DAF ZERO TRUST (ZT) LANDSCAPE | COVER PAGE

Adapting and modernizing DAF's Cybersecurity Architecture to enhance security and mission performance for the warfighter

SAF/CN
Publication: 04 JUNE 2025

Increasing competition on the global stage necessitates a more modern security architecture to protect our critical business & mission systems and promote digital readiness. The DAF is adopting a ZT security posture in alignment with the DoD ZT Strategy to a**dvance the CIO Strategic Priorities and address the DoD ZT Mandate**. Implementing a Zero Trust Architecture (ZTA) impacts the DAF IT delivery ecosystem and reinforces the DAF's need for enterprise information sharing capabilities among Joint US Forces, Mission and Industry Partners to enhance operational prowess of joint and coalition warfighting missions.

> "Zero Trust should be the focusing lens that all DAF IT Integration is seen through to ensure Cybersecurity is interlaced across the entire terrain… delivering the right data at the right time to the warfighter."
>
> *- Mr. Heitmann, DAF CTO*

ZT LANDSCAPE SYNOPSIS

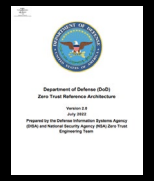
PURPOSE | *The ZT Landscape is a conceptual, capability-centric description of the ZTA and is intended to support capability planning, portfolio management, and IT investment decisions.*

SCOPE | *The SAF/CN, DAF ZT Team, & SIS EA Team developed this diagram to describe how the ZT Transformational Catalysts operate in the DAF environment. This document is intended to be the first step in DAF ZT architecture development and can be iterated on as additional viewpoints are developed that will support the comprehensive DAF ZT reference architecture and other related materials.*

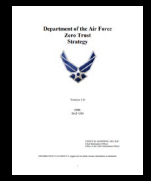
VISION & GOALS | *The ZT Landscape represents a north star enterprise architecture that will facilitate the integration & interoperability of DAF Critical Enabling IT Capabilities, highlight the interdependencies between ZT Core Capabilities, or "transformational catalysts," and showcase how a **ZTA provides Airmen and Guardians with the data they need anytime, anywhere**.*

REFERENCE MATERIALS

DoD Fulcrum IT Advancement Strategy



DoD Zero Trust Reference Architecture



DAF Zero Trust Strategy

DAF Zero Trust I-Plan

OUTCOMES FOR THE WARFIGHTER

WARFIGHTER LETHALITY

Integrate state-of-the-art software and hardware across the DAF to supply capabilities necessary to maintain the competitive edge

UBIQUITOUS CONNECTIVITY

Provide Airmen & Guardians real-time data sharing anytime, anywhere via a resilient and encrypted network

CYBER OPTIMIZATION & RESILIENCE

Strengthen the DAF's ability to rapidly execute the warfighter's mission through a strong, durable, and sustainable cyber posture

ZT TRANSFORMATIONAL CATALYSTS

>NGG

Provides reliable transport to the tactical edge, relieves tech debt of DAF boundaries, implements ZT foundations for DAF Data Centers and Cloud, and ensures the DAF network will be able to respond quickly in a "fight tonight" scenario.

>SDP

Reduces the attack surface by hiding resources and ensuring only authenticated and authorized users have access to the data they need, maintaining scalability without compromising on security.

>ICAM

Centralizes authentication to enable access to the right data at the right time for authorized individuals and NPEs, upholding integrity of systems across the DAF.

>MICROSEGMENTATION

Protects data by limiting communication to only what is necessary for mission objectives and by ensuring every data access request is from an authenticated and authorized source.

