TYTO'S ZERO TRUST ARCHITECTURE PERSPECTIVE

Department of Defense Stance on Zero Trust

Policy and Strategic Directives

The DoD has formally embraced Zero Trust as a foundational element of its cybersecurity strategy. The DoD Zero Trust Strategy, released in 2022, established an ambitious goal to achieve a target-level Zero Trust framework by FY2027. This initiative supports and aligns with broader federal mandates, including:

- **Executive Order (EO) 14028: *Improving the Nation's Cybersecurity***
- **National Cybersecurity Strategy (2023)**
- **CISA Zero Trust Maturity Model Version 2.0**
- **DISA Zero Trust Reference Architecture (v2.0, DISA & DoD CIO, July 2022)**
- **NIST Special Publication (SP) 800-207: *Zero Trust Architecture***

Leadership for Zero Trust implementation resides with the DoD's Chief Information Officer (CIO) and the Defense Information Systems Agency (DISA). Together, they are driving the integration of Zero Trust principles across all DoD networks, cloud environments, and operational systems. The DISA Reference Architecture codifies these efforts under the strategic guidance of EO 14028, reinforcing the department's commitment to a secure, adaptive, and threat-informed cyber defense posture.

Executive Summary

The Department of Defense (DoD) is operating in an increasingly complex and dynamic cyber threat landscape. As adversaries grow more sophisticated and the attack surface expands through cloud computing, mobile devices, and operational technology (OT) in tactical environments, traditional perimeter-based security models can no longer meet mission needs.

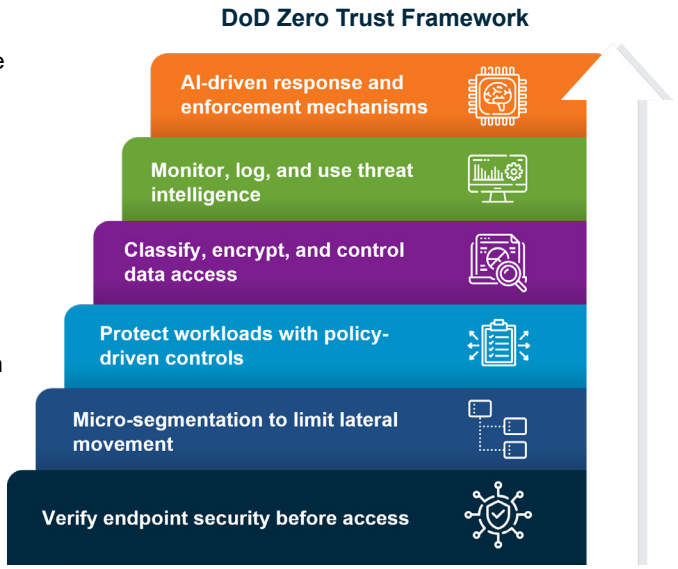
In response, the DoD is adopting Zero Trust Architecture (ZTA) as a cornerstone of its cybersecurity strategy. This white paper examines the DoD's Zero Trust commitment, identifies the operational and organizational challenges to implementation, and outlines the strategic benefits of adopting a Zero Trust approach. It also features three agency case studies that demonstrate how organizations have successfully navigated operational, technical, and cultural hurdles, resulting in stronger cyber resilience, improved mission success, and greater warfighter effectiveness.

Zero Trust Core Principles

Zero Trust is built on the fundamental belief that “never trust, always verify” applies to all users, devices, and systems. The DoD implements this philosophy through seven foundational pillars of Zero Trust, as defined by the DISA Zero Trust Reference Architecture:

1. **User Identity** — Continuous authentication of all users based on least privilege access.
2. **Device Security** — Verification of endpoint security posture before granting access.
3. **Network Environment** — Micro-segmentation to limit lateral movement within and across environments.
4. **Application Workload** — Protection of software and cloud workloads through policy-driven access controls.
5. **Data Protection** — Enforcement of data classification, encryption, and access restrictions.
6. **Visibility & Analytics** — Continuous monitoring, logging, and integration of threat intelligence for situational awareness.
7. **Automation & Orchestration** — AI-driven response and enforcement mechanisms.

Together, these pillars establish a risk-informed, adaptive access model that protects DoD assets across all domains, regardless of user location.



