ZTEdge™
By Ericom Software

CMU/SEI Industry Day
Powering Zero Trust with ZTEdge

Dr. Chase C Cunningham
Chief Strategy Officer

email: cunningham.chase@googlemail.com

A large U.S. federal agency provides services used by global users.

The agency currently is operating a hybrid, multi-cloud enterprise that supports about 45,000 federal employees and 15,000 contractors.

The enterprise's networks break down into Information Technology (IT) (75%), Operational Technology (OT) (15%), and Supervisory Control and Data Acquisition (SCADA) (10%).

The OT and SCADA networks support the agency's smart buildings' controls/operations and distribution centers.

Currently, the agency has identified three high-value assets (HVAs): two legacy systems and one database containing Protected Personal Information (PPI).

The agency is currently using four different identity and access management systems (Okta Identity Cloud, Cirrus Identity, Azure AD, and Google Cloud Identity) and lacks a centralized security operations center (SOC).

The agency is currently unable to integrate logging information due to the continued use of legacy systems: an organizational structure where SOC operations are broken across different teams and a hybrid, multi-cloud implementation where services provide different formats for the information.

The agency must implement two-factor authentication but also must provide multi-factor authentication (MFA) for some parts of the enterprise.

The agency has a budget of $3 million and a one-year timeline during which it must start to address M-22-09. Given this last constraint, each proposal should address its compatibility with the agency's existing hardware and software infrastructure.

On January 26, 2022, the Office of Management and Budget (OMB) released the Federal Zero Trust Strategy in support of Executive Order 14028, “Improving the Nation’s Cybersecurity”, to adapt civilian agencies’ enterprise security architecture to be based on zero trust principles. The strategy is published as OMB Memorandum M-22-09, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles”. The goal of the strategy is to accelerate agencies toward a shared baseline of early zero trust maturity.

OMB memo M-22-09 provides guidance on how to achieve the Zero Trust mandates of the Executive Order. It further codifies the importance of moving off of legacy security structures into a Zero Trust architecture to include:

- No longer depend on conventional perimeter-based defenses to protect critical systems and data.
- Provide secure access applications over the public Internet without relying on a virtual private network (VPN).
- Encrypting DNS and HTTP traffic using TLS 1.3 for all internal and external connections to include APIs.

Zero Trust **is not a product – but products power strategy**

Move from CIA to RTA posture

Vision

Zero Trust Strategy Goals

Identities – Secure and "Use" Them

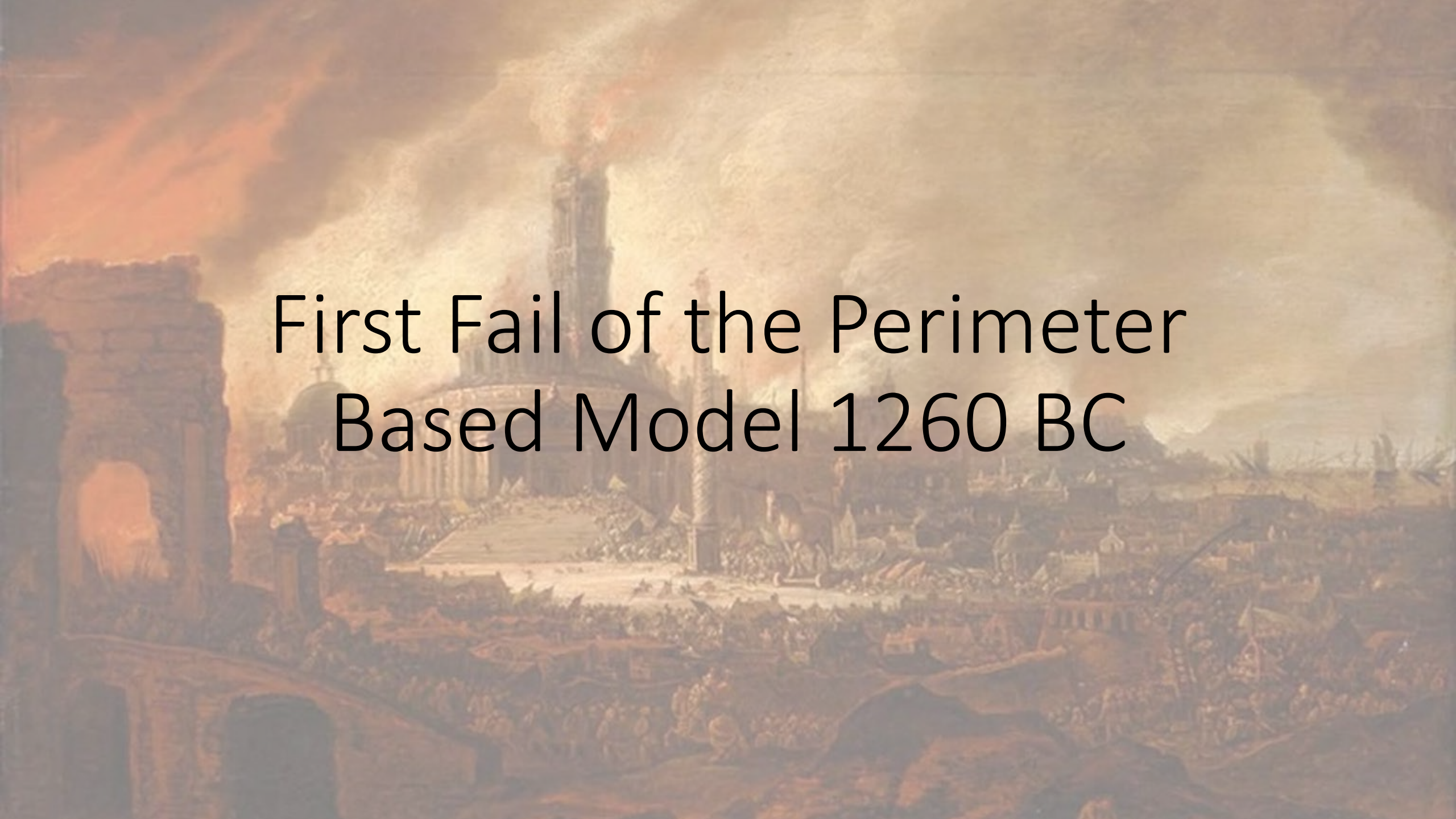
Devices – Enable BYoD Smartly

Networks – Unclass Work Anywhere, Network Agnostic

Applications and Workloads – Let Legacy Live, Enable Future Work, Secure Backend, Cloud Agnostic

Data – Policy Driven Access, Secure in Transit and at Rest

Users – Let Them Work, Securely, Anywhere on Any Device and Any Network (Reduce Phishing Related Budget)

