black hat USA 2022

TRAINING

TECHNICAL BUILDING BLOCKS OF ZERO TRUST

Aug-07-2022

Carlos Martinez
Solutions Architect

Matt Schiller
Senior Software Engineer

Welcome!

Training Goals

- Understanding of the core Zero Trust Network Architecture (ZTNA) components
- Deploy personalized ZTNA demo environment
  - Hands on lab
- Insight and tips for getting started with your Zero Trust initiative

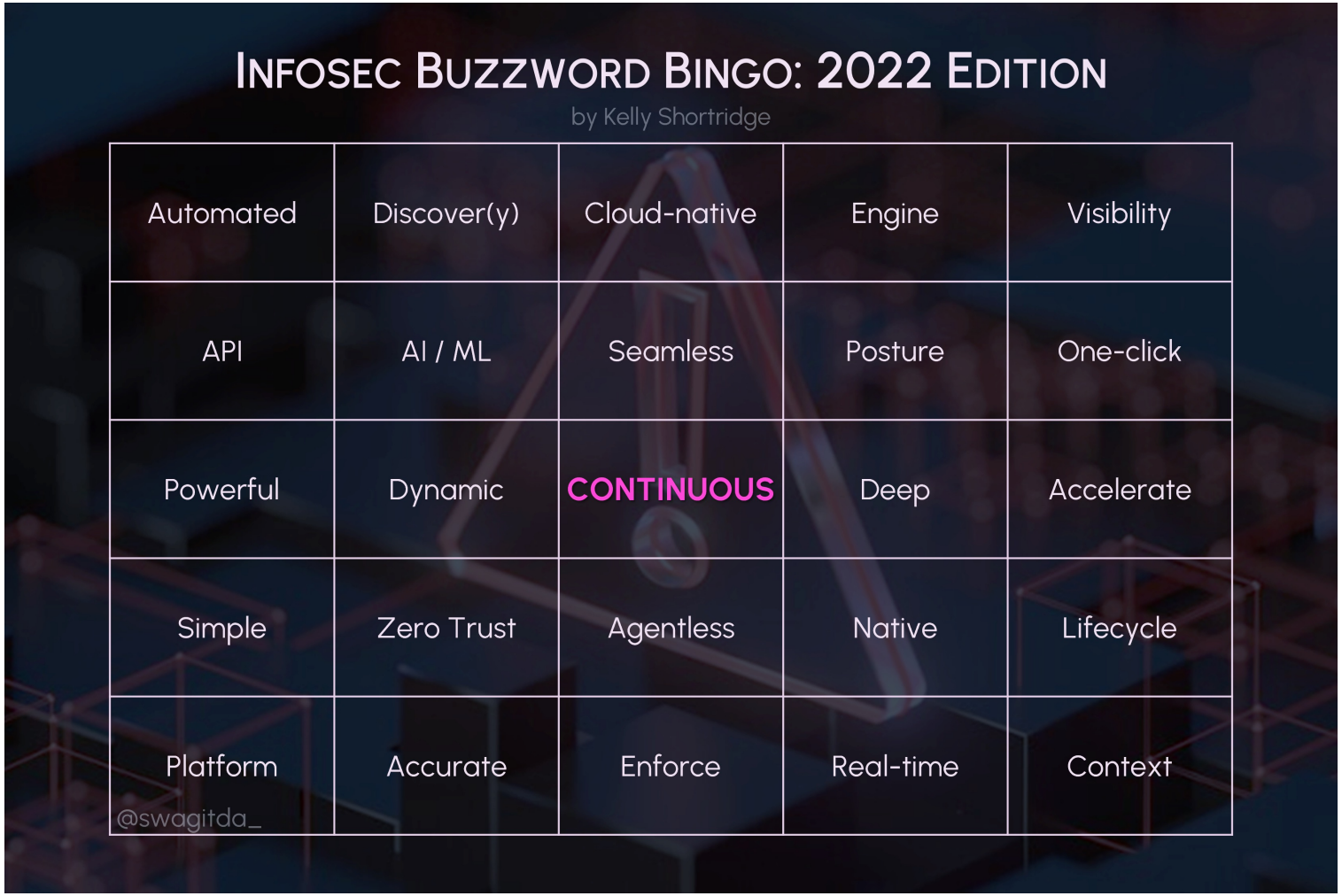
Agenda – Day 1

- Objectives
- Schedule
  - 12:30pm-1:45pm – Lunch
  - 1:45pm-4pm - Class
  - 4:00pm-4:15pm - Break

