References

- DoD V1.1 ZT Reference Architecture
  - Zero Trust Reference Architecture
  - https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf
- NIST Special Publication 800-207
  - Zero Trust Architecture
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Zero Trust

- Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the Internet) or based on asset ownership (enterprise or personally owned).”
  - Zero Trust requires **designing a simpler and more secure architecture** without impeding operations or compromising security. The classic perimeter/defense-in-depth cybersecurity strategy repeatedly shows to have limited value against well-resourced adversaries and is an ineffective approach to address insider threats.
- DOD Chief Information Officer’s (CIO) vision for creating “a more secure, coordinated, seamless, transparent, and cost- effective IT architecture that transforms data into actionable information and ensures dependable mission execution in the face of a persistent cyberthreat.”

Level Set

- Zero Trust (ZT) is a cybersecurity strategy and framework that embeds security throughout the architecture to prevent malicious personas from accessing our most critical assets.
- This Reference Architecture describes Enterprise standards and capabilities.
  - Single products/suites can be adopted to address multiple capabilities.
  - **Integrated vendor suites of products rather than individual best of breed components will assist in reducing cost and risk to the government.**

Level Set

- Implementing Zero Trust requires designing a simpler and more efficient architecture without impeding operations to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services viewed as compromised.
- Zero Trust implements continuous **multi-factor authentication, micro- segmentation, encryption, endpoint security, analytics, and robust auditing to DAAS** seven pillars to deliver cyber resiliency.
- A Zero Trust framework reduces the attack surface, reduces risk, and ensures that if a device, network, or user/credential is compromised, the damage is quickly contained and remediated.

Modernize Information Enterprise to Address Gaps and Seams

- Usability and security challenges stem from years of building infrastructure along organizational, operational and doctrinal boundaries, with multiple security and support tiers, enclaves and networks. **Capabilities developed in silos have inevitably resulted in disconnects and gaps in the command structure and processes that preclude establishing a comprehensive, dynamic, and near-real time common operating picture (COP).** Adversaries have exploited these logical, technological, and organizational gaps and seams.

Simplify Security Architecture.

- **A fragmented approach to information technology and cybersecurity has led to excessive technical complexity**, which creates vulnerabilities in our cyber hygiene, inadequately addresses internal and lateral threats and results in high levels of latency.
- Complex security techniques render the user experience painfully unresponsive and unusable.

Produce Consistent Policy.

- This is a critical lesson-learned from industry that **automated cybersecurity policies must be consistently applied across environments (on/off premises) for maximum effectiveness.** Technology leaders have relied on perimeter defense systems that fetter access and grant implicit trust based on network location. Waivers and exceptions to written policies, based on short term operational needs, have led to inconsistently managed, reconfigured, and/or disabled security systems, thereby making them porous and ineffective.

Optimize Data Management Operations

- The success of DOD missions, ranging from payroll to missile defense, are **increasingly dependent on structured and tagged data**. Advanced analytics also depend on this. While data standards and policy exist, they are disparate and inconsistently implemented. This results in:
  - Interoperability challenges between applications, organizations, and with external partners,
  - Inherent system inefficiencies and vulnerabilities,
  - Poor/frustrating user experience, and
  - Hampered abilities to fully leverage the benefits of cloud computing, data analytics, machine learning, and artificial intelligence

Provide Dynamic Credentialing and Authorization.

- Persona based identities, credentials, and attributes are not dynamic or context aware and come from disparate sources.
  - Two factor authentications, in the form of the Common Access Card (CAC), has not kept pace with multi-factor authentication advances in industry.
  - Non-person identities are not widely addressed, nor are identities for bots and the Internet of Things (IoT).

Goals

- Support the DOD vision of “a more secure, coordinated, seamless, transparent, and cost-effective IT architecture... that ensures dependable mission execution in the face of a persistent cyber threat.”
- Incremental migration approach to cybersecurity with an end state of an interoperable, fully functioned, optimized cybersecurity architecture that secures our critical assets and data from intentional or unintentional malicious activity.
  - The desired outcome is the roll out of an employable set of enterprise Zero Trust capabilities each consisting of standards, devices, and processes that are measurable, repeatable, supportable, and extensible, to any organization on the DODIN, and federated across the DODIN.

