Zero Trust Security

Geoffrey Sanders

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM21-0325

Agenda

Foundations

Architecture

Implementation

Zero Trust Security

Foundations

Overview

Security model developed by John Kindervag at Forrester (2009).

Goals

- Remove implicit trust.
- Move security from the network to users, applications, and workloads.

Principles

Ensure all resources are accessed securely, regardless of location.

Adopt a least privilege strategy and strictly enforce access control.

Inspect and log all traffic.

Ensure all components support APIs for event and data exchange.

Automate actions across environments and systems, driven by context and events.

Deliver tactical and strategic value.

Ref: [Zero Trust Security]

Working Definition

A Zero Trust system is an integrated security platform that uses contextual information from identity, security and IT infrastructure, and risk analytics tools to inform and enable the dynamic enforcement of security policies uniformly across the enterprise. Zero Trust shifts security from an ineffective perimeter-centric model to a resource and identity-centric model. As a result, organizations can continuously adapt access controls to a changing environment, obtaining improved security, reduced risk, simplified and resilient operations, and increased business agility.

Ref: [Zero Trust Security]

Platform Requirements

1. Data plane communications must be encrypted. Any exceptions must be deliberate (e.g., DNS).
2. System must be able to enforce access controls for all types of resources. Access control mechanisms must be driven by identity-centric and contextual policies.
3. Data resource protections should be able to use identity and contextual policies to control access.
4. System and policy model must support securing all users in all locations. Policy model and controls must be consistent for remote and on-premise users.
5. Devices must be able to be inspected for their security posture and configuration prior to being granted access, and periodically thereafter.

Platform Requirements

6. It must be possible to distinguish BYOD from corporate-managed devices, and control the level of access accordingly.
7. Access to any network resource must be explicitly granted by policy. No user or device should inherently have broad network access.
8. Access controls must be able to distinguish between different services on the same network resource. For example, access to HTTPS must be granted separately from access to SSH.
9. Access to specific data elements contained within the applications or containers that have different classifications must be enforced based on business policy.
10. Network traffic metadata must be logged and enriched with identity context.

Platform Requirements

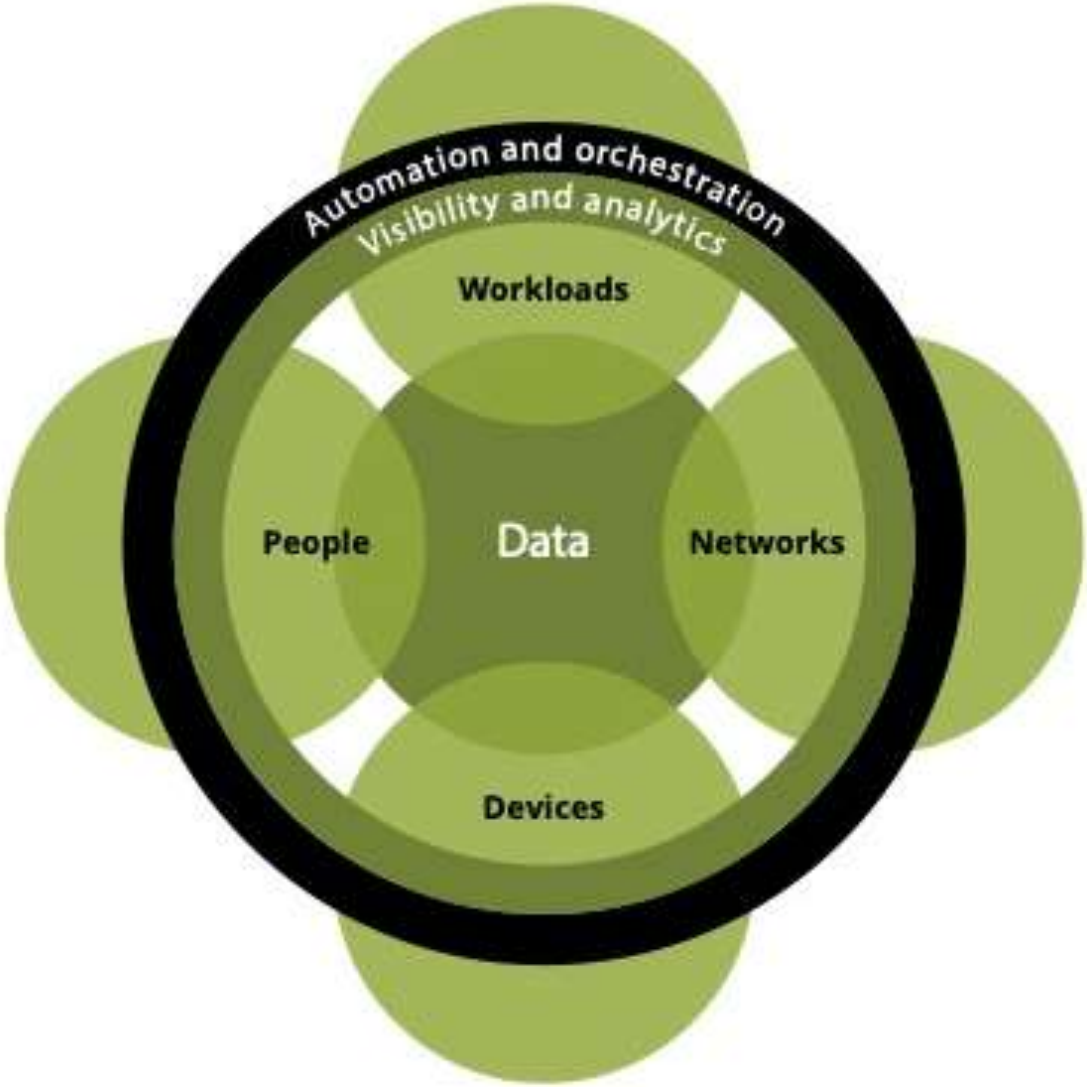
11. Network traffic must be able to be examined for security and data loss purposes.
12. Workloads transferred into the cloud should include the same access control policies as defined by on-premises solutions.
13. Automation must include identity-centric details to provide efficient and effective incident response.
14. Logs must be included in analytics tools for effective and dynamic enforcement of policies.