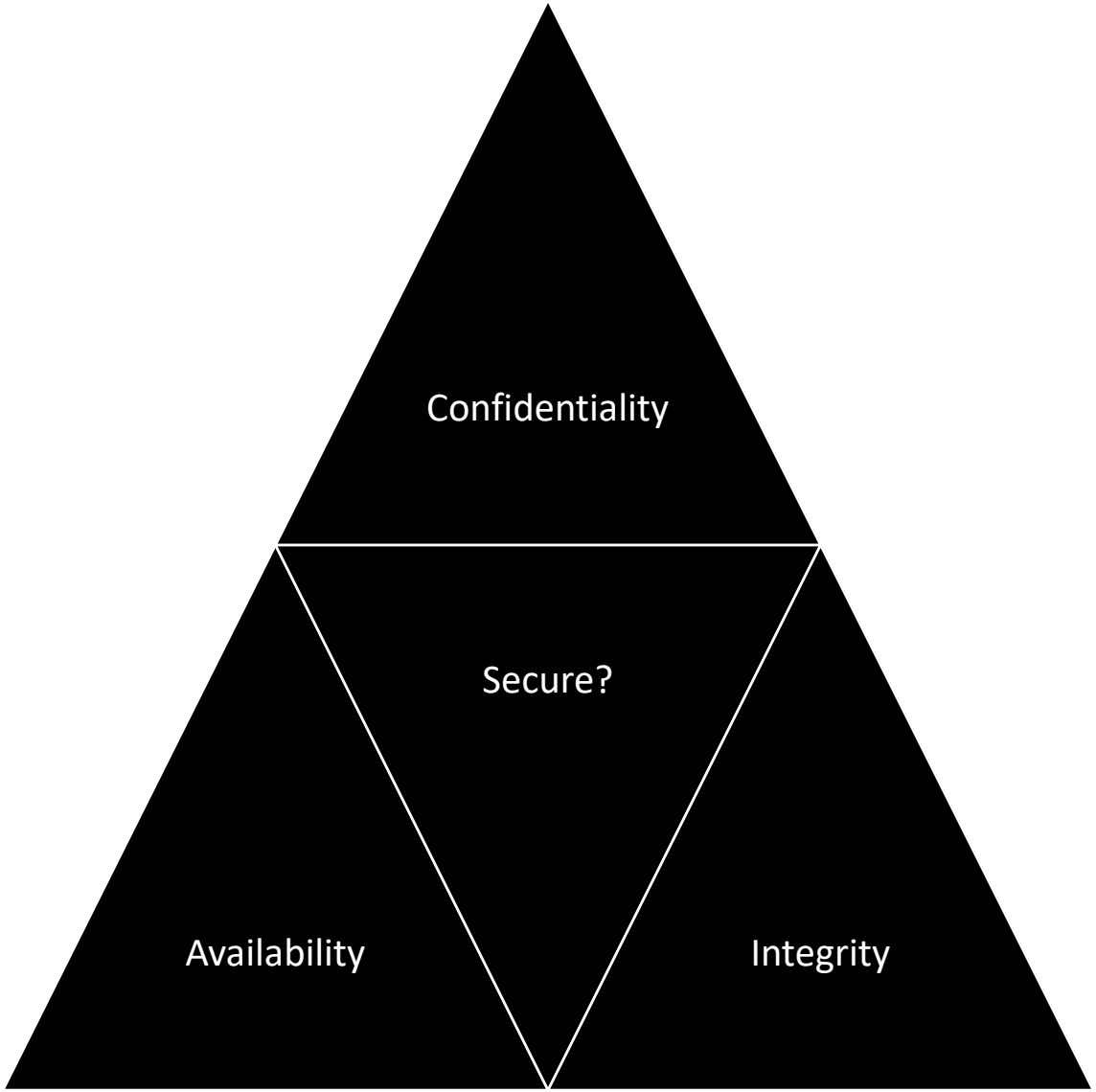


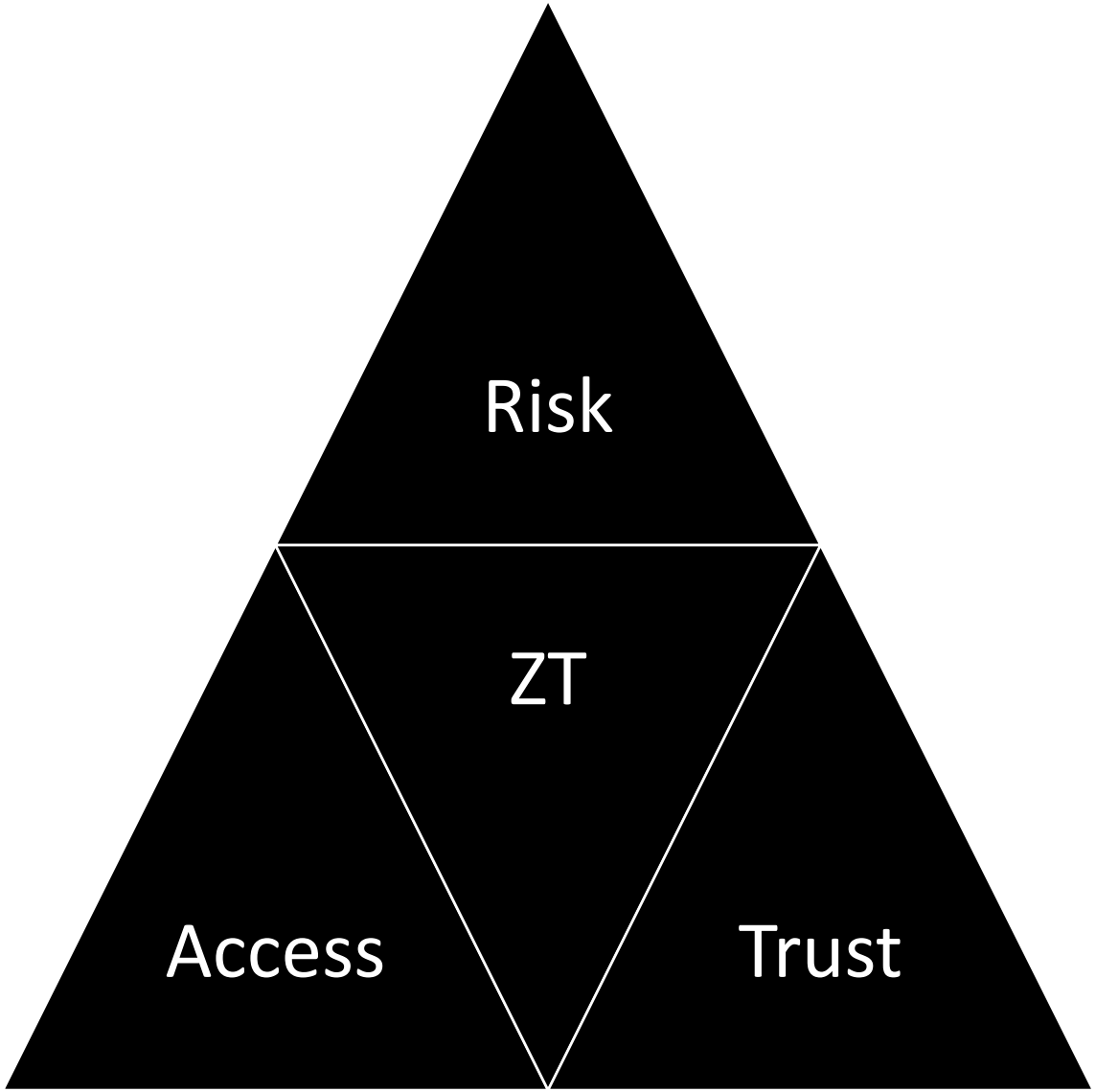
First Fail of the Perimeter Based Model 1260 BC

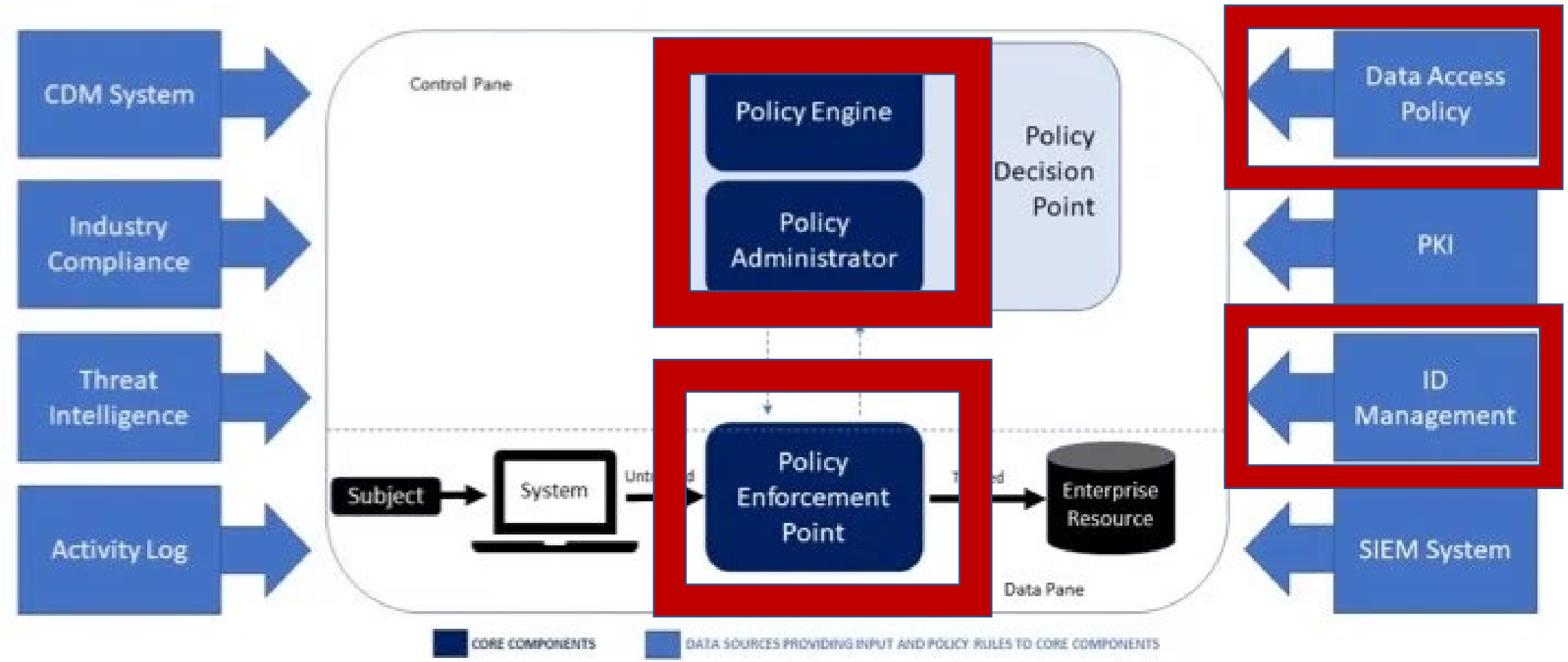
Zero Trust is an information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their associated devices. Zero Trust advocates these three core principles: all entities are untrusted by default, least privilege access is enforced, and comprehensive security monitoring is implemented.

