Zero Trust Software Registry

Software and Supply Chain Assurance Fall forum

Sept 13, 2023

Amit Kapoor, Chief Security Officer, INTEGRITY Security Services

Content

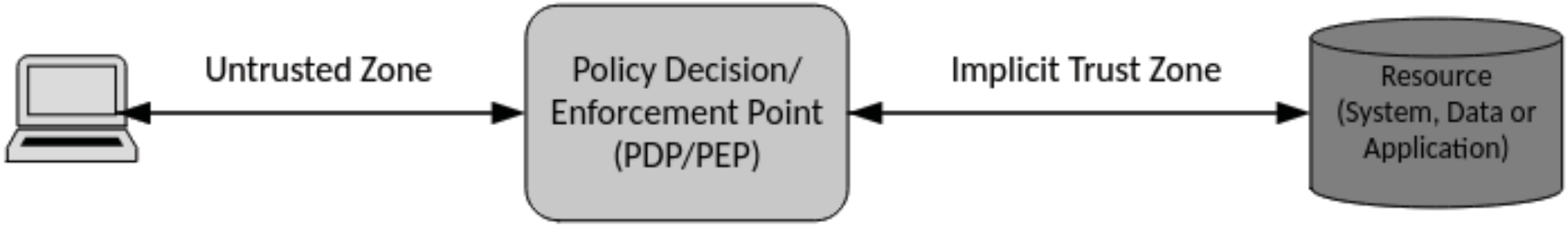
- What is Zero Trust (ZT)
  - Principles
  - Access Model
- Zero Trust Architecture (ZTA)
  - Policy Management
  - Logical Components
- Why Zero Trust for Software Supply Chain
- Zero Trust Software Registry Architecture
  - ZT PKI
  - ZT Software Registry
- Questions
- References

Zero Trust: Background

Zero Trust Principles

- 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—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes
- The enterprise monitors and measures the integrity and security posture of all owned and associated asset
- 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