Ref: [Zero Trust Security]

Zero Trust Security

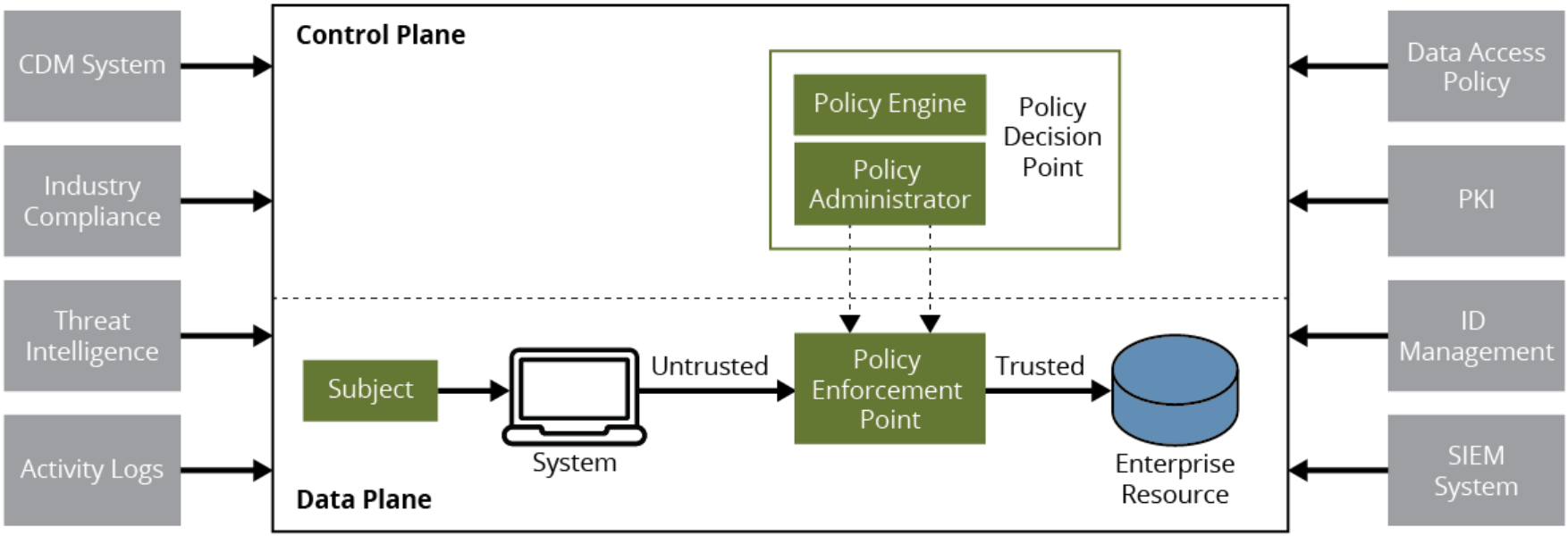
Architecture

Forrester Zero Trust eXtended (ZTX) Model



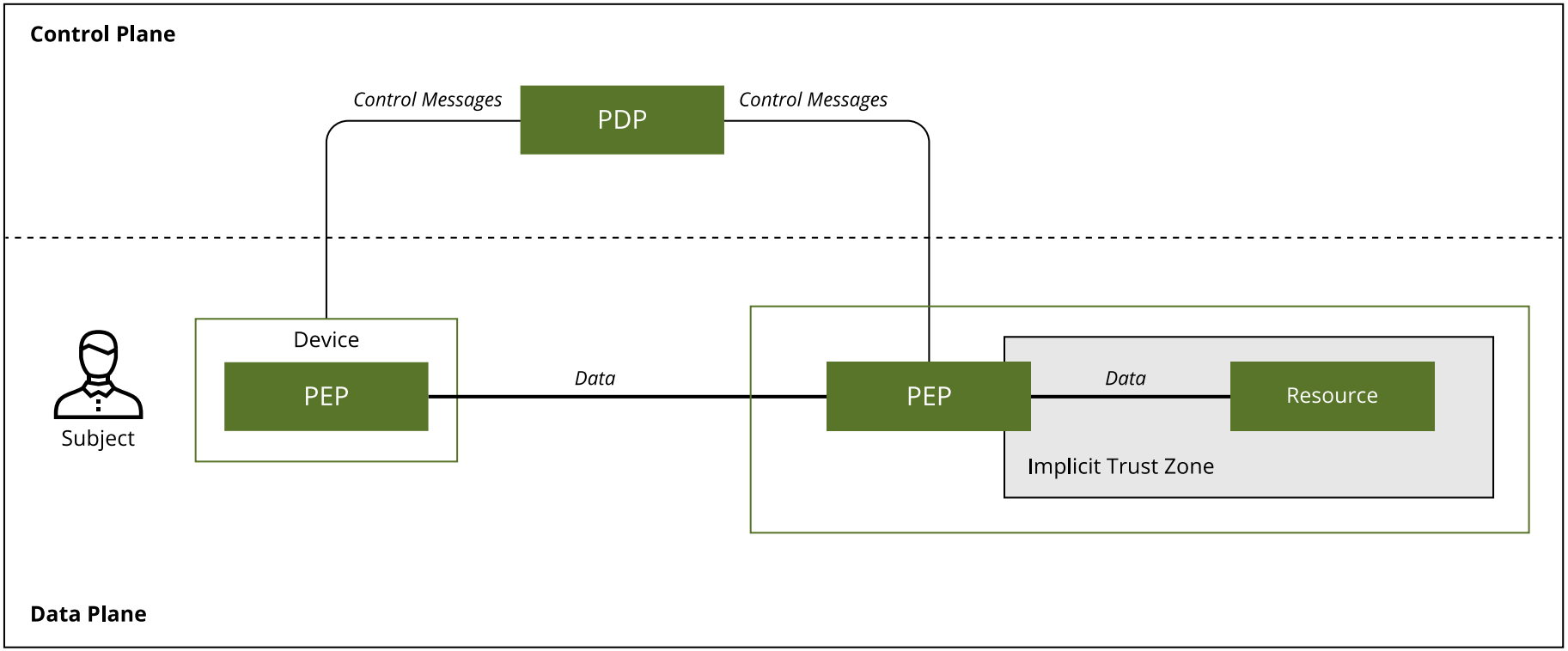
Ref: [ZTX]

