DocuSign Envelope ID: 2A9B4AF6-0C64-4DB5-8B8E-D1FA887E91ED

Zero Trust Architecture (ZTA)

Buyer's Guide

GSA June 2021 Version 1.0

DocuSign Envelope ID: 2A9B4AF6-0C64-4DB5-8B8E-D1FA887E91ED

Table of Contents

1. Executive Summary 1
2. Purpose 1
3. Audience 1
4. What is a Zero Trust Model? 1
5. NIST ZTA 2
   5.1 Tenets of ZTA 2
   5.2 Logical Components of ZTA 3
6. Pillars of ZTA 3
7. Implementing a ZTA 4
8. Key Considerations for Products, Services, and Solutions 4
9. Contact Information for This ZTA Buyer's Guide 5
Appendix A – GSA-Offered Products, Services, and Solutions for ZTA 6
Appendix B – GSA Zero Trust Reference Architecture 19

DocuSign Envelope ID: 2A9B4AF6-0C64-4DB5-8B8E-D1FA887E91ED

Foreword

This guide is intended to assist agencies with acquiring products and services to support and align with their Zero Trust Security Strategy. We fully recognize that each agency starts the process of implementing a Zero Trust Strategy from their own unique place based on their current IT Security maturity and must address the most critical and foundational aspects of a Zero Trust to address their own unique needs.

There is no Zero Trust "Silver Bullet," and no single product is likely to achieve Zero Trust alone. Zero Trust is, in fact, more like a journey than a destination. Moving to a Zero Trust architecture will take time, and agencies will be at different levels of achievement. GSA's Highly Adaptive Cybersecurity Services (HACS), Continuous Diagnostics and Mitigation (CDM) Tools special item numbers (SINs), and many of our other solutions can be utilized to support efforts to design and deploy architectures that follow the zero trust basic tenets.

The information provided in this guide can help you identify a broad range of products and services to help you develop, implement, and mature your Zero Trust implementation plans. GSA's IT Category is available to answer any questions and provide subject matter expertise related to any aspect of this guide and any other IT needs.

DocuSigned by:
Allen Hill
A14C728B5EFE455...
Allen Hill
Deputy Assistant Commissioner
Category Management (CM)
Information Technology Category (ITC)
Federal Acquisition Service (FAS)

DocuSign Envelope ID: 2A9B4AF6-0C64-4DB5-8B8E-D1FA887E91ED

1. Executive Summary

To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must continue to modernize its approach to cybersecurity. The approach to doing so will focus on increasing the adoption of security best practices, increasing adoption of a Zero Trust Architecture (ZTA), and accelerating movement to secure cloud services in a way that appropriately enhances cybersecurity including visibility of threat activity and risk.

2. Purpose

The purpose of the buyer's guide is to assist customers with acquiring products and services that align with their Zero Trust Security Strategy.

This guide introduces an approach to ZTA which represents a fusion of different Zero Trust security models from the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE), American Council for Technology - Industry Advisory Council (ACT-IAC), and best practices from industry leaders. This approach includes eight (8) pillars of Zero Trust: User, Device, Network, Infrastructure, Application, Data, Visibility and Analytics, and Orchestration and Automation. The pillars are defined and explained later in this document.

3. Audience

This buyer's guide is for acquisition, network architect, and cybersecurity professionals who are seeking to implement a ZTA. Familiarity with Software-Defined Networking (SDN), access management, identity management, and firewall concepts are a prerequisite, as well as knowledge of Zero Trust core components. The core components are highlighted in NIST Special Publication (SP) 800-207, *Zero Trust Architecture*, dated August 2020.

4. What is a Zero Trust Model?

Zero Trust is not a technology, but a shift in approach to cybersecurity. In 2010, a Zero Trust model was architected by John Kindervag, Principal Analyst at Forrester Research, who coined the term "Zero Trust" network architecture. Kindervag based the proposed architecture on the understanding that the typical "defense-in-depth" approach was flawed due to the inherit trust model. He asserted, "We needed a new model that allows us to build security into the DNA of the network itself." Essentially, in the Zero Trust model, all traffic is deemed hostile. Kindervag noted five (5) concepts to make Zero Trust Architecture actionable:

1. All resources must be accessed in a secure manner
2. Access control is on a need-to-know basis
3. Do not trust people, verify what they are doing
4. Inspect all log traffic coming in on the network for malicious activity
5. Design networks from the inside out

DocuSign Envelope ID: 2A9B4AF6-0C64-4DB5-8B8E-D1FA887E91ED

5. NIST ZTA

NIST SP 800-207 contains cybersecurity measures and guidelines highlighting the ZTA core components. Specifically, the SP provides Federal agencies with detailed recommendations on how to maintain and protect an agency's data using Zero Trust systems, which prioritizes the safeguarding of individual resources rather than network segments. Zero Trust initiatives provide added security in modern enterprise networks which include cloud-based assets and remote users. In short, Zero Trust shifts focus away from protecting the network perimeter and prohibits access until the access request, identification of the requestor, and requested resource are validated. After a request is granted for accessing Zero Trust networks, security teams are required to continuously monitor how the organization is using and distributing the data.

5.1 Tenets of ZTA

Zero Trust strictly follows a set of seven (7) tenets that regulate user access and data management across all enterprises. These include:

1. **Rigorously enforce authentication and authorization –** All resources require mandatory authentication, often paired with technologies such as multifactor authentication (MFA), before granting access. According to Zero Trust principles, no account has implicit access without explicit permission.
2. **Maintain data integrity –** Enterprises measure and monitor the security and integrity of all owned and associated assets, assess their vulnerabilities, patch levels, and other potential cybersecurity threats.
3. **Gather data for improved security –** Enterprises should collect current information from multiple sources, such as network infrastructure and communication, to regulate and improve security standards.
4. **Consider every data source and computing device as a resource –** Enterprises should consider any device with access to an enterprise-level network as a resource.
5. **Keep all communication secured regardless of network location –** Physical network locations alone should never imply trust. People connecting via enterprise and non-enterprise networks must undergo the same security requirements for resource access.
6. **Grant resource access on a per-session basis** – Enterprises should enforce a least-privilege policy: a user should only be granted the minimum privileges required to complete a task. Every access request requires evaluation and, when granted, does not immediately provide access to other resources. Users will need to submit a separate request for subsequent data access.
7. **Moderate access with a dynamic policy –** Enterprises need to protect resources with a transparent policy that continuously defines resources, accounts, and the type of privileges linked to each account. The process may involve attributes, such as device characteristics (i.e., software versions) and network locations.

5.2 Logical Components of ZTA

NIST SP 800-207 explains the functionality of three (3) logical components to establish and maintain a ZTA. These components include:

1. **Policy Engine (PE)** - The PE provides the final decision in granting access to a resource.
2. **Policy Administrator (PA)** - The PA establishes access to a resource.
3. **Policy Enforcement Point (PEP)** - PEPs serve as a system gateway for activating, monitoring, and terminating connections between authorized users and their accessed resources.

6. Pillars of ZTA

The foundational ZTA pillars depicted in this guide represent a fusion of several Zero Trust security models currently in use by leading industry vendors and academic sources. Zero Trust security models currently range between five and seven pillars. For the purposes of facilitating an acquisition-based perspective, GSA chose to represent a combination of eight (8) unique pillars. The following table provides a description of each pillar.

Zero Trust Pillars	
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.

When evaluating a solution that aligns with an Agency's planned deployment of a Zero Trust Architecture, agencies should consider how well the product or service addresses these eight (8) pillars and to what extent.

DocuSign Envelope ID: 2A9B4AF6-0C64-4DB5-8B8E-D1FA887E91ED

7. Implementing a ZTA

When implementing a ZTA, an agency must first identify a protect surface. The protect surface contains the agency's most valuable Data, Assets, Applications, and Services (DAAS), which represents the most critical elements of an agency's operation. From a design perspective, the protect surface should be relatively small in comparison to the entire attack surface so that it is easier to identify.

With the protect surface identified, the agency should then focus on analyzing both the ingress and egress network flows in relationship to the protect surface. Understanding who the users are, which applications they are using, and how they are connecting is the only way to determine and enforce policy that ensures secure access to the data. This interdependencies analysis between the DAAS, infrastructure, services, and users will reveal where precisely the agency must put controls in place which results in defining multiple micro-perimeters for each DAAS.