Benefits of Zero Trust

Enhanced Cyber Resilience

Zero Trust reduces the risk of advanced persistent threats (APTs), insider threats, and nation-state attacks by limiting the attack surface, preventing lateral movement, and enforcing continuous verification across users and systems.

Improved Mission Assurance

Zero Trust ensures that only authorized users and trusted devices access mission-critical systems. It strengthens continuity of operations (COOP), safeguards the supply chain, and secures battlefield communications.

Secure Cloud and Edge Deployments

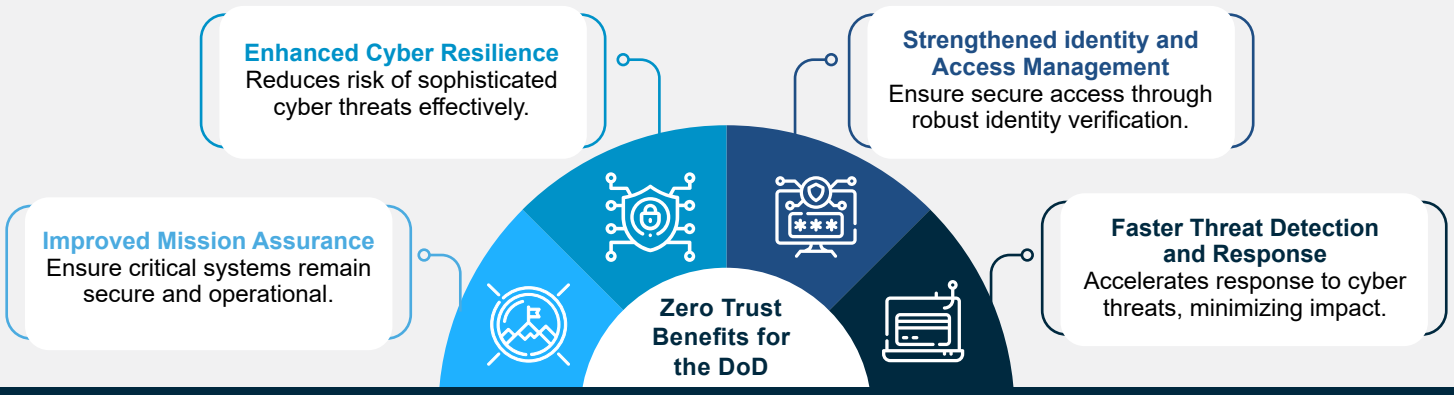
As the DoD transitions to hybrid cloud and edge computing, Zero Trust provides a scalable, software-defined security framework that protects forward-deployed forces, remote workers, and IoT-based operational technology (OT).

Strengthened Identity, Credential, and Access Management (ICAM)

Zero Trust enhances Identity, Credential, and Access Management (ICAM) by combining multi-factor authentication (MFA), behavioral analytics, and AI-driven anomaly detection—ensuring compromised credentials do not result in unauthorized access.

Faster Threat Detection and Response

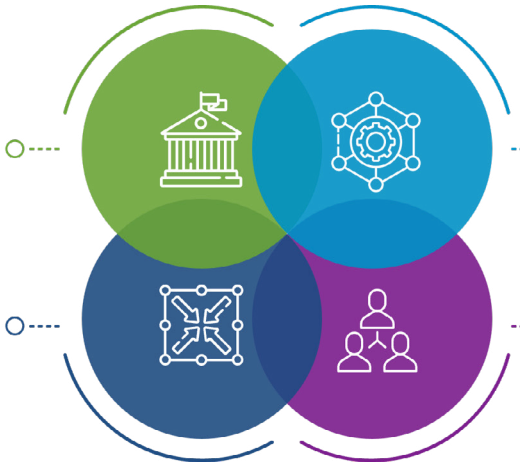
Through continuous monitoring and automated security enforcement, Zero Trust reduces dwell time, enhances threat intelligence sharing, and accelerates incident response, minimizing cyber risk before it disrupts DoD mission operations.



Key Challenges in Implementing Zero Trust

Despite its clear security advantages, implementing Zero Trust across the DoD presents several complex and interrelated challenges:

Challenges in implementing Zero Trust in DoD



Policy & Governance Alignment

Policy alignment is crucial for impactful Zero Trust adoption despite low complexity.