NIST Zero Trust Model Components



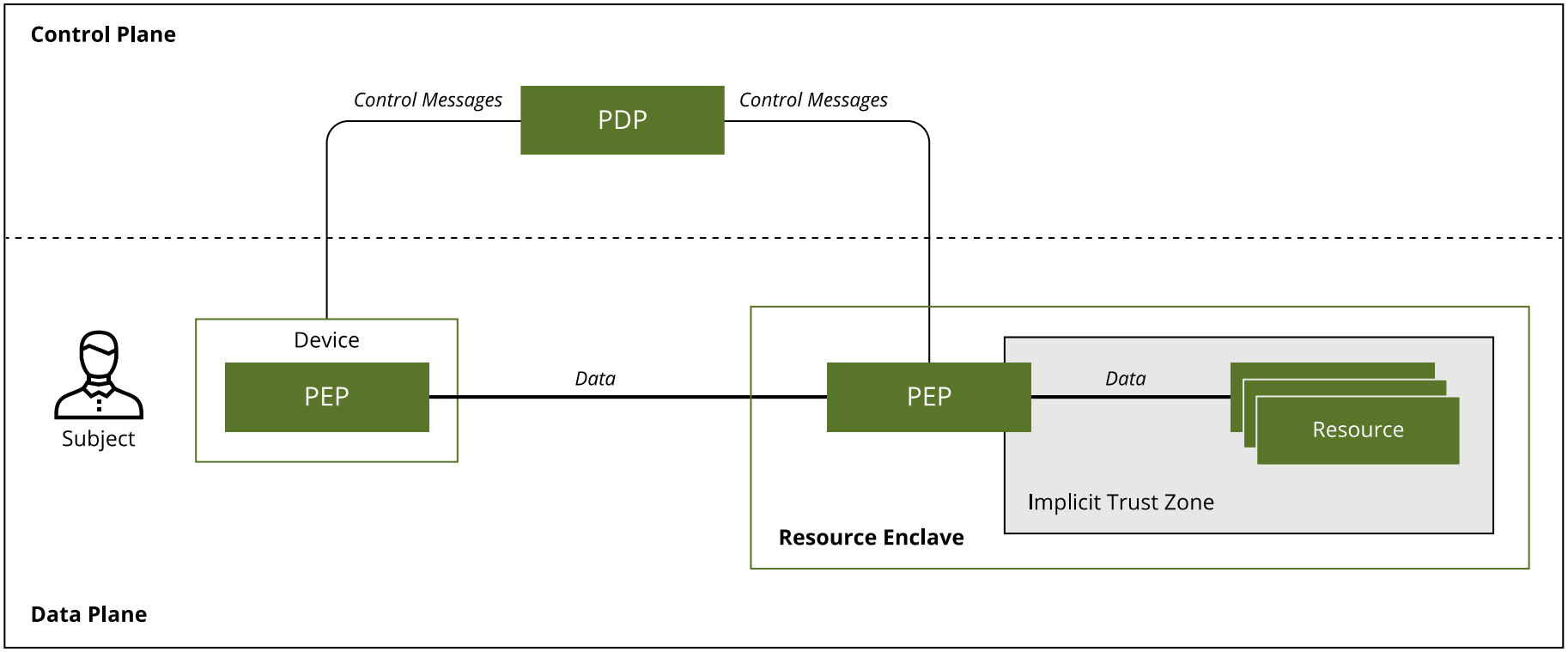
Ref: [NIST 800-207]