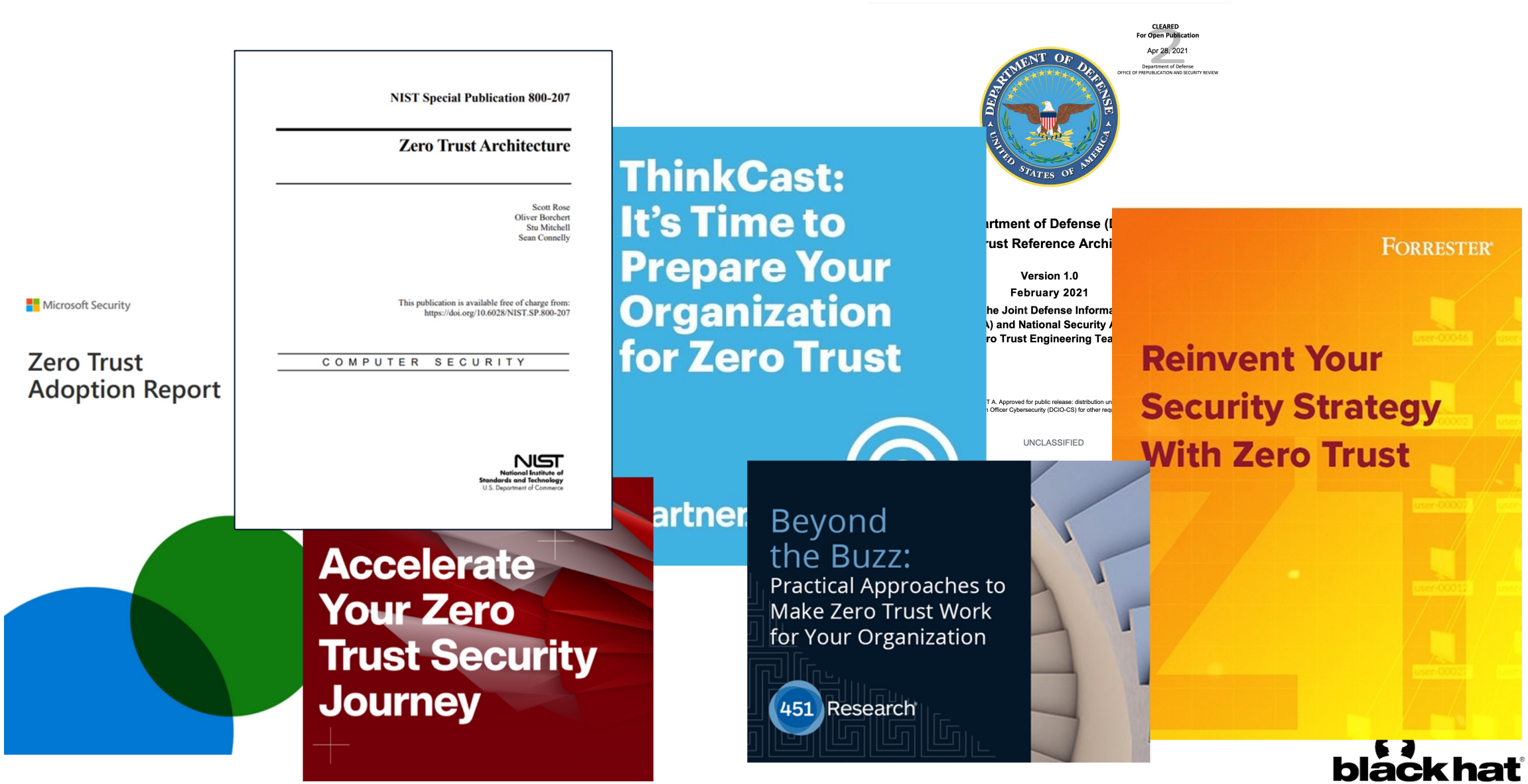
Housekeeping Items

- Lab requirements
  - Computer (Win/MacOS)
    - AWC CLI
    - Terraform
  - AWS account (https://aws.amazon.com/free/)
  - ~~Okta developer account~~
- WiFi
  - SSID: ShellSeekersAB
  - Pwd: TanMicrophone
- Questions and participation

Let’s play buzzword bingo



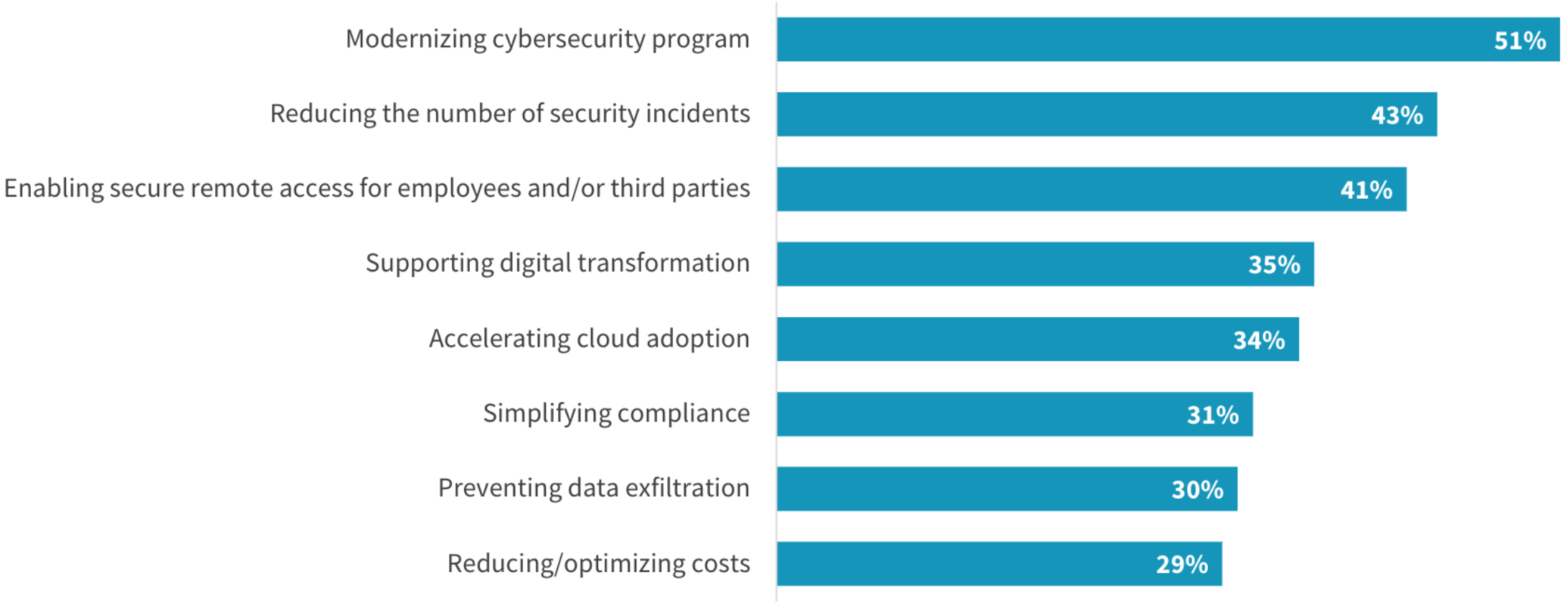
Beyond the Marketing Buzz



ZTA drives multiple business outcomes

1. Security with a dissolved perimeter
2. Resiliently respond to evolving threats
3. Provide least privilege access to resources
4. Reduce attack surface
5. Regulatory compliance
6. Improved user experience

Top drivers of zero-trust strategies



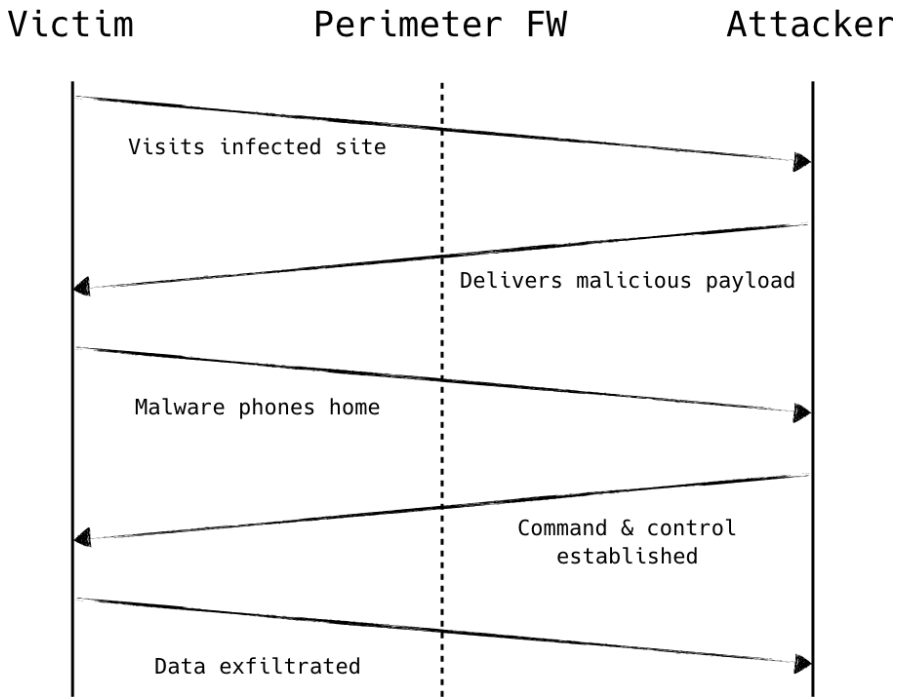
(2021) Enterprise Strategy Group - The State of Zero-trust Security Strategies