NIST 800-207

1. All data sources and computing services are considered resources. – Future of Work
2. All communication is secured regardless of network location. - BYoD
3. Access to individual enterprise resources is granted on a per-session basis. - Sessions
4. 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. – Policy and ML
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets. – Device and Asset Interrogation
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed. – IAM and Policy Integration
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. – Logging -> Telemetry -> Policy

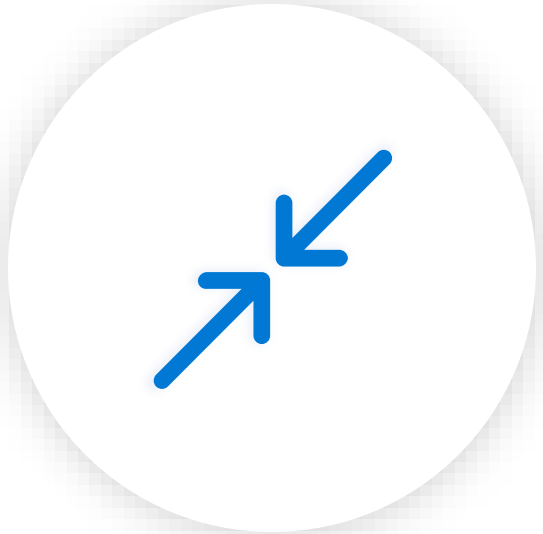

Confidentiality
Secure?
Availability
Integrity


Risk
ZT
Access
Trust

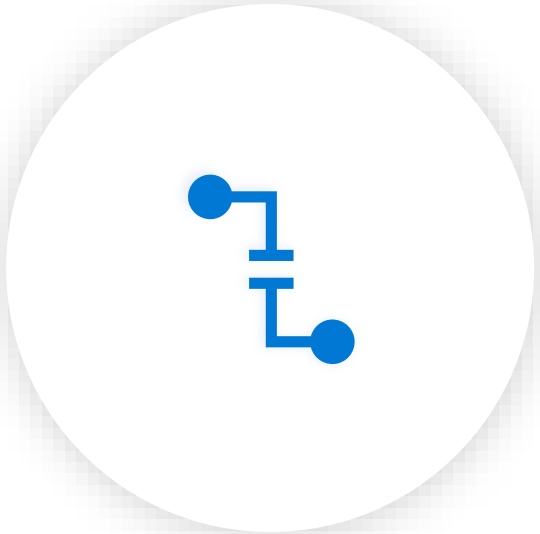


Principles for Zero Trust

Verify explicitly



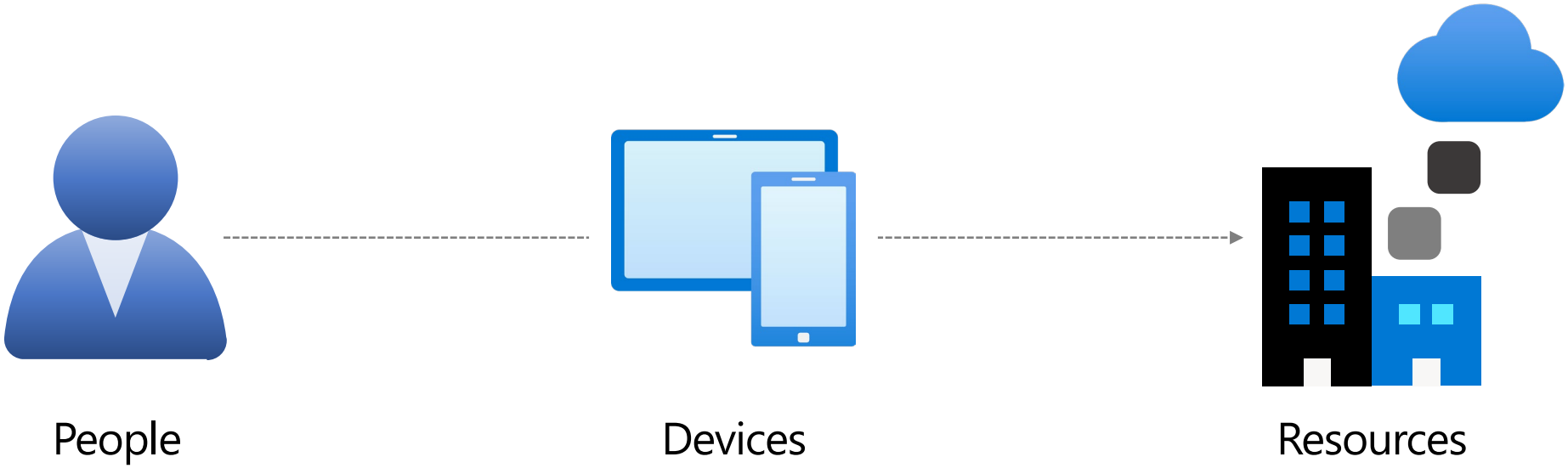
Use least privilege access



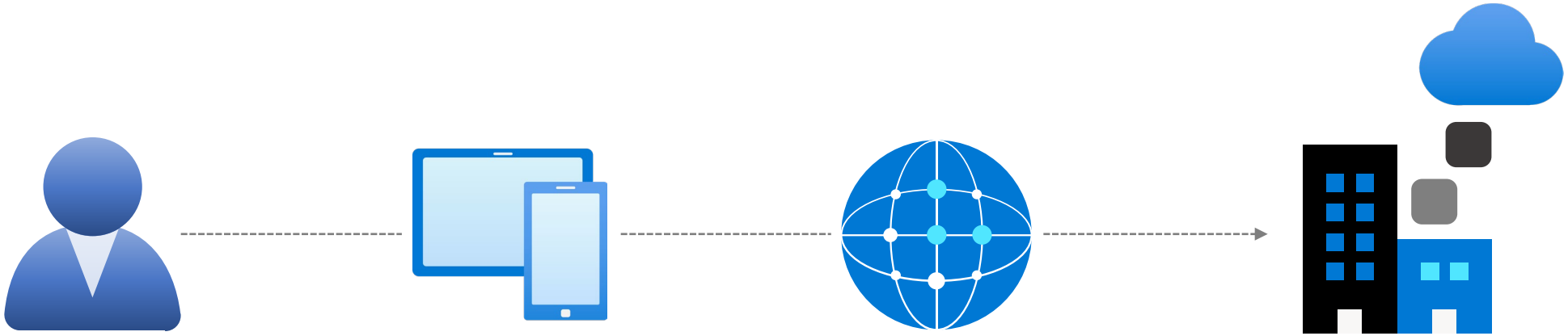
Assume breach

Zero Trust

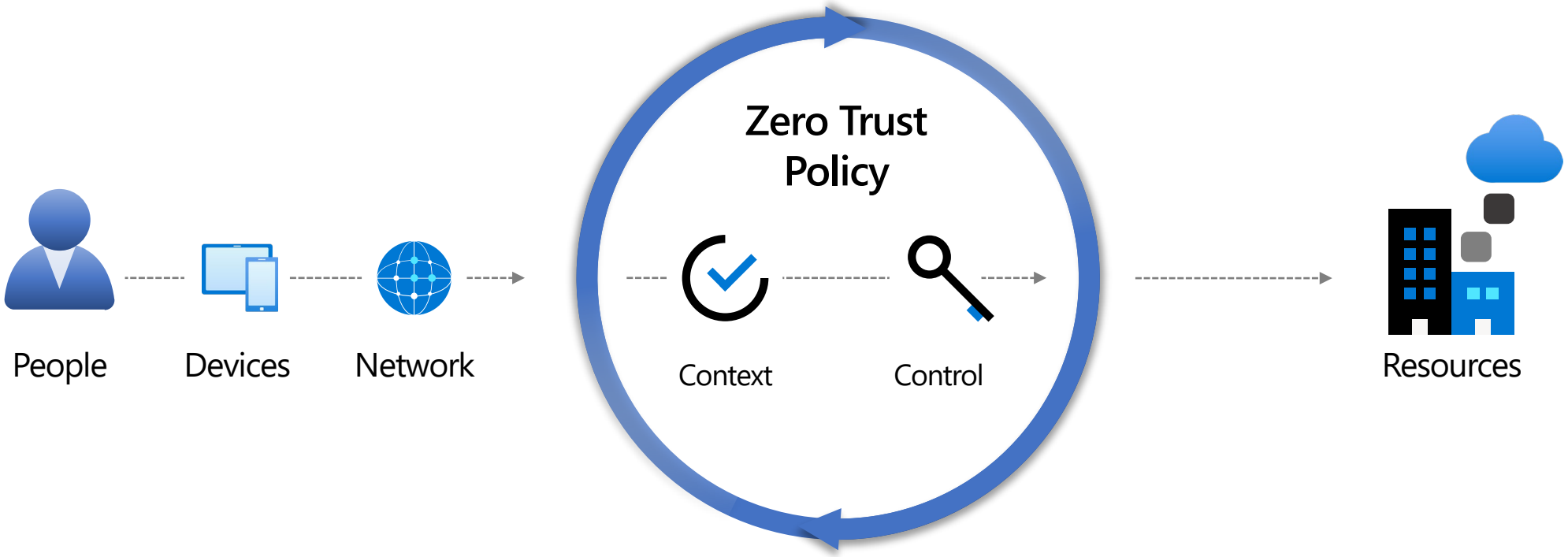
Zero Trust



Zero Trust



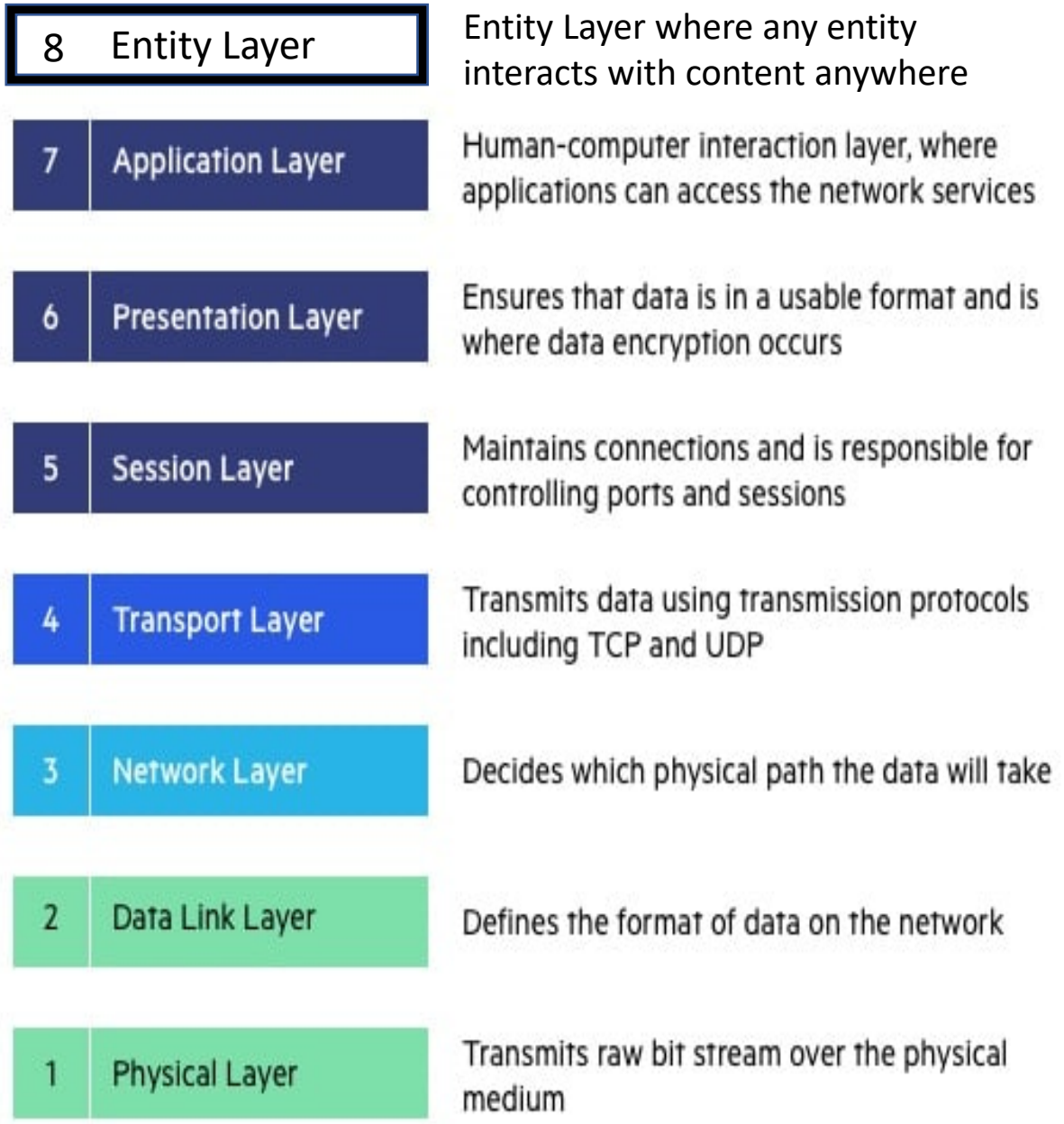
