insights from federated services to enhance implementation and operational strategies.
- **Focus on User Experience:** Balance ZTA deployment with a commitment to optimizing user experiences to maintain productivity and engagement.
- **Invest in Workforce Development:** Build in-house expertise through training, certifications, and skills-based hiring to ensure long-term capability and resilience.

Incorporating the Risk Management Framework (RMF) for ZTA Implementation: Agencies should adopt the following RMF steps to guide ZTA deployment:

1. **Prepare:** Conduct thorough organizational and system-level preparation for ZTA implementation.
2. **Categorize:** Define and categorize systems to establish the scope and criticality of assets.
3. **Select:** Identify and tailor security controls in alignment with organizational needs.
4. **Implement:** Deploy selected security controls and ensure effective integration.
5. **Assess:** Evaluate the effectiveness of security controls through rigorous assessments.
6. **Authorize:** Obtain formal authorization to operate the system securely.
7. **Monitor:** Continuously monitor security controls to adapt to evolving risks and maintain effectiveness.

CONCLUSION

Achieving the objectives of implementing a ZTA requires more than a single technology, product, or service. Instead, a truly effective ZTA integrates a suite of technologies that collectively enhance security across organizational environments. These technologies must:

- Authenticate, monitor, and validate user identities and trustworthiness.
- Automate security monitoring and establish seamless connectivity across information systems.
- Analyze user behavior and other data to enable real-time event observation and proactively align network defenses.
- Identify, monitor, and manage devices and other endpoints within a network.
- Control and manage access rights and data flows across networked environments.
- Secure and accredit applications within the technology stack.
- Support both IPv4 and IPv6 protocols.

ZTA empowers agencies to embed zero trust principles into their industrial and enterprise infrastructure and workflows, enabling enhanced resilience against evolving cyber threats while supporting modernization objectives.

GSA IS HERE TO HELP

If you would like more information on the topics covered in this paper, please reach out to your designated GSA representative at <https://gsa.gov/nspsupport> or call 855-482-4348 to get in touch. GSA has multiple offerings for products, services, and solutions to support your planning, implementation, and continued support of the components of your ZTA.

Zero Trust Architecture Use Case

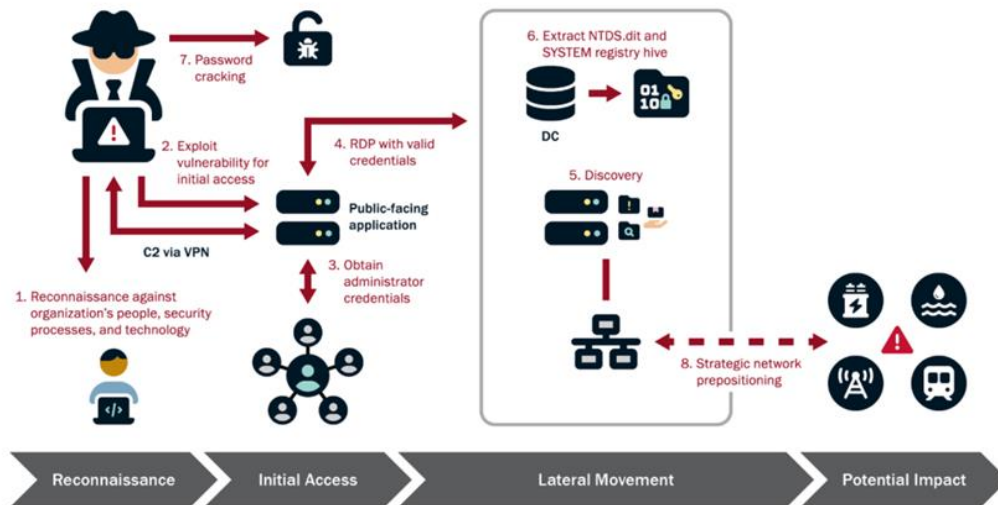
The following use case highlights vulnerabilities and network security concepts, illustrating how integrated Zero Trust solutions can effectively mitigate risk. These solutions leverage a diverse range of resources, including the Department of Defense (DoD) Zero Trust Reference Architecture and the Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model, as foundational references for the design and implementation of the integrated approaches.