Audience Poll

- What are the drivers for you?
- Where are you in their journey?
  - Discussion
  - Planning
  - Implementation

Traditional Perimeter Security

- Implicit trust granted based on network location
  - External access is untrusted
  - Internal access is trusted
- Problems with traditional tactics
  - Modern attacks are inside out
  - Lateral movement
  - Lacking central governance
  - Overly-broad access



Zero Trust Architecture - History

- Jericho Forum (2004)
  - De-perimiterization – limit implicit trust based on network location
- John Kindervag/Forrester (2010)
  - Coined ‘Zero Trust’ term
  - Concepts
    - Verify and secure all resources
    - Limit and strictly enforce access control
    - Inspect and log all network traffic
- BeyondCorp Published (2014)
    - Service access not determined by the network from which you connect
    - Service access granted based on contextual factors (user and device)
    - Access must be authenticated, authorized, and encrypted

Five Fundamental Assertions of Zero Trust

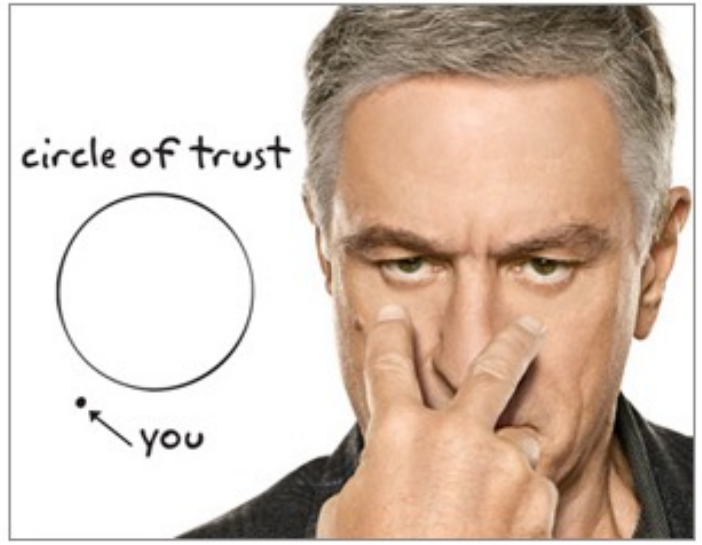
1. The network is always assumed to be hostile
2. External and internal threats always exist on the network
3. Network locality is not sufficient for deciding trust in a network
4. Every device, user, and network flow is authenticated and authorized
5. Policies must be dynamic and calculated from as many sources of data as possible

Zero Trust Network

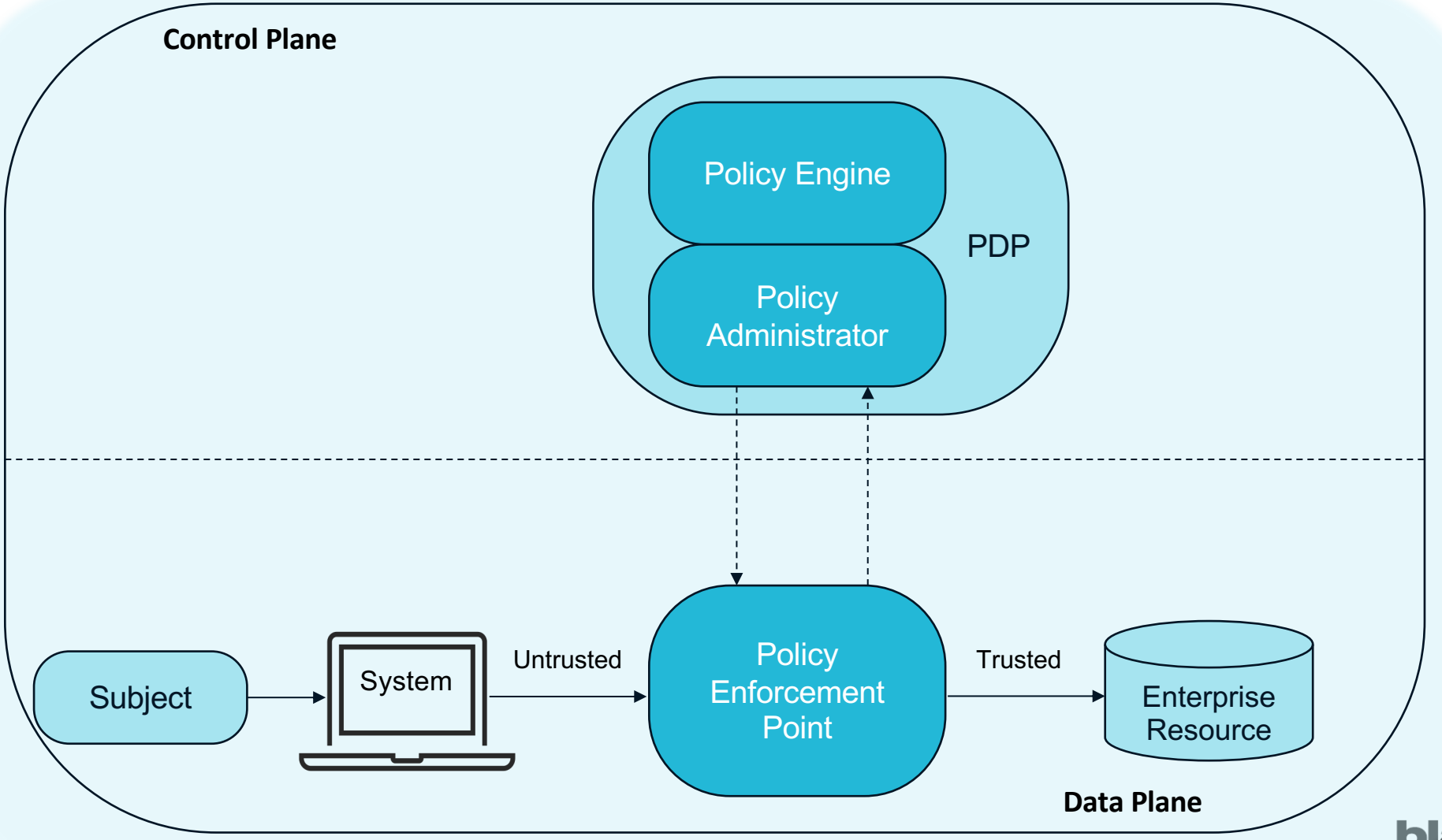
- Zero Trust concept is a set of security principals
- Zero Trust principals can be applied across your organization
  - User-to-service
    - Remote Access (ZTNA)
    - Workplace
  - Service-to-service (workloads)
    - Microsegmentation
- Zero Trust should be a journey
  - Start small, gain experience, expand
  - Complete zero trust security posture may never be fully achieved

