



U.S. General Services Administration



Zero Trust Strategy Buyer's Guide

Department of Defense (DoD) Zero Trust Strategy

Table of Contents

1	Executive Summary	1
2	Purpose.....	1
3	Audience.....	1
4	History of the DoD ZT Strategy	2
5	What is DoD's Zero Trust Strategy?	2
6	Applicability	2
7	DoD ZT Strategy Vision	3
8	DoD ZT Strategy Outcomes	3
9	DoD ZT Strategy Approach.....	4
10	DoD Zero Trust Strategic Goals and Objectives	7
11	DoD Zero Trust Execution Approach.....	7
12	High-Level Capability Roadmap	7
13	Measurement and Metrics	8
14	Governance.....	8
15	Key Considerations for Products, Services, and Solutions	8
16	Summary.....	9
17	ZT Strategy Buyer's Guide Contact Information	9
	Appendix A – GSA-Offered Products, Services, and Solutions for Zero Trust.....	10
	Appendix B – DoD Zero Trust References	18
	Appendix C – DoD Zero Trust Reference Architecture.....	19

Tables and Figures

Table 1 - User Pillar - Zero Trust Strategy Buyer's Guide for GSA-Offered Products, Services, and Solutions	10
Table 2 - Device Pillar - Zero Trust Strategy Buyer's Guide for GSA-Offered Products, Services, and Solutions	12
Table 3 - Application and Workload Pillar - Zero Trust Strategy Buyer's Guide for GSA-Offered Products, Services, and Solutions	13
Table 4 - Data Pillar - Zero Trust Strategy Buyer's Guide for GSA-Offered Products, Services, and Solutions	14
Table 5 - Network and Environment Pillar - Zero Trust Strategy Buyer's Guide for GSA-Offered Products, Services, and Solutions	15
Table 6 - Automation and Orchestration Pillar - Zero Trust Strategy Buyer's Guide for GSA-Offered Products, Services, and Solutions	16
Table 7 - Visibility and Analytics Pillar - Zero Trust Strategy Buyer's Guide for GSA-Offered Products, Services, and Solutions	16

Services, and Solutions 17

Table of Figures

Figure 1- DoD Zero Trust Pillars 5
Figure 2- DoD Zero Trust Capabilities 6
Figure 3- DoD Zero Trust Reference Architecture 19

Foreword

This guide is intended to assist agencies under the United States (U.S.) Department of Defense (DoD) with acquiring products, services, and solutions to support and align with the DoD Zero Trust (ZT) Strategy. General Services Administration (GSA) fully recognizes that the starting point for implementing a ZT Strategy will vary among the DoD Components depending on maturity level. However, DoD Components should strive to align their Zero Trust solution architectures and execution plans according to this strategy so that overall DoD Enterprise Zero Trust outcomes are achieved and in alignment with the DoD Zero Trust Capability Execution Roadmap.

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 at different speeds. GSA offers solutions such as the Highly Adaptive Cybersecurity Services (HACS) Special Item Number (SIN) and Continuous Diagnostics and Mitigation (CDM) Tools which can be utilized for designing and deploying architectures that follow the basic tenets of Zero Trust.

To support the DoD efforts outlined in the DoD ZT Strategy, and to accelerate Zero Trust adoption, the information provided in this guide can help defense agencies identify a broad range of products, services, and solutions to help develop, implement, and mature Zero Trust execution plans. GSA’s Information Technology (IT) Category is available to answer any questions and provide subject matter expertise related to any aspect of this guide.

Approval

DocuSigned by:
Laura Stanton
99B68D3F19DB4B4...

Laura Stanton
Assistant Commissioner
Information Technology Category (ITC)
Federal Acquisition Service (FAS) General Services Administration (GSA)

1 Executive Summary

Warfare is no longer limited to the physical battlefield. Defense agencies have become a more agile, more mobile, cloud-supported workforce, collaborating with the entire DoD enterprise. These efforts include Federal and non-Federal agencies and partners working on a variety of missions. As a result, DoD is more vulnerable to adversaries such as individual malicious actors, hackers, cyberterrorists, and nation state-sponsored hackers.

To ensure our nation's security, DoD must take decisive action to keep pace with today's dynamic and increasingly sophisticated cyber threat environment by modernizing its approach to cybersecurity. DoD must adopt security best practices and advance toward a risk-based Zero Trust Framework.

On 21 May 2021, the Biden Administration issued Executive Order (E.O.) 14028, *“Improving the Nation’s Cybersecurity,”* emphasizing the need for agencies to adopt Zero Trust cybersecurity principles and adjust their network architectures accordingly. On 26 January 2022, the Office of Management and Budget (OMB) published Memorandum (M)-22-09 titled, *“Moving the U.S. Government Toward Zero Trust Cybersecurity Principles.”* To help this effort, the DoD developed a ZT Strategy to assist defense agencies as they implement Zero Trust Architectures. The DoD strategy complements the OMB Memorandum and is designed to provide DoD agencies with a roadmap and resources to achieve an optimal Zero Trust environment.

2 Purpose

The purpose of this Zero Trust Strategy Buyer’s Guide is to assist defense agencies with acquiring products, services, and solutions that align with the DoD’s ZT Strategy. While this buyer’s guide is in alignment with the DoD ZT Strategy, DoD Components are not required or obligated to utilize this buyer’s guide.