Zero Trust


People
Devices
Network
Zero Trust Policy
Context
Control
Resources

Enabling ZT

- Determine HVA’s and associated data
  - ZT Data Security
- Inventory assets and access and control points
  - Device inventory and asset interception
- Plot controls strategy
  - All the things
- Enable segmentation
  - Data
  - Device
  - Workloads
  - Network
  - Users
- Vector policy
  - ML Based Learning Module
- Rinse and repeat
  - Continuous validation and updating

ZT End State



Manage users and their accesses and potential for compromise both internally and externally

Requires – RBAC/IAM and RBI

Secure but do not manage (agent based and agentless) the devices that Federal staff use to enable BYoD.

Requires – Device Interrogation and WAI

Isolate systems are from each other, and the network traffic flowing between and within them is reliably encrypted.

Requires – Network Segmentation and Isolation

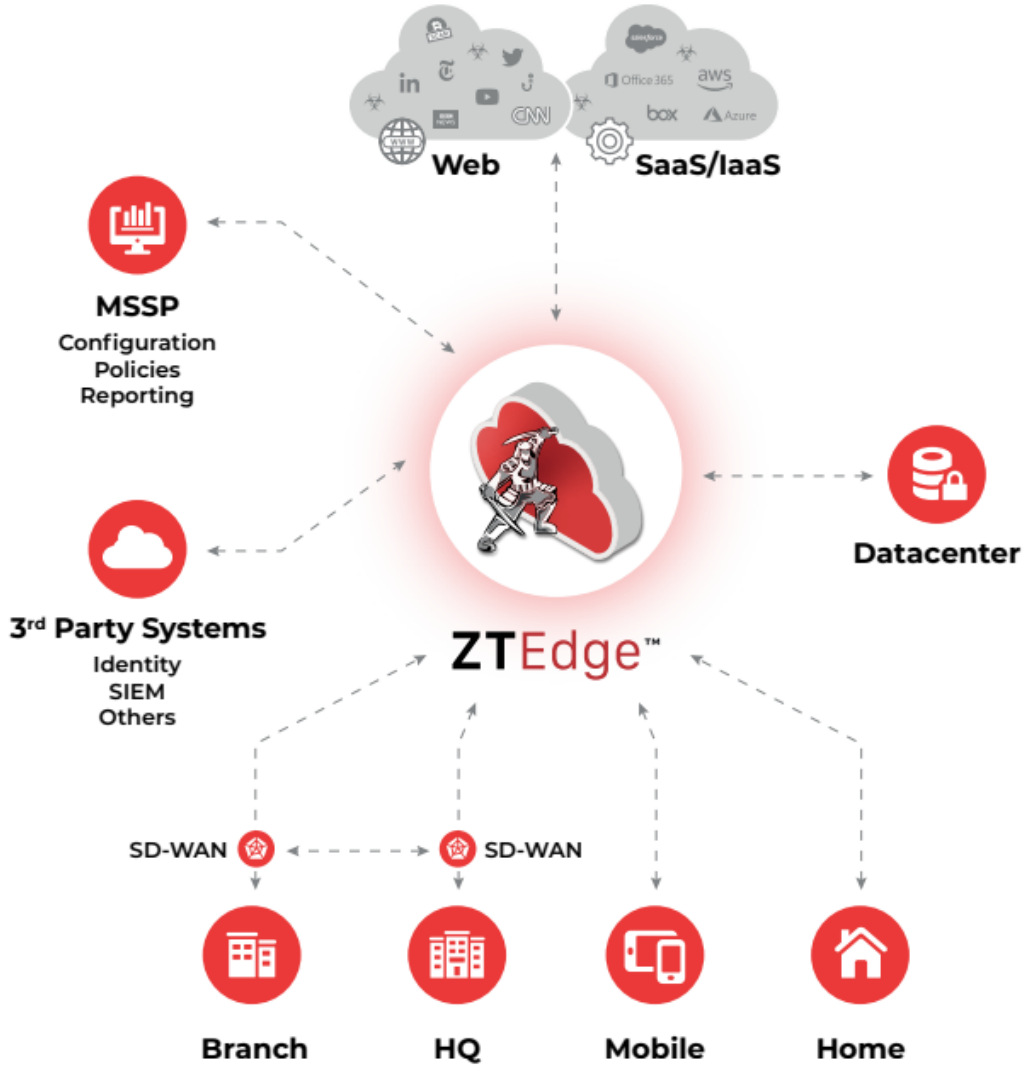
Applications are secured and protected and are made available to staff securely over the internet.