By design, these micro-perimeters will be defined as close to the protect surface as possible and will logically move with the protect surface, wherever it goes. The agency will effectively create micro-perimeters by deploying a segmentation gateway(s) to ensure only known allowed traffic or legitimate applications have access to the protect surface.

A segmentation gateway is a network component (hardware or software) capable of granular enforcement of access control at the Application Layer (Layer 7). The segmentation gateway functions as the PEP, utilizing a policy based on the Kipling Method, which defines Zero Trust policy based on who, what, when, where, why, and how. This Zero Trust policy determines who can transit a micro-perimeter at any point in time, preventing unauthorized user access and the exfiltration of sensitive data.

Once the agency has built a Zero Trust policy around the protect surface, agencies must continue to monitor and maintain in real-time, refining the protect surface, interdependencies not yet accounted for, and ways to improve policy.

8. Key Considerations for Products, Services, and Solutions

On some level, any security vendor could claim to provide a ZTA offering. Agencies should follow the guidance found in NIST SP 800-207, which provides systematic guidelines for updating network cybersecurity in a world where remote work is prevalent, and traditional network defenses are inadequate. In following this guidance, agencies can improve their security posture by implementing the Zero Trust principles documented in NIST SP 800-207 with optimal configurations according to their business needs.

It is important to note that although vendors have made great strides in building Zero Trust based solutions, there is no single end-to-end, comprehensive Zero Trust Network solution. Additionally, agencies should realize it is not necessary to rip and replace existing cybersecurity

DocuSign Envelope ID: 2A9B4AF6-0C64-4DB5-8B8E-D1FA887E91ED

tools, but rather take small incremental steps in deploying ZTA tools on top of existing infrastructure.

In developing a ZTA implementation strategy for essential Zero Trust offerings such as identity and access management, encryption, multifactor authentication, and next generation firewalls, agencies should consider General Services Administration (GSA) Offered Products, Services, and Solutions for a ZTA. In designing a ZTA, agencies may also leverage the logical diagram depicted in Appendix B, GSA Zero Trust Reference Architecture.

9. Contact Information for This ZTA Buyer's Guide

Contact information for this ZTA Buyer's Guide is as follows:

- E-mail ITSecurityCM@gsa.gov for Customer Support with the ZTA Buyer's Guide
- E-mail RMASS@gsa.gov for any ZTA buyer's guide comments, suggestions, and options
- Contact the respective acquisition support for the GSA Schedules identified in Appendix A of this ZTA Buyer's Guide

DocuSign Envelope ID: 2A9B4AF6-0C64-4DB5-8B8E-D1FA887E91ED

Appendix A – GSA-Offered Products, Services, and Solutions for ZTA

The below table lists GSA schedules to obtain ZTA related products, services, and solutions.

Zero Trust Buyer's Guide for GSA-Offered Products, Services, and Solutions			
Pillar	**Component**	**Component Description**	**GSA Technology Purchasing Program**
User	Access Management • Identity Access Management • Privilege Access Management • Whitelisting	Defines and manages the roles and access privileges of individual network users and the circumstances in which users are granted (or denied) those privileges.	For purchasing Identity, Credential and Access Management (ICAM) Tools, see Special Item Number (SIN) 541519ICAM
	Authentication • Single Sign-On • Multifactor Authentication • Passwordless Authentication	Provides an assertion, such as the identity of a computer system user.	GSA eLibrary SIN 541519ICAM GSA eLibrary Alliant 2 For purchasing CDM Tools, see SIN 541519CDM
	User and Event Behavior Analytics	Uses machine learning and deep learning to model the behavior of users on networks and highlights anonymous behavior that could be the sign of a cyber-attack.	For purchasing CDM Tools, see SIN 541519CDM EIS leveraging the Managed Security Service (MSS), Managed Network Service (MNS), Managed Mobility Service (MMS), Software Defined Wide Area Network Service (SDWANS), and/or Software-as-a-Service (SaaS)
	Identity Management	A framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources.	GSA eLibrary SIN 541519ICAM GSA eLibrary VETS 2 GSA eLibrary Mobile Identity Management SIN 517312
	Conditional Access	Protects content by requiring certain criteria to be met before granting access to the content.	GSA eLibrary SIN 541519ICAM EIS leveraging the Managed Security Service (MSS), Managed Network Service (MNS), Managed Mobility Service (MMS), Software Defined Wide