This guide introduces an implementation approach to Zero Trust Architecture (ZTA), which aligns with the DoD’s ZT Strategy. The approach includes seven (7) pillars of Zero Trust: User, Device, Application and Workload, Data, Network and Environment, Automation and Orchestration, and Visibility and Analytics. The pillars are defined and explained in Section 9, DoD ZT Strategy Approach, of this document.

3 Audience

This Buyer’s Guide is for acquisition, network, and cybersecurity professionals who are seeking to implement DoD’s ZT Strategy. Familiarity with Software-Defined Networking (SDN), access management, identity management, firewall, and Zero Trust core component concepts are helpful but not necessary. The core components are highlighted in the *DoD Zero Trust Reference Architecture*, Version 2.0, dated July 2022.

4 History of the DoD ZT Strategy

The concept of Zero Trust was present in cybersecurity before the term “Zero Trust” was coined. The Defense Information Systems Agency (DISA) and the DoD published their work on a more secure enterprise strategy dubbed “Black Core” (BCORE) in 2007. BCORE involved moving from a perimeter-based security model to one that focused on the security of individual transactions.

Prior to this time, the work of the Jericho Forum in 2004¹ publicized the idea of deperimeterization, which focused on limiting implicit trust based on network location, and the limitations of relying on single, static defenses over a large network segment. The concept of deperimeterization evolved and improved into the larger concept of Zero Trust, which was later coined by John Kindervag, Principal Analyst at Forrester Research, in 2010. Zero Trust then became the term used to describe various cybersecurity solutions that moved security away from the implied trust based on network location and instead focused on evaluating trust on a per-transaction basis. The DoD has started to undergo the move from a static, networked-based perimeter to a security strategy based on the Zero Trust principle of “Never Trust, Always Verify.”

5 What is DoD's Zero Trust Strategy?

In November 2022, DoD publicly released the *DoD Zero Trust Strategy* document and the *DoD Zero Trust Capability Roadmap*. The strategy envisioned a DoD Information Enterprise secured by a fully implemented, Department-wide Zero Trust cybersecurity framework that would reduce the attack surface, enable risk management and effective data-sharing in partnership environments, and quickly contain and remediate adversary activities.

The DoD ZT Strategy is a comprehensive cybersecurity approach requiring the entire DoD to adopt and integrate Zero Trust capabilities, technologies, solutions, and processes. It extends beyond IT and requires DoD Components to address Zero Trust with their staffing, training, and professional development processes. Zero Trust assumes no implicit trust is granted to assets or users based on their physical or network location or asset ownership. It is important to note that the DoD ZT Strategy serves only as a strategy, not a solution architecture.

6 Applicability

Because warfare requires secure, interoperable information systems, Zero Trust supports and enhances these missions. The outcomes and actions from the DoD ZT Strategy must be applied to all military multi-domain operations, bases, posts, camps, and stations around the globe including cyber, space, air, land, and sea, and support and protect business assets. As cyber threats evolve, DoD is adopting a coordinated, defensive response that is adaptive, flexible, and agile.

The DoD ZT Strategy puts forth a clear path so that it can be achieved and provides a road map

¹ https://community.isc2.org/ijoyk78323/attachments/ijoyk78323/tech-talk/3081/2/commandments_v1.2.pdf

via seven (7) DoD Zero Trust Pillars. The pillars provide a capabilities-based execution plan across the DoD Information Enterprise (IE), within the Joint Information Environment (JIE), the DoD Information Network (DODIN), and across systems and networks like their Non-classified Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet). Zero Trust is a major cultural change and a philosophy shift from legacy authentication and security mechanisms allowing effective data sharing in partnered environments.

7 DoD ZT Strategy Vision

The *DoD Zero Trust Strategy* document, published on 21 October 2022, projects five (5) years into the future, at which time the risk-based Zero Trust Framework has been implemented and is preventing increasingly sophisticated attacks. Zero Trust is integrated into the five (5) key cybersecurity framework functions: Identify, Protect, Detect, Respond, and Recover. Therefore, any attempts to deny, degrade, disrupt, deceive, or destroy information systems are mitigated. The timelines defined in the *DoD Zero Trust Strategy* document reiterate the importance of implementing a Zero Trust Architecture, with a five (5)-year plan that needs to be executed starting in Fiscal Year (FY) 2023.

8 DoD ZT Strategy Outcomes

With the DoD ZT Strategy, the DoD realizes several significant benefits. It is better able to execute missions because it can:

- Allow users to access required data from any authorized and authenticated device, fully secured and continuously verified.
- Secure and protect information systems that facilitate the DoD's evolution into a more agile, mobile, cloud-supported workforce.
- Reduce attack surface risk profiles.
- Remediate threats to the cloud, artificial intelligence, command, control, communications, computers, and intelligence.
- Effectively contain, mitigate, and remediate damage when a device, network, user, or credential is compromised.
- Include consistent, aligned, and effectively resourced capabilities for advanced cybersecurity operations.
- Recover rapidly from attacks.

9 DoD ZT Strategy Approach

To accelerate adoption, the DoD ZT Strategy includes key assumptions, principles, and pillars that guide executing the strategy. The pillars create a framework for DoD and its Components to build a Zero Trust organization and align current and future Zero Trust efforts, investments, and initiatives across the entire DoD.