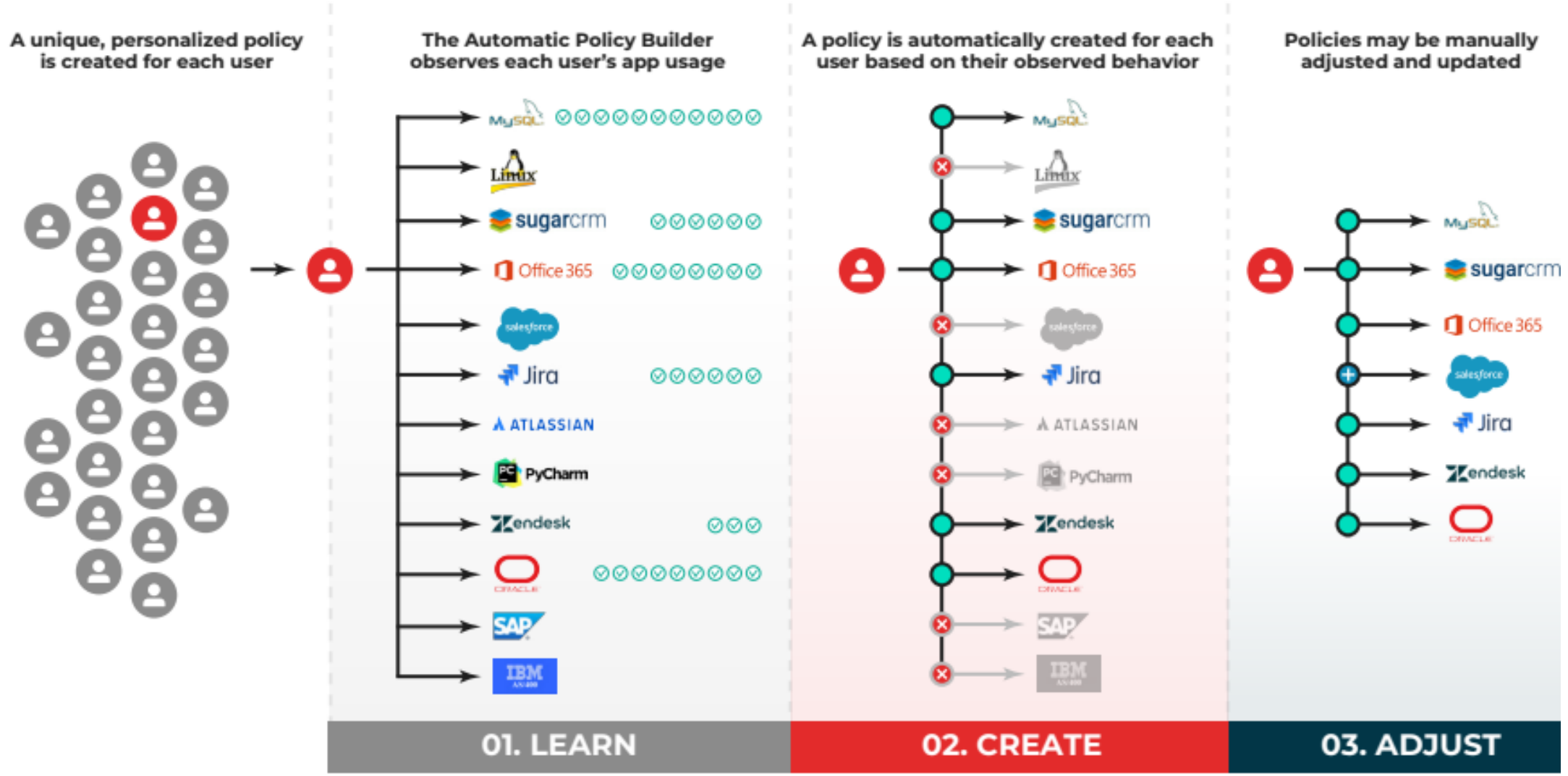
Requires – WAI

Identify, categorize, track, and redact data dynamically based on the other tenets of the ZT implementation.

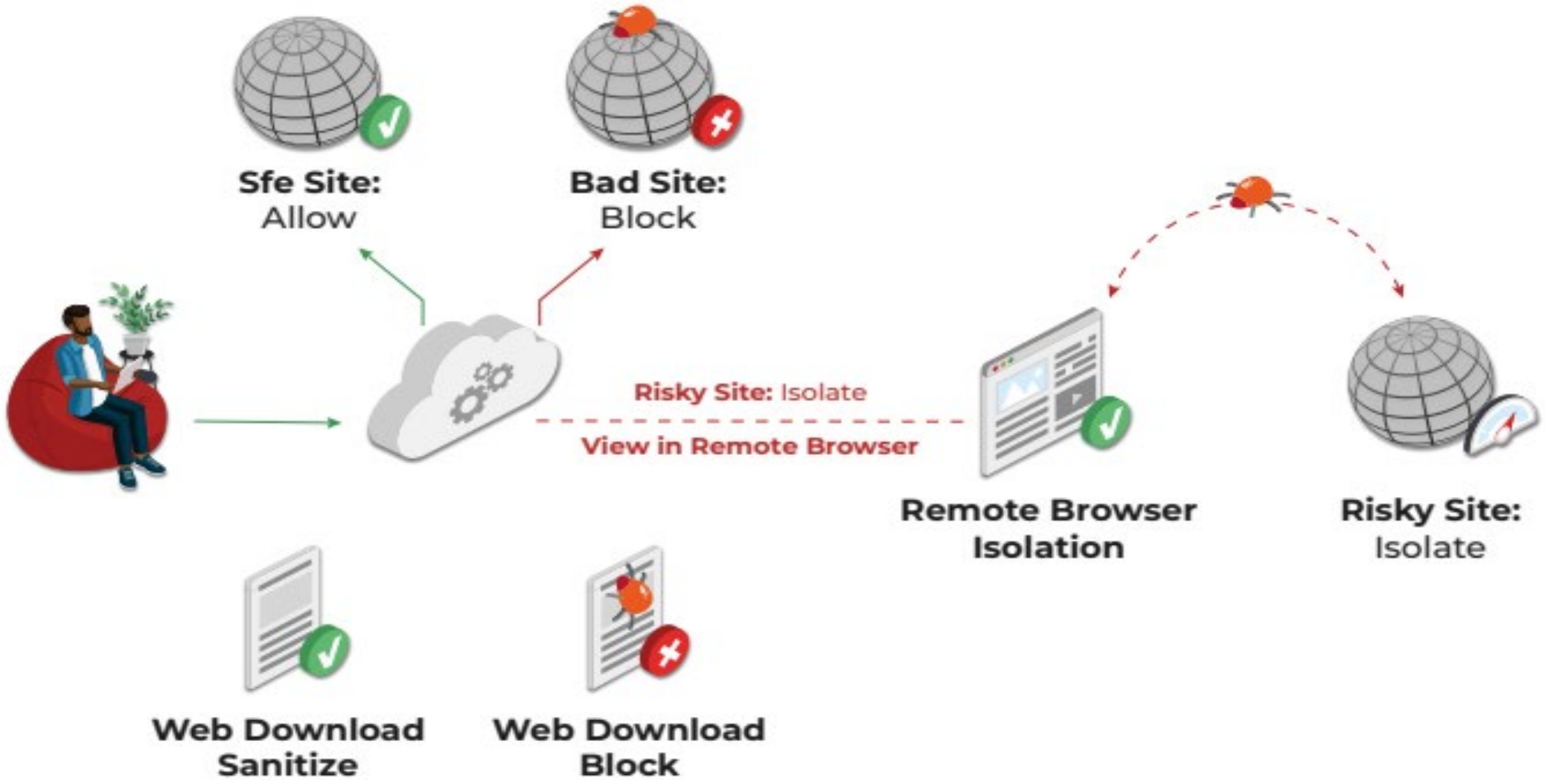
Requires – Dynamic Data Security

- Must be cloud agnostic
- MSSP Optimized
- Agent based or agentless
- Keeps the user secure on the internet
- Policy Driven with Proprietary ML
- Powers Device Interrogation and Control
- Helps move from legacy networking to CAN/SDWAN
- App agnostic
- Secure Remote Desktop
- Leverages Data Discovery and Redaction based on IAM/Roles
- Secure Virtual Meetings
- API Integrated
- IAM/MFA/2FA from ZTEdge or any

