Leveraging Zero Trust Frameworks Enabling Businesses to Operate with Clarity

How the pillars of Zero Trust frameworks enable a variety of products, controls, and services to defend against threats across devices, clouds, users, data, networks, and communication channels.

ISACA
Los Angeles Chapter

Never trust. Always verify.

Zero Trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero Trust Architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.

Common Challenges

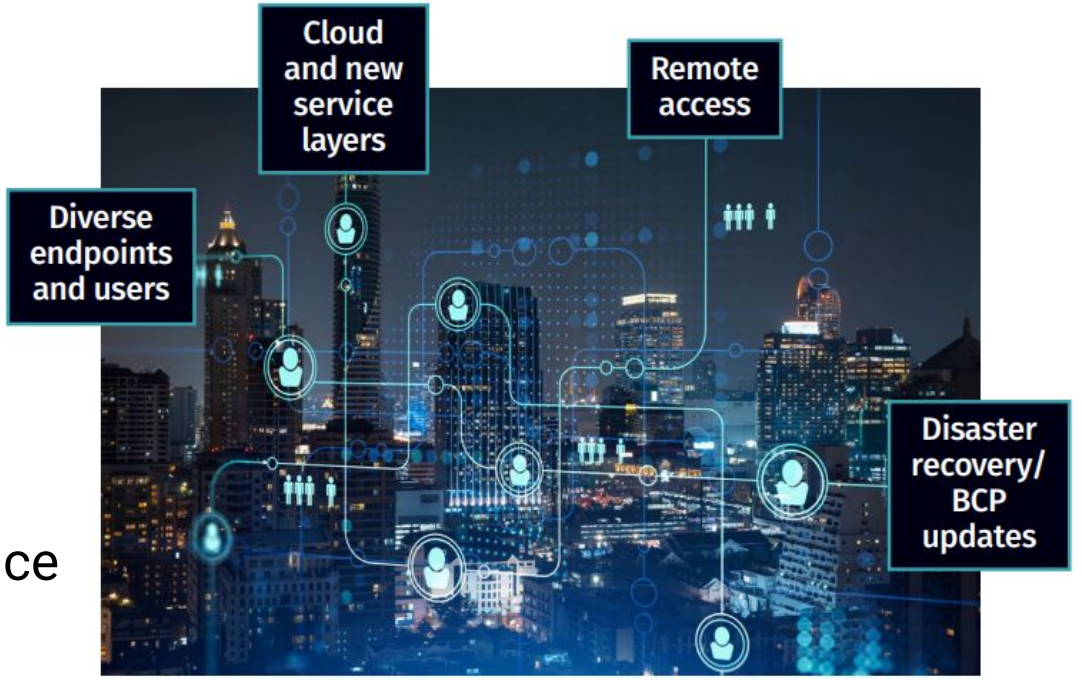
1 – Improving the ability to detect & respond to threat attacks

- Lack of skilled resources
- Work from anywhere

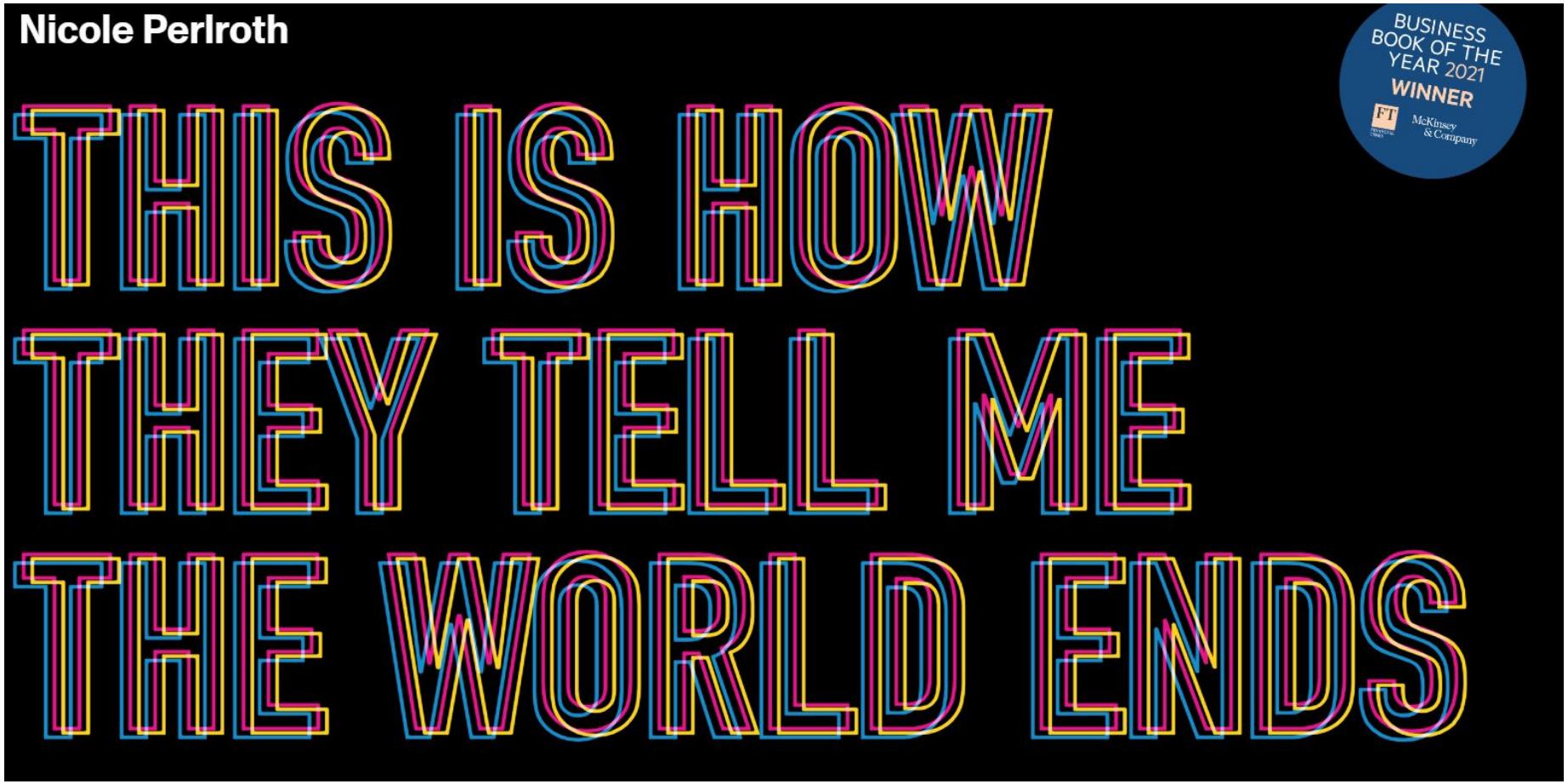
2 – Managing access to data.