Legacy Infrastructure

Legacy infrastructure poses high complexity and significant impact on Zero Trust implement.

Resource Constraints

Resource constraints are straightforward but have limited impact on Zero Trust.

Workforce Training

Workforce training is complex but impacts Zero Trust implementation minimally.

Legacy Infrastructure and Technical Debt

Many DoD systems rely on legacy architectures not designed for Zero Trust. Integrating modern security frameworks with on-premises networks, classified systems, and industrial control systems (ICS) is both technically complex and costly.

Mission-Critical Interoperability

Zero Trust must support seamless operations across classified and unclassified networks, joint forces, and allied partners. Ensuring interoperability, especially with coalition forces that may not fully adhere to Zero Trust principles, requires deliberate coordination and flexible implementation.

Policy and Governance Alignment

The Zero Trust model introduces strict access controls and policy enforcement that may conflict with existing operational models. Successful adoption demands updated governance frameworks, acquisition strategies, and workforce training protocols that support decentralized decision-making.

Workforce Training and Cultural Shift

Zero Trust adoption is not purely a technical challenge — it requires a cultural shift. Many DoD personnel are accustomed to role-based access models and traditional perimeter security. Transitioning to continuous verification and least-privilege access necessitates extensive cybersecurity training and leadership buy-in.

Resource Constraints

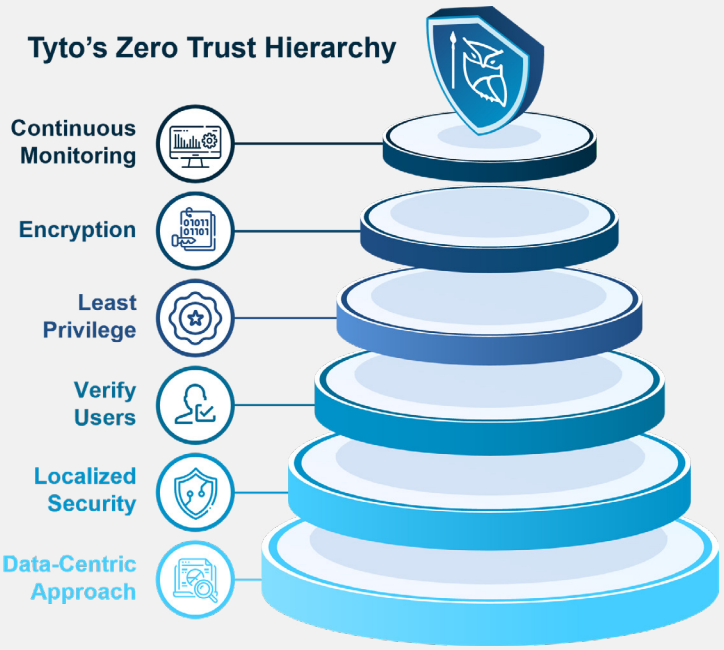
While Zero Trust enhances security, it requires significant investment in cybersecurity tools, cloud-native architectures, and AI-driven analytics. Budget limitations, procurement complexities, and system integration costs can all delay or limit implementation.

The Tyto Approach to Zero Trust

Tyto's Design Principles

Tyto's Zero Trust strategy is grounded in **attribute-based access control (ABAC)**—a model that evaluates access based on dynamic, context-aware policies. These policies consider not just user identity, application, or device, but also additional factors such as behavioral patterns, security posture, and operational context, including location and time.

Recognizing that Zero Trust is not a one-size-fits-all solution, Tyto recommends an implementation approach built on a set of core principles that ensure adaptability, scalability, and mission alignment across complex environments.



Take A Data-Centric Approach	Automized data records or data sets must become the central resources that an effective ZTA implementation manages, enforces, and monitors access to.
Localize Security Boundaries as much as Possible	Micro-segmentation of networks, systems, and applications enables access decisions to be enforced as close to data and other key resources as possible. This approach makes it more difficult for adversaries to move laterally within the network.
Never Trust, Always Verify	Users and devices must be authenticated using a contextual, risk-informed approach before being evaluated at a Policy Decision Point (PDP). The PDP then assesses user and device authentication (AuthN), along with other attributes, to determine authorization (AuthZ) based on dynamic application policies.
Principles of Least Privilege and Functionality	Every user enters the network as a general user. Elevated privileges (e.g., administrator access) are granted only when explicitly authorized and only for a limited time. Additionally, each application is configured to support only essential functionality, restricting any non-essential or unnecessary functions.
End-To-End Encryption	When implemented properly, end-to-end encryption prevents attackers from eavesdropping on communication between applications, even if they gained a foothold within the network.
Data Encryption at Rest	Encryption of data at rest ensures that information remains protected in the event of unauthorized access. Sensitive files can be encrypted prior to transfer or full-disk encryption can be applied to the entire storage medium. An encryption key is required to access encrypted data.
Continuous Monitoring	While continuous monitoring is already in place, ZTA enhances this capability by integrating advanced data analytics for greater visibility into system behavior and emerging threats.