Zero Trust Mandates

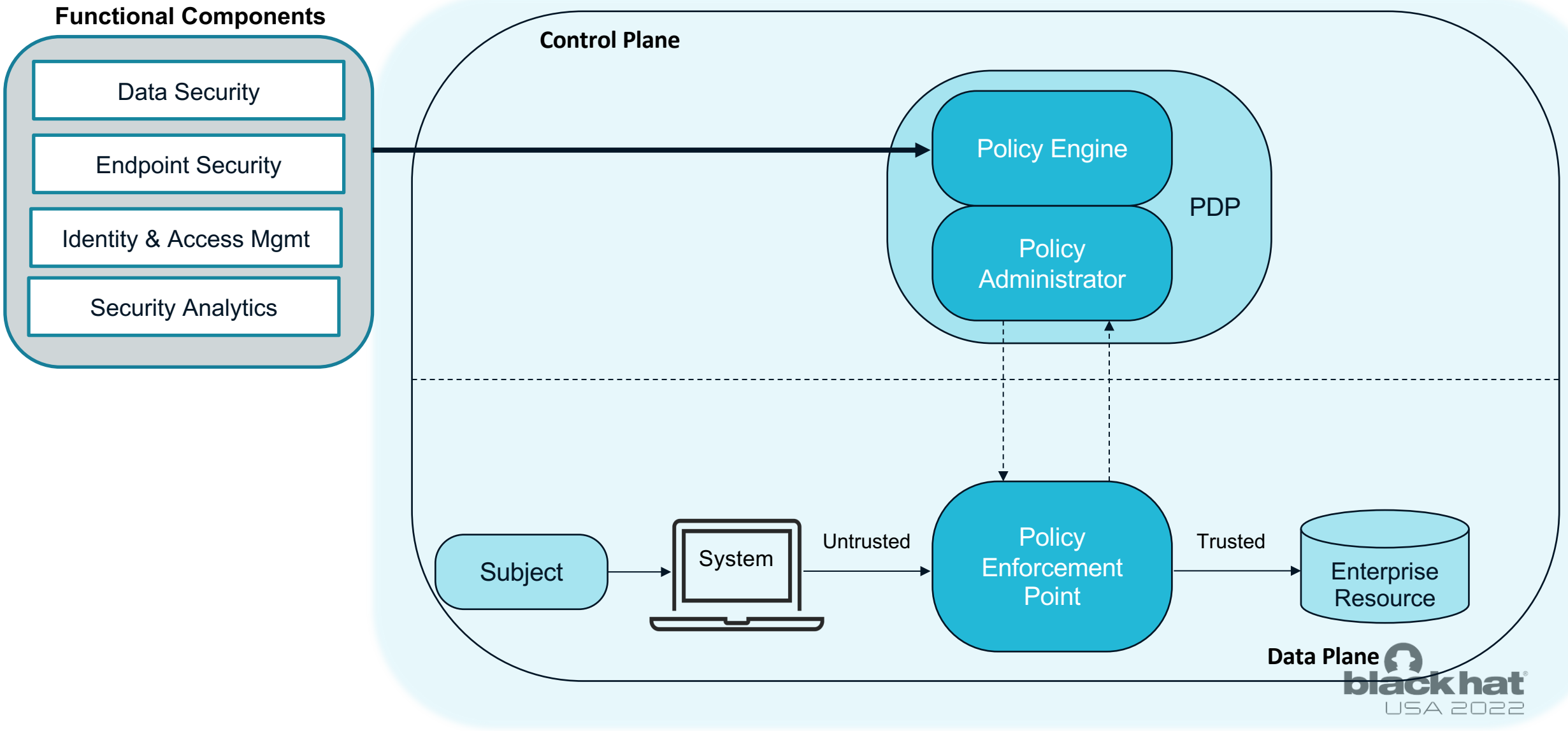
- All communication is inspected and secured regardless of network location
- Access to enterprise resources granted on a per-session basis
- Access is determined by dynamic, contextual-based policies
  - Least privilege access enforced
  - State of client identity or asset requesting access
  - Type of application (sensitive data, role-based access)