The described outcomes are not intended to advocate for a single product capable of addressing all Zero Trust pillars and capabilities, nor do they aim to represent the highest maturity level of Zero Trust implementation. Instead, this use case focuses on presenting a broad cross-section of strategies and methodologies that support the development of comprehensive and integrated Zero Trust solutions.

ZERO TRUST TO PROACTIVELY COMBAT INTRUSION ATTACKS (SALT TYPHOON)

This use case examines how Zero Trust Architecture could have been employed to mitigate the risks posed during the Salt Typhoon cyberattack. The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC), Canadian Cyber Security Centre (CCCS), and New Zealand's National Cyber Security Centre (NCSC-NZ) jointly issued warnings regarding a cyber espionage campaign conducted by threat actors affiliated with the People's Republic of China (PRC). These actors compromised the networks of major global telecommunications providers as part of a significant and far-reaching cyber espionage operation.

The Salt Typhoon campaign, also known as GhostEmperor, FamousSparrow, or UNC2286, has been attributed to a Chinese hacking group believed to operate under the direction of China's Ministry of State Security. Active between 2020 and 2024, this sophisticated campaign exploited vulnerabilities in critical telecommunications infrastructure, targeting systems used by companies such as Verizon, AT&T, Lumen Technologies, and T-Mobile.



The attackers accessed sensitive call record metadata, including details about call participants, durations, and locations, posing significant risks to individuals and organizations. High-ranking government officials were also targeted, further underscoring the gravity of this breach. The complexity of the scenario was heightened by the occasional travel of users to high-threat nations known for state-sponsored cyber activities. Additionally, attackers exploited attempts by users to access third systems without having the necessary administrator privileges.

Through the adoption of Zero Trust principles, agencies and organizations could have proactively addressed these vulnerabilities. By implementing robust identity verification, continuous monitoring, and least-privilege access controls, ZTA frameworks offer enhanced protection against sophisticated cyber espionage campaigns such as Salt Typhoon.

FIGURE 1: TYPICAL VOLT TYPHOON ACTIVITY⁵

⁵ <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>

The highlighted areas of exploitation and compromise associated with the activities of these threat actors align with existing weaknesses in the following domains:

- **Victim Infrastructure Weaknesses:** Gaps in the architecture and management of systems make them susceptible to exploitation.
- **Vulnerable Devices and Services:** Inadequate patching practices leave critical devices and services exposed to known vulnerabilities.
- **General Security Practices:** Inefficient or incomplete security measures fail to provide comprehensive protection against sophisticated threats.
- **Intrusion Mitigation:** Enhancing security measures reduces the opportunities for attackers to infiltrate systems and mitigates the potential impact of their activities.

As part of the Secure by Design initiative, federal agencies along with global partners provided joint guidance identifying the most critical risks within the threat landscape. This guidance highlights practices to avoid and categorizes these poor practices into three distinct areas:

- **Product Properties:** Observable security-related qualities of a software product that contribute to its overall vulnerability.
- **Security Features:** Functionalities provided by a product to support and enhance security measures.
- **Organizational Processes and Policies:** Actions taken by software manufacturers to ensure strong security practices and transparency.

The Salt Typhoon and similar cyber espionage campaigns underscore the urgent need for robust cybersecurity frameworks, particularly the adoption of ZTA. By addressing infrastructure vulnerabilities, ensuring timely patching for at-risk devices and services, and implementing comprehensive security practices, organizations can reduce the likelihood of intrusions and mitigate the impact of sophisticated attacks.

The Secure by Design initiative, emphasizes the importance of avoiding poor practices in product properties, security features, and organizational processes. By adhering to these recommendations, organizations can enhance transparency and strengthen their overall security posture, effectively defending against state-sponsored cyber threats.