Strategic Assumptions

The DoD ZT Strategy relies on the following eight (8) core assumptions to drive planning:

1. Complex security threats persist and require ongoing corrective action.
2. Culture must be addressed, not just technology.
3. Modernization requires rethinking how existing infrastructure is utilized.
4. Expanded global and industry partner collaboration is increasingly important.
5. Zero Trust requires concurrent enterprise and mission owner implementation.
6. Real-time, risk-based response is imperative as threats become more complex.
7. Legacy IT remains a challenge.
8. Leadership and operator buy-in is a must for a successful ZT Strategy.

Strategic Principles

DoD also lays out strategic principles to serve as guardrails or parameters when leadership makes decisions regarding implementation and execution. These principles include:

- **Mission-oriented** to allow for both hybrid work and location-agnostic access to collaborate, work, and execute missions.
- **Organizational** principles that presume a breach and segment access to limit the “blast radius” and incorporate Zero Trust across all elements of Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTmLPF-P).
- **Governance** to simplify and automate, and to never trust, always verify explicitly before granting access.
- **Technical** principles that provide the least amount of privilege, scrutinize, and analyze behavior, align architecture with Zero Trust design tenets, and reduce complexity.

DoD Zero Trust Pillars

The DoD ZT Strategy defines seven (7) pillars that provide the foundation for the DoD Zero Trust Security Model and the DoD Zero Trust Architecture. The pillars are described in Figure 1 below.

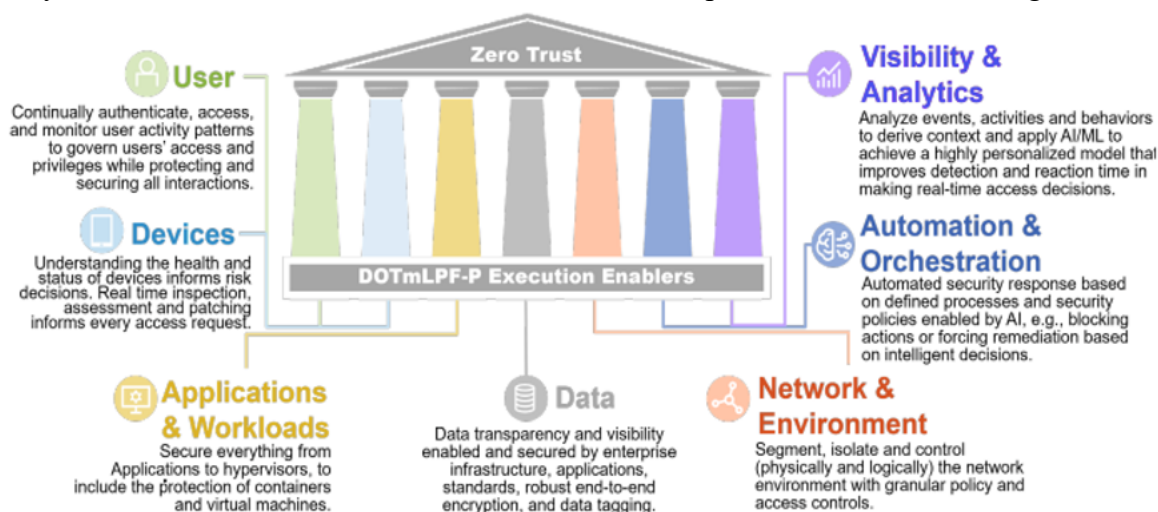


Figure 1- DoD Zero Trust Pillars ²

The foundation for the DoD Zero Trust Security Model and the DoD Zero Trust Architecture is described in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, *Zero Trust Architecture*, released in August 2020, which lists seven (7) essential principles for Zero Trust implementation. The seven (7) principles of Zero Trust are:

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

² According to the DoD ZT Strategy, DOTmLPP-P Execution Enablers are cross-cutting, non-technical capabilities and activities that address Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities, and Policy. Enablers identified to date include: ZT Awareness & Culture, Adaptive Implementation Governance, ZT Policy Framework, ZT Training, and others.

7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications; and uses it to improve its security posture.

DoD has divided 45 distinct capabilities into a subset inside the seven (7) pillars. To offer further direction about the DoD Zero Trust implementation, each capability is broken down into several related tasks. According to the DoD ZT Strategy, Components must reach the “Target Level” of Zero Trust as soon as practicable (no later than FY 2027) and then progress toward the “Advanced Level” of Zero Trust.

In the DoD ZT Strategy, it is crucial to remember that “reaching an advanced state does not mean an end to maturing Zero Trust; instead, protection of attack surfaces will continue to adapt and refine as the malicious events methods advance and mature.” Putting in place a Zero Trust Architecture is a journey toward greater security rather than a “one-and-done” project.

DoD Zero Trust Capabilities

The 45 capabilities of DoD Zero Trust are depicted in Figure 2 below.