- Attack surface complexity
- Evolving threats (Ransomware, OT weaponization)
- Training/Awareness

3 – Compliance with Regulations, Data Privacy, and Insurance Mandates



Why is it necessary?



ISACA
Los Angeles Chapter

How did it come about?

Defense Information Systems Agency (DISA) & Department of Defense – black core (BCORE) – 2004 De-perimiterization: Evaluating trust on a per-transaction basis.

A LOT of resources

CMMC

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

800-207
800-171
800-053

ISACA CERTIFICATIONS


CISA—Certified Information Systems Auditor


CISM—Certified Information Security Manager


CRISC—Certified in Risk and Information Systems Control


CGEIT—Certified in the Governance of Enterprise IT


CDPSE—Certified Data Privacy Solutions Engineer


CET—Certified in Emerging Technology Certification


ITCA—Information Technology Certified Associate


CSX-P—CSX Cybersecurity Practitioner Certification

ISACA CERTIFICATES

- IT Audit Fundamentals Certificate
- IT Risk Fundamentals Certificate
- Certificate of Cloud Auditing Knowledge
- Cybersecurity Audit Certificate
- Computing Fundamentals Certificate
- Networks and Infrastructure Fundamentals Certificate
- Cybersecurity Fundamentals Certificate
- Software Development Fundamentals Certificate
- Data Science Fundamentals Certificate
- Cloud Fundamentals Certificate
- Blockchain Fundamentals Certificate
- IoT Fundamentals Certificate
- Artificial Intelligence Fundamentals Certificate
- COBIT Design and Implementation
- Implementing the NIST Cybersecurity Framework Using COBIT 2019
- COBIT Foundation
- COBIT 5 Certificates

SANS

CSA cloud security alliance®

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

ISACA Los Angeles Chapter

This will not be an exercise in comparing standards and relevant controls

ISACA
Los Angeles Chapter

Tenets of Zero Trust

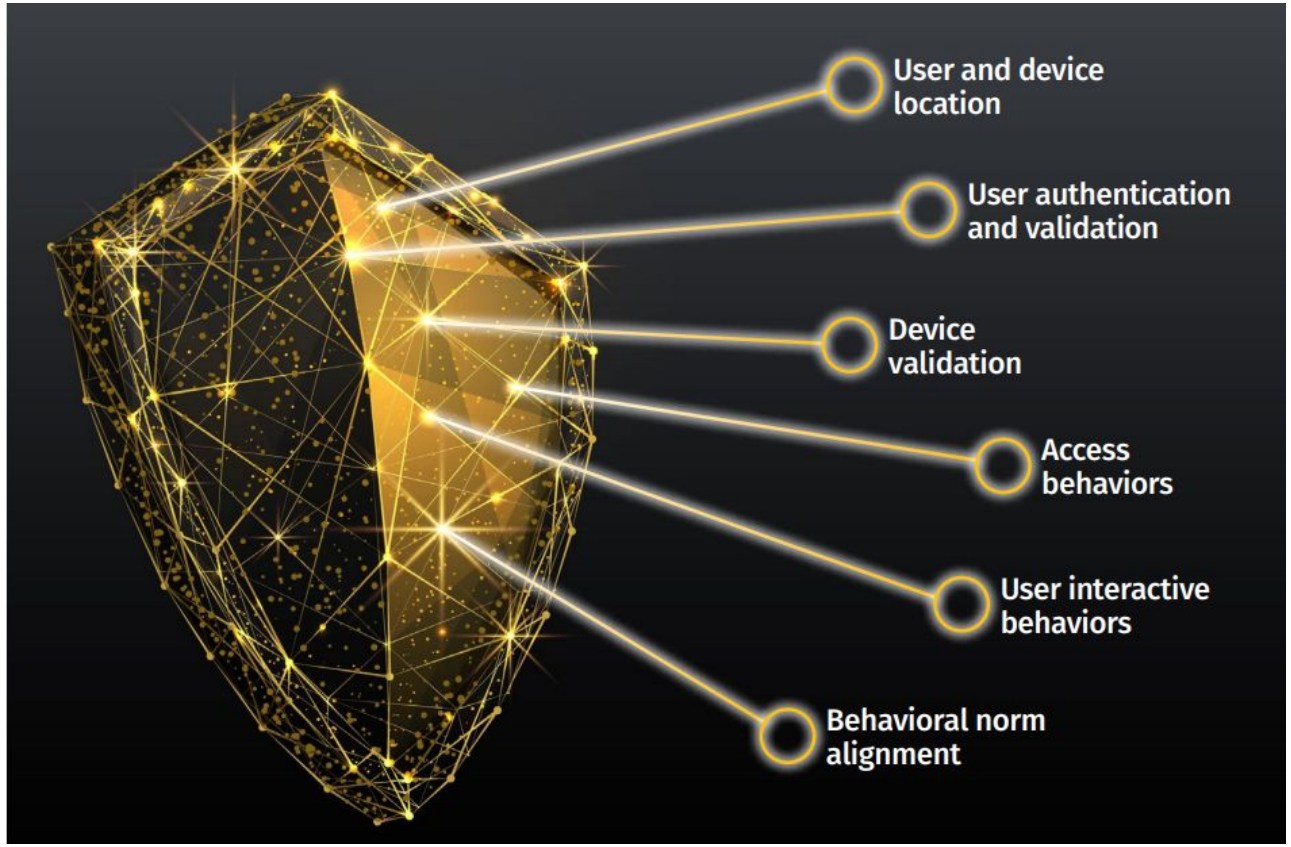
1. All data sources and computing services are considered resources
2. All communication is secured regardless of network location
3. Access to individual enterprise resources is granted on a per-session basis
4. Access to resources is determined by dynamic policy – including the observable state of client identity, application/services, and the requesting asset – and may include other behavioral and environmental attributes
5. The enterprise monitors and measure the integrity and security posture of all owned and associated assets
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed
7. 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.