Zero Trust Access Model

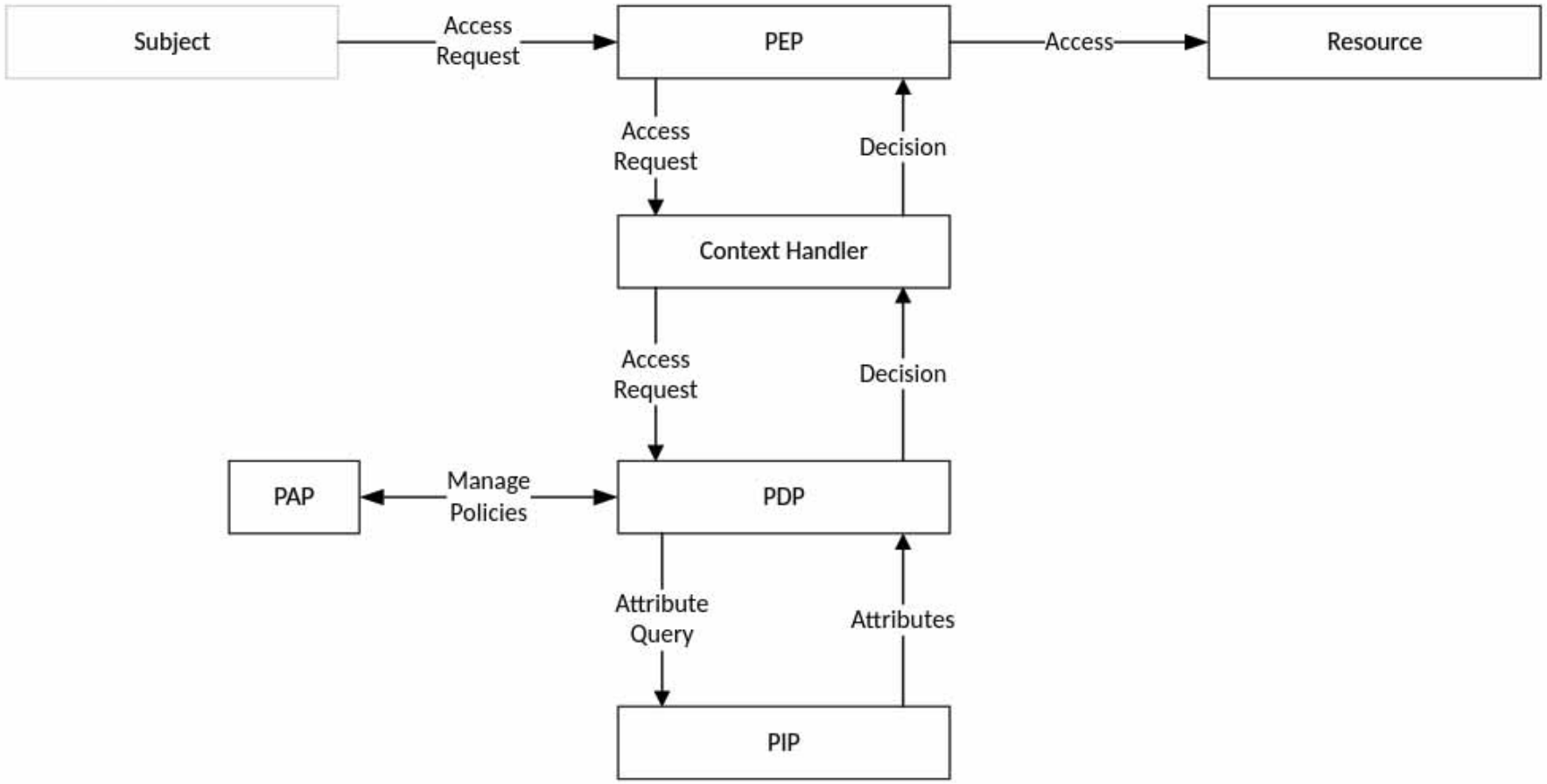


Contrast with Perimeter Security

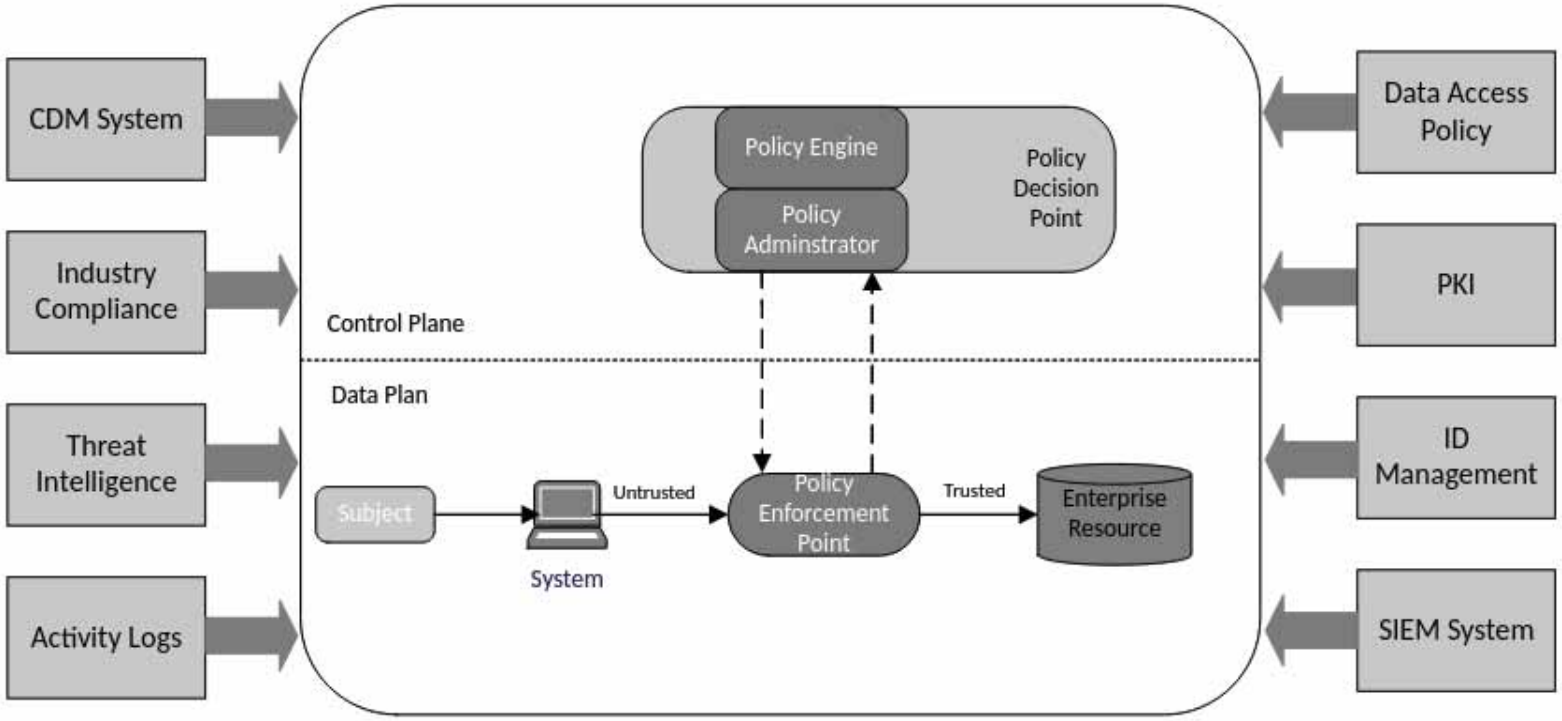
- Organizations typically defend their systems via castle-and-moat approach (example, firewalls) where goal is to prevent external actors from accessing them
- Implications:
  - This approach assumes every user inside a network is trustworthy and should have access
  - If a bad actor has network access, they can laterally move within the network to expose sensitive data, install malware, and cause data breaches
  - Makes it difficult for partners and employees to access systems from outside
  - Creates a fundamental contradiction between the two conflicting goals, one is about enabling outside access while the other is trying to keep bad actors out.