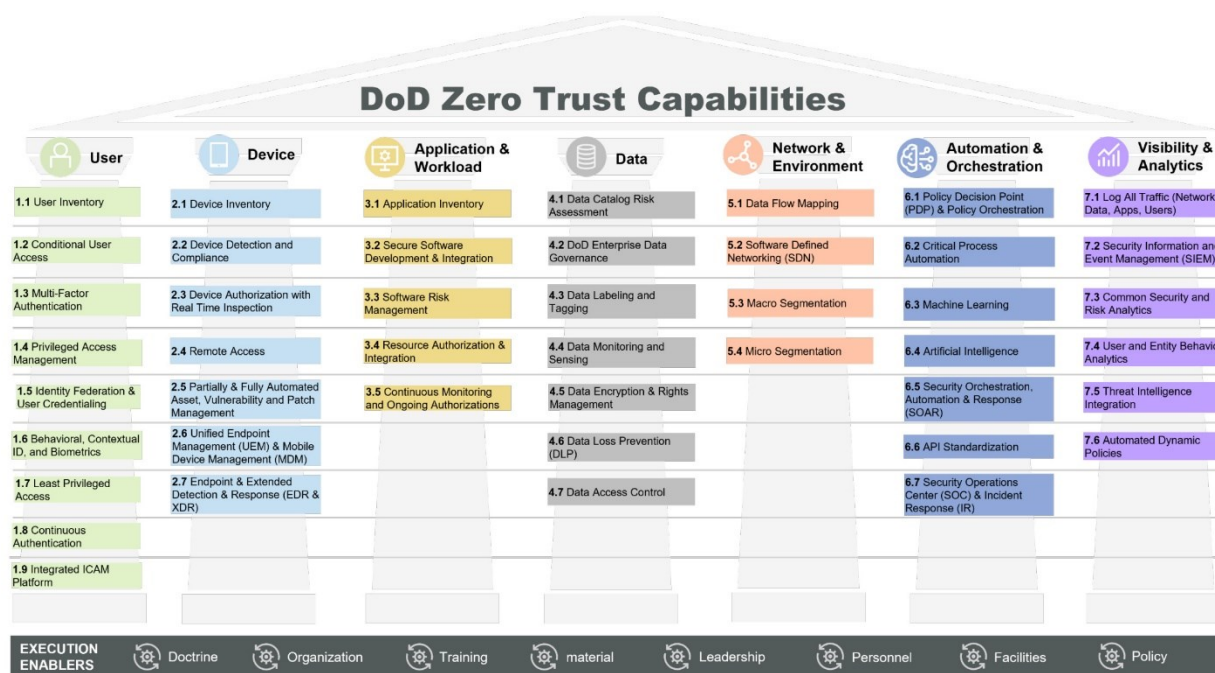


Figure 2- DoD Zero Trust Capabilities

10 DoD Zero Trust Strategic Goals and Objectives

The goals and objectives defined in the DoD ZT Strategy address the cultural, technological, and environmental requirements for successfully adopting and implementing Zero Trust. The four (4) strategic goals outlined in the strategy are:

- Goal 1: Zero Trust Cultural Adoption** - A Zero Trust security framework and mindset that guides the design, development, integration, and deployment of information technology across the DoD Zero Trust Ecosystem.
- Goal 2: DoD Information Systems Secured and Defended** - DoD cybersecurity practices incorporate and operationalize Zero Trust to achieve enterprise resilience in DoD information systems.
- Goal 3: Technology Acceleration** - Zero Trust-based technologies deploy at a pace equal to or exceeding industry advancements to remain ahead of the changing threat environment.
- Goal 4: Zero Trust Enablement** - DoD Zero Trust execution integrates with Department-level and Component-level processes resulting in seamless and coordinated Zero Trust execution.



To achieve a fully secured and defended DoD Information Enterprise (IE) (Goal 2), the DoD and Components must achieve all 45 Zero Trust capabilities depicted in Figure 2.

11 DoD Zero Trust Execution Approach

To ensure the goals and objectives of the DoD ZT Strategy are attained, DoD created a multi-pronged approach to address people, processes, resources, governance, risk management, and technology. It is designed to plug solution gaps and implement the Zero Trust framework across the entire DoD. Achieving impactful security benefits with Zero Trust requires an iterative process that must be continuously refined as the strategic context evolves.

12 High-Level Capability Roadmap

The *DoD Zero Trust Capability Roadmap* provides a guide of how the DoD envisions Zero Trust being implemented across the organization. It outlines the courses of action required per the 45 DoD Zero Trust capabilities, as well as the dependencies and interdependencies. It also provides a general timeline to achieve outcomes starting in FY 2023 to attain the “Target Level” of Zero Trust by the end of FY 2027; activities required for “Advanced Level” Zero Trust are also outlined through FY 2032.

Resourcing and Acquisition

Appropriately managing and procuring Zero Trust resources is part of the DoD's ZT Strategy as described below.

- **Resourcing:** DoD takes a multi-pronged approach for each organization within DoD so that they can appropriately identify and prioritize new and existing resources to execute the ZT Strategy. DoD works with its Components to address shortfalls and guide resource priorities.
- **Acquisition:** The acquisition strategy is meant to align with DoD's priority to build a resilient defense ecosystem. The DoD Chief Information Officer (CIO) coordinates the identification and determination of what assets will be acquired at the enterprise level but leaves overall management and oversight of technology development, acquisition, and product support to individual DoD Components.

13 Measurement and Metrics

DoD plans to use specific, qualitative, and quantitative metrics to measure its progress toward achieving its Zero Trust goals. These metrics will help determine the status and effectiveness of the Zero Trust implementation and are used to validate system and network security. Each DoD Component is required to contribute data to support the analysis of the systems.