Assumptions in Zero Trust Networking

1. The entire enterprise private network is not considered an implicit trust zone.
2. Devices on the network may not be owned or configurable by the enterprise.
3. No resource is inherently trusted.
4. Not all enterprise resources are on enterprise-owned infrastructure.
5. Remote enterprise subjects and assets cannot fully trust their local network
6. Assets and workflows moving between enterprise and non-enterprise infrastructure should have a consistent security policy and posture.

ZTNA Platform Requirements

- User & Device Location
- User Authentication & Validation
- Device Validation
- Access Behaviours
- User Interactive Behaviours
- Behavioural Norm Alignment



Zero Trust in the digital world

Preventing Unauthorized Access to enterprise resource(s)

Subjects

Passengers

Users

Assets

Credentials,
MFA, EUBA

Authentication

Policy Decision Point

Policy Decision/
Enforcement Point
PEP/PDP

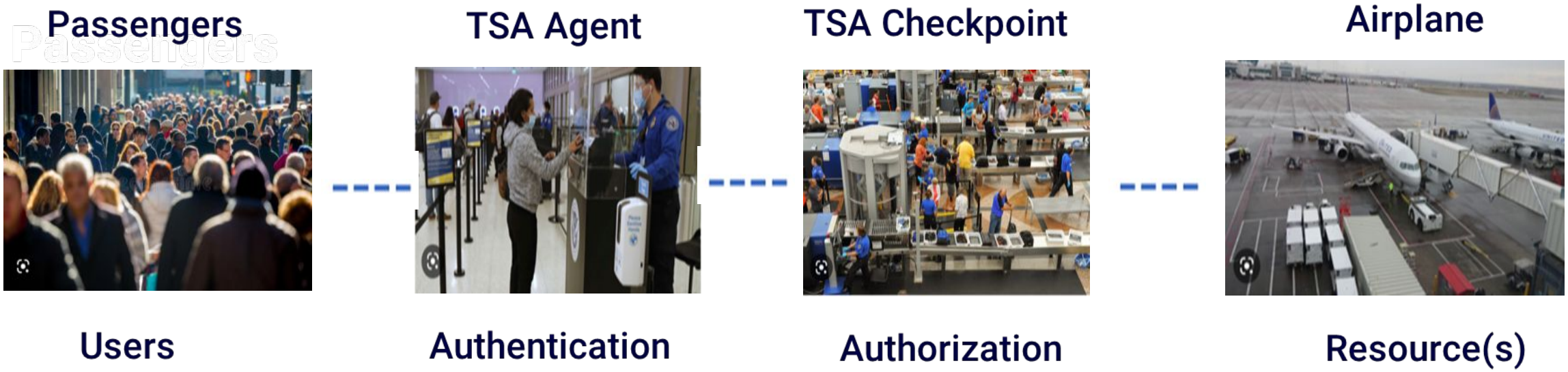
Authorization

Enterprise Resource

Resource(s)

ISACA
Los Angeles Chapter

- Zero Trust Everyday Example
  - Preventing Unauthorized Access to Airplanes (Resource)