Zero Trust Architecture – Core Components

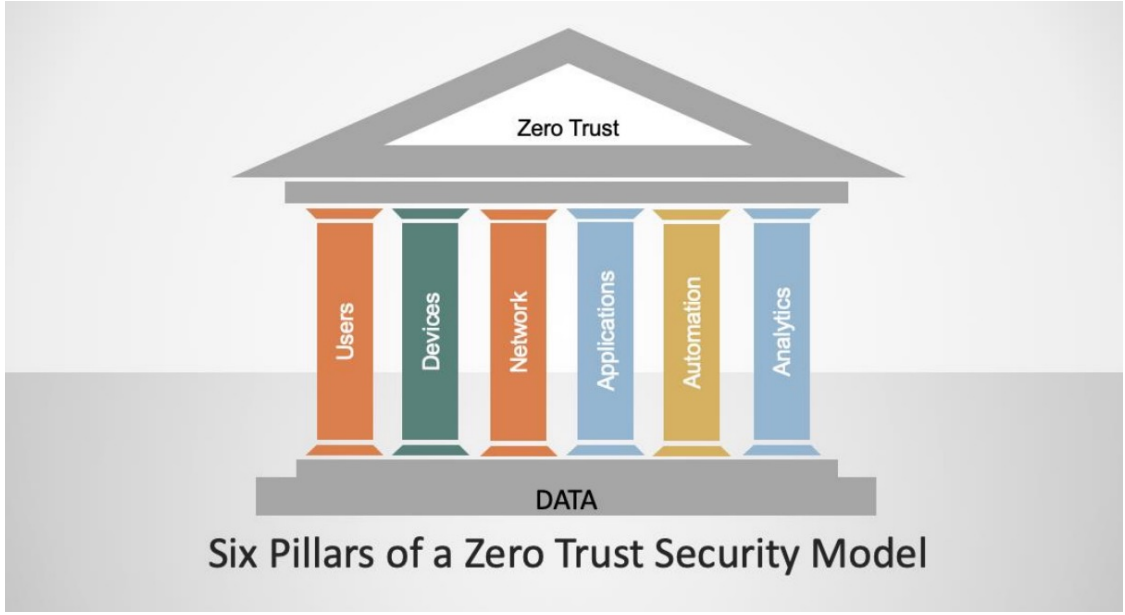


Zero Trust Architecture – Functional Components



Six Pillars of a Zero Trust Security Model

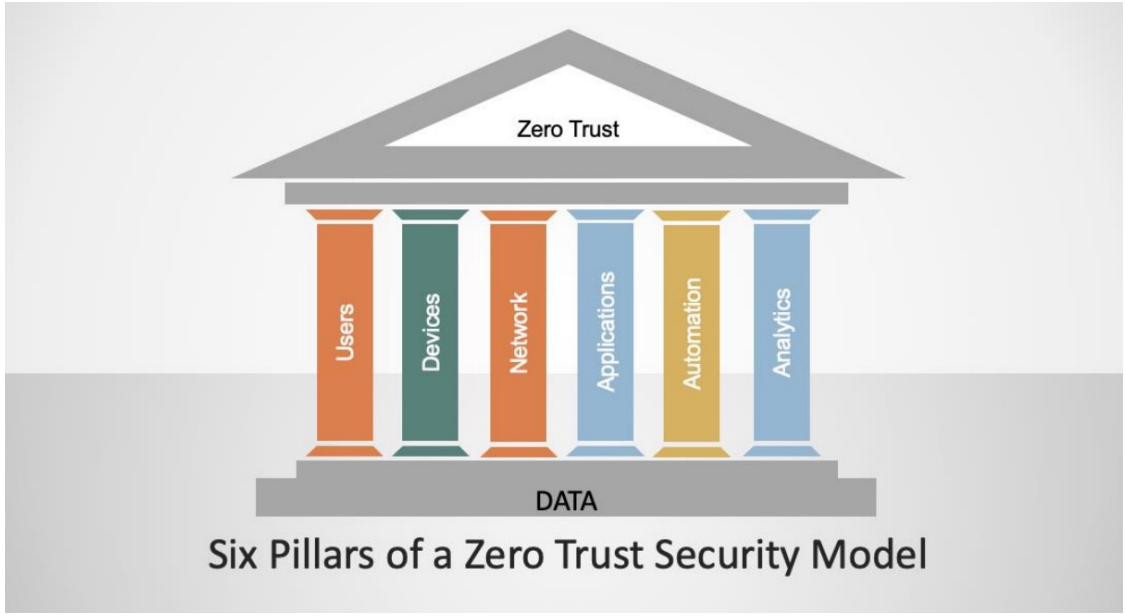
- **Data Foundation**
  - All about protecting your data
- Pillar #1 – People/Identity Security
  - Ongoing authentication
  - Strong assertion of user
- Pillar #2 – Device Security
  - Real-time posture check
  - Utilizing ‘sytem of record’ solutions



American Council for Technology-Industry Advisory Council (ACT-IAC)

Pillars of Zero Trust

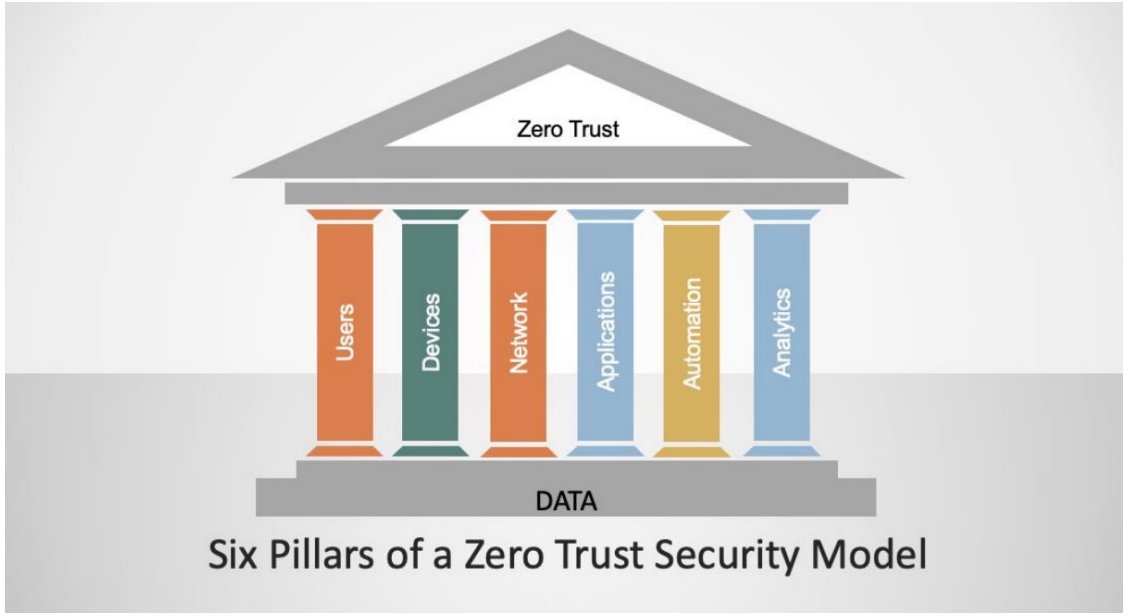
- Pillar #3 – Network Security
  - Control Priv. Network Access
  - Manage internal/external data flows
  - Prevent lateral movement
  - Visibility to make dynamic policy/trust decisions
- Pillar #4 – App & Workload Security
  - Consistent authN/authZ schemes
  - Roles and least priv access
  - Coarse vs. fine-grained controls



American Council for Technology-Industry Advisory Council (ACT-IAC)

Pillars of Zero Trust

- Pillar #5 – Automation
  - Integration with existing security tools and processes
- Pillar #6 – Analytics
  - user/device/resource/activity correlation
  - Leverage existing logging tools



American Council for Technology-Industry Advisory Council (ACT-IAC)

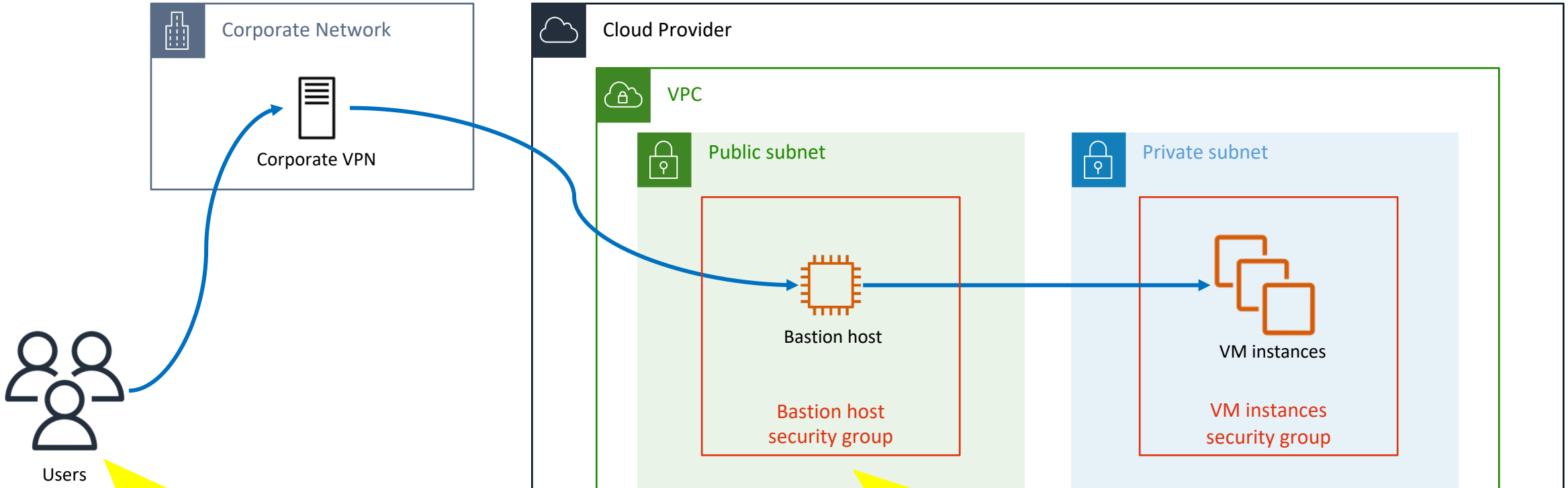
Zero Trust Network Access (ZTNA)