14 Governance

Zero Trust falls under the existing DoD CIO committee structure. The primary responsibility for technical and strategic direction lies within the DoD Cyber Council.

15 Key Considerations for Products, Services, and Solutions

Although any security vendor could claim to provide a ZTA offering at some level, agencies should follow the guidance found in NIST SP 800-207. NIST 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 Zero Trust principles 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 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 the GSA-Offered Products, Services, and Solutions for Zero Trust listed in Appendix A.



DoD Agencies should check with the Deputy CIO (DCIO) for Cybersecurity (CS) for any mandated Zero Trust solutions before acquiring products, services, and solutions via the contract vehicles in this Buyer's Guide.

16 Summary

Zero Trust can significantly offset vulnerabilities and threats across DoD networks by creating discrete, granular access rules for specific applications and services within a network. Some of the most severe cases of network breaches, such as: SolarWinds (September 2019 – December 2020), MS Exchange Server (September 2019 – December 2020), Colonial Pipeline (May 2021), Log4J (December 2021), and VMWare (May 2022), could have been prevented using basic Zero Trust principles. Continuous attacks on DoD systems with escalating sophistication has made it clear that the traditional security model of protecting our perimeters is no longer sufficient.

Cybersecurity is a moving target, and DoD aims to adapt and refine its ZT Strategy to mitigate ever-evolving cyber threats. Coordinated efforts of the entire defense ecosystem are required to achieve the ZT Strategy goals and objectives. The DoD has already made significant inroads in cybersecurity and must pursue the strategic goals laid out in the DoD ZT Strategy as an enterprise. Ongoing and open communication and coordination, along with proper funding and resourcing, will be key to the success of the strategy.

17 ZT Strategy Buyer's Guide Contact Information

For questions related to any aspect of this guide, or ZT Strategy products, services, or solutions, contact:

- ITSecurityCM@gsa.gov for Customer Support with the Zero Trust Strategy Buyer's Guide.
- RMASS@gsa.gov for any Zero Trust Strategy Buyer's Guide comments, suggestions, and opinions.
- ITCSC@gsa.gov for general questions.
- The respective acquisition support for the GSA Schedules identified in Appendix A of this Zero Trust Strategy Buyer's Guide

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

The below tables list GSA Schedules to obtain Zero Trust-related products, services, and solutions.

Table 1 - User Pillar - Zero Trust Strategy Buyer's Guide for GSA-Offered Products, Services, and Solutions

Component	GSA Technology Purchasing Program	GSA Technology Purchasing Program - Continued
1.1 User Inventory	<ul style="list-style-type: none"> ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Purchasing of New Electronic Equipment SIN 33411 	<ul style="list-style-type: none"> IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Cloud SIN 518210C Software SIN 511210
1.2 Conditional User Access	<ul style="list-style-type: none"> 8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S 	<ul style="list-style-type: none"> Software Maintenance Services SIN 54151 Identity, Credentialing and Access Management SIN 541519ICAM Homeland Security Presidential Directive 12 Product and Service Components SIN 541519PIV Public Key Infrastructure Shared Service Providers Program SIN 541519PKI Cloud SIN 518210C Software SIN 511210
1.3 Multifactor Authentication	<ul style="list-style-type: none"> 8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S 	<ul style="list-style-type: none"> Software Maintenance Services SIN 54151 Identity, Credentialing and Access Management SIN 541519ICAM Homeland Security Presidential Directive 12 Product and Service Components SIN 541519PIV Public Key Infrastructure Shared Service Providers Program SIN 541519PKI Cloud SIN 518210C Software SIN 511210
1.4 Privileged Access Management	<ul style="list-style-type: none"> 8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S 	<ul style="list-style-type: none"> Software Maintenance Services SIN 54151 Identity, Credentialing and Access Management SIN 541519ICAM Homeland Security Presidential Directive 12 Product and Service Components SIN 541519PIV Public Key Infrastructure Shared Service Providers Program SIN 541519PKI Cloud SIN 518210C Software SIN 511210
1.5 Identity Federation and User Credentialing	<ul style="list-style-type: none"> 8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS 	<ul style="list-style-type: none"> IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Identity, Credentialing and Access Management SIN 541519ICAM Homeland Security Presidential Directive 12 Product and Service Components SIN 541519PIV Public Key Infrastructure Shared Service Providers Program SIN 541519PKI Cloud SIN 518210C Software SIN 511210