Zero Trust Buyer's Guide for GSA-Offered Products, Services, and Solutions			
Pillar	**Component**	**Component Description**	**GSA Technology Purchasing Program**
			Area Network Service (SDWANS), and/or Software-as-a-Service (SaaS)
	Dynamic Risk Scoring	Uses artificial intelligence to score users as to how infringing and high risk they are.	EIS leveraging the Managed Security Service (MSS), Managed Network Service (MNS), Managed Mobility Service (MMS), and/or Software-as-a-Service (SaaS)
Device	Vulnerability Management	The cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating vulnerabilities.	GSA eLibrary Alliant 2 GSA eLibrary VETS2 GSA eLibrary SIN 54151HACS GSA eLibrary IT Professional Services SIN 54151S EIS leveraging the Managed Security Service (MSS), and/or Software-as-a-Service (SaaS)
	Device Security	A tool that is designed to protect sensitive information stored on and transmitted by laptops, smartphones, tablets, wearables, and other portable devices.	For purchasing Wireless Mobility Solutions, see SIN 517312 For purchasing CDM Tools, see SIN 541519CDM EIS leveraging the Managed Security Service (MSS), Managed Network Service (MNS), Managed Mobility Service (MMS), Software Defined Wide Area Network Service (SDWANS), and Software-as-a-Service (SaaS)
	Device Identity	A tool used to collect unique information about a device that can then be used to link	GSA eLibrary SIN 541519ICAM

Zero Trust Buyer's Guide for GSA-Offered Products, Services, and Solutions			
Pillar	**Component**	**Component Description**	**GSA Technology Purchasing Program**
		the device to an individual user.	GSA eLibrary VETS 2 For purchasing Wireless Mobility Solutions, see SIN 517312 EIS leveraging the Managed Security Service (MSS), Managed Mobility Service (MMS), and Software-as-a-Service (SaaS)
	Device Compliance	A tool used to track the policy compliance of all enrolled devices. A compliant device means it has received specified assigned configuration policies.	Alliant 2 GSA eLibrary SIN 541990IPS GSA eLibrary SIN 541990RISK EIS leveraging the Managed Security Service (MSS), Managed Mobility Service (MMS), and/or Software-as-a-Service (SaaS)
	Device Authentication	A security mechanism designed to ensure that only authorized devices can connect to a given network, site, or service.	GSA eLibrary SIN 541519ICAM GSA eLibrary Alliant 2 EIS leveraging the Managed Security Service (MSS), Managed Mobility Service (MMS), and/or Software-as-a-Service (SaaS)
	Device Management	The process of managing the implementation, operation, and maintenance of a physical and/or virtual device.	GSA eLibrary SIN 541519ICAM GSA eLibrary Alliant 2 GSA eLibrary VETS2 For purchasing Wireless Mobility Solutions, see SIN 517312 GSA eLibrary SIN 54151HACS

Zero Trust Buyer's Guide for GSA-Offered Products, Services, and Solutions			
Pillar	**Component**	**Component Description**	**GSA Technology Purchasing Program**
			GSA eLibrary IT Professional Services SIN 54151S For purchasing CDM Tools, see SIN 541519CDM EIS leveraging the Managed Security Service (MSS), Managed Mobility Service (MMS), and/or Software-as-a-Service (SaaS)
	Device Inventory • Hardware Management • Software Management	A tool that allows tracking of network devices and all of their relevant software and hardware.	GSA eLibrary Alliant 2 GSA eLibrary 8ASTARS2 For purchasing CDM Tools, see SIN 541519CDM EIS leveraging the Managed Security Service (MSS), Managed Network Service (MNS), Managed Mobility Service (MMS), Software Defined Wide Area Network Service (SDWANS), and/or Software-as-a-Service (SaaS)
	Enterprise Mobility Management	The set of people, processes, and technology focused on managing mobile devices, wireless networks, and other mobile computing services in a business context.	For purchasing Wireless Mobility Solutions, see SIN 517312 EIS leveraging the Managed Mobility Service (MMS), Software-as-a-Service (SaaS), and/or the Managed Security Service (MSS)
Network	Zero Trust Architecture	The design of a communications network using the Zero Trust model. It includes the physical and logical layout of the network; the framework of accepted standards and	EIS leveraging the Managed Network Service (MNS) and the Managed Security Service (MSS)