Zero Trust Architecture Capability

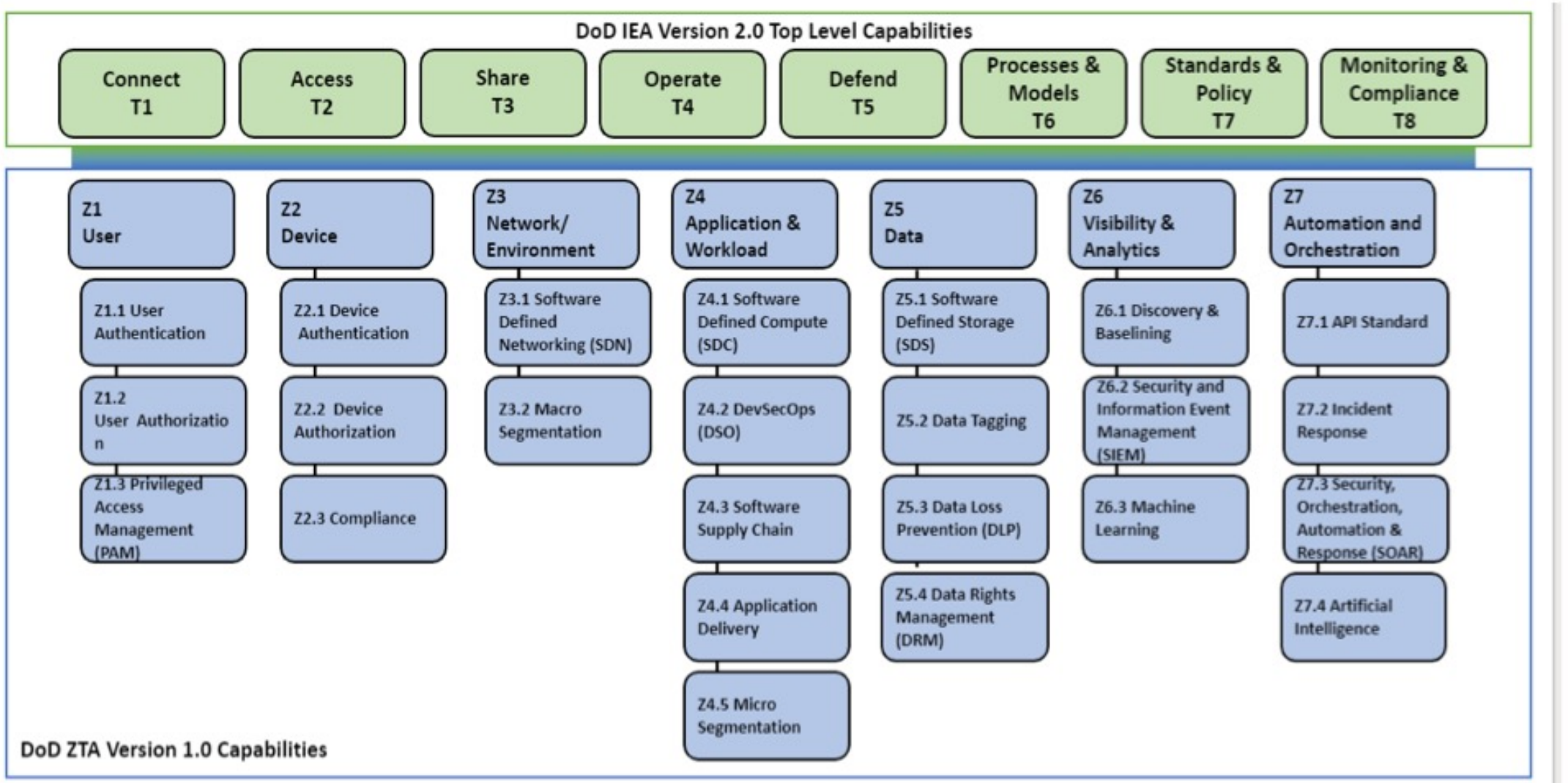

Figure 1: Capabilities Taxonomy (CV-2)