Component	GSA Technology Purchasing Program	GSA Technology Purchasing Program - Continued
1.6 Behavioral, Contextual ID, and Biometrics	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • 2GIT PRODUCTS • Purchasing of New Electronic Equipment SIN 33411 • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S 	<ul style="list-style-type: none"> • Software Maintenance Services SIN 54151 • Identity, Credentialing and Access Management SIN 541519ICAM • Homeland Security Presidential Directive 12 Product and Service Components SIN 541519PIV • Public Key Infrastructure Shared Service Providers Program SIN 541519PKI • Cloud SIN 518210C • Software SIN 511210
1.7 Least Privileged Access	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • 2GIT PRODUCTS • Purchasing of New Electronic Equipment SIN 33411 • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S 	<ul style="list-style-type: none"> • Software Maintenance Services SIN 54151 • Identity, Credentialing and Access Management SIN 541519ICAM • Homeland Security Presidential Directive 12 Product and Service Components SIN 541519PIV • Public Key Infrastructure Shared Service Providers Program SIN 541519PKI • Cloud SIN 518210C • Software SIN 511210
1.8 Continuous Authentication	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • 2GIT PRODUCTS • Purchasing of New Electronic Equipment SIN 33411 • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S 	<ul style="list-style-type: none"> • Software Maintenance Services SIN 54151 • Identity, Credentialing and Access Management SIN 541519ICAM • Homeland Security Presidential Directive 12 and Service Components SIN 541519PIV • Public Key Infrastructure Shared Service Providers Program SIN 541519PKI • Cloud SIN 518210C • Software SIN 511210
1.9 Integrated ICAM Platform	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • 2GIT PRODUCTS • Purchasing of New Electronic Equipment SIN 33411 • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S 	<ul style="list-style-type: none"> • Software Maintenance Services SIN 54151 • Identity, Credentialing and Access Management SIN 541519ICAM • Homeland Security Presidential Directive 12 Product and Service Components SIN 541519PIV • Public Key Infrastructure Shared Service Providers Program SIN 541519PKI • Cloud SIN 518210C • Software SIN 511210

Table 2 - Device Pillar - Zero Trust Strategy Buyer's Guide for GSA-Offered Products, Services, and Solutions

Component	GSA Technology Purchasing Program	GSA Technology Purchasing Program - Continued
2.1 Device Inventory	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Purchasing of New Electronic Equipment SIN 33411 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Cloud SIN 518210C • Software SIN 511210
2.2 Device Detection and Compliance	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Purchasing of New Electronic Equipment SIN 33411 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Cloud SIN 518210C • Software SIN 511210
2.3 Device Authorization with Real Time Inspection	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Purchasing of New Electronic Equipment SIN 33411 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Cloud SIN 518210C • Software SIN 511210
2.4 Remote Access	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Purchasing of New Electronic Equipment SIN 33411 • Highly Adaptive Cybersecurity Services SIN 54151HACS 	<ul style="list-style-type: none"> • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Public Key Infrastructure Shared Service Providers Program SIN 541519PKI • Commercial Satellite Communications Solutions SIN 517410 • Cloud SIN 518210C • Software SIN 511210
2.5 Partially & Fully Automated Asset, Vulnerability, and Patch Management	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • 2GIT PRODUCTS • Purchasing of New Electronic Equipment SIN 33411 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Cloud SIN 518210C • Software SIN 511210
2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	<ul style="list-style-type: none"> • 8(a) STARS III • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Wireless Mobility Solutions SIN 517312 	<ul style="list-style-type: none"> • Commercial Satellite Communications Solutions SIN 517410 • Cloud SIN 518210C • Software SIN 511210
2.7 Endpoint & Extended Detection & Response (EDR & XDR)	<ul style="list-style-type: none"> • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Complex Commercial SATCOM Solutions (CS3) • 2GIT PRODUCTS • Purchasing of New Electronic Equipment SIN 33411 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Cloud SIN 518210C • Software SIN 511210

Table 3 - Application and Workload Pillar - Zero Trust Strategy Buyer's Guide for GSA-Offered Products, Services, and Solutions

Component	GSA Technology Purchasing Program	GSA Technology Purchasing Program - Continued
3.1 Application Inventory	<ul style="list-style-type: none"> • ALLIANT 2 • Enterprise Infrastructure Solutions (EIS) • Purchasing of New Electronic Equipment SIN 33411 • Highly Adaptive Cybersecurity Services SIN 54151HACS 	<ul style="list-style-type: none"> • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Cloud SIN 518210C • Software SIN 511210
3.2 Secure Software Development & Integration	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) 	<ul style="list-style-type: none"> • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Cloud SIN 518210C • Software SIN 511210
3.3 Software Risk Management	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • 2GIT PRODUCTS 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • Cloud SIN 518210C • Software SIN 511210
3.4 Resource Authorization & Integration	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Highly Adaptive Cybersecurity Services SIN 54151HACS 	<ul style="list-style-type: none"> • IT Professional Services SIN 54151S • Homeland Security Presidential Directive 12 Product and Service Components SIN 541519PIV • Cloud SIN 518210C • Software SIN 511210
3.5 Continuous Monitoring and Ongoing Authorizations	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Purchasing of New Electronic Equipment SIN 33411 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Cloud SIN 518210C • Software SIN 511210

Table 4 - Data Pillar - Zero Trust Strategy Buyer's Guide for GSA-Offered Products, Services, and Solutions