Tyto's Perspective on the Role of ICAM in DoD's Zero Trust Strategy

For the DoD, ICAM is a critical enabler for securing and governing access to sensitive data, systems, and services. ICAM is a framework of policies, processes, and technologies designed to manage digital identities and control access to information systems and resources.

Identity Management: Creating, managing, and validating digital identities for users, devices, and non-person entities (NPEs), such as applications, bots, and services. NPE identity management is especially important in episodic or tactical OT network environments.

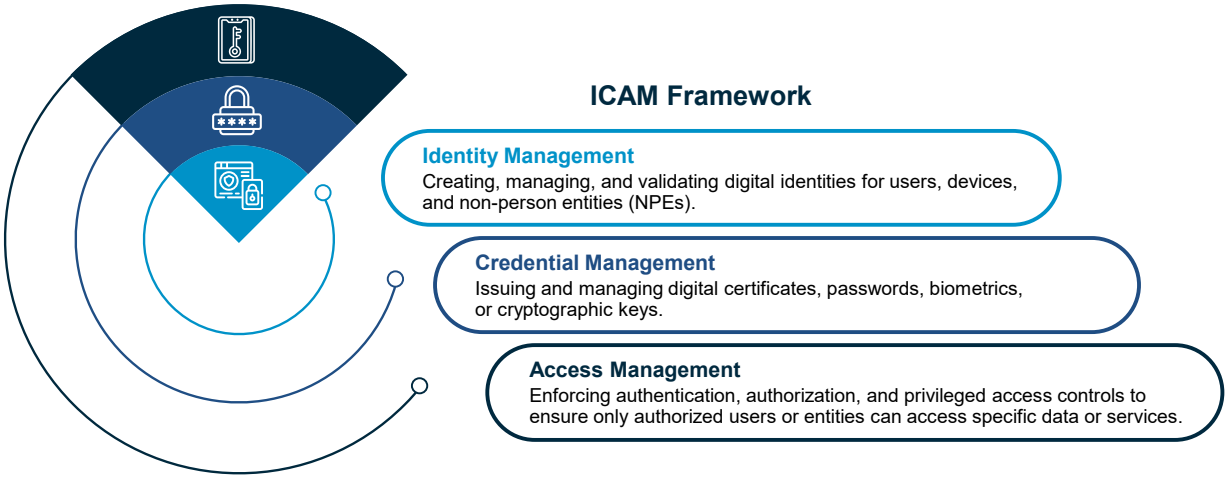
Credential Management: Issuing and managing digital certificates, passwords, biometrics, or cryptographic keys used to verify identity.

Access Management: Enforcing authentication, authorization, and privileged access controls to ensure only authorized users or entities can access specific data or services. Audit capability also plays a critical role in access management.

The DoD Zero Trust Strategy, formalized in the DISA Zero Trust Reference architecture in 2022, aims to transform the DoD's cybersecurity posture by operating under an "assume breach" mindset and enforcing strict access controls based on continuous verification rather than implicit trust. Tyto views ICAM as a foundational requirement for enabling Zero Trust. It provides the ability to deliver granular, dynamic, and adaptive access controls based on verified identity attributes and real-time risk assessments.