Zero Trust Buyer's Guide for GSA-Offered Products, Services, and Solutions			
Pillar	**Component**	**Component Description**	**GSA Technology Purchasing Program**
		specifications of elements, equipment, services, protocols and functions, growth and change assumptions; and high-level operational principles and procedures.	
	Software-Defined Networking • Software-Defined Wide Area Network • Software-Defined Perimeter	An approach to network management that enables a dynamic, programmatically efficient network configuration in order to improve network performance and monitoring, making it more like cloud computing than traditional network management.	EIS leveraging the Software Defined Wide Area Network Service (SDWANS), Managed Security Service (MSS), Software-as-a-Service (SaaS), and/or the Managed Network Service (MNS)
	Segmentation • Micro segmentation • Macro segmentation	An approach in computer networking that is the act or practice of splitting a computer network into subnetworks, each being a network segment.	EIS leveraging the Software Defined Wide Area Network Service (SDWANS), Managed Security Service (MSS), Software-as-a-Service (SaaS), and/or the Managed Network Service (MNS)
	Network Security	A set of rules and configurations designed to protect the integrity, confidentiality, and accessibility of computer networks and data using both software and hardware technologies.	GSA eLibrary Alliant 2 GSA eLibrary VETS2 GSA eLibrary SIN 54151HACS GSA eLibrary IT Professional Services SIN 54151S EIS leveraging the Managed Security Service (MSS), Managed Network Service (MNS), Managed Mobility Service (MMS), Software Defined Wide Area Network Service (SDWANS), and/or Software-as-a-Service (SaaS)

Zero Trust Buyer's Guide for GSA-Offered Products, Services, and Solutions			
Pillar	**Component**	**Component Description**	**GSA Technology Purchasing Program**
	Zero Trust Network Access	A category of technologies that provides secure remote access to applications and services based on defined access control policies.	GSA eLibrary Alliant 2 GSA eLibrary VETS2 GSA eLibrary SIN 54151HACS GSA eLibrary IT Professional Services SIN 54151S EIS leveraging the Managed Security Service (MSS), Managed Network Service (MNS), Managed Mobility Service (MMS), Software Defined Wide Area Network Service (SDWANS), and/or Software-as-a-Service (SaaS)
	Network Access Control	Solutions that support network visibility and access management through policy enforcement on devices and users of corporate networks.	GSA eLibrary Alliant 2 GSA eLibrary VETS2 GSA eLibrary SIN 54151HACS GSA eLibrary IT Professional Services SIN 54151S EIS leveraging the Managed Security Service (MSS), Managed Network Service (MNS), Managed Mobility Service (MMS), Software Defined Wide Area Network Service (SDWANS), and/or Software-as-a-Service (SaaS)
	Transport Encryption	Keeps data encrypted while in transit between the enterprise server and the device itself.	GSA eLibrary Alliant 2 EIS leveraging the Virtual Private Network Service

Zero Trust Buyer's Guide for GSA-Offered Products, Services, and Solutions			
Pillar	**Component**	**Component Description**	**GSA Technology Purchasing Program**
			(VPNS), Managed Security Service (MSS), Managed Network Service (MNS), Managed Mobility Service (MMS), Software Defined Wide Area Network Service (SDWANS), and/or Software-as-a-Service (SaaS)
	Session Protection	The process of keeping session communication between a server and a client secure.	GSA eLibrary Alliant 2 EIS leveraging the Managed Security Service (MSS), Managed Network Service (MNS), Managed Mobility Service (MMS), Software Defined Wide Area Network Service (SDWANS), and/or Software-as-a-Service (SaaS)
Infrastructure	Cloud Workload Protection	The process of keeping workloads that move across different cloud environments secure.	Federal Risk and Authorization Management Program (FedRAMP) EIS leveraging the Software Defined Wide Area Network Service (SDWANS), Virtual Private Network Service (VPNS), Managed Security Service (MSS), Software-as-a-Service (SaaS), and/or the Managed Network Service (MNS)
	Cloud Access Security Broker	On-premises or cloud-based software that sits between cloud service users and cloud applications and monitors all activity and enforces security policies.	Federal Risk and Authorization Management Program (FedRAMP) EIS leveraging the Managed Security Service (MSS) and/or Software-as-a-Service (SaaS)
	Software-as-a-Service (SaaS) Management Platform	The business practice of proactively monitoring and managing the purchasing, onboarding, licensing, renewals, and offboarding of all SaaS applications within	Federal Risk and Authorization Management Program (FedRAMP) EIS leveraging Software-as-a-Service (SaaS) and the

