Brief

Forcepoint Zero Trust Brief for the Department of Defense

"The Department of Defense (DOD) next generation cybersecurity architecture will become data centric and based upon Zero Trust principles."

SOURCE:
DOD ZERO TRUST REFERENCE ARCHITECTURE, FEB 2021

WHY ZERO TRUST:

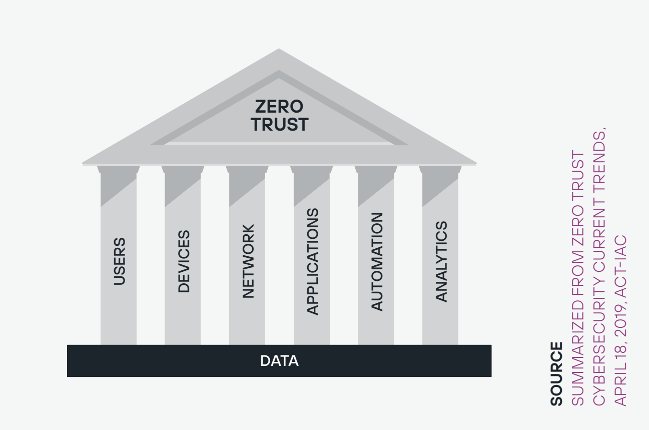
According to the Executive Order on Improving the Nation's Cybersecurity, federal government agencies must develop plans to adopt Zero Trust architectures within 60 days following the issuance of the order. The EO also requires agencies to implement a series of migration steps, create a schedule for implementation, identify activities that will have the most immediate security impacts, and more.

But what is "Zero Trust"? How is it defined? What are its key components?

UNDERSTANDING THE ZERO TRUST MODEL:

> "Agencies should take a balanced approach when adopting Zero Trust architecture. Ultimately the end goal is not about compliance, but about the pieces of the architecture coming together. Many technologies can offer important pieces toward Zero Trust, but ultimately the inter-dependency of behaviors across users, devices, applications, and data matter."
>
> **PETKO STOYANOV, CTO OF FORCEPOINT,**
> DEFINING ZERO TRUST IN THE WAKE OF THE BIDEN ADMINISTRATION'S CYBERSECURITY EXECUTIVE ORDER BLOG

The GSA ACT-IAC States that there are 6 Pillars of a Zero Trust Model, summarized as:



SOURCE SUMMARIZED FROM ZERO TRUST CYBERSECURITY CURRENT TRENDS, APRIL 18, 2019, ACT-IAC

1. **PILLAR #1: Users—Including People and Identity**
   - Ongoing authentication of trusted users.
   - Continuously monitoring user trustworthiness to govern their access and privileges. Technologies for securing and protecting users' interactions: identity, credential and access management (ICAM), multi-factor authentication, and traditional web gateway solutions.

2. **PILLAR #2: Devices—Device security**
   - Tracking real-time trustworthiness of devices.
   - Maintaining real-time cybersecurity posture of devices.
   - Provide device assessments for every access requests—examinations of compromise state, software versions, protection status, encryption enablement technologies that can provide device-trust assessments: Mobile Device Managers.

3. **PILLAR #3: Network—Network Security**
   - Zero Trust Networks actually attempt to move perimeters in from the network edge and segment and isolate critical data from other data.
   - The ability to segment, isolate, and control the network continues to be a pivotal point of security—including software defined wide area networks and internet based technologies.
   - It is critical to (a) control privileged network access, (b) manage internal and external data flows, (c) prevent lateral movement in the network, and (d) have visibility to make dynamic policy and trust decision on network and data traffic.

4. **PILLAR #4: Applications—Application and Workload Security**
   - Securing and properly managing the application layer, compute containers and virtual machines is central to ZT adoption.
   - Identifying and controlling the technology stack facilitates more granular and accurate access decisions.

   Technologies that are increasingly part of proper access control to applications: Multi-factor authentication

5. **PILLAR #5: Automation—Security Automation and Orchestration**
   - Utilize security automation response tools that automate tasks across products through workflows while allowing for end-user oversight and interaction.
   - Connect security tools and assist in managing disparate security systems to greatly reduce manual effort, event reaction times, and costs.