- ZTNA protects company resources by enabling least-privilege access to hosted applications and infrastructure
- ZTNA use cases
  - Modernize/replace legacy VPN solutions
  - DevOps
  - Additional use cases
    - 3rd Party Access (Vendors, Contractors)
    - BYOD
    - M&A

Desired ZTNA Properties

- Consistent identification, authentication, and authorization scheme
- Access to resource assessed on per-session basis
- Access requests evaluated/enforced dynamically based on defined policies
  - Traffic is secure
  - All requests are logged (SIEM)
- Integration with existing identity management services (SSO)
- Continuously reassess (reauthentication & reauthorization)
  - Mitigate unauthorized access to resources

Traditional access to cloud resources



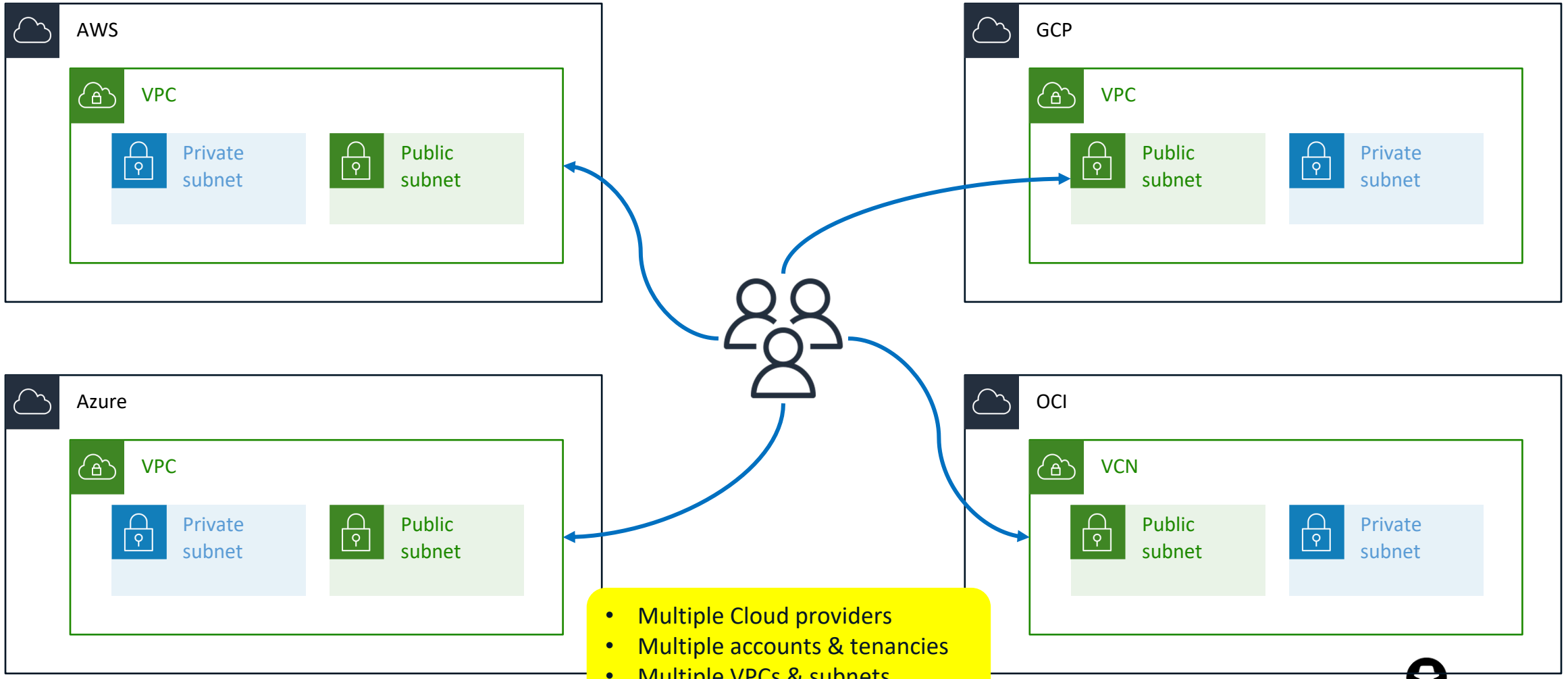
Users need to use multiple credentials:
1. VPN
2. Bastion host
3. Application/service

Admins need to manage multiple systems:
1. VPN access
2. Keys on bastion
3. Firewall rules
4. Authentication to application/service

Traditional approach poses many challenges

- Onboarding/offboarding of users
  - Keeping track of users and environments
- Handing static VPN/SSH keys to all users
  - Key rotation?
- Complex networking with ephemeral IPs
  - Web services on top of K8s
- Exposed system creds
  - How to respond when compromised?