Implementing Zero Trust Architecture

The adoption of a comprehensive ZTA is a strategy for preventing attacks and containing vulnerabilities. A well-designed ZTA model eliminates implicit trust, enforces continuous verification of the identities and permissions of users and devices, and incorporates considerations for the entire network operating environment, including applications, workloads, and data.

By implementing a ZTA model that integrates core functional areas such as visibility and analytics, automation and orchestration, and governance, organizations can significantly mitigate the impact of sophisticated cyberattacks, including campaigns such as Salt Typhoon. This proactive approach enhances security posture, minimizes vulnerabilities, and provides robust defenses against evolving threats.

While even a basic implementation of ZTA can mitigate the impact of cyber-attacks, achieving a more mature ZTA significantly enhances an agency's ability to reduce or eliminate vulnerabilities. ZTA is not a product or service to be purchased but a strategic approach to cybersecurity that comes with associated costs. Although incorporating ZTA standards introduces complexity and redundancy into the network environment, it is imperative to establish these standards as requirements for providers, network engineers, and network defenders to bolster security effectively.

ZTA can be implemented incrementally, and even at a foundational level, it can deter and mitigate risks through the application of several key principles:

1. **Least Privilege Access:** ZTA operates on the principle of least privilege, granting users and devices only the permissions necessary to perform their designated tasks. This minimizes the attack surface and limits opportunities for attackers to access sensitive data. In the case of the Salt Typhoon attack, restricting access would have curtailed the attacker's ability to exploit vulnerabilities and move laterally within the network.
2. **Continuous Authentication and Authorization:** Unlike traditional security models that assume implicit trust for users and devices inside the network, ZTA mandates continuous authentication and authorization at every stage of interaction. This ensures only authorized users access resources, regardless of their location. During the Salt Typhoon attack, continuous verification would have detected and prevented unauthorized access attempts in real-time.
3. **Micro-Segmentation:** ZTA employs micro-segmentation, dividing the network into smaller segments with distinct security policies. This strategy restricts attackers from moving laterally within the network in the event of a breach. For the Salt Typhoon attack, micro-segmentation would have contained the intrusion, preventing access to critical systems and sensitive data.
4. **Strong Authentication Methods:** ZTA incorporates robust authentication mechanisms such as multi-factor authentication (MFA) to verify user and device identities before granting access. Implementing MFA during the Salt Typhoon attack would have added an additional security layer, complicating attackers' efforts to exploit compromised credentials.
5. **Network Traffic Monitoring:** Continuous monitoring of network traffic and activity is integral to ZTA. By identifying suspicious behaviors in real-time, this approach enables rapid detection and response to cyber threats. During the Salt Typhoon attack, network monitoring would have flagged unusual patterns and triggered alerts, facilitating a swift and effective response.

By adopting these principles, telecommunications providers could have substantially mitigated the risks associated with the Salt Typhoon attack. ZTA emphasizes continuous verification and least privilege access, ensuring that even if attackers gain initial access, their ability to move laterally and compromise sensitive data is significantly constrained. Agencies must adopt a similar approach to strengthen their cybersecurity posture against evolving threats.

The Salt Typhoon cyberattack underscores the urgent need to adopt robust cybersecurity frameworks such as ZTA. Through the implementation of ZTA, organizations can significantly strengthen the protection of critical infrastructure and sensitive data, thereby enhancing their overall security posture against sophisticated cyber threats.

Zero Trust Architecture Benefits

By implementing ZTA principles, organizations can address critical considerations to strengthen their cybersecurity framework. ZTA enhances the visibility of networked environments, reduces the attack surface through least privilege access controls, and provides a structured approach to intrusion mitigation. To establish a resilient cybersecurity foundation, organizations must prioritize the application of protection methodologies by adopting foundational network security principles that form a robust baseline for risk mitigation. Additionally, enhancing oversight of devices and endpoints interacting with systems and applications improves monitoring and control, addressing visibility gaps. Implementing proactive intrusion mitigation strategies reduces vulnerabilities and prevents unauthorized access to organizational resources, ensuring a comprehensive defense against evolving threats.

