Adopting the Zero Trust Paradigm

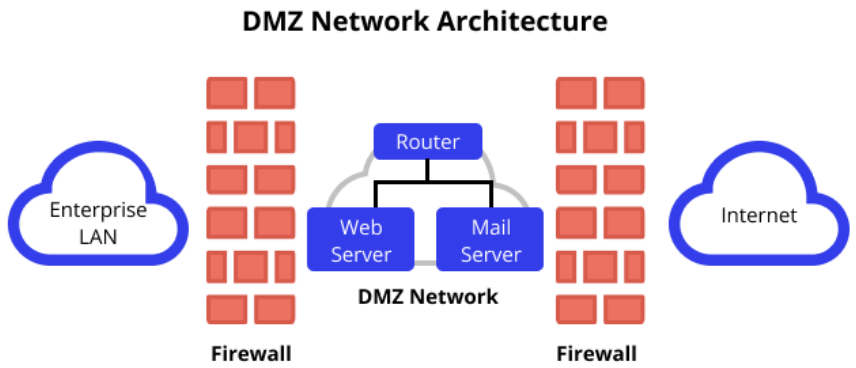
Eric Hibbard, CISSP, FIP, CISA
Samsung Semiconductor, Inc.

SNIA COMPUTE, MEMORY, AND STORAGE SUMMIT

Solutions, Architectures, and Community
VIRTUAL EVENT, MAY 21-22, 2024

Perimeter Security Model

- Many organizations use a traditional perimeter security model
- Assumes that all users inside the network can be trusted while all users outside the network are untrustworthy
- Assumes an effective barrier can be established and maintained
- Resources accessed from the Internet are often located within a DMZ
- Firewalls, intrusion detection systems (IDS), and virtual private networks (VPN) are common elements of perimeter security



Zero Trust (ZT) Security Model

- Primarily focused on data and service protection; can also include
  - all enterprise assets (devices, infrastructure components, applications, virtual and cloud components)
  - subjects (end users, applications and other non-human entities that request information from resources)
- Assumes that an attacker is present in the environment
- Assumes an enterprise-owned environment is no different (i.e., no more trustworthy) than any non-enterprise-owned environment

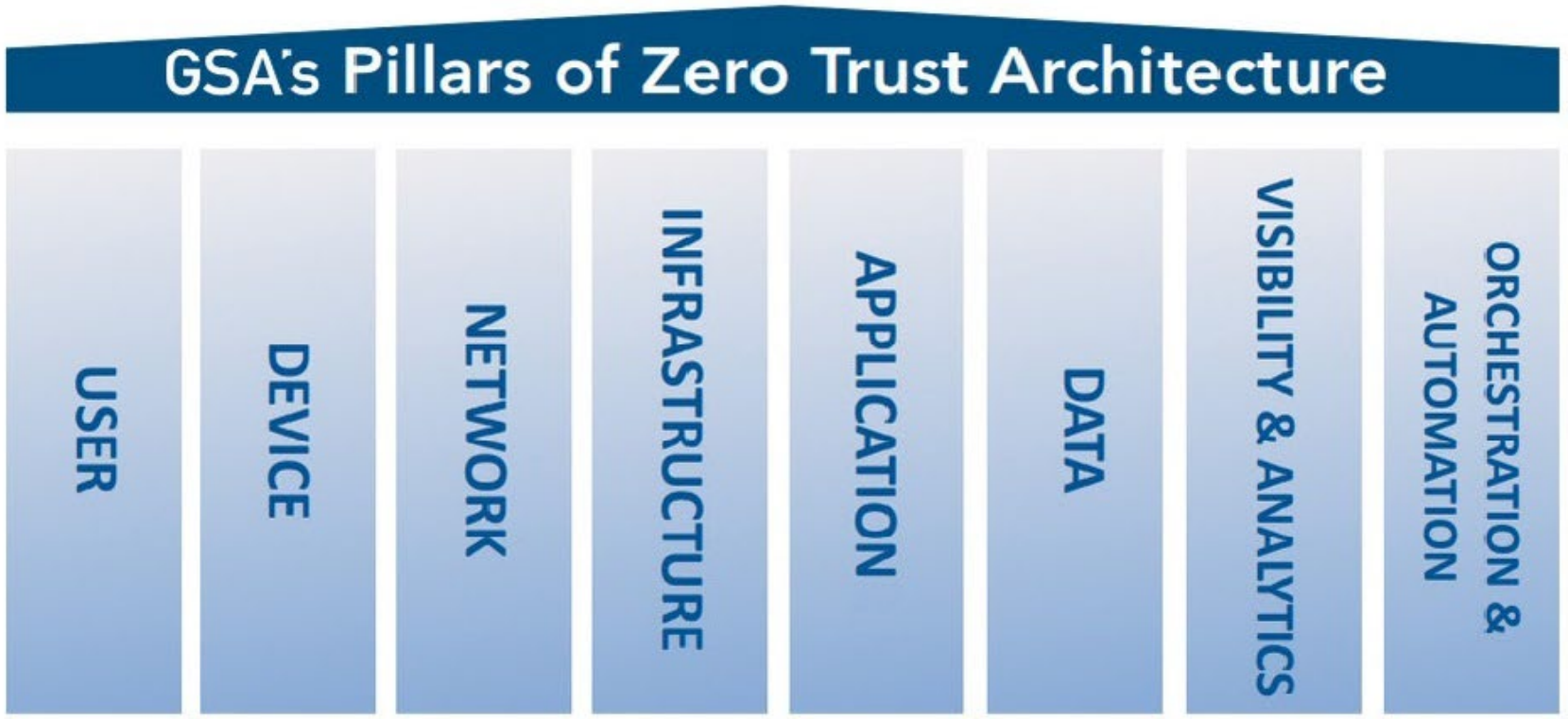
- In this paradigm, there is no implicit trust