Component	GSA Technology Purchasing Program	GSA Technology Purchasing Program - Continued
4.1 Data Catalog Risk Assessment	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • 2GIT PRODUCTS <p>1.</p>	<ul style="list-style-type: none"> • Purchasing of New Electronic Equipment SIN 33411 • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Cloud SIN 518210C • Software SIN 511210
4.2 DoD Enterprise Data Governance	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) 	<ul style="list-style-type: none"> • Purchasing of New Electronic Equipment SIN 33411 • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151
4.3 Data Labeling and Tagging	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) <p>2.</p>	<ul style="list-style-type: none"> • Purchasing of New Electronic Equipment SIN 33411 • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Cloud SIN 518210C • Software SIN 511210
4.4 Data Monitoring and Sensing	<ul style="list-style-type: none"> • 8(a) STARS III • VETS 2 • Enterprise Infrastructure Solutions (EIS) 	<ul style="list-style-type: none"> • Cloud SIN 518210C • Software SIN 511210
4.5 Data Encryption & Rights Management	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) 	<ul style="list-style-type: none"> • Cloud SIN 518210C • Software SIN 511210
4.6 Data Loss Prevention (DLP)	<ul style="list-style-type: none"> • 8(a) STARS III • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Purchasing of New Electronic Equipment SIN 33411 	<ul style="list-style-type: none"> • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Cloud SIN 518210C • Software SIN 511210
4.7 Data Access Control	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) 	<ul style="list-style-type: none"> • Cloud SIN 518210C • Software SIN 511210

Table 5 - Network and Environment Pillar - Zero Trust Strategy Buyer's Guide for GSA-Offered Products, Services, and Solutions

Component	GSA Technology Purchasing Program	GSA Technology Purchasing Program - Continued
5.1 Data Flow Mapping	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Electronic Commerce and Subscription Services SIN 54151ECOM • Purchasing of New Electronic Equipment SIN 33411 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Commercial Satellite Communications Solutions SIN 517410 • Cloud SIN 518210C • Software SIN 511210
5.2 Software Defined Networking (SDN)	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Electronic Commerce and Subscription Services SIN 54151ECOM • Purchasing of New Electronic Equipment SIN 33411 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Commercial Satellite Communications Solutions SIN 517410 • Cloud SIN 518210C • Software SIN 511210
5.3 Macro Segmentation	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Electronic Commerce and Subscription Services SIN 54151ECOM • Purchasing of New Electronic Equipment SIN 33411 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Commercial Satellite Communications Solutions SIN 517410 • Cloud SIN 518210C • Software SIN 511210
5.4 Micro Segmentation	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Electronic Commerce and Subscription Services SIN 54151ECOM • Purchasing of New Electronic Equipment SIN 33411 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Commercial Satellite Communications Solutions SIN 517410 • Cloud SIN 518210C • Software SIN 511210

Table 6 - Automation and Orchestration Pillar - Zero Trust Strategy Buyer's Guide for GSA-Offered Products, Services, and Solutions

Component	GSA Technology Purchasing Program	GSA Technology Purchasing Program - Continued
6.1 Policy Decision Point (PDP) & Policy Orchestration	<ul style="list-style-type: none"> • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Purchasing of New Electronic Equipment SIN 33411 • Highly Adaptive Cybersecurity Services SIN 54151HACS 	<ul style="list-style-type: none"> • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Cloud SIN 518210C • Software SIN 511210
6.2 Critical Process Automation	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) 	<ul style="list-style-type: none"> • Automated Contact Center Solutions SIN 561422 • Cloud SIN 518210C • Software SIN 511210
6.3 Machine Learning	<ul style="list-style-type: none"> • 8(a) STARS III • Enterprise Infrastructure Solutions (EIS) • Automated Contact Center Solutions SIN 561422 	<ul style="list-style-type: none"> • Cloud SIN 518210C • Software SIN 511210
6.4 Artificial Intelligence	<ul style="list-style-type: none"> • 8(a) STARS III • Enterprise Infrastructure Solutions (EIS) • Automated Contact Center Solutions SIN 561422 	<ul style="list-style-type: none"> • Cloud SIN 518210C • Software SIN 511210
6.5 Security Orchestration, Automation & Response (SOAR)	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Purchasing of New Electronic Equipment SIN 33411 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Cloud SIN 518210C • Software SIN 511210
6.6 API Standardization	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) 	<ul style="list-style-type: none"> • IT Professional Services SIN 54151S • Cloud SIN 518210C • Software SIN 511210
6.7 Security Operations Center (SOC) & Incident Response (IR)	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Purchasing of New Electronic Equipment SIN 33411 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Cloud SIN 518210C • Software SIN 511210

Table 7 - Visibility and Analytics Pillar - Zero Trust Strategy Buyer's Guide for GSA-Offered Products, Services, and Solutions

Component	GSA Technology Purchasing Program	GSA Technology Purchasing Program - Continued
7.1 Log All Traffic (Network, Data, Apps, Users)	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • Identity, Credentialing and Access Management SIN 541519ICAM • Cloud SIN 518210C • Software SIN 511210
7.2 Security Information and Event Management (SIEM)	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • Identity, Credentialing and Access Management SIN 541519ICAM • Cloud SIN 518210C • Software SIN 511210
7.3 Common Security and Risk Analytics	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • 2GIT PRODUCTS <p>3.</p>	<ul style="list-style-type: none"> • Purchasing of New Electronic Equipment SIN 33411 • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Cloud SIN 518210C • Software SIN 511210
7.4 User and Entity Behavior Analytics	<ul style="list-style-type: none"> • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • 2GIT PRODUCTS • Purchasing of New Electronic Equipment SIN 33411 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Cloud SIN 518210C • Software SIN 511210
7.5 Threat Intelligence Integration	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • 2GIT PRODUCTS 	<ul style="list-style-type: none"> • Wireless Mobility Solutions SIN 517312 • Cloud SIN 518210C • Software SIN 511210
7.6 Automated Dynamic Policies	<ul style="list-style-type: none"> • 8(a) STARS III • ALLIANT 2 • VETS 2 • Enterprise Infrastructure Solutions (EIS) • Electronic Commerce and Subscription Services SIN 54151ECOM • Purchasing of New Electronic Equipment SIN 33411 	<ul style="list-style-type: none"> • Highly Adaptive Cybersecurity Services SIN 54151HACS • IT Professional Services SIN 54151S • Software Maintenance Services SIN 54151 • Commercial Satellite Communications Solutions SIN 517410 • Cloud SIN 518210C • Software SIN 511210