Zero Trust Architecture Model

Policy Based Model



Logical Components of Zero Trust Architecture



CDM: Continuous Diagnostics & Monitoring
PKI: Public Key Infrastructure
SIEM: Security Information & Event Management

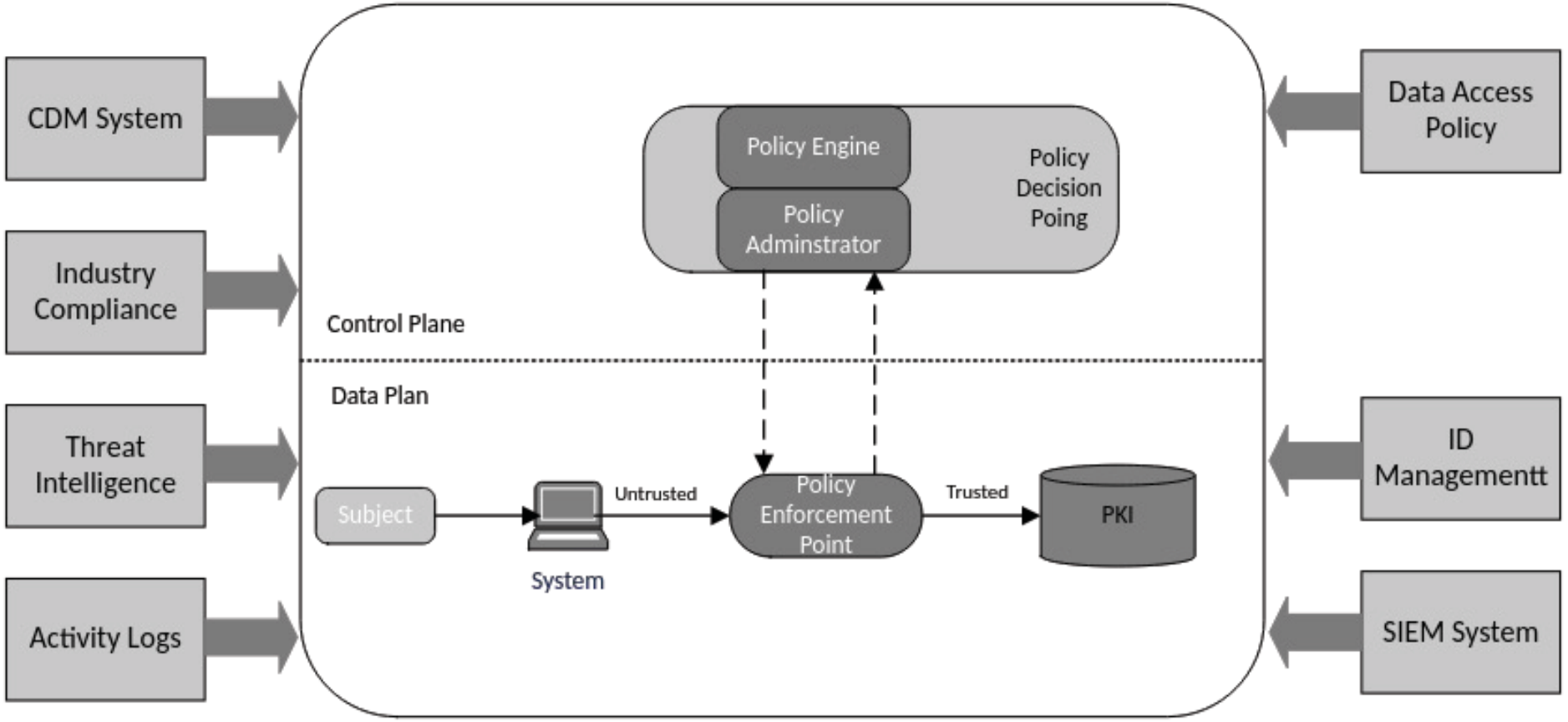
Why Zero Trust for Software Supply Chain