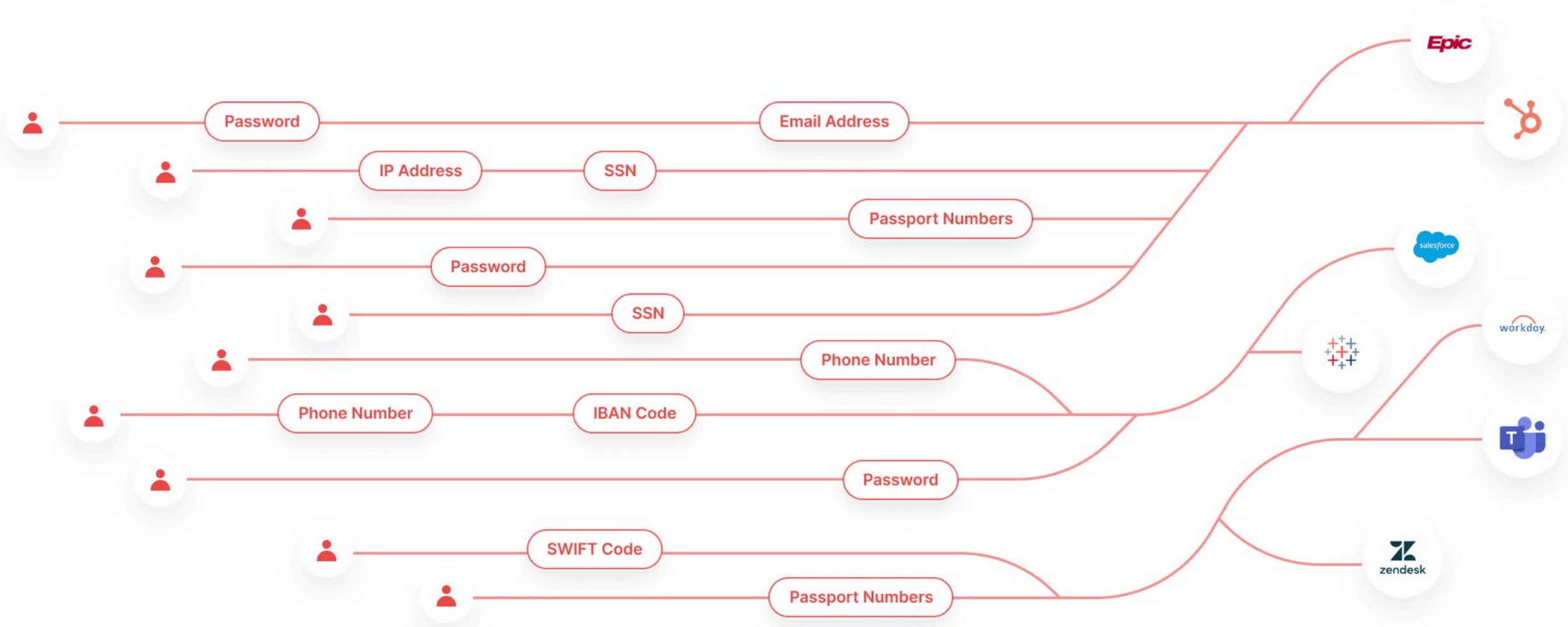




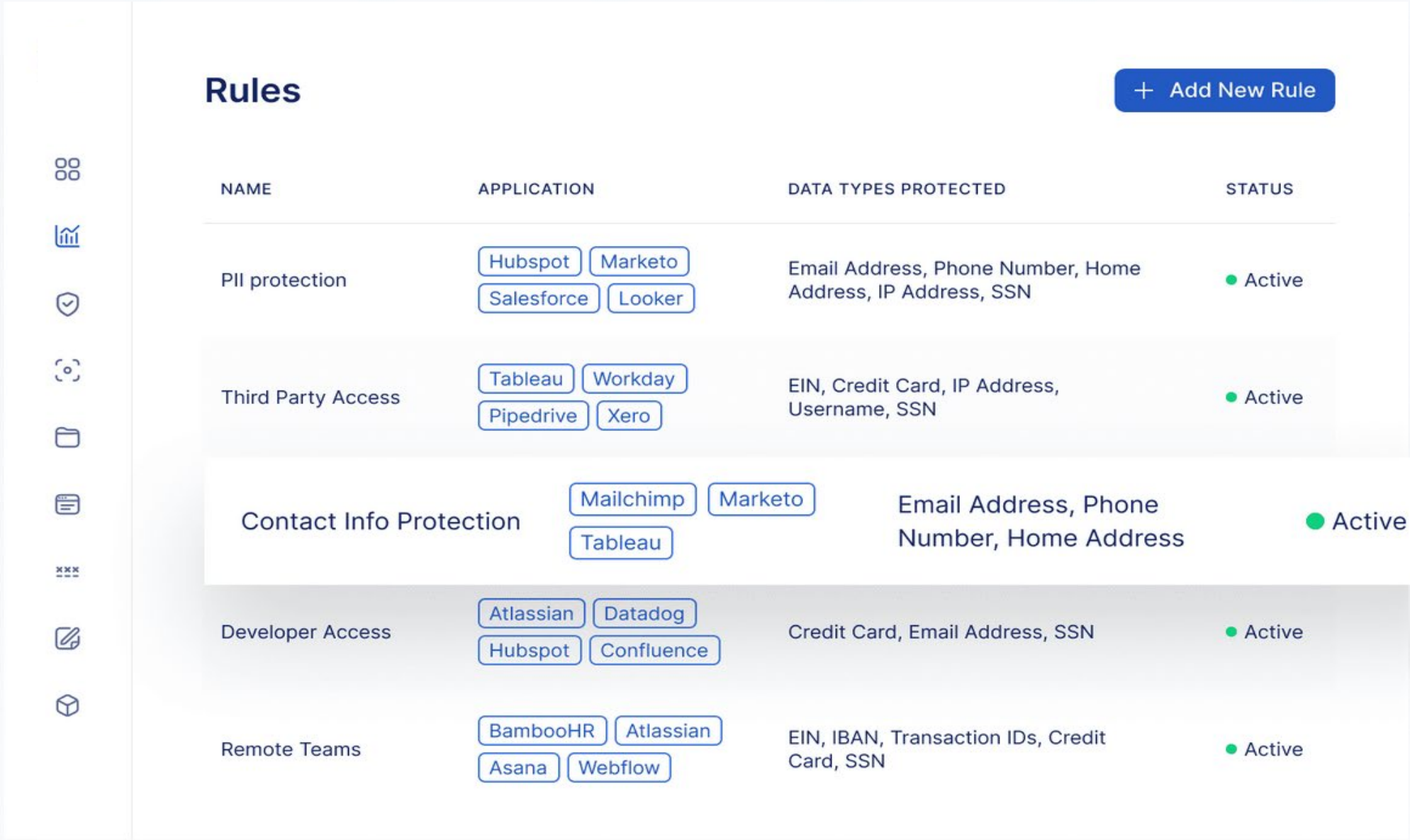
ML Designed Policy Develops Based on User and Application/Network Interaction