Resource-Based Deployment Model



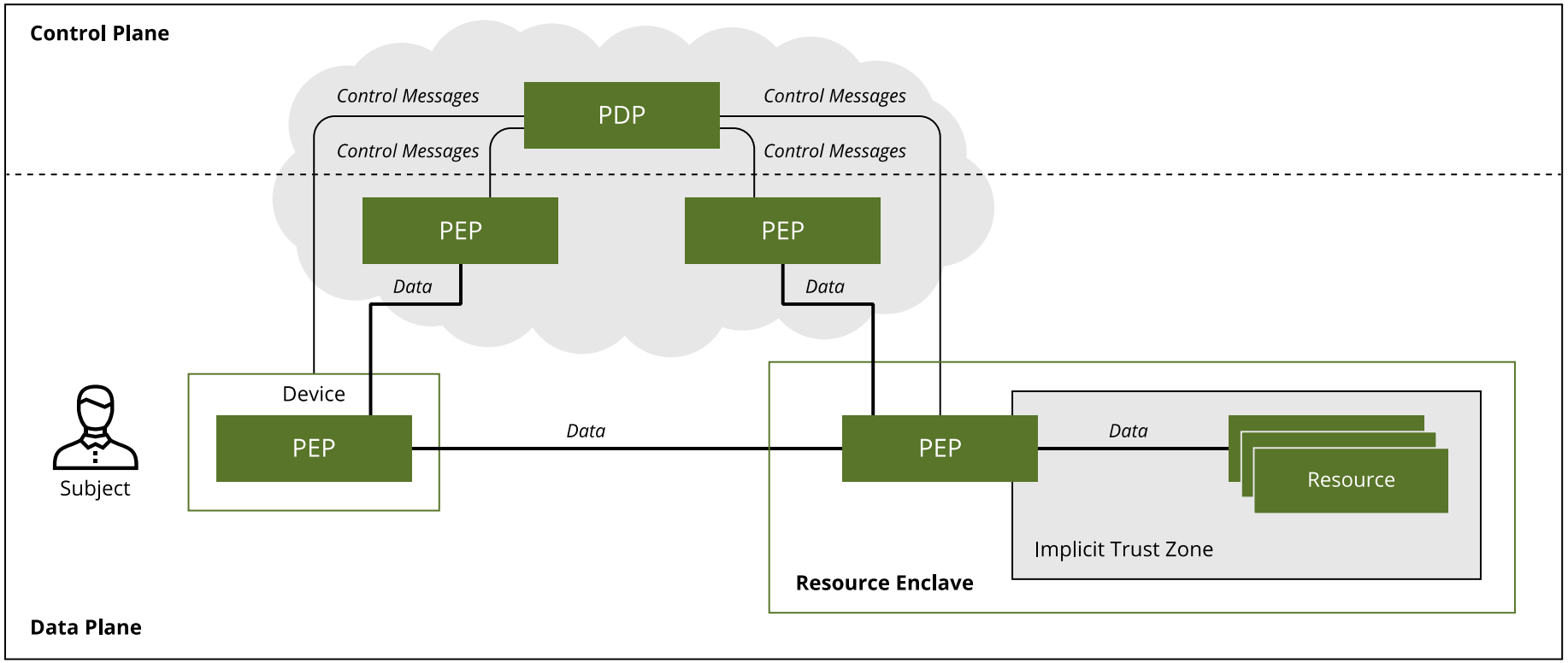
Ref: [Zero Trust Security]

Enclave-Based Deployment Model



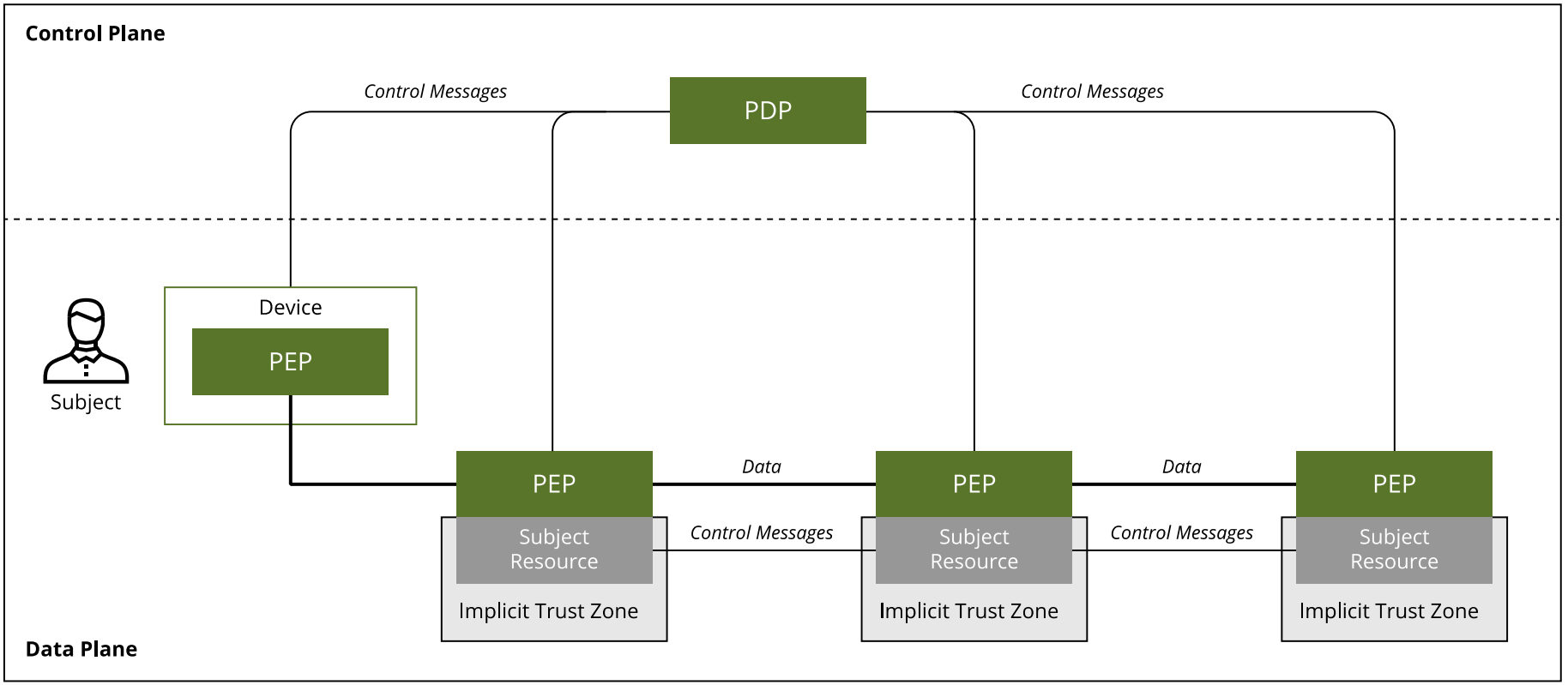
Ref: [Zero Trust Security]