Core ICAM Functions Enabling Zero Trust

- **Identity Federation and Interoperability:** ICAM supports federated identity management across DoD agencies and mission partners, enabling seamless and secure cross-domain access while maintaining ABAC. This capability is essential for Joint All-Domain Command and Control (JADC2) and coalition operations, where interoperable access control is mission-critical.
- **Continuous Identity Verification:** Zero Trust mandates continuous authentication rather than a one-time login. ICAM enforces real-time identity validation by, evaluating contextual attributes such as device trust level, geolocation, and behavioral analytics. Access permissions dynamically are adjusted dynamically through data tagging and metadata analysis.
- **Least-Privileged Access Control:** ICAM enables dynamic policy enforcement to ensure that users and entities receive only the minimum access required to perform their duties. This minimizes the attack surface and reduces the potential impact of compromised credentials.
- **Privileged Access Management (PAM):** ICAM governs and audits privileged access to critical systems, protecting against insider threats and advanced persistent threats (APTs). When integrated with automated PAM tools, ICAM can enforce just-in-time (JIT) access and revoke privileges based on dynamic risk scoring.



ICAM Modernization Challenges in Zero Trust Implementation

While ICAM is a critical enabler of Zero Trust, the DoD faces several significant challenges in fully modernizing its ICAM infrastructure:

Legacy Systems Integration:

- Integrating legacy identity stores with modern ICAM solutions is complex and costly.
- Modernization requires automated identity lifecycle management and ABAC enforcement.

Mission Partner Access:

- Ensuring secure, federated identity management for mission partners is essential for JADC2 and coalition operations.
- Success depends on standardizing cross-domain identity federation protocols to ensure interoperability.

Scaling ICAM Across DoD Networks:

- Consistently applying Zero Trust policies across the DoD Information Network (DoDIN), including disconnected and tactical environments.
- Requires edge-based ICAM enforcement to support forward-deployed units with limited or intermittent connectivity.

Benefits of Data Tagging in Zero Trust

Data tagging assigns metadata labels or tags to data assets that describe the content, context, sensitivity classification, and ownership of the data.

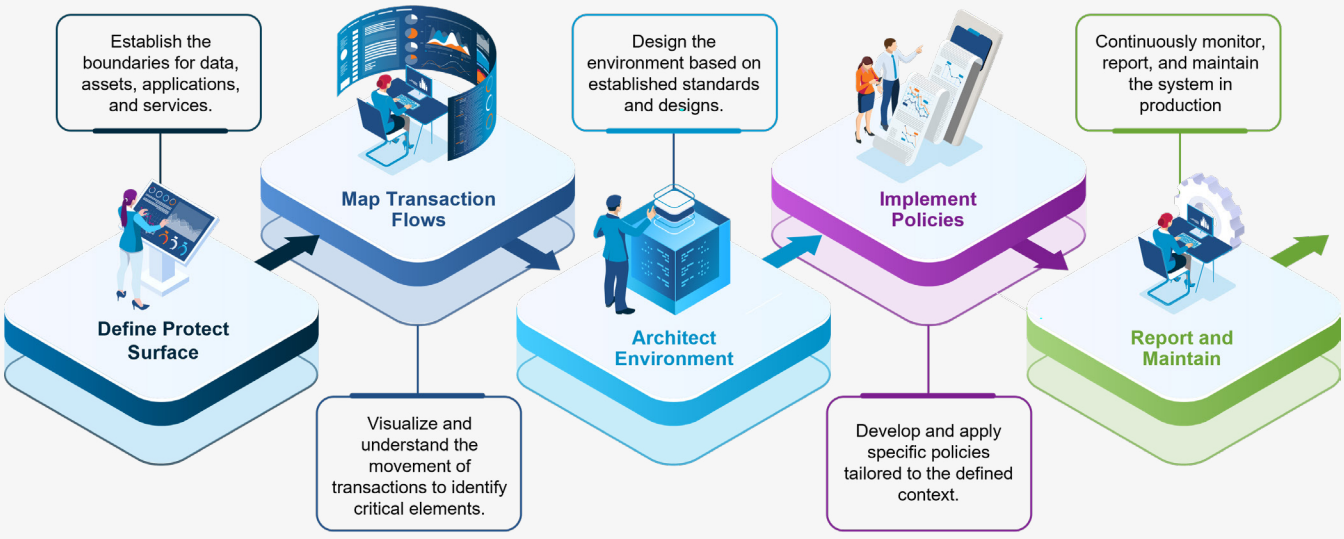
- Granular Access Control
- Improved Data Governance and Compliance
- Enhanced Data Visibility and Monitoring
- Dynamic Policy Enforcement
- Reduced Data Overexposure and Lateral Movement
- Accelerated Incident Response