ISACA Los Angeles Chapter

- NIST 800-207 Reference Architecture
  - Zero Trust Core

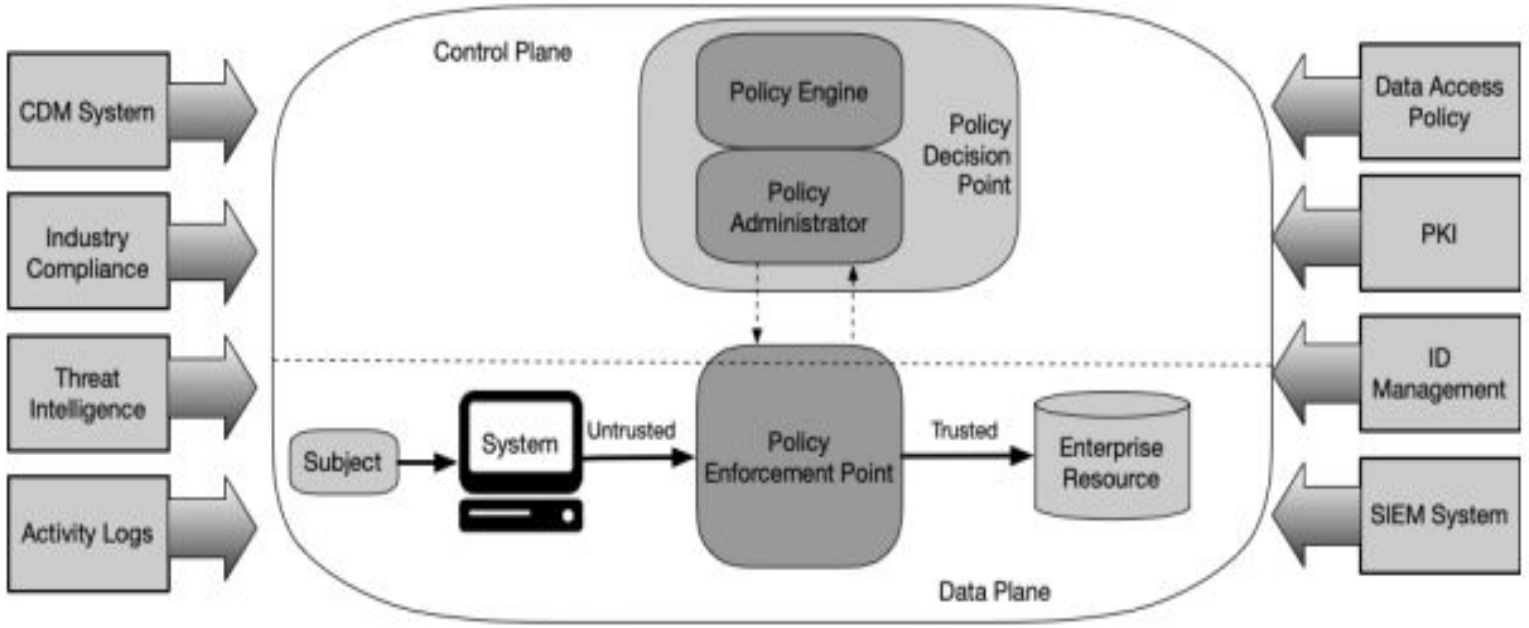
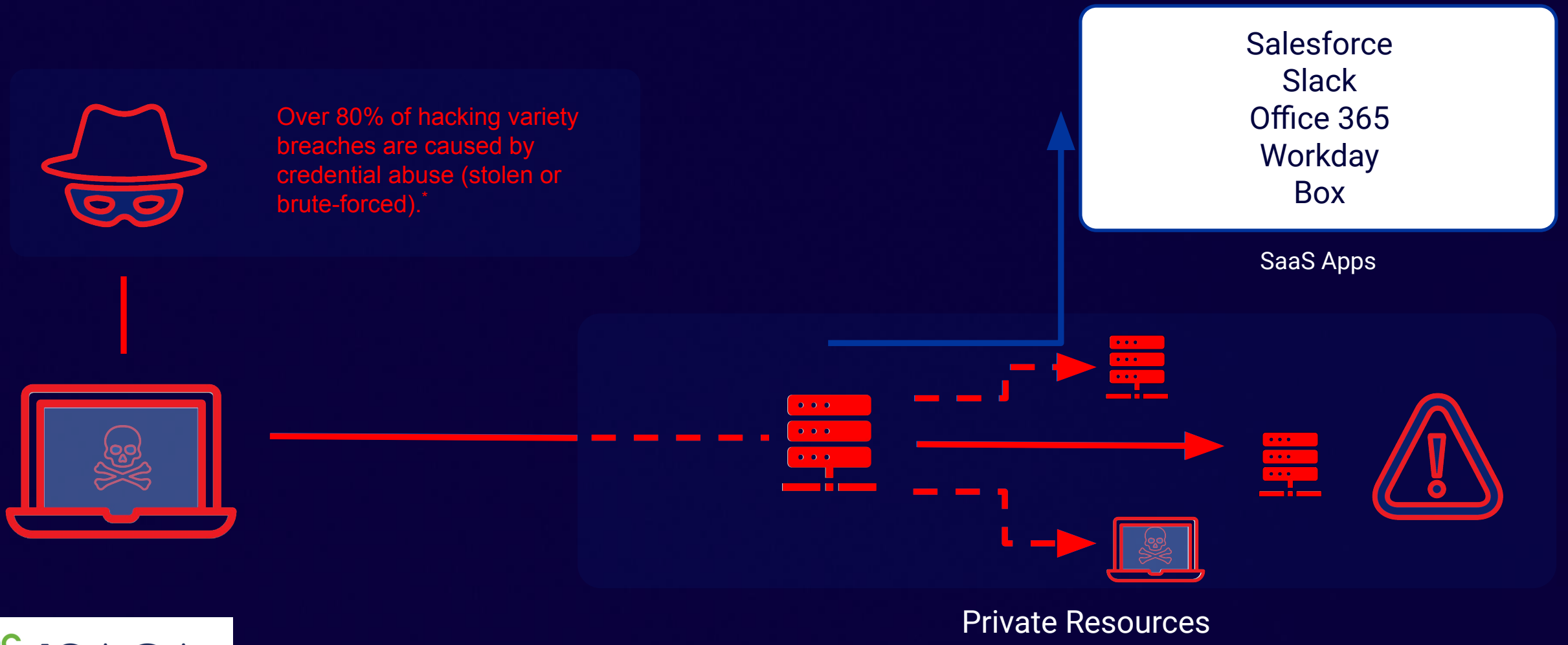


Figure 2: Core Zero Trust Logical Components

SP 800-207, Zero Trust Architecture | CSRC (nist.gov)