The CISA, NSA, FBI, and international partners highlight critical actions outlined in the [Enhanced Visibility and Hardening Guidance for Communications Infrastructure](#) to enhance network visibility and fortify systems against evolving threats. The following content explores the vital role ZTA plays in effectively implementing these key actions.

- **Strengthen Visibility:** ZTA enforces continuous monitoring of user, device, and entity activities across networked environments to identify potential threats.

- **Harden Network Devices:** The micro-segmentation and authentication capabilities of ZTA effectively mitigate vulnerabilities commonly exploited during cyber espionage campaigns.
- **Enhance Organizational Security:** ZTA supports the implementation of proactive defense measures by automating security tasks and unifying access controls.

ZTA incorporates advanced detection practices to identify and respond to threats in real time:

1. **Detailed Logging and Centralized Storage:**

- ZTA employs robust logging mechanisms to aggregate data in a centralized, write-once, read-many configuration, protecting against tampering.
- Referencing resources such as [CISA's Secure by Design](#) guidance ensures alignment with industry best practices.

2. **Baseline Establishment and Maintenance:**

- ZTA establishes continuous baselines for network, user, administrative, and application activity, incorporating least privilege restrictions to enhance security.

3. **Automated Log Review:**

- By leveraging machine learning and automation tools, ZTA continuously reviews logs for anomalies, generating alerts based on deviations from established baselines.

4. **Noise Reduction in Alerts:**

- ZTA prioritizes alerts by urgency and severity, reducing noise and enabling defenders to focus on the most critical threats.

5. **User and Entity Behavior Analytics (UEBA):**

- Behavior analytics within ZTA frameworks improve threat detection by monitoring unusual activities at both user and entity levels.

To complement detection capabilities, ZTA includes hardening practices designed to minimize vulnerabilities:

1. **Vendor-Recommended Guidance:**

- ZTA integrates vendor-provided security recommendations to fortify system resilience against exploitation.

2. **Application Allowlisting:**

- Allowlisting under ZTA restricts unauthorized applications and monitors common Living off the Land (LOTL) binaries for suspicious activity.

3. **Enhanced Network Segmentation:**

- ZTA strengthens segmentation and monitoring of IT and Operational Technology (OT) networks, limiting attackers' ability to move laterally within

environments.

4. **Authentication and Authorization Controls:**

- ZTA mandates stringent authentication and authorization measures for all interactions, reducing unauthorized access risks.

Even with advanced frameworks, defenders face challenges distinguishing malicious LOTL activity from legitimate operations:

- **Operational Silos:** ZTA fosters collaboration by integrating workflows between IT and security teams.
- **Reliance on Untuned Detection Systems:** ZTA's continuous verification and anomaly detection address limitations of untuned Endpoint Detection and Response (EDR) systems.
- **Default Logging Configurations:** ZTA ensures comprehensive logging and analysis of activities to differentiate legitimate actions from threats.
- **Large Data Volumes:** ZTA incorporates AI-driven tools to analyze large data volumes efficiently, aiding in threat identification.

ZTA aligns with best practices to mitigate vulnerabilities and reduce risks:

1. **Apply Patches for Internet-Facing Systems:** ZTA incorporates timely patching of systems targeted by threat actors.
2. **Enable Phishing-Resistant Multi-Factor Authentication (MFA):** ZTA requires MFA as a core access control feature.
3. **Activate Comprehensive Logging:** ZTA emphasizes centralized logging for effective monitoring and response.
4. **Plan “End of Life” for Technology:** ZTA recommends phasing out unsupported technologies to reduce vulnerabilities.
5. **Mitigate LOTL Techniques:** ZTA proactively identifies and neutralizes attacker techniques by monitoring system tools and behaviors.

ZTA emphasizes the importance of securing communication channels through end-to-end encryption services. Secure communication apps, such as WhatsApp and Signal, offer examples of how safeguards messaging between devices like iPhones and Androids, ensures confidentiality and integrity of communications.