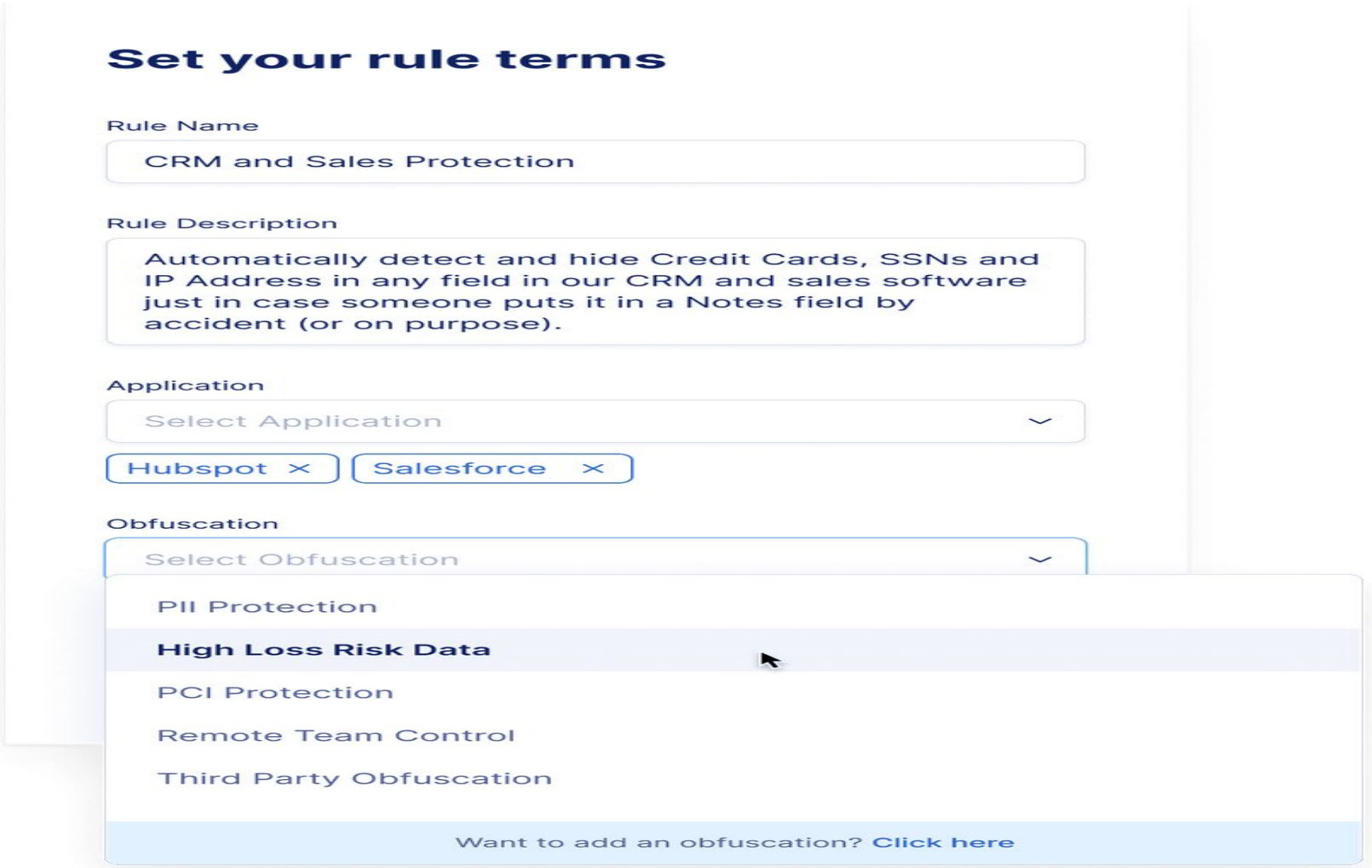
Users Work Anywhere On Any Device Policy Secures Online Interactions Dynamically



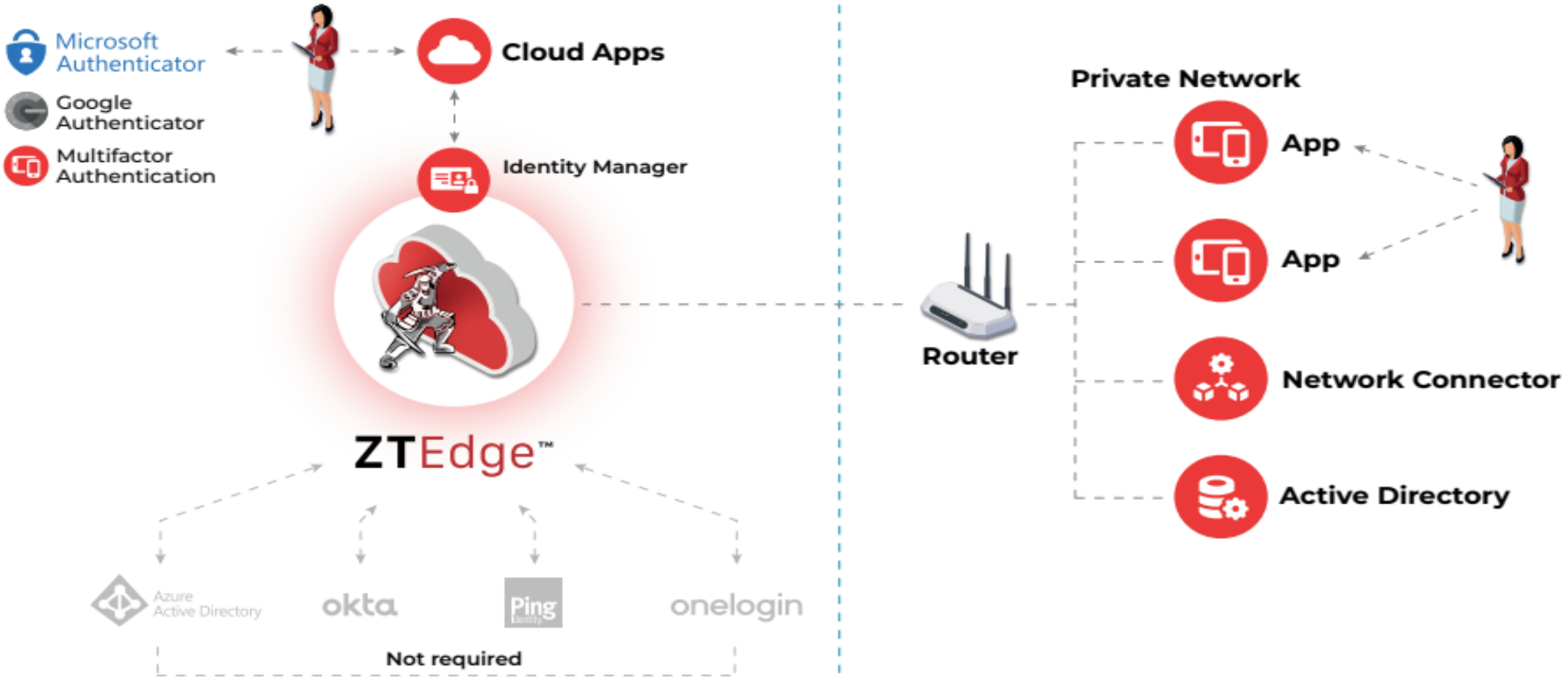
Data Is Discovered As It is Used By Users, Access, Applications Transiting the Network in Real Time



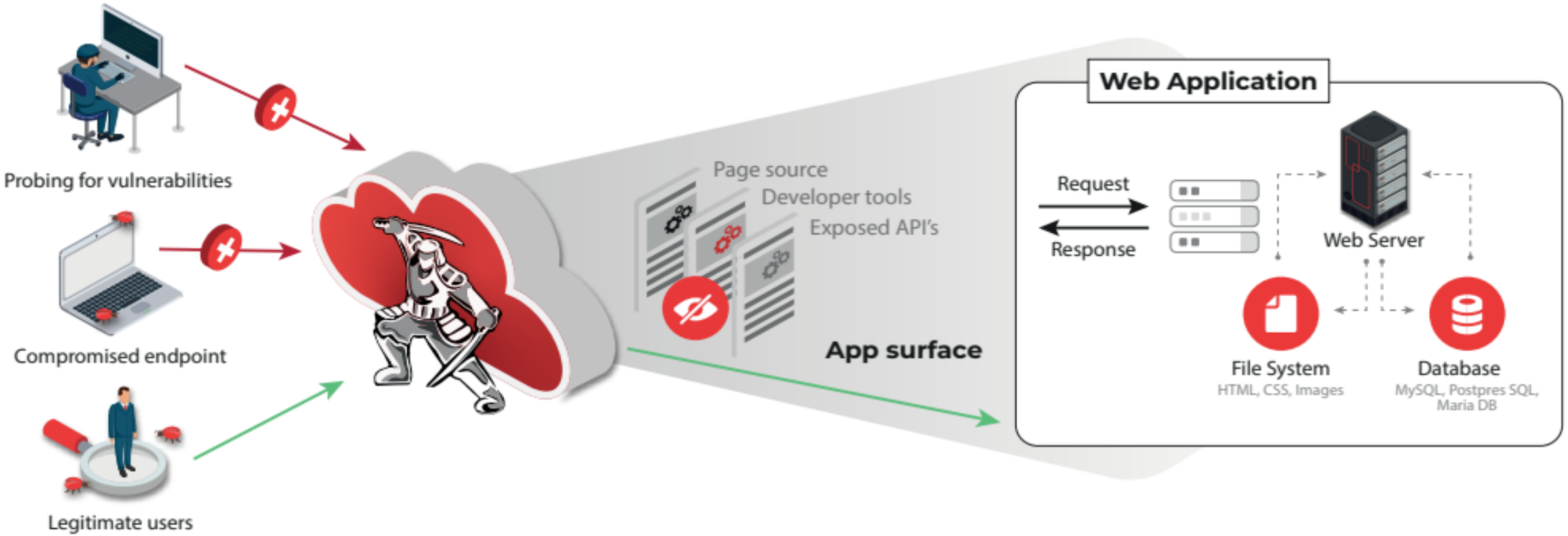
Data Is Categorized, Applications Are Identified,
Protection Status Verified



