Thunderdome

Realizing Zero Trust

INTRO

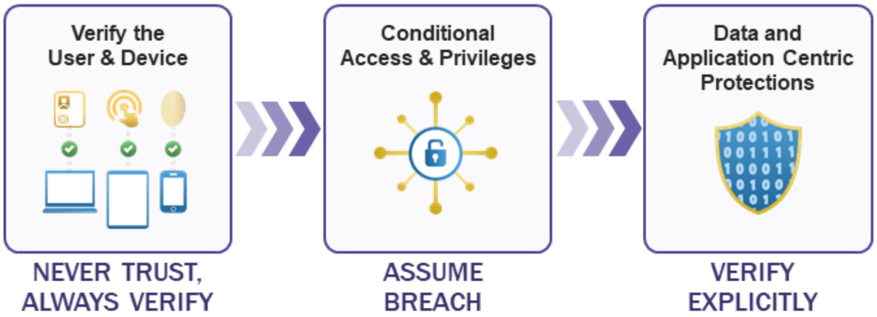
Thunderdome is DISA’s implementation of a zero trust security model at the enterprise level. It is a fundamental change in how we currently are architected to enhance both security and network performance. Zero trust assumes the network is already compromised and is a process that validates the user, device, application and data in a controlled manner.

What this means is that Thunderdome will incorporate greater cybersecurity centered around data protection. As an enhanced security set of capabilities, Thunderdome will significantly help to defend and guard our systems against sophisticated adversaries.

IMPACT

Thunderdome takes us away from the siloed nature of the classic defense-in-depth security model and moves toward integrating security from the end user all the way to the data being accessed. Thunderdome will create a more secure network by emphasizing strong identity and access management controls. The architecture is rooted in identity, with enhanced security controls to provide access to only those individuals who have a need to know.

Thunderdome will incorporate the three basic zero trust principles.



Verify the User & Device
Conditional Access & Privileges
Data and Application Centric Protections
NEVER TRUST, ALWAYS VERIFY
ASSUME BREACH
VERIFY EXPLICITLY

IMPLEMENTATION

Cyberspace attacks across government and private industry continue to rise. To meet this security imperative, Thunderdome will revolutionize our networks so that they are structured and able to provide access control to safeguard data resources and promote advanced data security practices.

- This will be accomplished by widely deploying DISA’s Enterprise Identity, Credential and Access Management (ICAM) solution as the basis for identity.
- DISA will develop a Secure Access Service Edge (SASE) solution for access to DOD workloads, both in the cloud and at on-premises data centers. In front of these workloads, there will be scalable container-based application security stacks.
- The Defense Information Systems Network (DISN) backbone will evolve to a Software Defined-Wide Area Network (SD-WAN) construct with edge-based security stacks deployed at the customer Point of Presence (PoP). This will provide upgraded networking capability and complete security for the DISN backbone.