And, it’s only getting more complex …



ZTNA for Cloud & DevOps

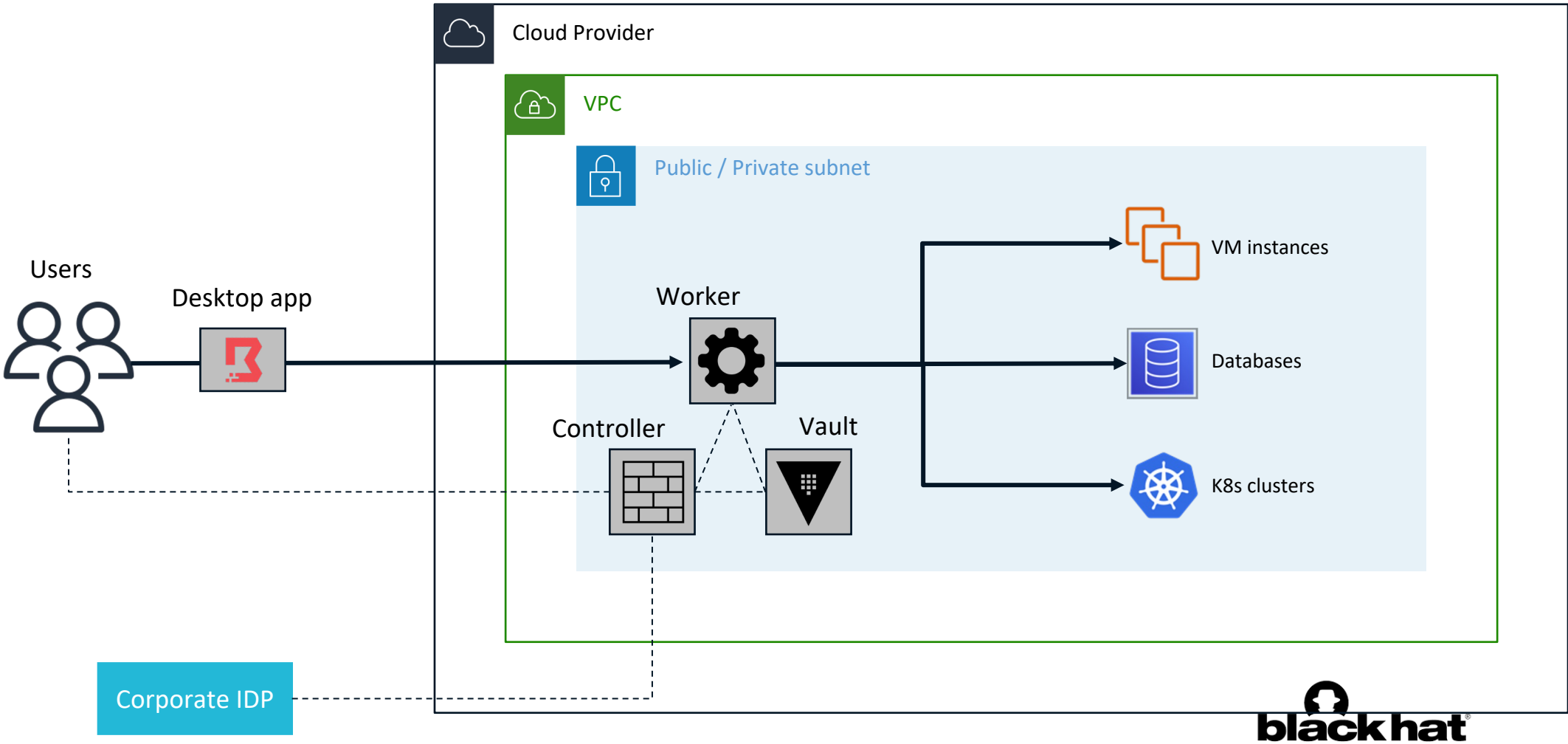
Benefits of the approach

- Improve user experience
  - Replace traditional methods with SSO via Corporate IDP
  - Service catalog to access resources
- Better security
  - Establish User/Device Trust
  - Define granular access roles/context
  - Increased visibility
- Simplified management
  - No complex ACLs
  - Less error prone for administrators

Lab 01 – Set up ZTNA environment

- Lab Zero Trust Infrastructure
- Deploy lab components
  - Boundary
  - Boundary Desktop