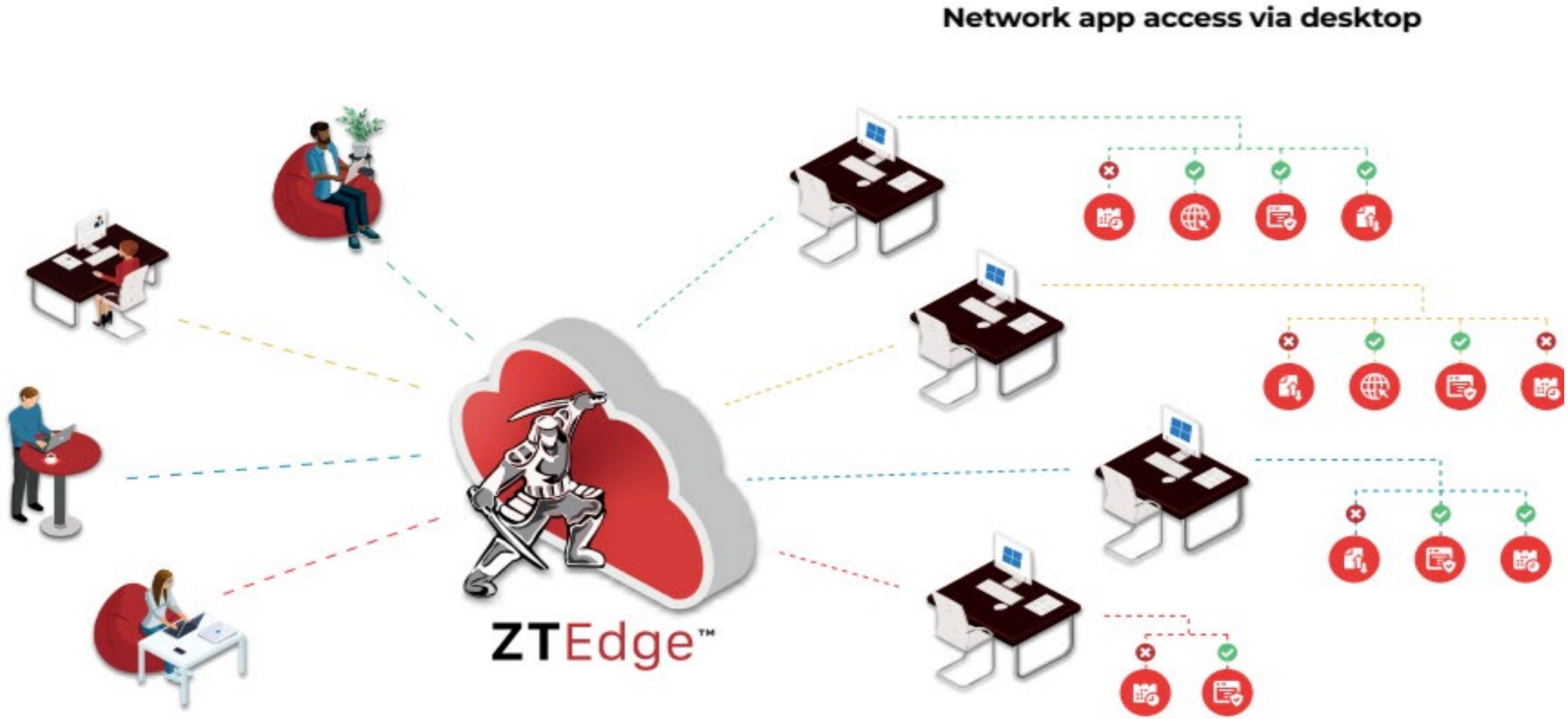
Data Access Policy Rules Are Modified Based On Usage and Security Requirements



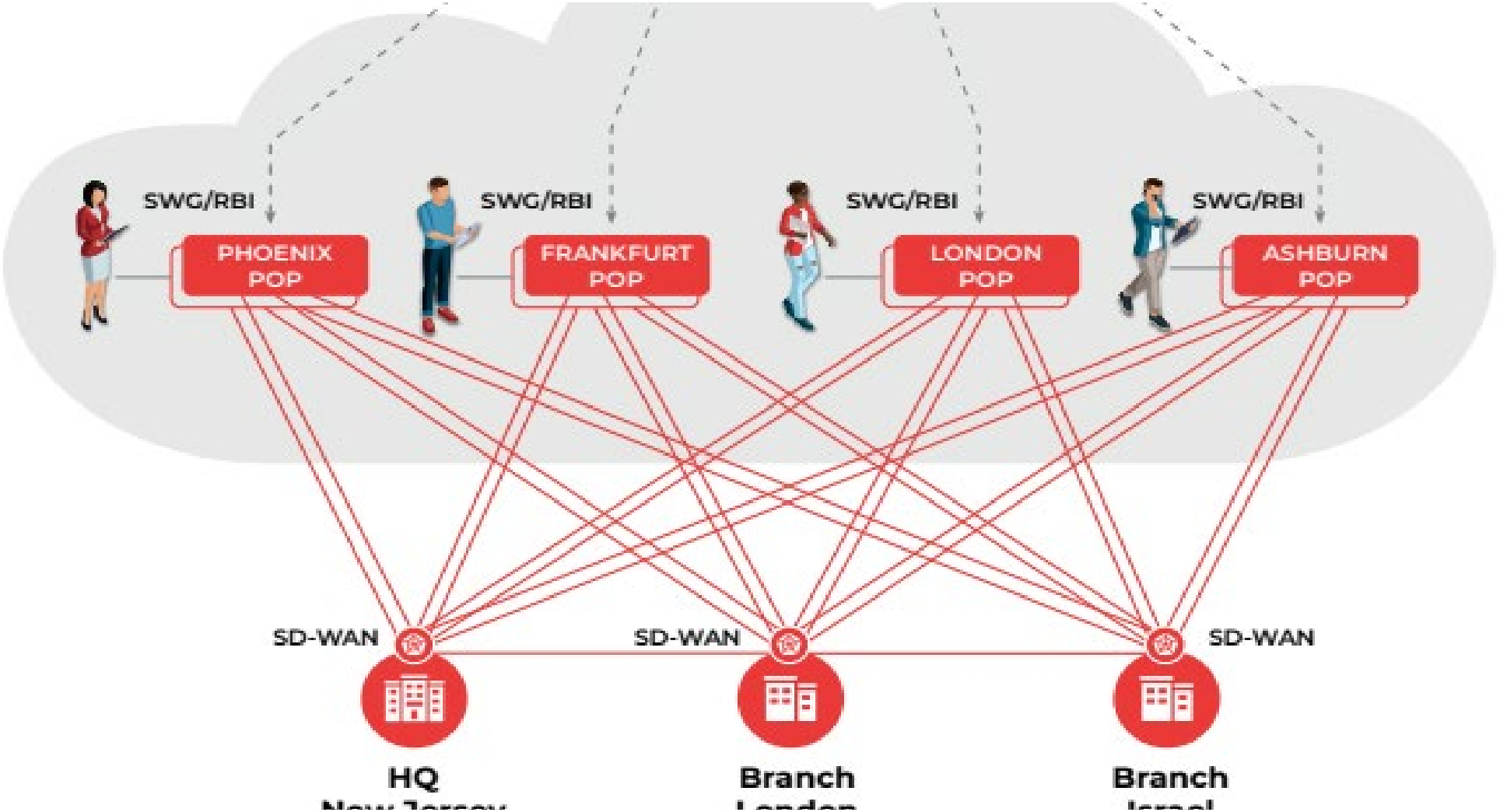
Access and Identities Are Validated Verified Via Any IAM Solution, Those Interactions/Accesses Feed Policy



Any Application Is Secured Via WAI Which Employs Policy Controls Before Access Is Provided and Requires No Device Management



Secure Administrator Access and Controls Provided
Via Proprietary Secure RDP, Policy Driven and
Integrated Across Network



Network and Cloud Agnostic Contollers Employ Policy
While Enabling Network Migration to SDWAN/CAN
Over Time, Secure Network Protocols Selectable

A large U.S. federal agency provides services used by global users.

The agency currently is operating a hybrid, multi-cloud enterprise that supports about 45,000 federal employees and 15,000 contractors.

The enterprise's networks break down into Information Technology (IT) (75%), Operational Technology (OT) (15%), and Supervisory Control and Data Acquisition (SCADA) (10%).

The OT and SCADA networks support the agency's smart buildings' controls/operations and distribution centers.

Currently, the agency has identified three high-value assets (HVAs): two legacy systems and one database containing Protected Personal Information (PPI).

The agency is currently using four different identity and access management systems (Okta Identity Cloud, Cirrus Identity, Azure AD, and Google Cloud Identity) and lacks a centralized security operations center (SOC).

The agency is currently unable to integrate logging information due to the continued use of legacy systems: an organizational structure where SOC operations are broken across different teams and a hybrid, multi-cloud implementation where services provide different formats for the information.

The agency must implement two-factor authentication but also must provide multi-factor authentication (MFA) for some parts of the enterprise.

The agency has a budget of $3 million and a one-year timeline during which it must start to address M-22-09.

Given this last constraint, each proposal should address its compatibility with the agency's existing hardware and software infrastructure.