PEO EIS
ENTERPRISE INFORMATION SYSTEMS
DEPARTMENT OF THE NAVY

Zero Trust Design Concepts

Current State

The Department of the Navy (DON) protects its data by relying heavily on external perimeter defense, network-based security, and trust relationships. Data breaches from trusted and untrusted actors have highlighted the deficiencies of this approach to cybersecurity. Digital transformation initiatives, such as mobility, renewed focus on user experience and flexible access, as well as the move to hybrid cloud operations further reduces the effectiveness and complicates the execution of perimeter defense. In response to these business and technology trends, industry is adopting and maturing the design concepts of Zero Trust. Leading IT companies that operate complex networks rely heavily on Zero Trust as a security design approach, enabling industry-leading security and improved customer experience.

Problem Statement

The DON requires incremental changes to its security approach and service delivery construct to enable better customer experience with flexible and dynamic access to services and data, while improving visibility and control over user behavior, and increasing data security, audit, and compliance capabilities

Zero Trust Design Concepts

Zero Trust Definition:
Zero Trust is an information security design approach using a set of intertwined and interdependent adaptive processes, capabilities, and controls, with data-driven feedback loops based on risk/trust levels.

Zero Trust Principles:

- Trust traffic inside the perimeter no more than external traffic
- Authenticate, validate, and verify every request for resource access; authorize only on need to know
- Inspect, log, and continuously monitor all traffic throughout sessions for anomalous behavior
- Authorize access based on risk profile (adaptive authorization)

Zero Trust Design Concepts:

- Fully automate user provisioning and monitoring
- Use multifactor authentication
- Eliminate automatic trust for users or machines
- Build context aware access
- Encrypt all traffic at rest and in transit
- Instrument for comprehensive, full-stack visibility
- Separate protections for network, applications, and data
- Perform Continual Adaptive Risk and Threat Assessment
- Augment detection and response using automated AI, ML, & orchestration
- Continuously discover, monitor, assess and prioritize risk and trust
- Use micro segmentation to create granular perimeter security zones
- Match security zone policies around context; do not treat all data and workloads the same
- Put continuous risk visibility, decisions and ownership into business units and product owners

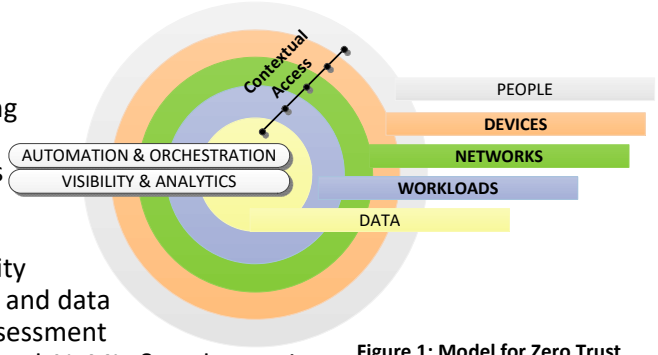

Figure 1: Model for Zero Trust

Related Service Groups, Projects, and Capabilities