TRADITIONAL VPN AND PERIMETER DEFENSE SOLUTIONS REQUIRE FULL TRUST IN BOTH THE USER AND DEVICE



ISACA Los Angeles Chapter

ZTNA ENSURES ONLY TRUSTED PARTICIPANTS ENGAGE IN LEGITIMATE ACTIVITY

Variations of Zero Trust Architecture & Deployment

Architecture Approaches

1. Enhanced Identity Governance
2. Micro-Segmentation
3. Network Infrastructure and Software Defined Perimeters

Deployed Variations

1. Device Agent/Gateway-Based
2. Enclave-Based
3. Resource Portal
4. Device Application Sandboxing

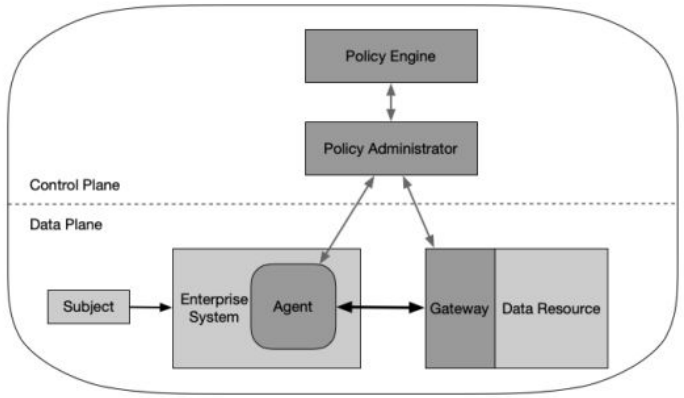


Figure 3: Device Agent/Gateway Model

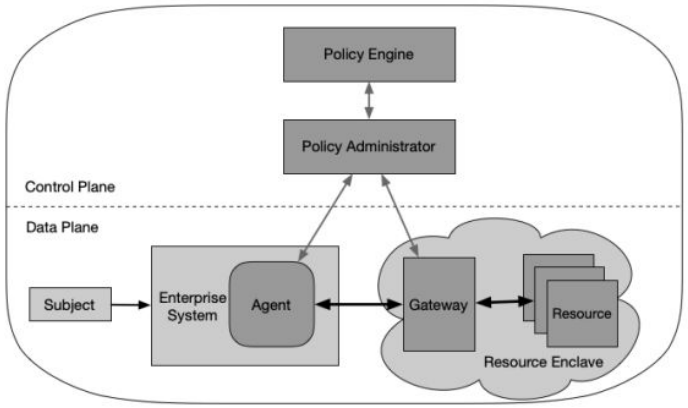


Figure 4: Enclave Gateway Model

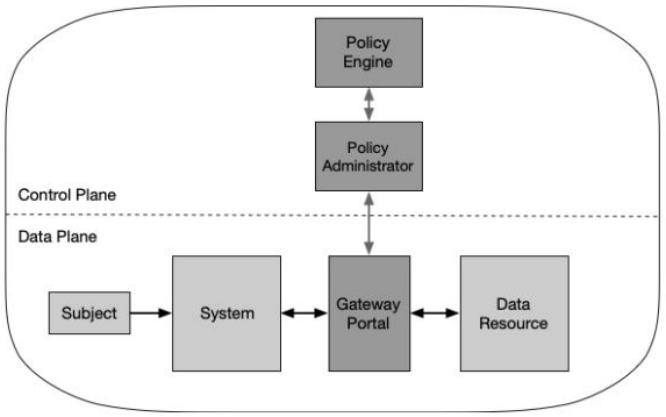


Figure 5: Resource Portal Model

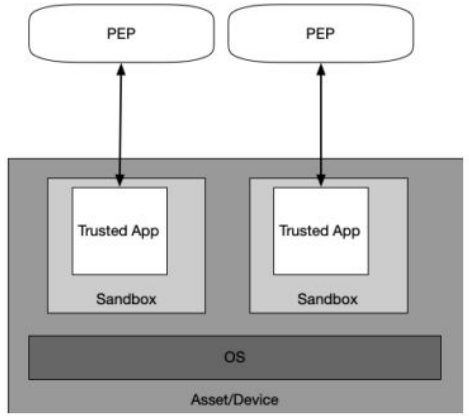


Figure 6: Application Sandboxes

ISACA Los Angeles Chapter

Trust Algorithm

Trust Algorithm Variations

Criteria vs Score Based – A minimum threshold for access or a confidence level based on values for every data source calculated against enterprise configured weights

Singular vs Contextual: Singular considers each request individually without considering historical data. Contextual TA considers the subject or network agent's history in the consideration. Speed vs consideration of acceptable subject behaviour.