Zero Trust Buyer's Guide for GSA-Offered Products, Services, and Solutions			
Pillar	**Component**	**Component Description**	**GSA Technology Purchasing Program**
		a company's technology portfolio.	Managed Security Service (MSS)
	Secure Access Service Edge	Simplifies wide area networking and security by delivering both as a cloud service directly to the source of connection rather than the enterprise data center.	Federal Risk and Authorization Management Program (FedRAMP) EIS leveraging the Software Defined Wide Area Network Service (SDWANS), Managed Security Service (MSS), Managed Mobility Service (MMS), Software-as-a-Service (SaaS), and/or the Managed Network Service (MNS)
Application	Web Application Firewall	A specific form of application firewall that filters, monitors, and blocks Hypertext Transfer Protocol (HTTP) traffic to and from a web service.	CDM Tools SIN 541519CDM EIS leveraging the Managed Security Service (MSS) and/or Software-as-a-Service (SaaS)
	Application Security	Encompasses measures taken to improve the security of an application often by finding, fixing, and preventing security vulnerabilities.	Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Alliant 2 GWAC VETS 2 EIS leveraging the Managed Security Service (MSS), Managed Mobility Service (MMS), and/or Software-as-a-Service (SaaS)
	Container Security	The process of implementing security tools and policies that will give the assurance that everything in the container is running as intended, and only as intended. This includes protecting the infrastructure, the software supply chain, runtime, and everything in between.	EIS leveraging the Managed Security Service (MSS), Managed Mobility Service (MMS), and/or the Cloud Services (IaaS, PaaS, SaaS)

Zero Trust Buyer's Guide for GSA-Offered Products, Services, and Solutions			
Pillar	**Component**	**Component Description**	**GSA Technology Purchasing Program**
	Secure Access Cloud	A SaaS solution that enables more secure and granular access management to any corporate resource hosted on-premises or in the cloud.	Federal Risk and Authorization Management Program (FedRAMP) EIS leveraging the Managed Security Service (MSS), and Software-as-a-Service (SaaS)
	Isolation	A sandboxing technology that provides attack surface reduction by applying the principle of least privilege.	EIS leveraging the Managed Security Service (MSS), Managed Mobility Service (MMS), and Software-as-a-Service (SaaS)
	Any Device Access	Provides instant and secure access to files at any given moment on any device.	EIS leveraging the Managed Security Service (MSS), Managed Mobility Service (MMS), and Software-as-a-Service (SaaS)
Data	Encryption • Data-at-Rest • Data-in-Transit • Data-in-Use	The process of encoding information.	Alliant 2 GWAC CDM Tools SIN 541519CDM IT Professional Services SIN 54151S VETS 2 EIS leveraging the Software Defined Wide Area Network Service (SDWANS), Virtual Private Network Service (VPNS), Managed Security Service (MSS), Managed Mobility Service (MMS), Software-as-a-Service (SaaS), and the Managed Network Service (MNS)
	Data Security • Data Discovery and Classification • Data Protection	The process of protecting data from unauthorized access and data corruption throughout its life cycle.	VETS 2 IT Professional Services SIN 54151S Alliant 2 GWAC