Tenets of Zero Trust

- All data sources and computing services are considered resources
- All communication is secured regardless of network location
- Access to individual enterprise resources is granted on a per-session basis
- Access to resources is determined by dynamic policy
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed
- The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture

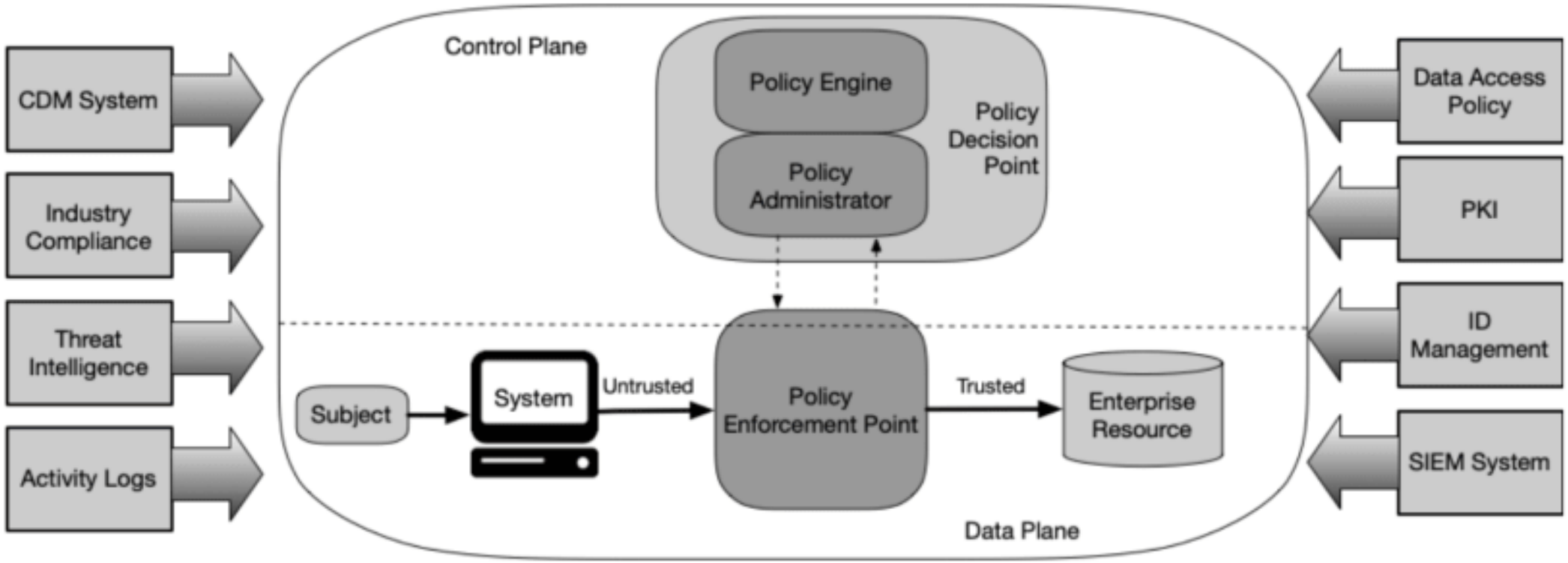
Source: NIST SP 800-207 Zero Trust Architecture

Elements of ZT Architecture



NOTE: The number of pillars/elements can vary within US Government entities.

Core ZT Logical Components



Enterprises need to develop and maintain dynamic risk-based policies for resource access and set up a system to ensure that these policies are enforced correctly and consistently for individual resource access requests.

Source: NIST SP 800-207

Core ZT Logical Components (cont.)

- **Policy engine (PE):** responsible for the ultimate decision to grant access to a resource for a given subject
- **Policy administrator (PA):** responsible for establishing and/or shutting down the communication path between a subject and a resource (via commands to relevant PEPs)
- **Policy enforcement point (PEP):** responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource
- **Continuous diagnostics and mitigation (CDM) system:** gathers information about the enterprise asset's current state and applies updates to configuration and software components

Status of ZT

- US Government is implementing in various agencies
- Many suppliers producing ZT products and services; some adoption in their own organizations
- International partners (e.g., NATO) are interested in ZT
- International specifications/standards:
  - ISO/IEC 27002:2022 includes six ZT principles that are starting to be leveraged
  - Draft IEEE P2887, Recommended Practice for Zero Trust Security
  - Draft IEEE P3409, Standard for a Zero Trust Security Framework

ISO/IEC 27002:2022 – ZT Principles

a) assume the organization's information systems are already breached and thus not be reliant on network perimeter security alone;

b) employing a "never trust and always verify" approach for access to information systems;

c) ensuring that requests to information systems are encrypted end-to-end;

d) verifying each request to an information system as if it originated from an open, external network, even if these requests originated internal to the organization (i.e., not automatically trusting anything inside or outside its perimeters);

e) using "least privilege" and dynamic access control techniques. This includes authenticating and authorizing requests for information or to systems based on contextual information such as authentication information, user identities, data about the user endpoint device, and data classification;

f) always authenticating requesters and always validating authorization requests to information systems based on information including authentication information and user identities, data about the user endpoint device, and data classification, for example enforcing strong authentication (e.g., multi-factor).

Summary

- ZT appears to be here to stay (i.e., not just the latest security fad)
- ZT is a significant departure from traditional perimeter security
- Transitioning to ZT requires careful planning and significant resource to accomplish
- It is possible to operate in a hybrid model; start small and focus on most critical/valuable assets

- Join IEEE Zero Trust Security WG (ZTSWG) standardization activities

Please take a moment to rate this session.

Your feedback is important to us.