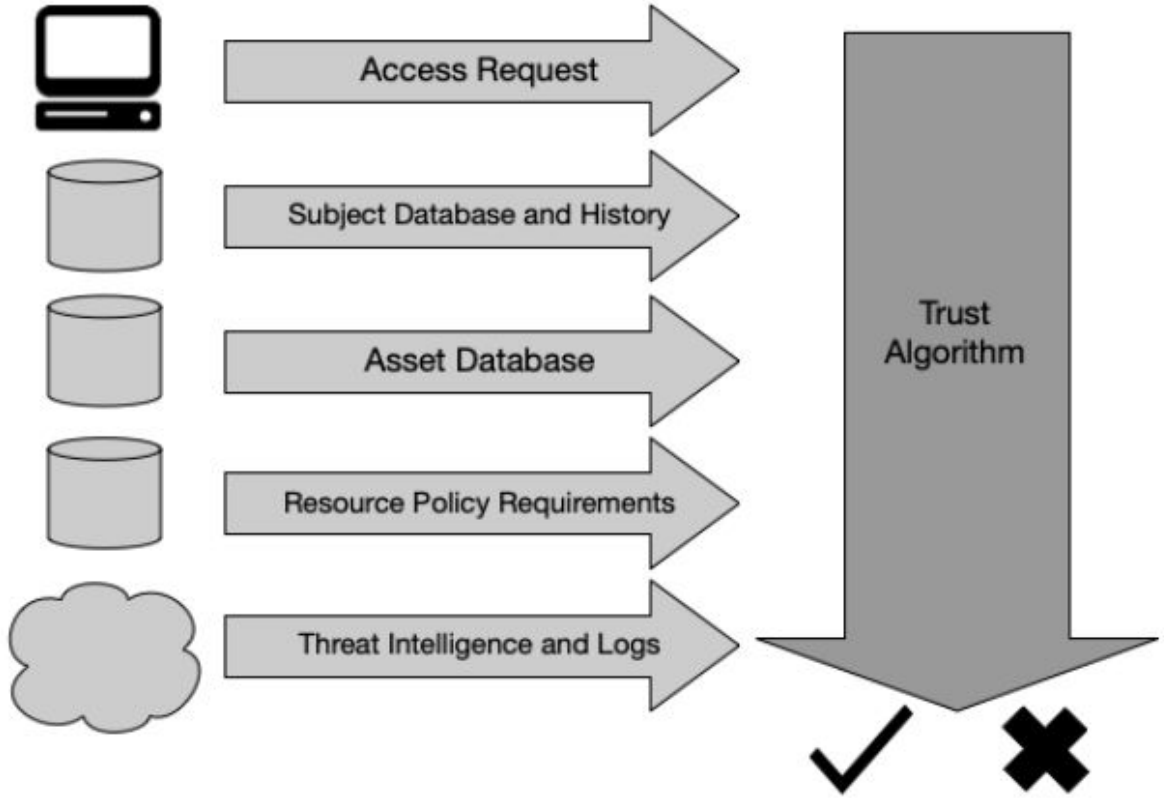


Figure 7: Trust Algorithm Input

ISACA Los Angeles Chapter

LEVERAGE CLOUD-AI TO ASSESS RISK IN THE NETWORK

Potential Risk Factors

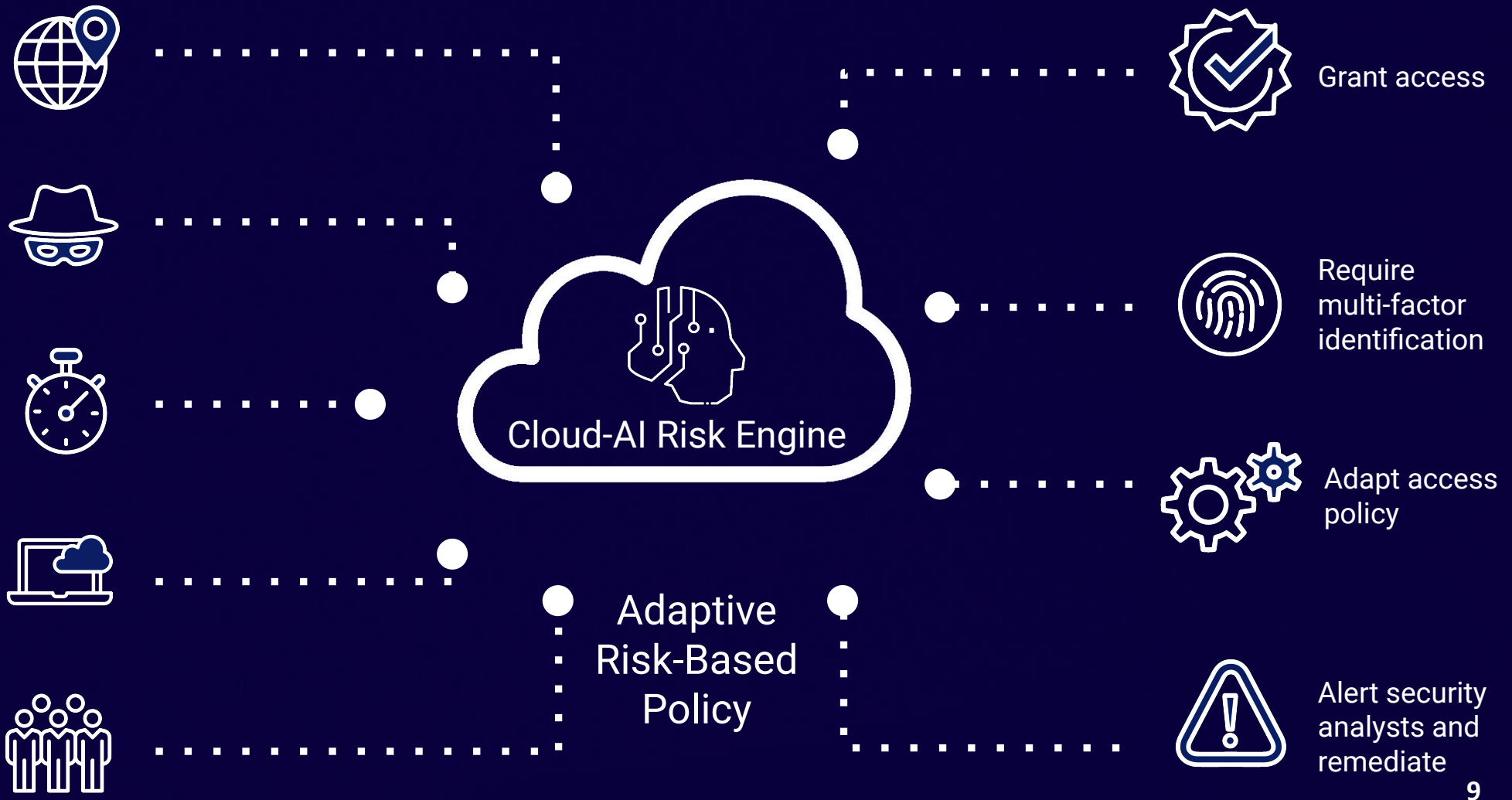
Is the user's IP address trusted?

Is the user who they say they are?

Are the times and frequency of access typical?

Is the user accessing the files and data they typically access?

Is the user's behavior consistent with that of other similar users?



Potential Actions

Grant access

Require multi-factor identification

Adapt access policy

Alert security analysts and remediate

Network Requirements to Support ZTA

- Enterprise assets have basic network connectivity
- Understanding of assets owned or managed by the enterprise
  - What is the devices security posture?
- Enterprise can observe all network traffic.
- Enterprise resource access requires accessing PEP first.
- Network data plane and control plane are logically separate.
- Enterprise assets can reach the PEP component.
- The PEP is the only component that accesses the policy administrator as part of a business flow.
- Remote enterprise assets should be able to access enterprise resources without need to traverse enterprise network infrastructure first.
- The infrastructure used to support the ZTA access decision process should be made scalable to account for changes in process load.
- Enterprise assets may not be able to reach certain PEPs due to policy or observable factors.