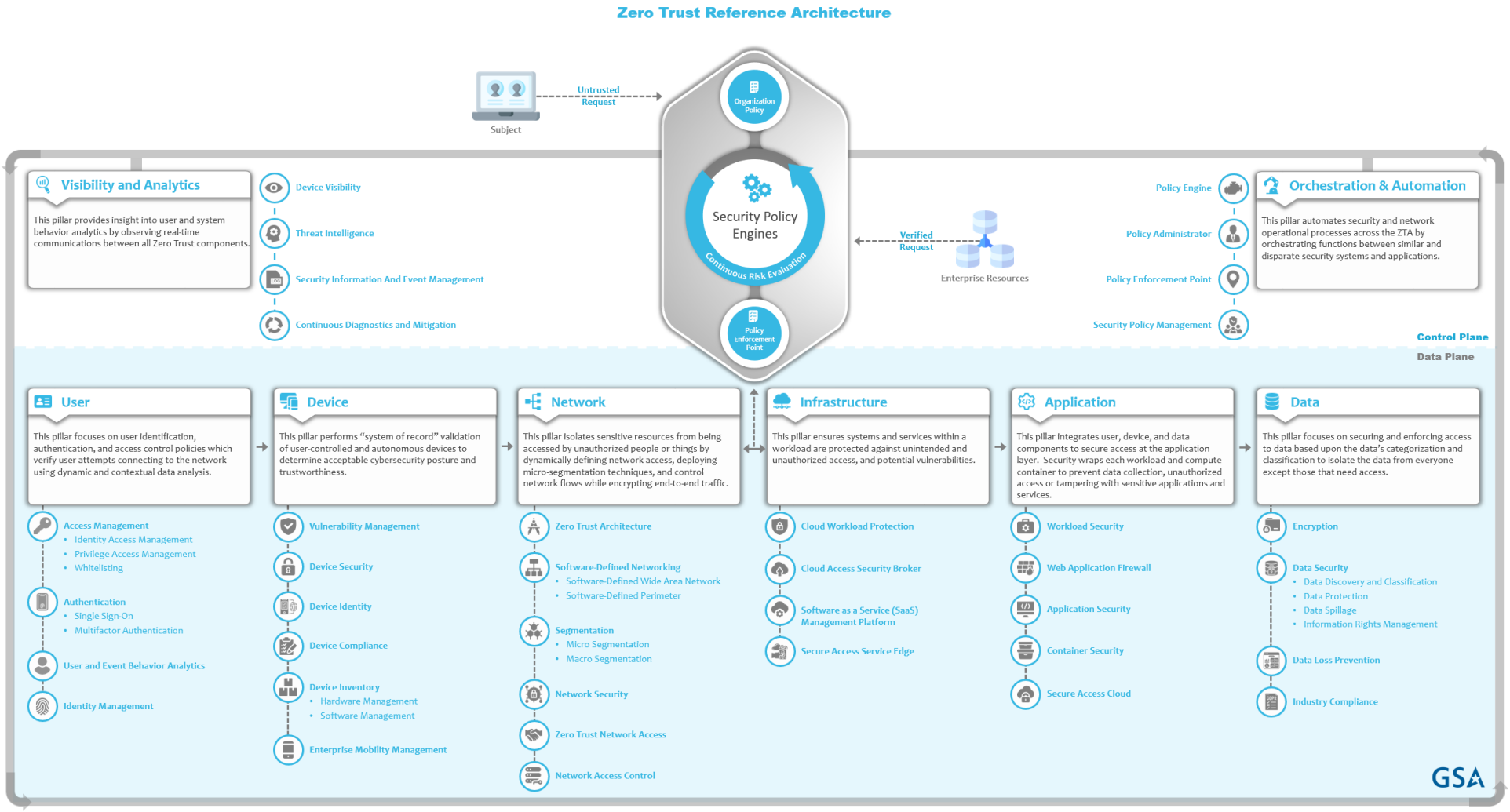
Zero Trust Buyer's Guide for GSA-Offered Products, Services, and Solutions			
Pillar	**Component**	**Component Description**	**GSA Technology Purchasing Program**
	• Data Spillage • Information Rights Management		CDM Tools SIN 541519CDM EIS leveraging the Managed Security Service (MSS), Managed Mobility Service (MMS), and Software-as-a-Service (SaaS)
	Data Loss Prevention	Detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting, and blocking sensitive data while in use, in motion, and at rest.	VET S 2 CDM Tool SIN 541519CDM IT Professional Services SIN 54151S Highly Adaptive Cybersecurity Services SIN 54151HACS EIS leveraging the Managed Security Service (MSS), Managed Mobility Service (MMS), and Software-as-a-Service (SaaS)
	Industry Compliance	Ensures that organizations take steps to comply with relevant laws, policies, and regulations.	Alliant 2 GWAC IT Professional Services SIN 54151S Highly Adaptive Cybersecurity Services SIN 54151HACS EIS
	Integrity	Refers to the accuracy and consistency (validity) of data over its life cycle	Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S
	Classification	The process of analyzing structured or unstructured data and organizing it into categories based on file type, contents, and other metadata.	Alliant 2 GWAC EIS leveraging the Managed Security Service (MSS) and Managed Network Service (MNS)