Cloud-Routed Deployment Model



Ref: [Zero Trust Security]

Microsegmentation Deployment Model



Ref: [Zero Trust Security]

Threats

1. Subversion of zero trust architecture decision process.
2. Denial-of-service or network disruption.
3. Stolen credentials/insider threat.
4. Visibility on the network.
5. Storage of system and network information.
6. Reliance on proprietary data formats or solutions.
7. Use of non-person entities (NPE) in zero trust architecture administration.

Ref: [NIST 800-207]

NIST 800-207 Threat Mapping

Zero Trust Architecture Threat	Components and Inputs	Proposed Mitigation
Subversion of ZTA Decision Process	Policy Engine Policy Administrator	Configuration Management Monitoring Detection
Denial-of-Service or Network Disruption	Policy Enforcement Point Policy Engine Policy Administrator	Resilience
Stolen Credentials/Insider Threat	ID Management Data Access Policy	Architecture Contextual Trust Algorithm
Visibility on the Network	Activity Logs SIEM	Network Traffic Inspection Network Traffic Logging Metadata Machine Learning
Storage of System and Network Information	Activity Logs CDM System Industry Compliance Data Access Policy PKI ID Management SIEM Information Policy Administrator Policy Engine	Restrictive Data Access Policies
Reliance on Proprietary Data Formats or Solutions	Activity Logs CDM System Industry Compliance Data Access Policy PKI ID Management SIEM Information Policy Administrator Policy Engine	Service Provider Evaluation Vendor Security Controls Enterprise Switching Costs Supply Chain Risk Management Performance Stability
Use of Non-person Entities (NPE) in ZTA Administration	Policy Engine Policy Administrator	Regular Retuning Analysis

Ref: [Zero Trust Journey]

Zero Trust Security

Implementation

Zero Trust is a Journey

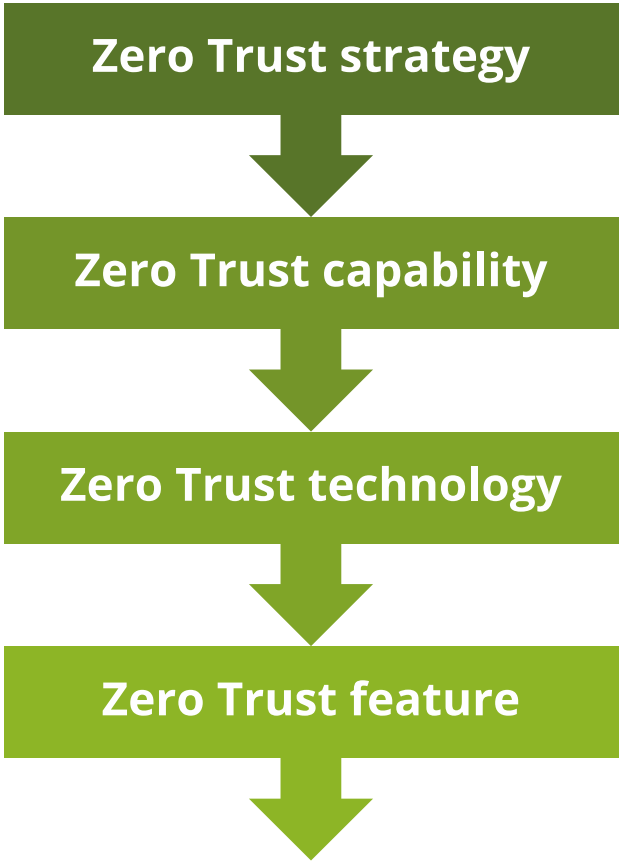
System-of-systems architecture.

Each journey is unique.

Common implementation methods.