   Technologies that assist: Security Automation, Orchestration, and Response (SOAR), and User and Entity Behavior Analysis.

6. **PILLAR #6: Analytics—Security Visibility and Analytics**
   - You can't combat a threat you can't see.
   - Prevention: analysis of cyber-related event data can develop proactive security measures before an actual incident occurs.

   Technologies that assist: security information management (SIM and SIEM), advanced security analytics platforms, and user behavior analytics enable security experts to observe in real time what is happening and orient defenses more intelligently.

The Base: Critical Data
- Categorize DAAS (Data as a service) in terms of mission criticality.
- Develop a comprehensive data management strategy.

Processes or technologies to assist: Categorizing data, developing schemas, encrypting data at rest and in transit, DRM, DLP, Software Defined Storage, and granular data tagging.

Adopting ZT architecture ensures a shift in security—enabling inter-dependency of behaviors across users, devices, applications, network activities, and data into insights. The output of this is creates a more modern approach to security, shifting towards visibility through analytics and towards automation.

Legacy	Modern
Static, Perimeter Based Security →	**Protection of Resources, Assets, and Users**
Trust within Perimeter/Perimeter Security →	**Potential Compromise Requiring Continuous Evaluation**
Comply to Connect into Networks →	**Comply to Connect to Resources**
Product/Tool Focused Security →	**Visibility, Analytics and Automation Across Organization**

SOURCE: SUMMARIZED FROM ZERO TRUST CYBERSECURITY CURRENT TRENDS, APRIL 18, 2019, ACT-IAC

Zero Trust in action—Ensuring for the future:

Understanding the requirements of a Zero Trust model is the first step—future proofing involves looking at the emerging needs on the horizon for the DoD. There are unique challenges that will intersect the ongoing DoD Zero Trust Architecture:

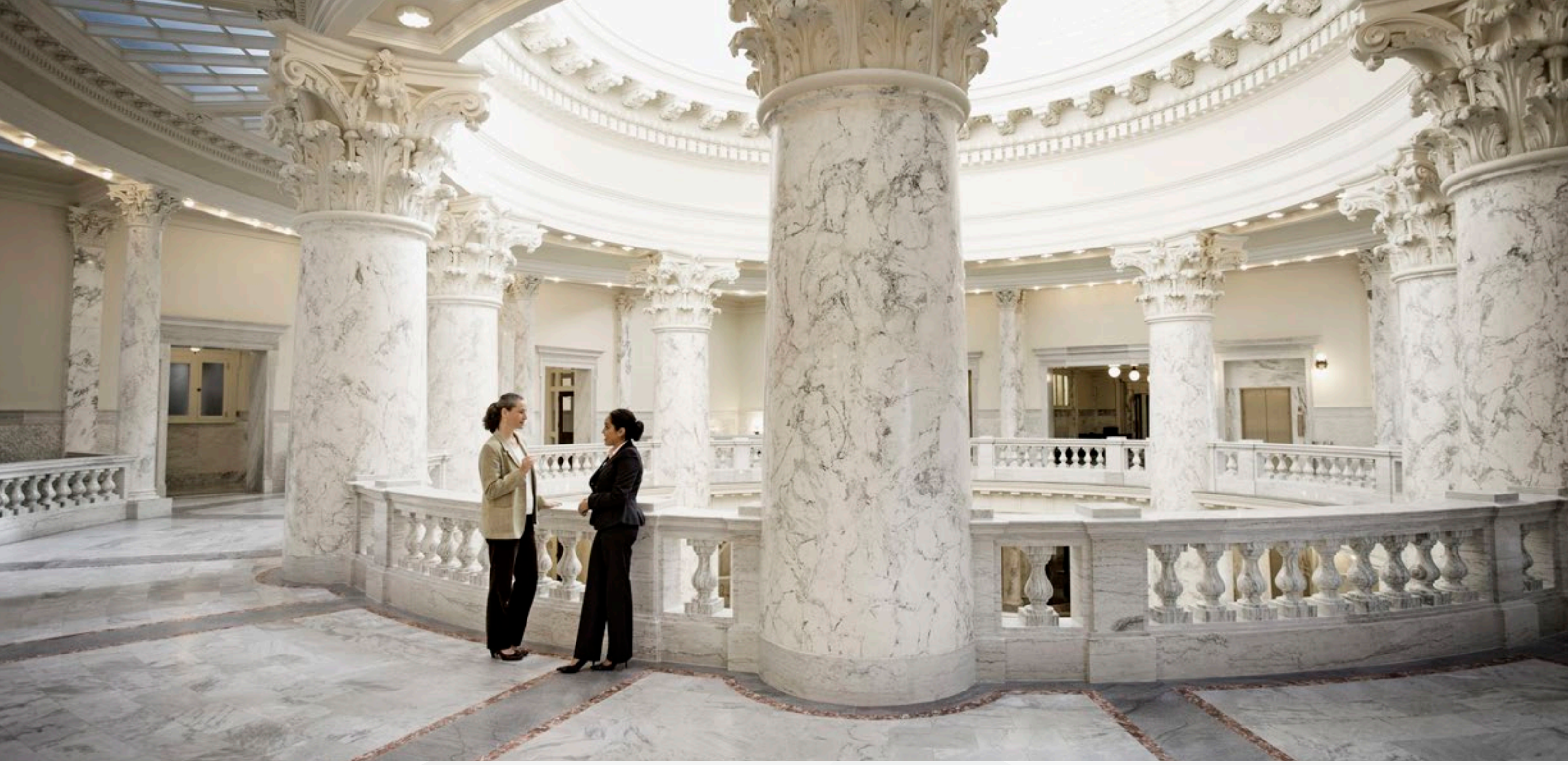
1. **Work from Anywhere Workforce:** With pandemic driving work from home requirements to tactical requirements for the field –enabling access and collaboration without increasing risk in security.
2. **Defensive Cyber Operations:** Defending Multiple Air-gapped networks that can experience simultaneous threats, such as external actors or stolen credentials, but may lack visibility to events or threats within each network.
3. **Remote Mission Critical Access:** Missions that require rapid volume and velocity of data to be shared between networks and partners – safely and securely.
4. **DevSecOps in highly secure environments—**Enabling modern software development tools, often cloud based, while maintaining software supply chain, without creating risk within the complex multi-level network environment.
5. **Performance, Behavior, and Activity Baselining—**Identifying anomalous activity is challenging without implementing a system or software technology to establish a baseline, i.e. defining normal.
6. **Unique needs of your organization—**Depending upon the complexity of your agency and the mission in which you are entrusted, taking emerging needs into account.

No One Vendor can Solve "Zero Trust"—it takes teamwork

It will include technology integration, the existing environment, and future capabilities and needs. It will have to be flexible to evolve over time, with your agency.

9 Questions that you should ask to integrate Zero Trust into your Security Model:

1. Does my current technology stack authorize and authenticate users access to assets and resources? Does it authorize and authenticate user access on a continuous basis?
2. Do my vendors provide an ability to create a common set of policies and protocols to manage identity and trust for all users and devices, including cloud or SaaS resources?
3. Does my environment involve Multi-Level Networks?
4. Would future needs include multi-directional transfer of data across those networks without violating or disrupting Zero Trust principles, or introducing risk?
5. Would future needs include accessing data within multiple air gap networks for a single end user, while maintaining Zero Trust for users?
6. Am I working with vendors that meet current NSA and NCDSMO Raise-The Bar Guidelines for Cross Domain solutions, ensuring the compliance can be met?
7. Do I have a need to gain visibility for end users, data, applications, or network activities in a single or multiple network framework?
8. Does my current technology stack turn analytics and insights into early risk detection for cybersecurity operations teams? And can it help provide automation to prevent additional activities where risk is high or anomalies are detected?
9. Can my vendors help provide forensic investigation assistance into security events, and integrate it into an automation solutions such as a SOAR?



Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

[Forcepoint-Zero-Trust-Brief-DOD-US-EN] 16Aug2021