

Department of Defense Zero Trust Plan








Description:

Executive Order 14028, “Improving the Nation’s Cybersecurity,” calls for the acceleration of adopting Zero Trust (ZT) principles across the Federal Government. The DoD established the ZT Program to hasten the implementation of ZT principles department-wide. The DoD will follow the ZT Frameworks outlined by NIST Special Publication (SP) 800-207 and the DoD Zero Trust Reference Architecture (ZTRA) Version 1.0 to achieve this goal.

NIST SP 800-207 defines Zero Trust Architecture (ZTA) as a cybersecurity plan which minimizes uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services, and encompasses component relationships, workflow planning, and access policies. ZTA represents a paradigm shift in how the department will secure its infrastructure, networks, and data. The ZTA model's foundational tenet dictates that no actor, device, network, or service entity operating outside or within the security perimeter will be automatically trusted, but must be continually vetted and verified. ZT assumes that there is no traditional network edge: networks can be local, in the cloud, or a combination or hybrid with resources in any location. ZTA is not a capability or device you buy, rather it is a security framework, an architectural approach, and a methodology to prevent malicious actors from accessing our most critical assets and reducing existing attack surfaces.

The DoD’s approach to ZT is composed of seven strategic pillars. These pillars identify the foundational areas to apply adaptive controls, continuous authentication and data management capabilities to achieve a ZT-enabled domain or information enterprise. Implementation of these ZT pillars along with the adoption of ZT principles, tenets, and frameworks into DoD architectures will support the department’s efforts to detect, deny, deter, and defend against malicious cyber activity.

Seven Pillars of ZT

	USER Leverages Identity, Credential, and Access Management (ICAM) services to include continuous multi-factor authentication (CMFA) to support access management and accountability within the ZT Framework.
	DEVICES Authorized based on a rich set of attributes regarding identity, suitability, readiness, and authorities. Real-time inspection, assessment and packing of devices in an enterprise are critical functions. Some solutions such as Mobile Device Managers or Comply-To-Connect programs provide data that can be useful for confidence assessments.
	NETWORK/ENVIRONMENT Employs control and capabilities to both logically and physically isolate the network environment with granular access and policy restrictions. As the perimeter becomes more robust through macro-segmentation and micro-segmentation, a ZT infrastructure provides greater protections and control of individual DAAS.
	APPLICATION/WORKLOAD ZT applications span the complete application layer of the OSI stack. Application delivery methods such as proxy technologies enable additional protections to include ZT decision and enforcement points. ZT leverages next generation firewalls (NGFWs), micro-segmentation and containerization to secure applications from mapping networks, escalating
	DATA ZT leverages technology that categorizes, protects, and encrypts data at rest and in transit. Key technologies aiding with this protection include robust encryption, Data Rights Management, data loss detection and prevention protocols, data tagging, and other data management capabilities.
	VISIBILITY & ANALYTICS Leverages tools like Security Information and Event Management (SIEM), advanced security analytics platforms, and other analytic utilities to enable cybersecurity experts to observe cyber-related event data in real time.
	AUTOMATION & ORCHESTRATION Security Orchestration, Automation & Response (SOAR) leverages artificial intelligence and machine learning to reduce mean time to detect (MTTD) and respond (MTTR), by qualifying and remediating security alerts in minutes, rather than days, weeks, or months.