Deployment Scenarios/Use Cases

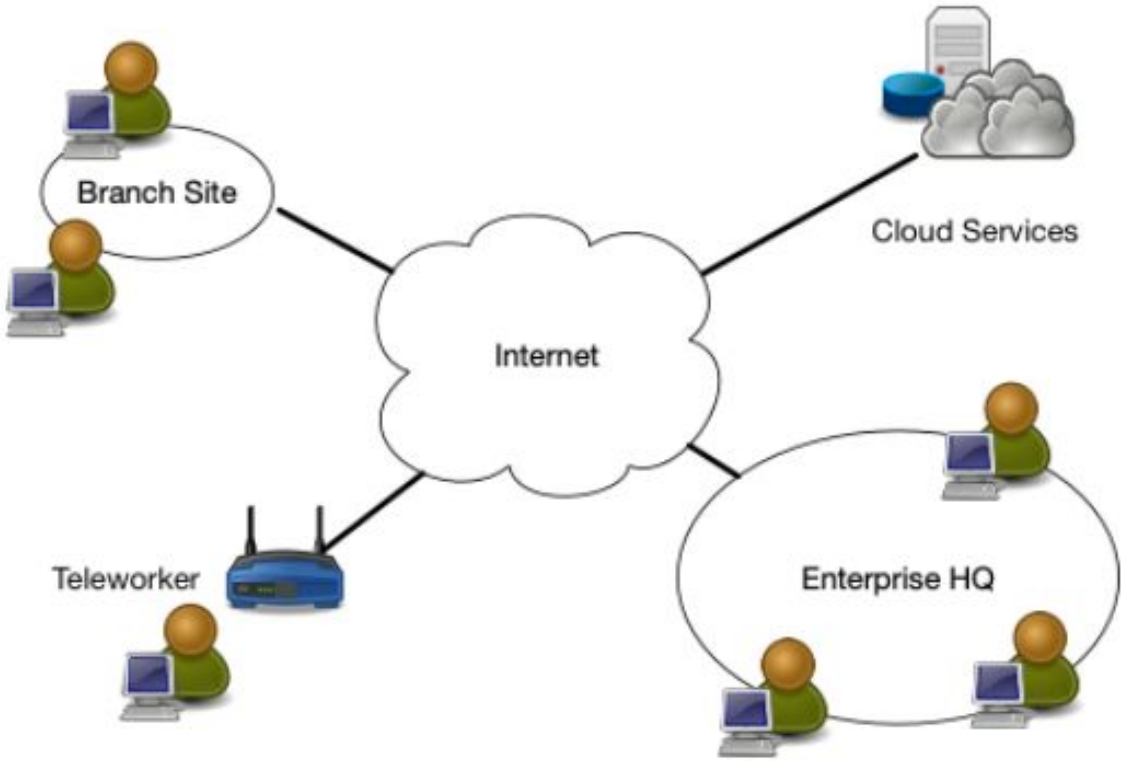


Figure 8: Enterprise with Remote Employees

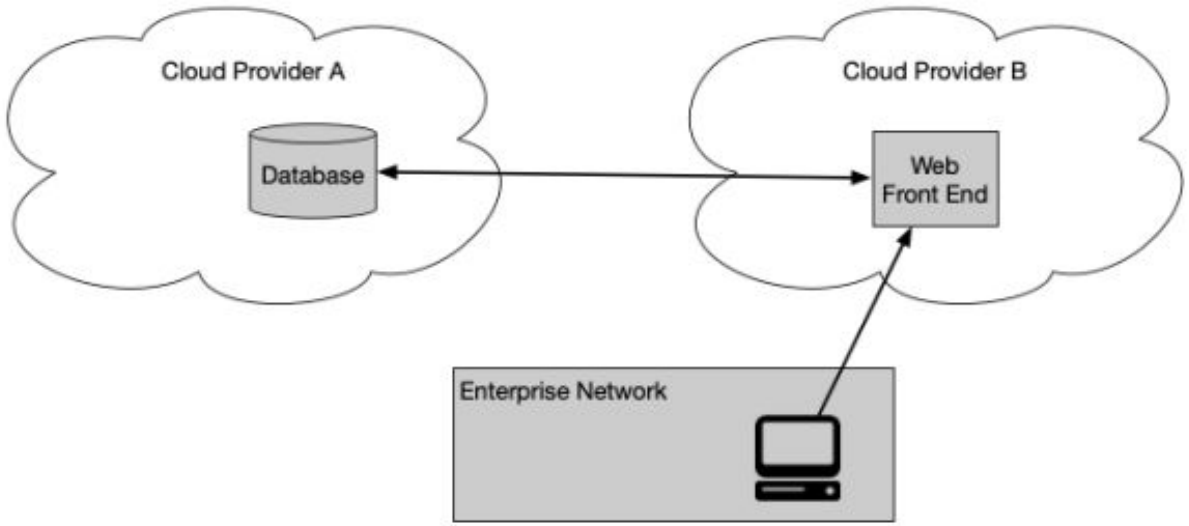


Figure 9: Multi-cloud Use Case

Deployment Scenarios/Use Cases

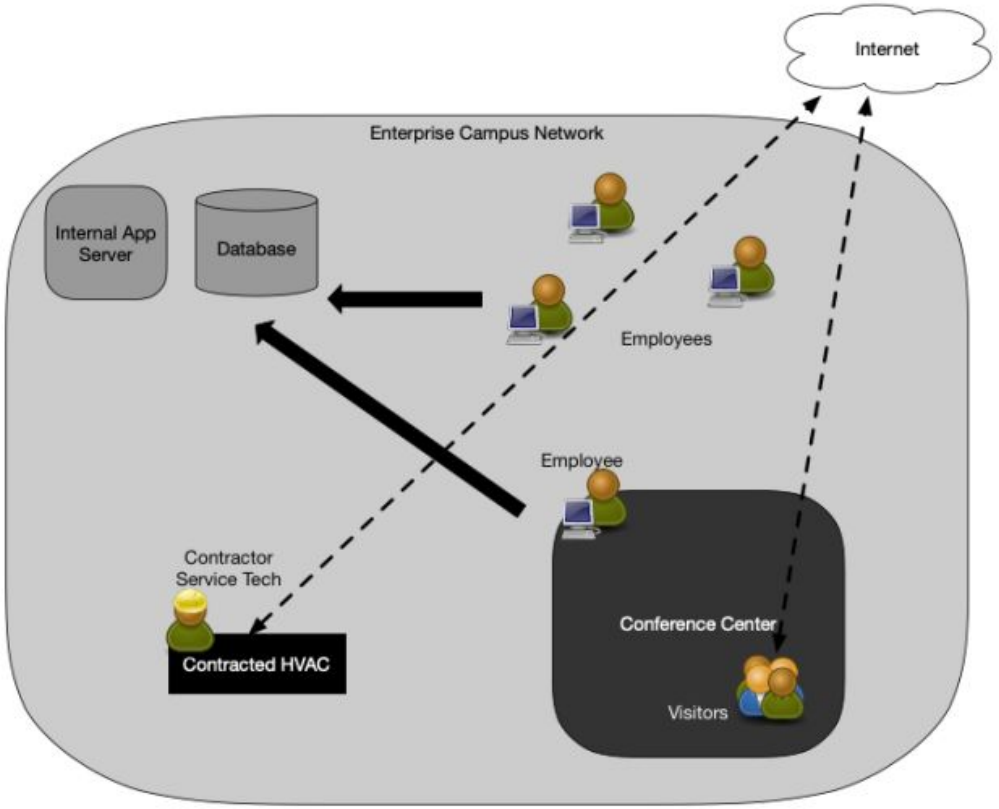


Figure 10: Enterprise with Nonemployee Access

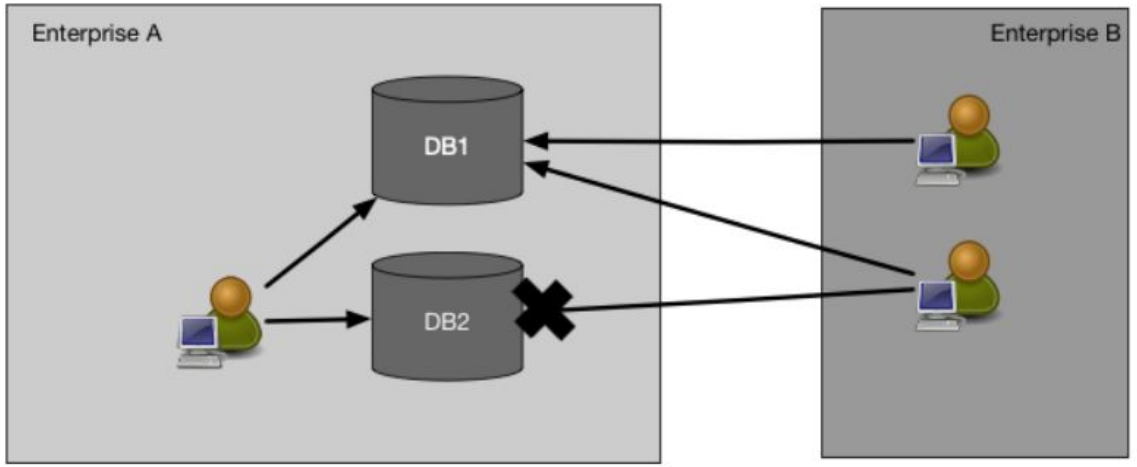


Figure 11: Cross-Enterprise Collaboration

Potential Threats within ZTA

Subversion of the ZTA Decision Process
Denial of Service or Network Disruption
Stolen Credentials / Insider Threat
Visibility on the Network
Storage of System and Network Information
Reliance on Proprietary Data Formats or Solutions
Use of Non-Person Entities (NPE) in ZTA Administration

Migrating to a Zero Trust Architecture

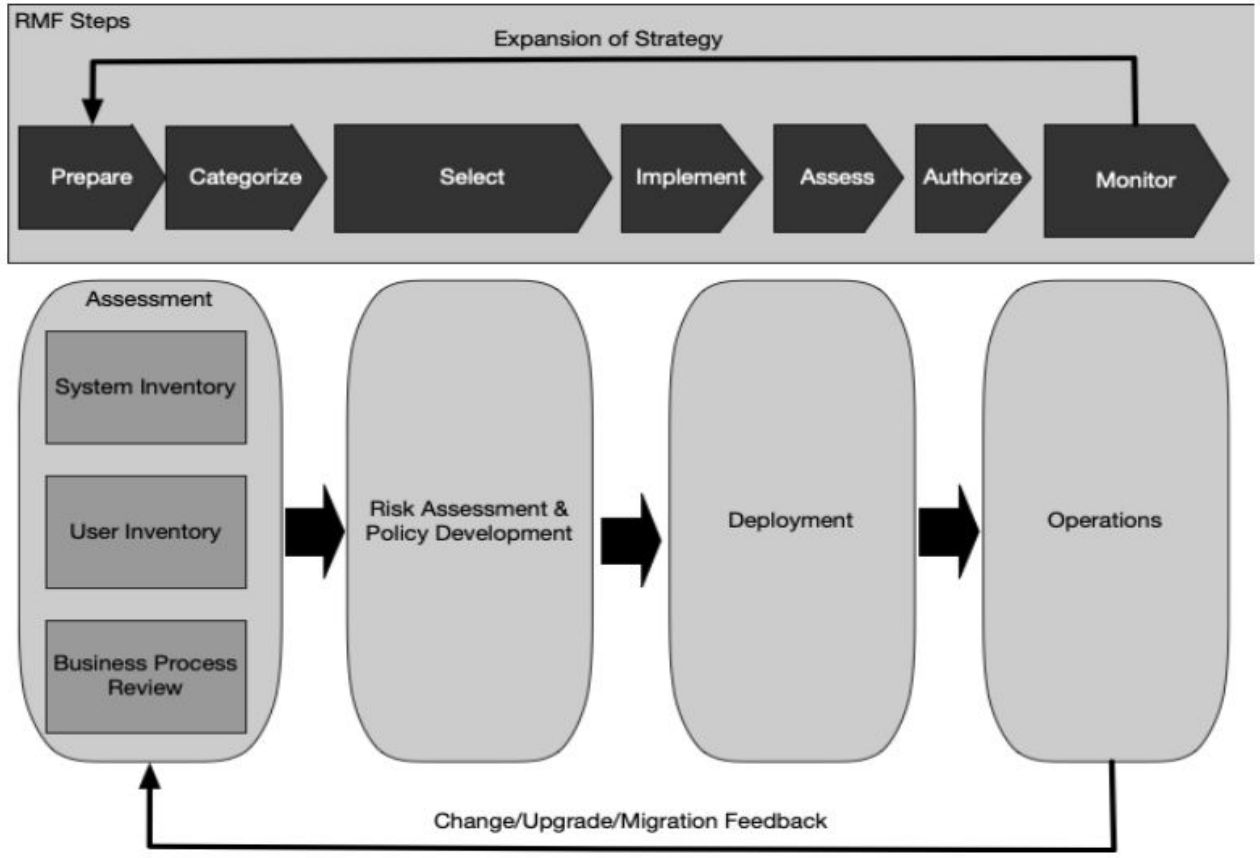


Figure 12: ZTA Deployment Cycle

1. Identify Actors on the Enterprise
2. Identify Assets Owned by the Enterprise
3. Identify Key Processes and Evaluate Risks Associated with Executing Process
4. Formulate Policies for the ZTA Candidate
5. Identifying Candidate Solutions
    I. Does the solution require components on the client asset?
    II. Does the solution work where the business process resources exist entirely on enterprise premises?
    III. Does the solution provide a means to log interactions for analysis?
    IV. Does the solution provide broad support for different applications, services, and protocols?
    V. Does the solution require changes to subject behaviour?
6. Initial Deployment and Monitoring
7. Expanding the ZTA

Questions?

Stolen Credentials, Insider Threat, or Business as Usual?