How to get Zero Trust Architecture Products and Services

ORDERING GUIDANCE

Developing specific agency requirements for Zero Trust Architecture is a critical first step. This step requires that an agency understand the current environment and its goals for the future environment, including:

- Network Architecture – traditional/ZTA
- Security Posture and Policy
- Consolidation of services
- On-premise, cloud-based, or a hybrid approach
- Single-vendor, multi-vendor, or hybrid solutions

Regardless of the approach, GSA has Best-in-class (BIC) contract vehicles, such as [Enterprise Infrastructure Solutions \(EIS\)](#), available to customize a solution to best fit your ZTA needs:

These EIS services combine on an individual case basis to customize the solution and integrate industry leaders in ZTA using Task Order Unique CLINs (TUCs) that allow flexibility.

- Managed Mobility Service (MMS)
- Managed Network Service (MNS)
- Managed Security Service (MSS)
- Platform-as-a-Service (PaaS)
- Infrastructure-as-a-Service (IaaS)
- Software-as-a-Service (SaaS)
- Software-Defined Wide Area Networking Service (SDWANS)
- Service-Related Equipment (SRE)
- Service-Related Labor (SRL)

TABLE 1: EIS SERVICES SUPPORTING THE IDENTITY PILLAR OF THE ZERO TRUST MATURITY MODEL

<i>Pillar 1: Identity</i>	MMS	MNS	MSS	PaaS	IaaS	SaaS	SDWANS	SRE	SRL
User Inventory	YES	NO	YES	NO	NO	YES	NO	NO	NO
Conditional Access	YES	YES	YES	NO	NO	YES	YES	YES	YES
Multifactor Authentication	YES	NO	YES	NO	NO	YES	NO	YES	YES
Privileged Access Management	YES	NO	YES	NO	NO	YES	NO	NO	NO
Identity Federation & User Credentialing	NO	NO	YES	NO	NO	YES	NO	NO	NO
Behavioral, Contextual ID, and Biometrics	NO	NO	YES	NO	NO	YES	NO	NO	NO
Least Privileged Access	YES	YES	YES	YES	YES	YES	YES	NO	NO
Continuous Authentication	YES	NO	YES	NO	NO	YES	YES	NO	NO
Integrated ICAM Platform	NO	NO	YES	NO	NO	YES	NO	NO	NO

TABLE 2: EIS SERVICES SUPPORTING THE DEVICES PILLAR OF THE ZERO TRUST MATURITY MODEL

<i>Pillar 2: Devices</i>	MMS	MNS	MSS	IaaS	PaaS	SaaS	SDWANS	SRE	SRL
Device Inventory	YES	YES	YES	NO	NO	YES	NO	YES	YES
Device Detection and Compliance	YES	YES	YES	NO	NO	YES	NO	YES	YES
Device Authorization with Real Time Inspection	NO	NO	YES	NO	NO	YES	NO	NO	NO
Remote Access	YES	YES	YES	YES	YES	YES	YES	NO	NO
Partially & Fully Automated Asset, Vulnerability, and Patch Management	YES	NO	YES	NO	NO	YES	NO	NO	YES
Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	YES	NO	YES	NO	NO	YES	NO	NO	YES
Endpoint & Extended Detection & Response (EDR & XDR)	YES	NO	YES	YES	YES	YES	NO	NO	YES

TABLE 3: EIS SERVICES SUPPORTING THE NETWORKS PILLAR OF THE ZERO TRUST MATURITY MODEL

<i>Pillar 3: Networks</i>	MMS	MNS	MSS	IaaS	PaaS	SaaS	SDWANS	SRE	SRL
Data Flow Mapping	YES	YES	YES	YES	YES	YES	YES	NO	NO
Software Defined Networking (SDN)	NO	YES	NO	YES	YES	YES	YES	NO	NO
Macro-segmentation	NO	YES	NO	YES	YES	YES	YES	YES	NO
Micro-segmentation	NO	YES	NO	YES	YES	YES	YES	YES	NO