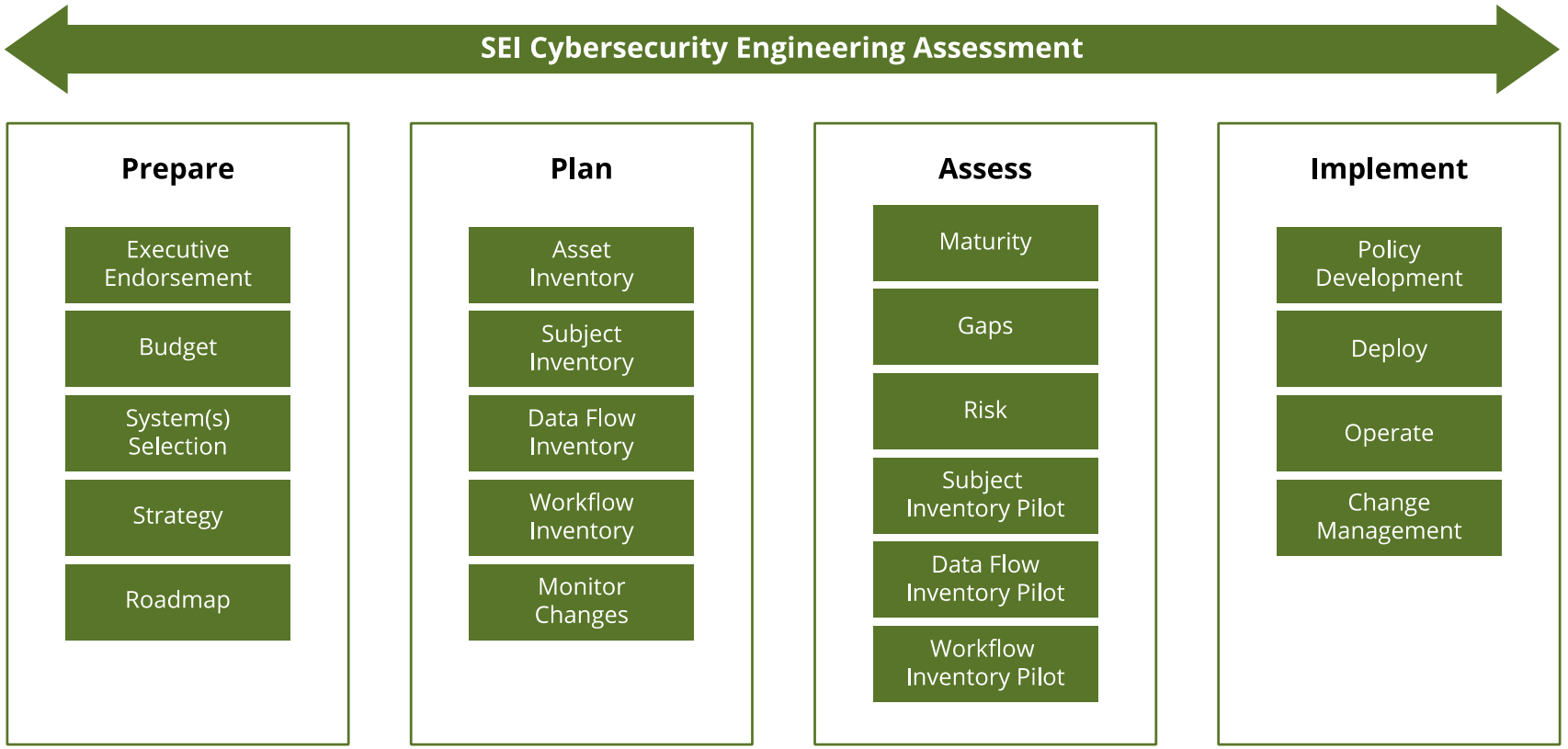
- Framework
- Roadmap
- Questionnaire

Forrester ZTX Framework



Ref: [ZTX]

SEI Zero Trust Journey



Current Trends

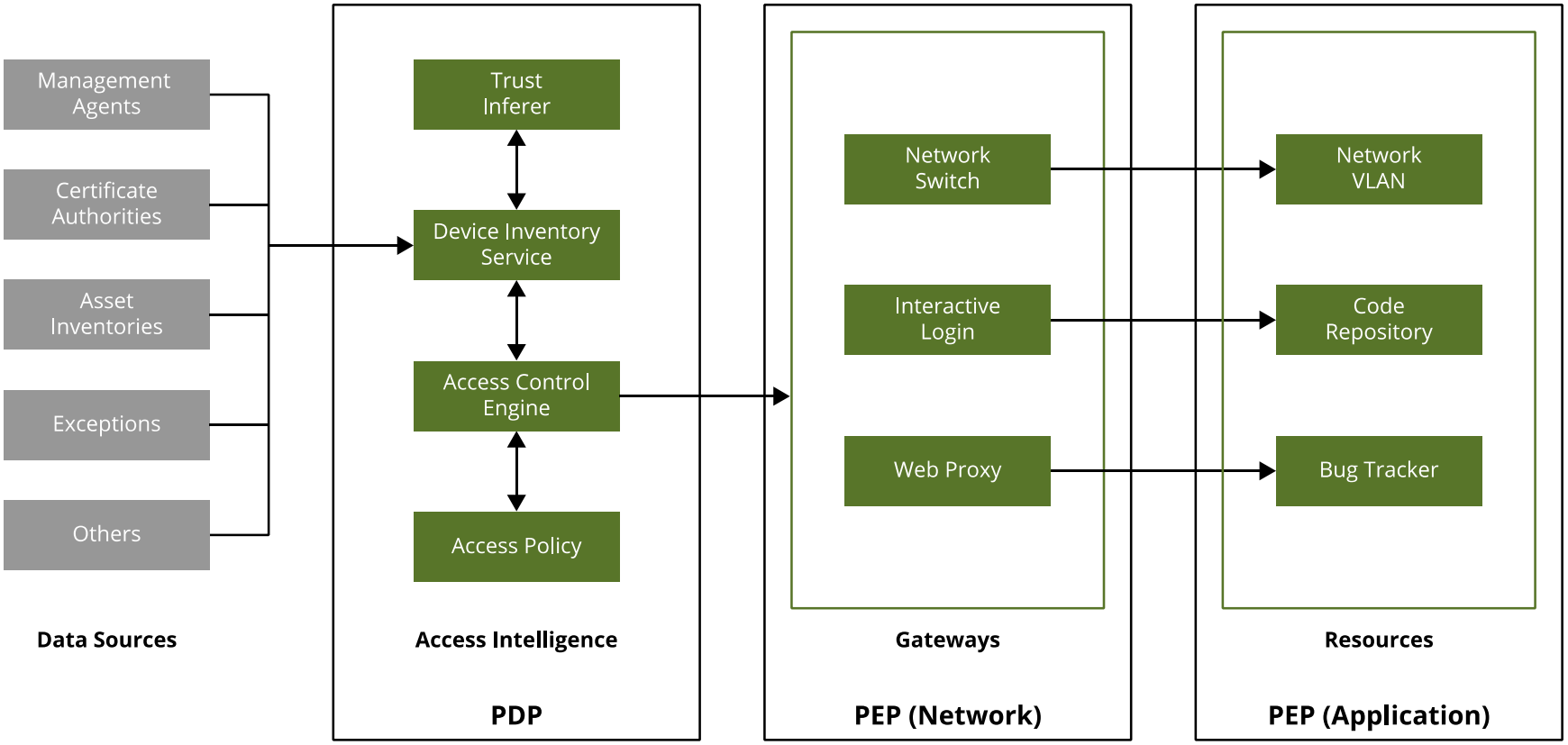
Large, well funded and high-performing organizations publish success stories.

