U.S. ARMY
CYBER COMMAND
www.arcyber.army.mil | Follow @arcyber

Zero Trust

WHAT IS ZERO TRUST (ZT)?

The Department of Defense (DoD) and the National Institute of Standards and Technology define ZT as an "evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources."

ZT assumes that no implicit trust is granted to assets or users based solely on their physical or network location or asset ownership, and continuously authenticates, authorizes, and validates access to systems, applications, and data. ZT systems go beyond managing entry, inserting security checks throughout entire systems, tagging data and verifying interaction, identification and verification of every part of a network from users to devices such as computers, servers, printers, phones, and radios.

WHAT IS THE ARMY ZT FUNCTIONAL MANAGEMENT OFFICE AND WHAT ARE ITS OBJECTIVES?

The Army recently established a ZT Functional Management Office (A-FMO ZT) to synchronize, integrate, implement, and execute the service-wide implementation of ZT in alignment with DoD and Army directives and objectives. Its vision is to create an Army unified network secured and defended by a ZT Architecture (ZTA) that enables the Army to operate as part of a joint or coalition force during competition, crisis, or conflict in support of Multi-Domain Operations.

To ensure unity of effort and implementation the A-FMO ZT executes its mission in close cooperation with a wide range of stakeholders. With the A-FMO ZT as its center, the Army core is comprised of policy organizations, including the Army Chief Information Officer, Army G-6, the Army Cyber Center of Excellence, and the Army Futures Command Cyber Capabilities Development Integration Directorate; operational organizations, including Army Cyber Command and the Army Network Enterprise Technology Command; and agencies such as the Assistant Secretary of the Army (Acquisition, Logistics and Technology), Army Program Executive Offices, and the Army Futures Command Network Cross-Functional Team that engage both policy development and operations.

This is supported by a large community of interest participating in ZT deployment across the Army and DoD, including the DoD Chief Information Officer; the Defense Information Systems Agency; the U.S. Navy and its Fleet Cyber Command; the National Security Agency; the Joint Staff Chief Information Officer (J-6); the Army Principal Cyber Advisor; the Army Deputy Chief of Staff for Operations, Plans and Training (G3/5/7); the Defense Acquisition University; Army Futures Command; the Army Training and Doctrine Command; Army Forces Command; Army Materiel Command; and partner organizations in industry and academia.

WHAT IS THE WAY AHEAD FOR ZT DEVELOPMENT?

The DoD has outlined several objectives for enabling and advancing ZT development, such as automating cyber and ZT with artificial intelligence; creating dynamic access control; building interoperability with secured data; continually updating ZT-enabled technology; visualizing and breaking down silos; simplifying architectures; automating data management; ensuring operations and performance are aligned and ZT supporting functions are effectively resourced; streamlining and accelerating acquisition and deployment of ZT capabilities; and building a workforce across the DoD that embraces and is committed to ZT cybersecurity.

The Army's way ahead involves continuous improvement, optimization and integration of an Army Unified Network to achieve ZT target levels by 2027; maturing ZT gap analysis to inform related technology decisions and implemntation for operationalizing Army ZTA; partnering with leading experts in government, industry and academia for additional opportunities to advance, accelerate and validate ZT solutions, integration and interoperability; continuing to align with DoD ZT directives, goals and objectives to establish an Army ZT Roadmap and Implementation Plan; and collaborating with generating and operational forces to develop and implement ZT curriculum, implementation guides and lessons learned.

WHAT IS THE DESIRED END STATE FOR THE ARMY'S ZTA?

The Army aims to ensure secure information at all operational levels, providing users with access to required resources from any devide at any location, enabled by:

- A data-centric ZTA
- Hybrid cloud resource hosting
- A service edge for brokered access to resources and control of internet access
- Cloud-based, Internet-accessible unified endpoint and security management
- An Internet-accessible identity provider
- Logging, analytics and automated response

For a full look at the DoD ZT Strategy and ZT Capability Roadmap, and ZT planning and execution, go to: https://dodcio.defense.gov/Library/