>C2C

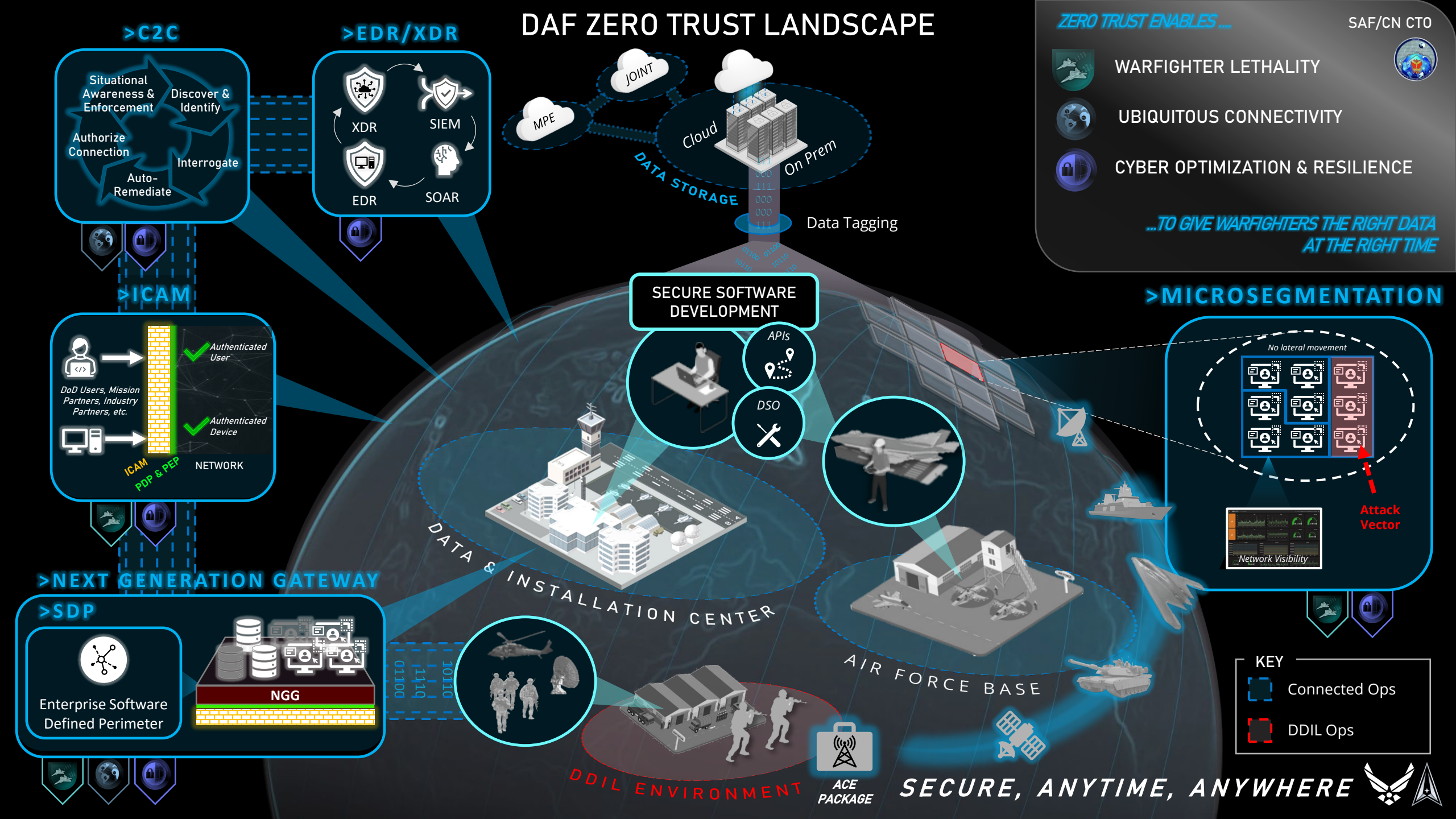
Ensures that devices meet compliance standards prior to granting network access and continuously monitors the connected devices in real-time, safeguarding data from endpoint-specific vulnerabilities.

>EDR/XDR

Powers advanced, cloud-centric endpoint security, leveraging AI/ML to deliver robust protection across all endpoints and servers.

The DAF Zero Trust Landscape serves as an authoritative source of information that should guide and constrain the development of future ZT architectures and solutions, providing a common framework for design and implementation. It will evolve over time as requirements, technology, and best practices change and mature. *For more information, please see the CTO Walking Deck here.*

DAF ZERO TRUST LANDSCAPE



DAF ZERO TRUST (ZT) LANDSCAPE | *ACRONYMS AND EXPANSIONS*

Acronym	Expansion
ACE	Agile Combat Employment
API	Application Programming Interface
CMDB	Configuration Management Database
CTO	Chief Technology Officer
C2C	Comply-to-Connect
DDIL	Denied, Degraded, Intermittent, and Limited
DoDIN	Department of Defense Information Networks
DSO	Development, Security, and Operations
EA	Enterprise Architecture
EDR	Endpoint Detection and Response
EIT	Enterprise Information Technology
EITaaS	Enterprise Information Technology as a Service
EUD	End User Device
FMO	Functional Management Office
ICAM	Identity, Credential, and Access Management
I-Plan	Implementation Plan

Acronym	Expansion
IT	Information Technology
MDM	Mobile Device Management
MPE	Mission Partner Environment
NGG	Next Generation Gateway
NIPRNet	Non-secure Internet Protocol Routed Network
NPE	Non-Person Entity
Ops	Operations
OV	Operational Viewpoint
PAM	Privileged Access Management
PDP/PEP	Policy Decision Point/Policy Enforcement Point
SDP	Software Defined Perimeter
SIEM	Security Information and Event Management
SIS	Enterprise Standards Division
SOAR	Security Orchestration, Automation, and Response
XDR	Extended Detection and Response
ZTA	Zero Trust Architecture