Making Zero Trust Work for You

Kevin Brooks
Principal Digital Strategist – DoD & US Intelligence Community
ServiceNow

Arun Iyer
Principal Executive Architect/Field CTO
ServiceNow

Zero Trust is what it sounds like. It is a security framework that operates on the tenant that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access. This is a dramatic paradigm shift in philosophy of how we secure our infrastructure, networks, and data, from verify once at the perimeter to continual verification of each user, device, application, and transaction.

Contemporary threat actors, from cyber criminals to nation-state actors, have become more persistent, stealthier, and more subtle. They demonstrate an ability to penetrate network perimeter defenses with regularity. Traditional perimeter-based network defenses with multiple layers of disjointed security technologies cannot meet the cybersecurity needs of this threat environment.

A transition to a Zero Trust Architecture (ZTA) is mandated by the Executive Order on Improving the Nation's Cybersecurity and steps to get there are detailed in OMB memos and Department cyber guidance. But more than meeting a mandate, the transition to Zero Trust makes sense as a way to maintain a strong, secure cyber infrastructure while enabling digital modernization – both critical for the success of our nation.

Zero Trust is not achieved with a single technology. Rather, it is dependent on multiple, complex technologies working together to provide the validation of trust in a way that is seamless to end users. It is an approach that requires cybersecurity teams to orchestrate multiple security solutions.

This session will examine the recommendations for implementing a successful ZTA to support Mission operations, service delivery and employee experiences. We will focus on:

- A single enterprise inventory system or CMDB with IT and OT visibility
- Improved attack-surface management and security posture.
- Improved remediation and patch management capabilities.
- Leverage new Machine Learning and AI capabilities where possible
- Automate, orchestrate, and integrate security incident response and detection capabilities
- Integration of specialized 3rd party applications such as SASE, BYOD, MDM, CASB, Container Development, endpoint detection, threat intelligence feeds and Identity and Access Management platforms.

Enable Enterprise Managed Accounts

OMB guidance directs agencies to ensure that "Federal staff have enterprise-managed accounts, allowing them to access everything they need to do their job while remaining reliably protected."

Identity, credential, and access management (ICAM) is designed to create a secure and trusted environment in which users can access authorized resources. ICAM allows the agency to see who is on the network at any given time.

Provide Dynamic Credentialing and Authorization

Identity, Credential, and Access Management (ICAM) is designed to create a secure and trusted environment for users to access resources they need to do their job. ICAM also enables an Agency to see who is on their network at any given time.

Manage Device and System Inventory

If you cannot see your IT environment you cannot manage it. The first step in Zero Trust is understanding what assets and systems are part of your environment. Agencies must effectively catalog their digital assets and intellectual property in terms of potential risk and implement procedures to identify, manage, and monitor the users, devices, and applications accessing this data.

Automate Processes Across Teams

Zero Trust requires coordination across tools and teams to detect and ultimately block access to sensitive information. Will review how a single data model and powerful cross-functional workflows that connect people, functions, and systems.

Simplify Security Architecture

The current, fragmented approach to cybersecurity has introduced technical complexity creating more (not less) vulnerabilities and high levels of latency. Zero Trust adds more tools so addressing complexity through integrations is critical.

Produce Consistent Policy

To achieve and maintain a zero trust architecture, federal agencies must be consistent when applying policies. Policies must be clearly defined, documented, and enforced by the Agency security applications to prevent breaches.