Appendix B – DoD Zero Trust References

The Zero Trust Strategy Buyer's Guide is developed in accordance with the following references.

References
Executive Order (EO) 14028, Improving the Nation's Cybersecurity, May 12, 2021
Office of Management and Budget (OMB) M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022
Department of Defense (DoD) Zero Trust Strategy, October 21, 2022
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 Zero Trust Architecture, August 2020
Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model Version 2.0, April 2023

Appendix C – DoD Zero Trust Reference Architecture

The below diagram depicts the DoD's Zero Trust Reference Architecture's targeted environment.

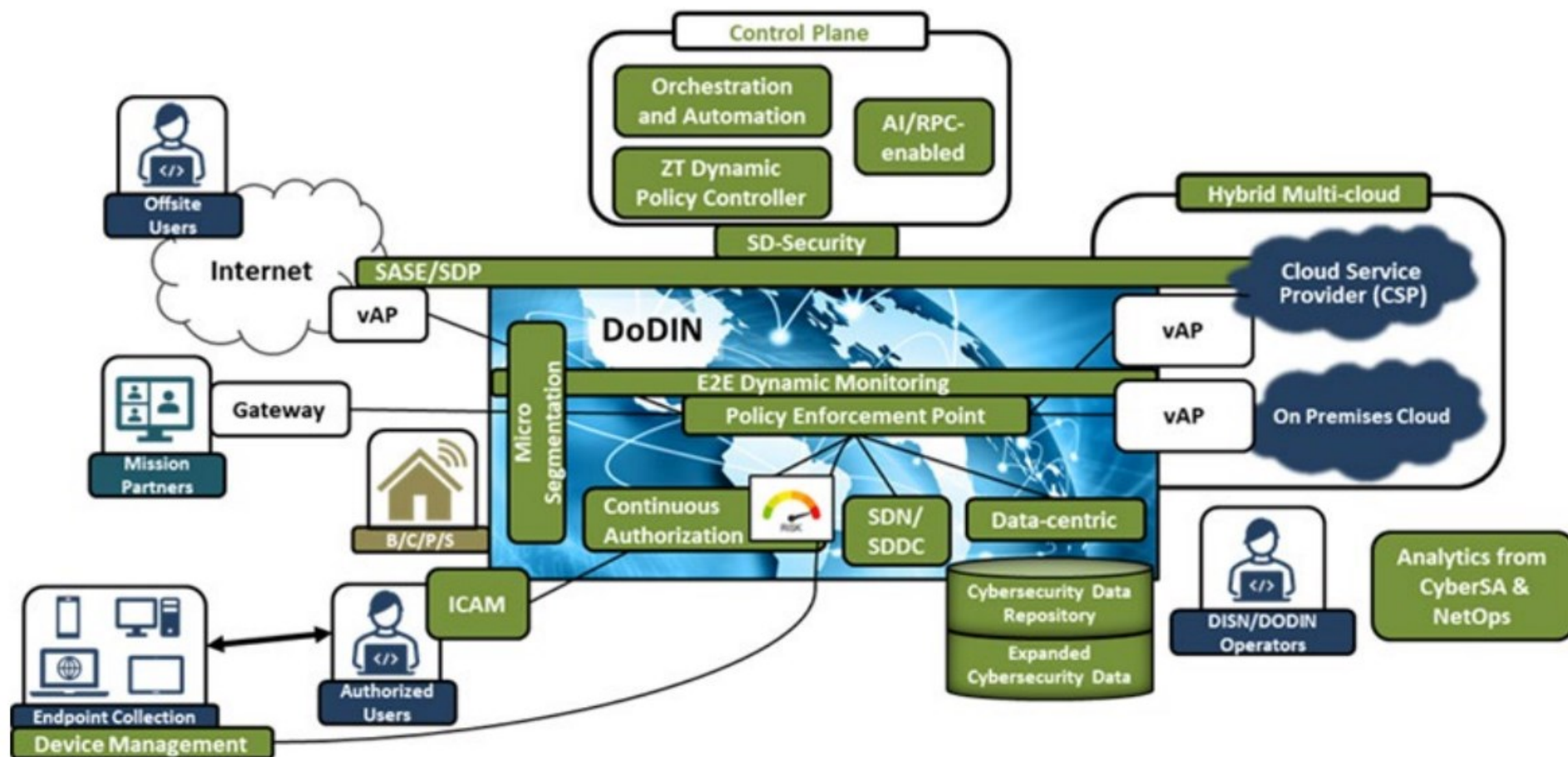


Figure 3- DoD Zero Trust Reference Architecture