Tyto's Perspective on Zero Trust Life Cycle Management

Tyto recommends customers follow a high-level Zero Trust five step process:

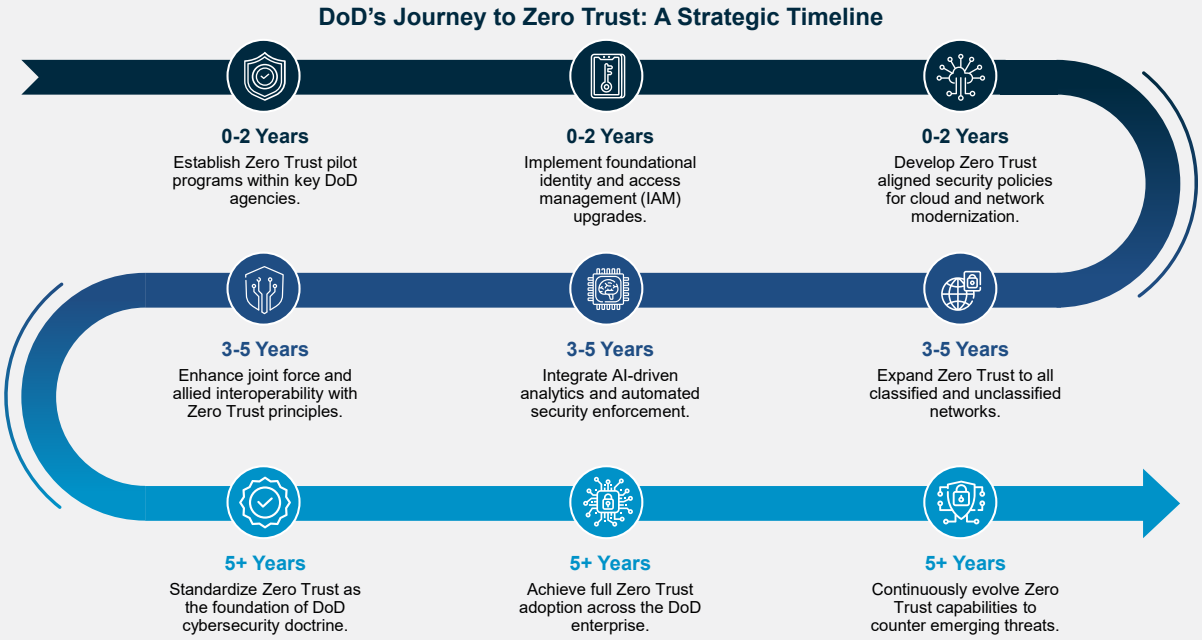
1 Define the Protect Surface	Identify the data, assets, applications, and services that require protection.
2 Map the Transaction Flows	Gain visibility into how transactions move across the environment. This provides clarity on the service wrap needed and helps identify the crown jewels.
3 Architect the environment	Review standards and design approaches to determine how Zero Trust will be implemented within the environment.
4 Policy implementation	Develop specific policies tailored to your environment based on insights from steps 1–3. Policies should reflect contextual understanding and mission needs.
5 Report and Maintain	Once in production, continuously monitor, report on, and maintain the Zero Trust environment to ensure effectiveness over time.

Achieving Zero Trust Life Cycle Management



Most importantly, determine WHY we are protecting assets and then think about HOW.

Conceptual Roadmap for DoD Zero Trust Implementation



Zero Trust Brings Observability And Resiliency To Life

Observability and resiliency, as natural byproducts of Tyto's Zero Trust roadmap, significantly enhance an organization's security posture.

- **Enhanced observability** provides comprehensive visibility into network activity, enabling proactive threat detection and real-time insights into critical system operations. Observability goes beyond telemetry data collection, it includes analysis and contextual understanding to drive informed. actionable decisions.
- **Improved resiliency** ensures the organization can swiftly detect, contain, and recover from security incidents. This minimizes the impact of breaches across the Protect Surface.

Together, these elements create a unified security framework that is both transparent and adaptable, fostering continuous improvement and robust threat management. This holistic approach ensures that organizations are well-equipped to navigate the evolving cybersecurity landscape, maintaining a strong and resilient defense against potential threats.