Zero Trust Buyer's Guide for GSA-Offered Products, Services, and Solutions			
Pillar	**Component**	**Component Description**	**GSA Technology Purchasing Program**
Visibility and Analytics	Device Visibility	Refers to visibility into the traffic, devices, and behaviors in complex enterprise Information Technology (IT) networks, which are constantly evolving, and continually connecting more and more networked devices.	Alliant 2 GWAC CDM Tools SIN 541519CDM VETS 2 EIS leveraging the Managed Security Service (MSS), Managed Mobility Service (MMS), and Software-as-a-Service (SaaS)
	Threat Intelligence	Evidence-based knowledge, including context, mechanisms, indicators, implications, and action-oriented advice about an existing or emerging menace or hazard to assets.	For purchasing Highly Adaptive Cybersecurity Services, see SIN 54151HACS IT Professional Services SIN 54151S EIS leveraging the Managed Security Service (MSS), Managed Mobility Service (MMS), and Software-as-a-Service (SaaS)
	Security Information and Event Management (SIEM)	A subsection within the field of computer security, where software products and services combine security information management and security event management.	For purchasing Highly Adaptive Cybersecurity Services, see SIN 54151HACS IT Professional Services SIN 54151S EIS leveraging the Managed Security Service (MSS) and Software-as-a-Service (SaaS)
	Continuous Diagnostics and Mitigation (CDM) system	Gathers information about the enterprise asset's current state and applies updates to configuration and software components.	CDM Tools, SIN 541519CDM VETS 2 EIS leveraging the Managed Security Service (MSS), Managed Mobility Service (MMS), and Software-as-a-Service (SaaS)

Zero Trust Buyer's Guide for GSA-Offered Products, Services, and Solutions			
Pillar	**Component**	**Component Description**	**GSA Technology Purchasing Program**
Orchestration and Automation	Policy Engine (PE)	Responsible for the ultimate decision to grant access to a resource for a given subject.	EIS leveraging the Managed Security Service (MSS), Managed Network Service (MNS), Managed Mobility Service (MMS), Software Defined Wide Area Network Service (SDWANS), and the Software-as-a-Service (SaaS)
	Policy Administrator (PA)	Responsible for establishing and/or shutting down the communication path between a subject and a resource.	EIS leveraging the Managed Security Service (MSS), Managed Network Service (MNS), Managed Mobility Service (MMS), Software Defined Wide Area Network Service (SDWANS), and the Software-as-a-Service (SaaS)
	Policy Enforcement Point (PEP)	Responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource.	EIS leveraging the Managed Security Service (MSS), Managed Network Service (MNS), Managed Mobility Service (MMS), Software Defined Wide Area Network Service (SDWANS), and the Software-as-a-Service (SaaS)
	Security Policy Management	The process of identifying, implementing, and managing the rules and procedures that all individuals must follow when accessing and using an organization's IT assets and resources.	Alliant 2 GWAC IT Professional Services SIN 54151S Highly Adaptive Cybersecurity Services SIN 54151HACS VETS 2 EIS leveraging the Managed Security Service (MSS), Managed Network Service (MNS), Managed Mobility Service (MMS), Software Defined Wide Area Network Service (SDWANS), and the

DocuSign Envelope ID: 2A9B4AF6-0C64-4DB5-8B8E-D1FA887E91ED

Zero Trust Buyer's Guide for GSA-Offered Products, Services, and Solutions			
Pillar	**Component**	**Component Description**	**GSA Technology Purchasing Program**
			Software-as-a-Service (SaaS)

Appendix B – GSA Zero Trust Reference Architecture

The below diagram depicts an industry standard logical Zero Trust Architecture. **Note:** Not all the components listed in Appendix A are listed in the GSA Zero Trust Reference Architecture. Only core components are listed due to space limitations.