TABLE 4: EIS SERVICES SUPPORTING THE APPLICATIONS & WORKLOADS PILLAR OF THE ZERO TRUST MATURITY MODEL

<i>Pillar 4: Applications & Workloads</i>	MMS	MNS	MSS	IaaS	PaaS	SaaS	SDWANS	SRE	SRL
Application Inventory	NO	NO	YES	NO	NO	YES	NO	NO	YES
Secure Software Development & Integration	NO	NO	YES	NO	NO	YES	NO	NO	YES
Software Risk Management	NO	NO	YES	NO	NO	YES	NO	NO	NO
Resource Authorization & Integration	NO	NO	YES	NO	NO	YES	YES	NO	NO
Continuous Monitoring and Ongoing Authorizations	NO	NO	YES	NO	NO	YES	NO	NO	YES

TABLE 5: EIS SERVICES SUPPORTING THE DATA PILLAR OF THE ZERO TRUST MATURITY MODEL

<i>Pillar 5: Data</i>	MMS	MNS	MSS	IaaS	PaaS	SaaS	SDWANS	SRE	SRL
Data Catalog Risk Assessment	NO	NO	YES	NO	NO	NO	NO	NO	NO
DoD Enterprise Data Governance	NO	NO	NO	NO	NO	NO	NO	NO	YES
Data Labeling and Tagging	NO	YES	YES	NO	NO	YES	NO	NO	NO
Data Monitoring and Sensing	NO	NO	YES	NO	NO	YES	NO	NO	NO
Data Encryption & Rights Management	NO	NO	YES	NO	NO	NO	NO	YES	NO
Data Loss Prevention (DLP)	NO	NO	YES	NO	NO	YES	NO	NO	NO
Data Access Control	NO	NO	YES	NO	NO	YES	YES	NO	NO

TABLE 6: EIS SERVICES SUPPORTING THE VISIBILITY AND ANALYTICS CROSS-CUTTING CAPABILITY OF THE ZERO TRUST MATURITY MODEL

<i>Cross-Cutting Capability 1: Visibility and Analytics</i>	MMS	MNS	MSS	IaaS	PaaS	SaaS	SDWANS	SRE	SRL
Log All Traffic (Network, Data, Apps, Users)	YES	YES	YES	YES	YES	YES	YES	NO	NO
Security Information and Event Management (SIEM)	NO	NO	YES	NO	NO	YES	NO	NO	NO
Common Security and Risk Analytics	YES	NO	YES	NO	NO	YES	NO	NO	YES
User and Entity Behavior Analytics	NO	NO	YES	NO	NO	YES	NO	NO	YES
Threat Intelligence Integration	NO	NO	YES	NO	NO	YES	NO	NO	YES
Automated Dynamic Policies	YES	YES	YES	NO	NO	NO	YES	NO	NO

TABLE 7: EIS SERVICES SUPPORTING THE AUTOMATION AND ORCHESTRATION CROSS-CUTTING CAPABILITY OF THE ZERO TRUST MATURITY MODEL

<i>Cross-Cutting Capability 2: Automation and Orchestration</i>	MMS	MNS	MSS	IaaS	PaaS	SaaS	SDWANS	SRE	SRL
Policy Decision Point (PDP) & Policy Orchestration	YES	NO	YES	NO	NO	NO	NO	NO	YES
Critical Process Automation	NO	NO	NO	NO	NO	NO	NO	NO	YES
Machine Learning	YES	YES	YES	YES	YES	YES	YES	NO	YES
Artificial Intelligence	YES	YES	YES	YES	YES	YES	YES	NO	YES
Security Orchestration, Automation & Response (SOAR)	YES	NO	YES	NO	NO	YES	NO	NO	YES
API Standardization	NO	NO	NO	NO	NO	NO	NO	NO	YES
Security Operations Center (SOC) & Incident Response (IR)	NO	NO	YES	NO	NO	NO	NO	YES	YES