Integrating observability and resiliency into a **data-centric** Zero Trust strategy significantly enhances an organization's security posture.

1. Enhanced Observability: A data-centric Zero Trust strategy ensures comprehensive visibility into all data interactions. Continuous monitoring, real-time analytics, and integrated security tools provide detailed insights into how data is accessed, used, and transferred. This allows organizations to accurately assess internal states and rapidly detect anomalies.
2. Improved Resiliency: Zero Trust strengthens resiliency by prioritizing data protection through robust encryption, continuous verification, and adaptive access controls. These safeguards ensure that even if a breach occurs, sensitive data remains secure and the organization can recover swiftly.

Overall, a data-centric Zero Trust roadmap that integrates observability and resiliency offers a comprehensive cybersecurity approach, providing deep visibility into data activity and the ability to respond effectively to disruptions.

Unified Security Posture: Combining observability and resiliency in a data-centric Zero Trust strategy delivers a unified security posture that is both transparent and adaptable. Organizations gain deeper insights into data interactions while being equipped to respond to threats dynamically.

Proactive Threat Management: Enhanced observability allows for proactive threat detection, while improved resiliency ensures that the organization can withstand and recover from attacks efficiently.

Unified Management: The integration of observability and resiliency fosters a culture of continuous improvement. Organizations can regularly assess their data security measures, adapt to evolving threats, and refine their strategies based on real-time data.

Tyto Delivers on Operational Zero Trust

Tyto brings extensive experience in integrating Operational Technology (OT) and tactical networks with Information Technology (IT) and enterprise networks. This expertise is demonstrated through our support on various DoD IT modernization projects, where we have successfully managed large and complex Electronic and Information Systems & Technology (EFIS&T) projects for DoD agencies across both CONUS and OCONUS theaters.

Tyto's capabilities include furnishing, upgrading, designing, testing, installing, and maintaining all NIPR and SIPR Base Area Network (BAN) wired and wireless components for multiple customers. Our proven track record —$1.07 billion in prime DoD network infrastructure modernization contracts, including 23 global infrastructure modernization Task Orders (TOs) totaling $455 million —highlights our ability to integrate diverse network environments and deliver mission-aligned, secure outcomes.

Justice Security Operations Center (JSOC)

Tyto delivers a fully managed Security Operations Center (SOC) as a Service for the Department of Justice (DOJ) and other Federal agencies. The JSOC currently supports over 40 Justice organizations across approximately 175 locations, serving more than 10,000 users and endpoints. As a multi-tenant service, JSOC also serves several other Federal agencies, with coverage spanning both CONUS and OCONUS sites.

JSOC is both ISO 20000-1 and 27001 certified and is the first and only Federal SOC shared services provider. JSOC holds Certified Cybersecurity Services Provider (CSP) and Center of Excellence (COE) designations from CISA Quality Services Management Office (QSMO). Notably, the DOJ remains the only SOC shared services provider, commercial or federal, validated by CISA

Legislative Branch Agency

Tyto is leading a major Zero Trust transformation effort for a Legislative Branch agency currently modernizing its IT infrastructure. This includes integrating independent networks, information systems, mobile devices, and cloud services into a cohesive and secure environment through the implementation of ZTA. Recognizing that traditional perimeter-based network security is no longer sufficient in the modern threat landscape, the agency is actively collaborating with internal stakeholders and partner organizations to drive this enterprise-wide transformation.

Current Progress and Focus Areas:

- Establishment of Core Capabilities and Performance Standards: Foundational capabilities required for effective ZTA implementation are being defined and institutionalized.
- Long-term Strategic Approach: The initiative is structured as a phased, long-term effort, with clearly defined tactical milestones to enable progressive capability maturity.
- Comprehensive Roadmap: A detailed strategy document outlines the scope of the initiative and provides a roadmap with specific milestones for achieving progressively maturing levels of security.

Through these ongoing efforts, the agency is strengthening its IT infrastructure to ensure robust security, operational resilience, and mission readiness in the face of evolving cyber threats. The project is advancing steadily, reflecting the agency's commitment to secure and efficient technology modernization.

Justice Edge Trust Service (JETS)

The Justice Edge Trust Service (JETS) is a Secure Access Secure Edge (SASE) capability provided by the DOJ to help agencies cost-effectively accelerate compliance with Executive Order 14028 and OMB Memo M-22-09.