Zero Trust Pillars and Capabilities

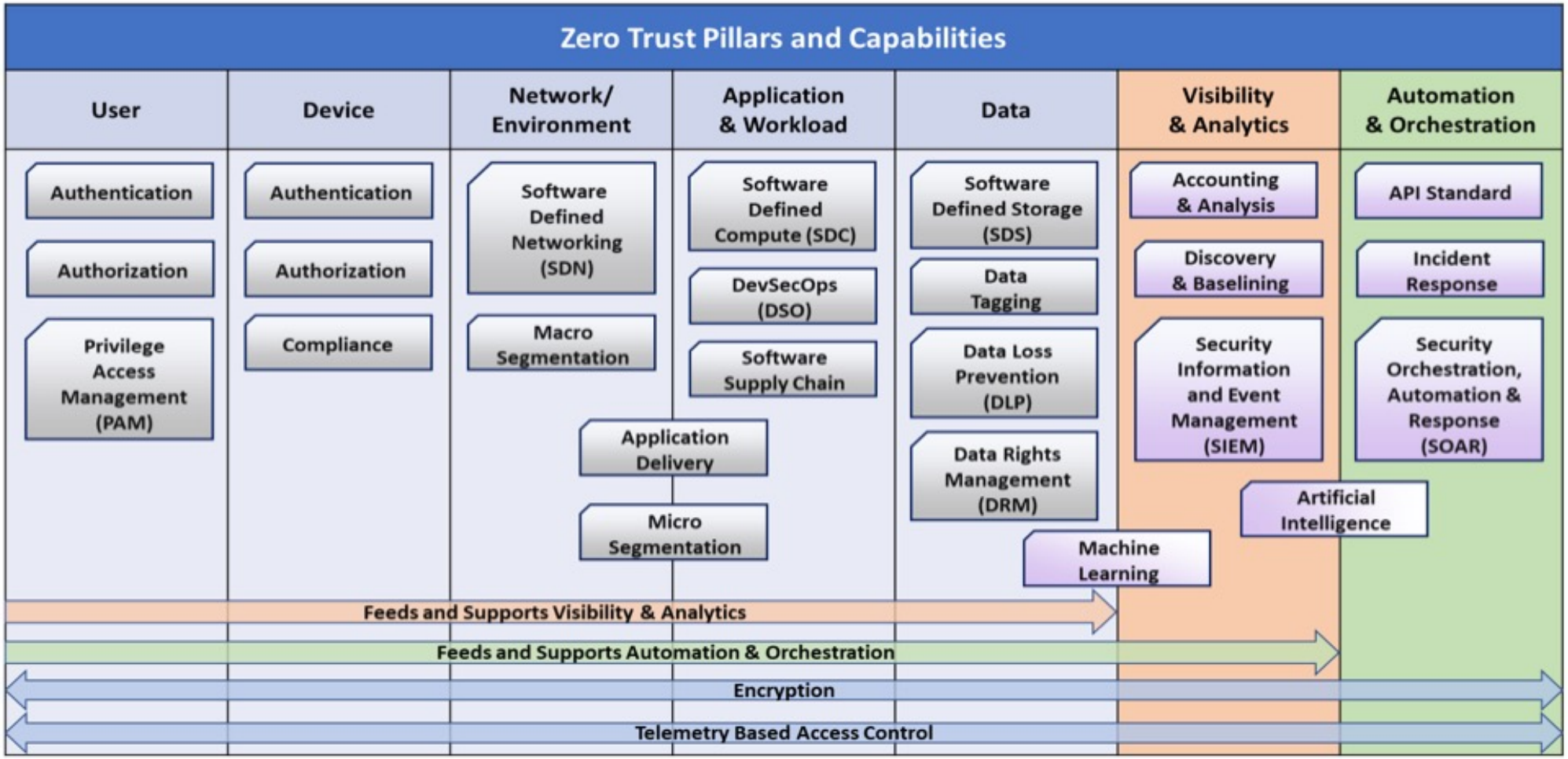

Figure 4: Zero Trust Pillars

High Level Operational Concept

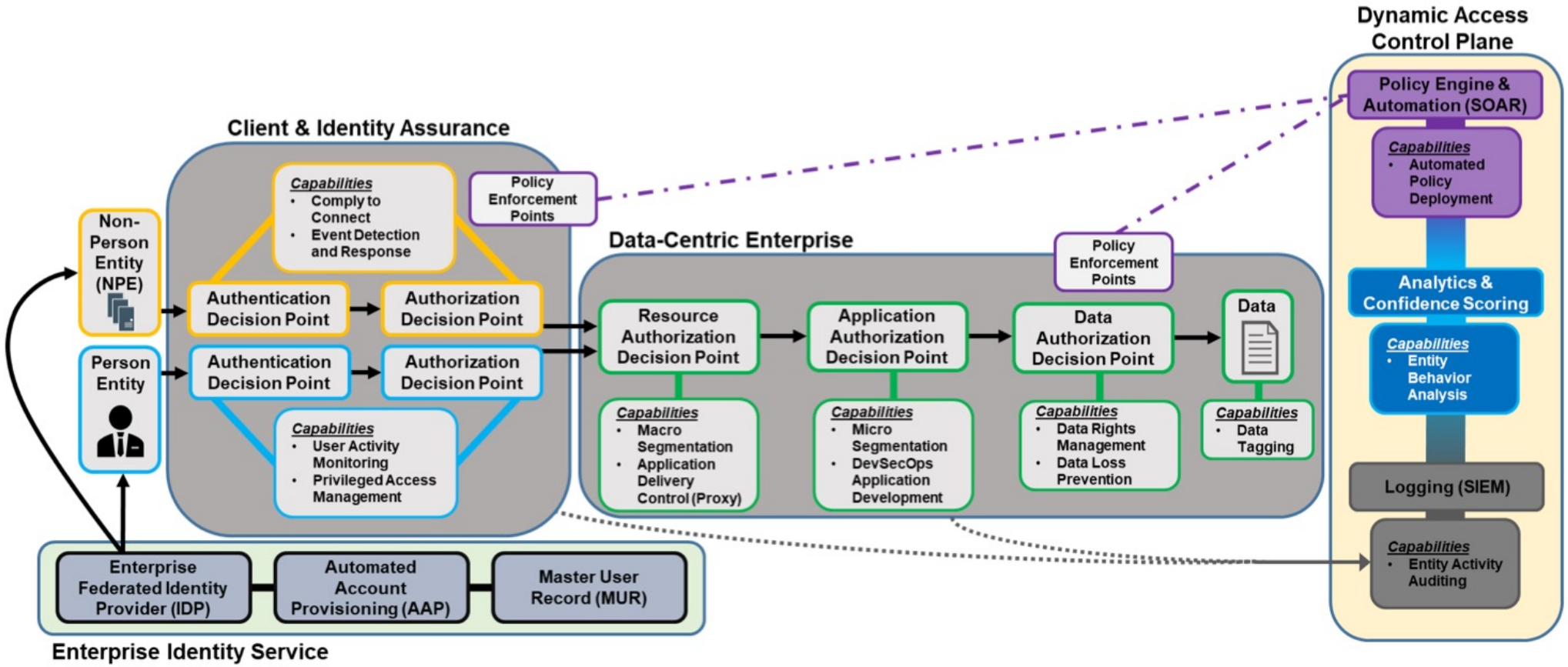

Figure 2: High-Level Operational Concept (OV-1)

Possible Actions

- Define data exchanges to achieve Zero trust
- PACE to collect Zero trust status from policy enforcement points
  - Collect and feed to provide policy engine and automation (SOAR)
- SIEM to collect and correlate events from pillars
- Analytics/Risk Scoring on top of SIEM for behavioral analysis