TABLE 8: EIS SERVICES SUPPORTING THE GOVERNANCE CROSS-CUTTING CAPABILITY OF THE ZERO TRUST MATURITY MODEL

<i>Cross-Cutting Capability 3: Governance</i>	MMS	MNS	MSS	IaaS	PaaS	SaaS	SDWANS	SRE	SRL
Documentation Development	YES	YES	YES	YES	YES	YES	YES	YES	YES
Policy Enforcement	YES	NO	YES	NO	NO	NO	YES	NO	YES
Compliance Monitoring	YES	NO	YES	NO	NO	YES	NO	NO	YES
Risk Assessment	NO	NO	YES	NO	NO	NO	NO	NO	YES

GSA IS HERE TO HELP

If you would like more information on the topics covered in this paper, please reach out to your designated GSA representative at <https://gsa.gov/nspsupport> or call 855-482-4348 to get in touch. GSA has multiple offerings for products, services, and solutions to support your planning, implementation, and continued support of the components of your ZTA. Thank you for reading!

Zero Trust Architecture Lessons Learned and Frequently Asked Questions

How do I gain buy-in from leadership and operations?

Use a top-down approach from leadership and a bottom-up strategy at the operational level to help them understand and overcome cultural and bureaucratic constraints.

Is Zero Trust Architecture a managed service?

ZTA can be considered a managed network service that actively monitors and controls access by continuously verifying user and device identities.

What if I can't modernize my environment?

Build ZTA around your environment instead of within it by creating isolated secure zones to protect critical operations.

Does ZTA replace Virtual Private Networks?

ZTA offers a more granular way to control application access for remote users and can act as an alternative to VPNs, depending on organizational needs.

Does ZTA require a single provider partner?

ZTA relies on an integrated multi-partner approach to ensure comprehensive protection of all endpoints.

What is the greatest challenge in implementing ZTA?

The scope of implementation presents challenges due to the vast amount of data, endpoints, and information that must be identified, protected, and isolated.

Appendix A - Abbreviations

Abbreviation	Full Phrase
ACSC	Australian Cyber Security Centre
AI	Artificial Intelligence
ASD	Australian Signals Directorate
AT&T	American Telephone and Telegraph Company
BIC	Best-in-class
CASB	Cloud Access Security Broker
CCCS	Canadian Cyber Security Centre
CISA	Cybersecurity and Infrastructure Security Agency
CLIN	Contract Line Item Number
CSP	Cloud Service Provider
DNS	Domain Name Service
DoD	Department of Defense
EIS	Enterprise Infrastructure Solutions
EO	Executive Order
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Management Act
FWaaS	Firewall-as-a-Service
GAO	Government Accountability Office
GSA	General Services Administration
GWAC	Governmentwide Acquisition Contract
HTTP	Hypertext Transfer Protocol

Abbreviation	Full Phrase
IaaS	Infrastructure-as-a-Service
ICB	Individual Case Basis
IPS	Internet Protocol Service
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information Technology
MAS	Multiple Award Schedule
MFA	Multi-factor Authentication
MNS	Managed Network Service
MSS	Managed Security Service
NCSC-NZ	New Zealand's National Cyber Security Centre
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OT	Operational Technology
PaaS	Platform-as-a-Service
PEP	Policy Enforcement Points
PRC	People's Republic of China
Q&A	Questions and Answers
SaaS	Software-as-a-Service
SASE	Secure Access Service Edge
SD-WAN	Software-Defined Wide Area Network

Abbreviation	Full Phrase
SDP	Software-Defined Perimeter
SDWANS	Software-Defined Wide Area Network Service
SRE	Service-Related Equipment
SRL	Service-Related-Labor
SSE	Security Service Edge
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TIC	Trusted Internet Connections
TUC	Task Order Unique CLIN
UCaaS	United-Communications-as-a-Service
VPN	Virtual Private Network
ZTA	Zero Trust Architecture
ZTMM	Zero Trust Maturity Model
ZTNA	Zero Trust Network Access

1 <https://csrc.nist.gov/projects/post-quantum-cryptography> - last accessed 3/27/2024
2 <https://www.congress.gov/bill/115th-congress/house-bill/6227>
3 <https://www.quantum.gov>