JETS supports the implementation of core Network/Environment capabilities within a ZTA, aligning with CISA's Zero Trust Maturity Model. DOJ leverages FedRAMP-authorized cloud software tools that enable user-based and device-based access control decision, brokering secure access to the internet, cloud services, and privately hosted applications.

JETS provides SASE capabilities that enable Zero Trust Architectures.

These tools were selected to replace traditional virtual private networks (VPNs) and outbound trusted internet connection (TIC) stacks for both remote and on-premises network users. JETS provides the following technical capabilities:

- Secure Socket Layer Visibility (SSLV)
- Web Proxy / URL Filtering
- Intrusion Detection System (IDS) and
- Intrusion Prevention System (IPS)
- Network Filtering
- Web Data Loss Prevention (DLP)
- Firewall
- Integration with CISA's E3A DNS sink-holing and Cloud Log Aggregation Warehouse (CLAW) capabilities, and planned support for CISA's Protective DNS capability

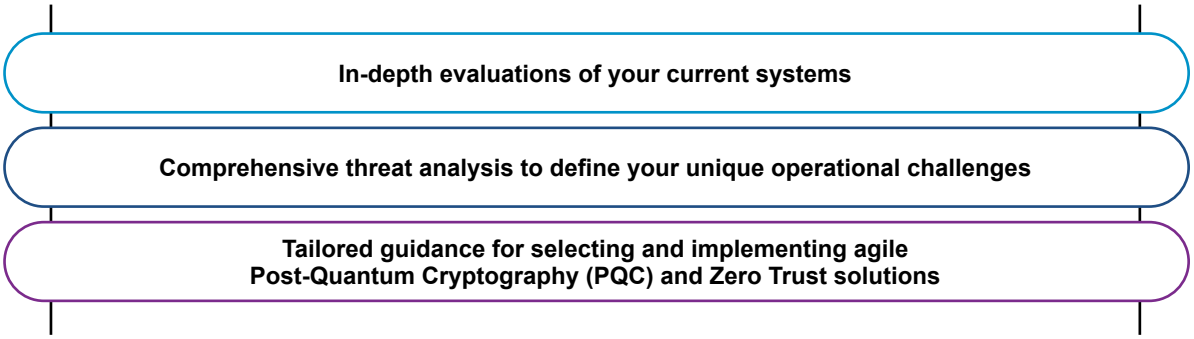
In addition to the software stack, DOJ offers participating federal agencies technical expertise and operational support to scope, plan, pilot, deploy, operate, and maintain their new SASE capabilities.

Conclusion - The Imperative for Zero Trust

The DoD's adoption of Zero Trust is not merely a cybersecurity enhancement —it is a mission-critical necessity. In an era defined by cyber warfare, insider threats, and hybrid attack vectors, traditional perimeter-based security models are no longer sufficient.

By prioritizing identity-centric security, continuous monitoring, and automated policy enforcement, Zero Trust enables the DoD to harden its cyber defenses, safeguard national security assets, and maintain operational superiority. While implementation challenges exist, the long-term benefits far outweigh the costs, ensuring the DoD remains resilient, adaptive, and secure in the face of evolving threats.

At Tyto Athene, we believe the journey to Zero Trust is not just about adopting a security solution—it's about empowering your organization to secure its future. Our approach goes beyond compliance. We provide the tools, frameworks, and expertise to protect your most valuable digital assets and elevate your security posture in a rapidly changing threat landscape. As a seasoned systems integrator, Tyto Athene delivers unmatched expertise in integration, interoperability, and future-proofing solutions to reduce business and mission risk. We are prepared to support your Zero Trust journey with:



Our cyber security and systems integration experts, working alongside trusted technology partners, will guide your organization through each phase of the Zero Trust implementation lifecycle. Achieving full Zero Trust maturity is a multi-year, multi-faceted transformation, and with Tyto Athene as your partner, you can move forward with confidence.

About Tyto Athene

Tyto Athene delivers mission-focused solutions that keep critical missions future-focused and future-ready. We utilize adaptive architecture and continuous integration to secure essential data, so our clients can make informed decisions, create decisive advantages, and drive dominance. We do more than solve the needs of now, we deploy what's next.

TYTO Athene
DATA TO DOMINANCE