Key Drivers

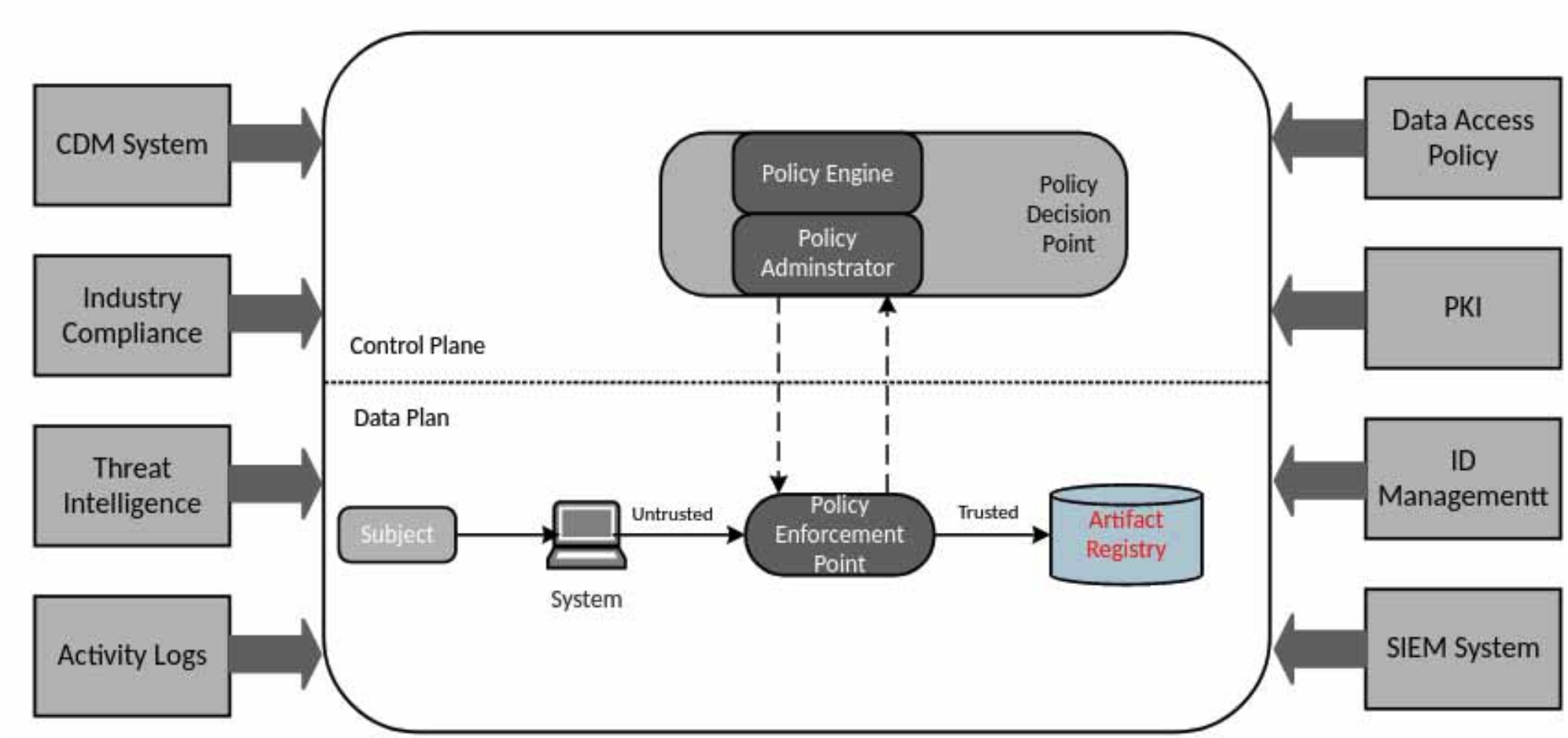
- President Biden's executive order (May 12, 2021) on improving national cybersecurity identifies software supply chain (Sec 4) as one of the critical components as part of the overall mandated Zero trust architecture implementation for Federal agencies
- Software Registry provides a single location for storing and managing your software packages and is paramount in ensuring these are not tampered with. Treating this an enterprise resource and molding it into ZTA will minimize potential attacks
- A ZTA for Software Registry can secure supply chains by removing organizations' implicit faith in device and employee security
- The constant re-validation in ZTA keeps attackers from compromising the system
- Dynamic policies will allow the system to respond to changing conditions

Zero Trust Software Registry Architecture

Core: Zero Trust PKI



Zero Trust Software Registry



References

- NIST
  - Zero Trust Architecture
  - Guide to Attribute Based Access Control (ABAC) Definitions and Considerations
- Office of US President
  - Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
- US Department of Defense (DoD)
  - Zero Trust Strategy
  - Zero Trust Capability Execution Roadmap (COA 1)
- U.S. Cybersecurity and Infrastructure Security Agency (CISA)
  - Securing the Software Supply Chain (Developers)
  - Securing the Software Supply Chain (Suppliers)