- Google
- Microsoft
- US Air Force (CloudOne/PlatformOne)

Remaining organizations focus on specific areas.

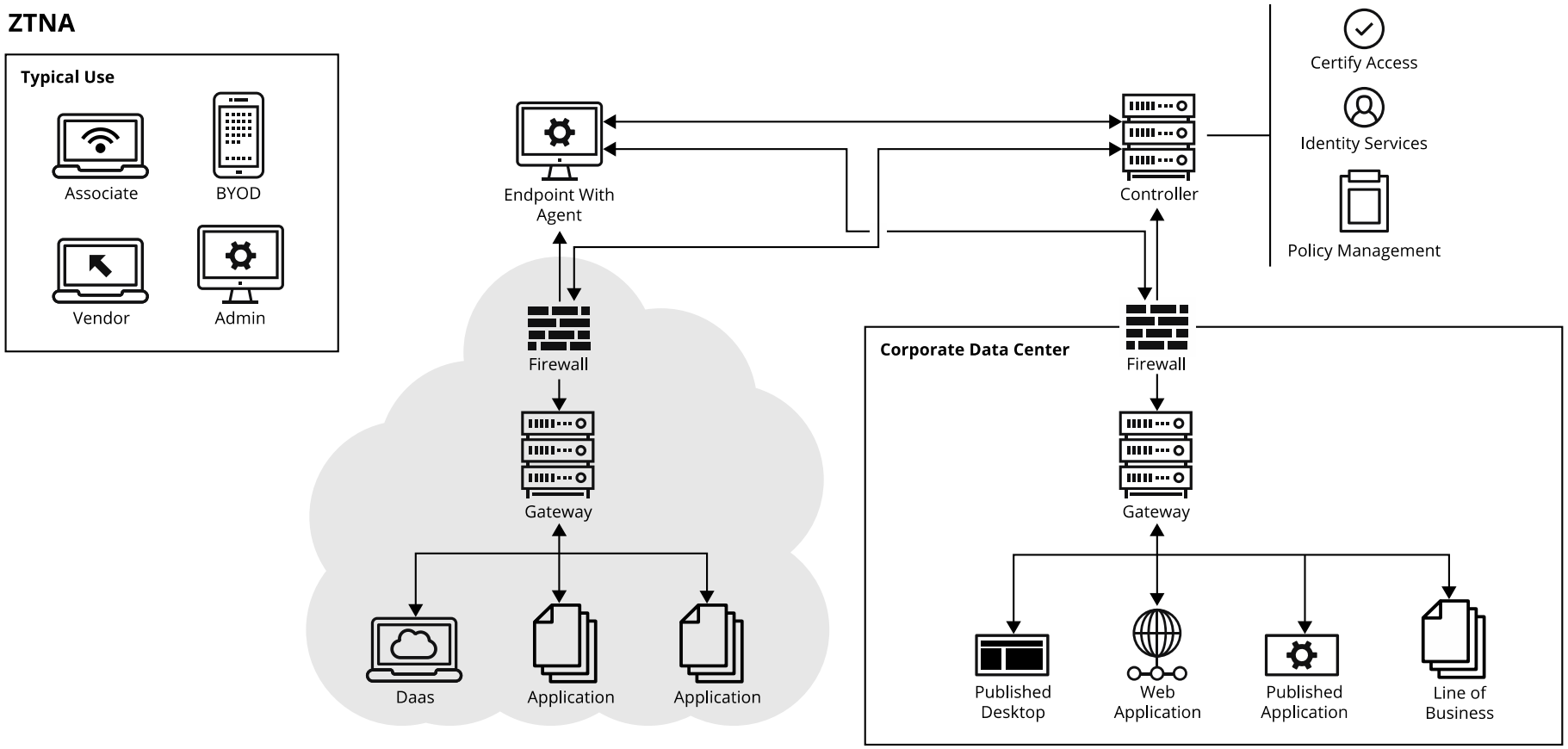
- Users, services, network access
- Zero Trust Network Access (ZTNA)
- Software Defined Perimeter (SDP)
- Cloud Access Security Broker (CASB)

Google BeyondCorp



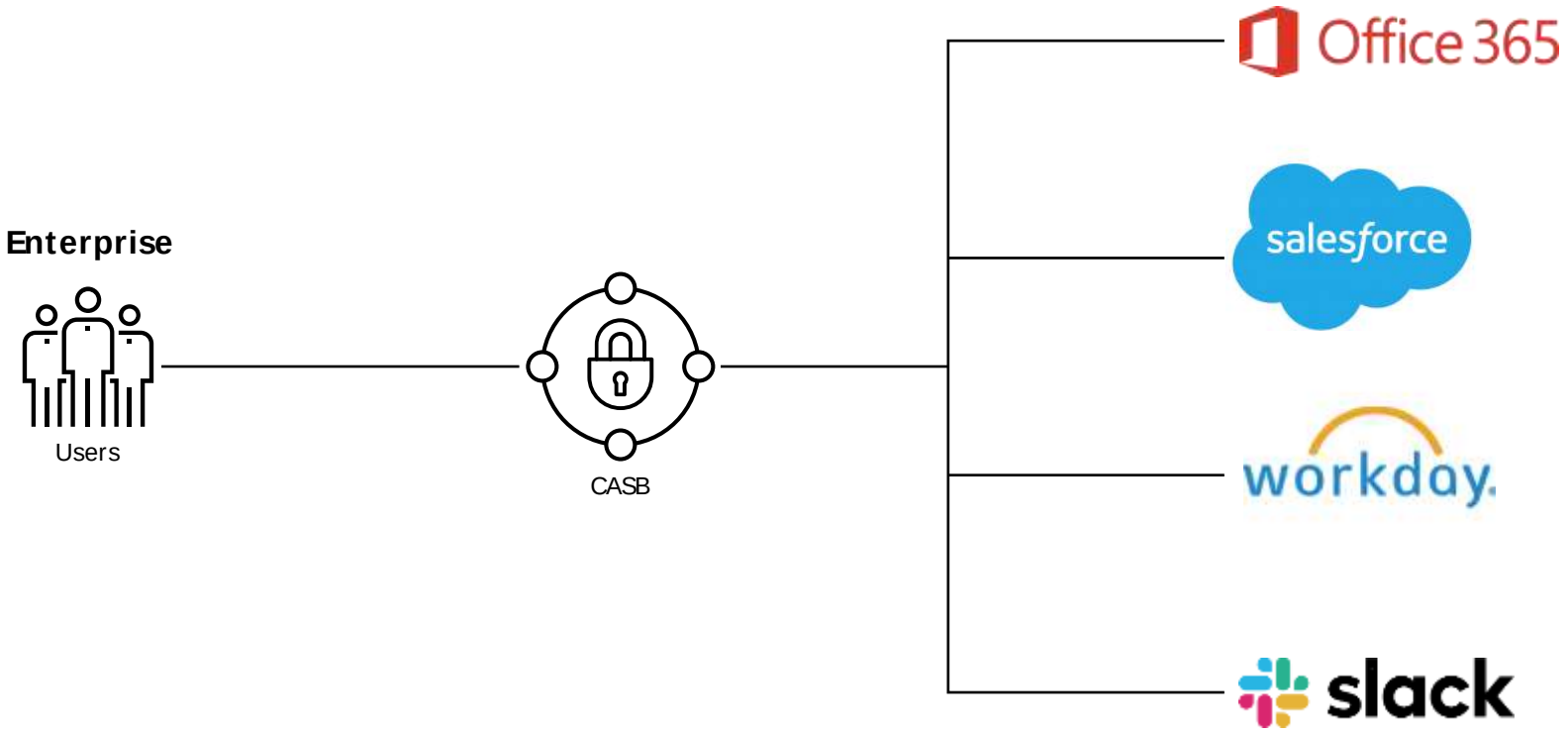
Ref: [Zero Trust Security]

SDP/ZTNA



Ref: [SBP]

CASB



Ref: [ECM]

References

[CSA SDP] Koilpillai, J. & Murray, N. (2020). Software Defined Perimeter (SDP) and Zero Trust. Bellingham, WA: Cloud Security Alliance.

[ECM] Disaboato, M. (2020). Effective Change Management in the Age of Rapid Updates. Stamford, CT: Gartner.

[NIST 800-207] Rose, S., Borchert, O., Mitchell, S., Connelly, S. (2020). NIST Special Publication 800-207: Zero Trust Architecture. Gaithersburg, MD: NIST.

[SBP] Lintemuth, T & Hevesi, P (2021). Security Best Practices for Work-From-Home Scenarios. Stamford, CT: Gartner.

[Zero Trust Adoption] Sanders, G. (2021). Zero Trust Adoption: Managing Risk with Cybersecurity Engineering and Adaptive Risk Assessment. Pittsburgh, PA: SEI/CMU.

References

[Zero Trust Security] Garbis, J. & Chapman, J. (2021). Zero Trust security : An Enterprise Guide. Berkeley, CA: Apress.

[ZTX] Cunningham, C. (2019). The Zero Trust eXtended (ZTX) Ecosystem. Cambridge, MA: Forrester.