Lab 01 – Set up ZTNA environment



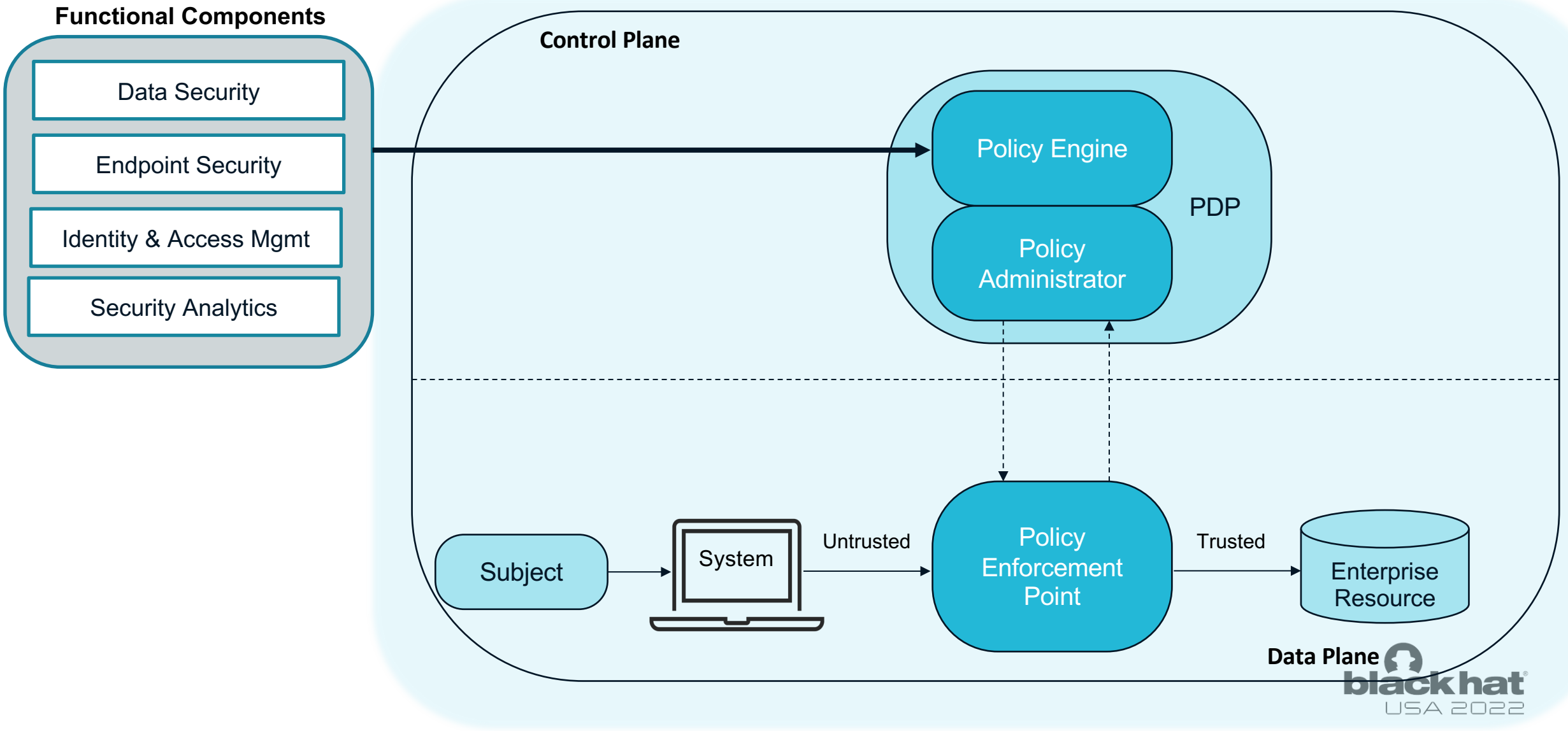
DAY 2

TECHNICAL BUILDING BLOCKS OF ZERO TRUST NETWORK ACCESS

Agenda – Day 2

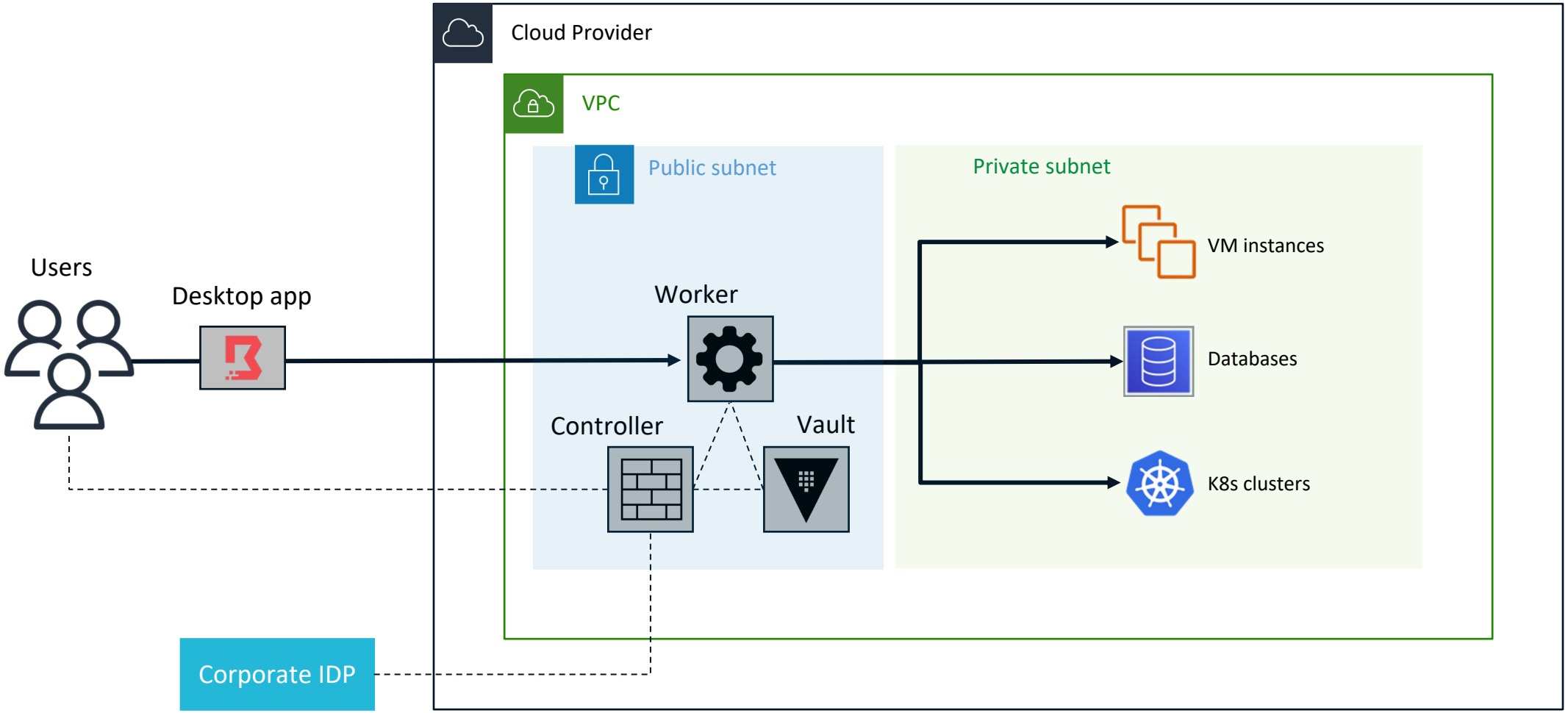
- Objectives
- Schedule
  - 10:00am-10:30am – Class
  - **10:30am-10:45am – Break**
  - 10:45-12:20pm - Class
  - **12:30pm-1:45pm – Lunch**
  - 1:45pm-4pm - Class
  - **4:00pm-4:15pm – Break**
  - 4:30pm-6pm - Class

Zero Trust Architecture – Functional Components

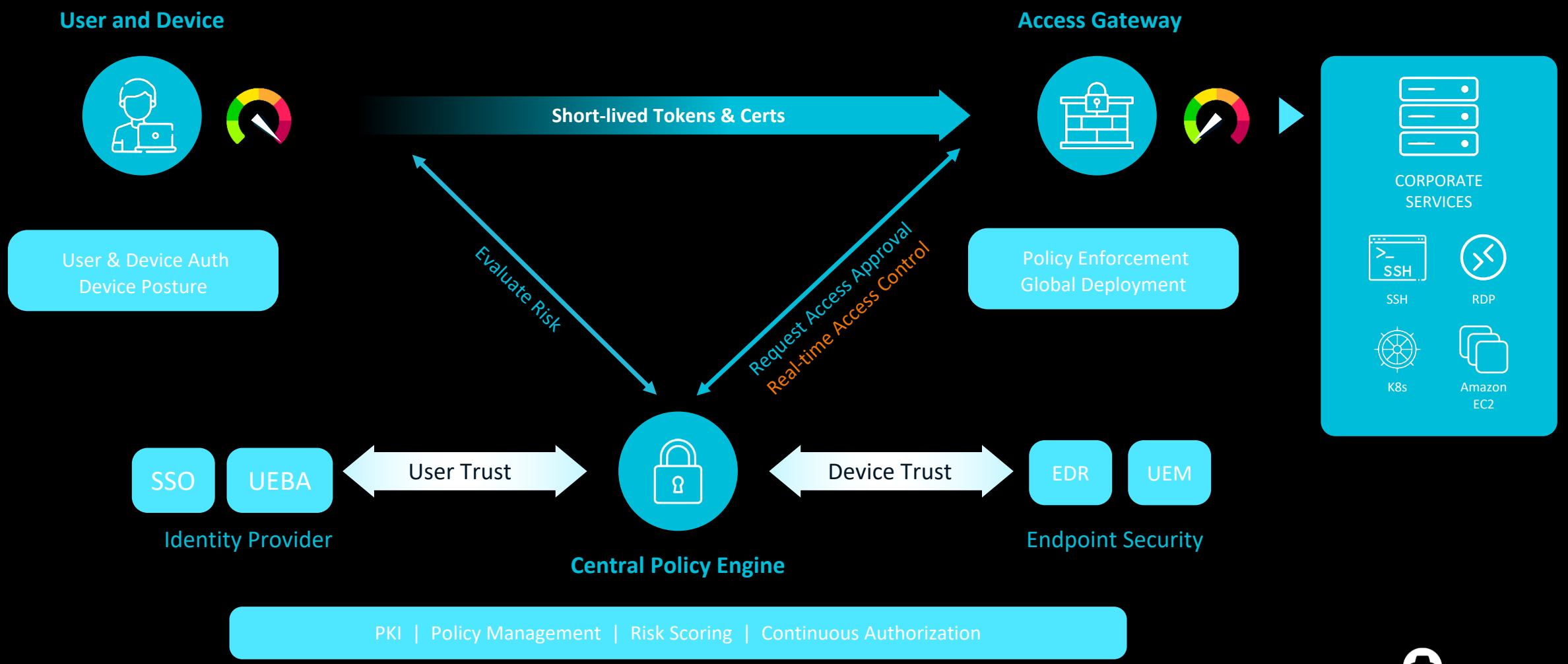


Reference architecture for self-hosted Zero Trust

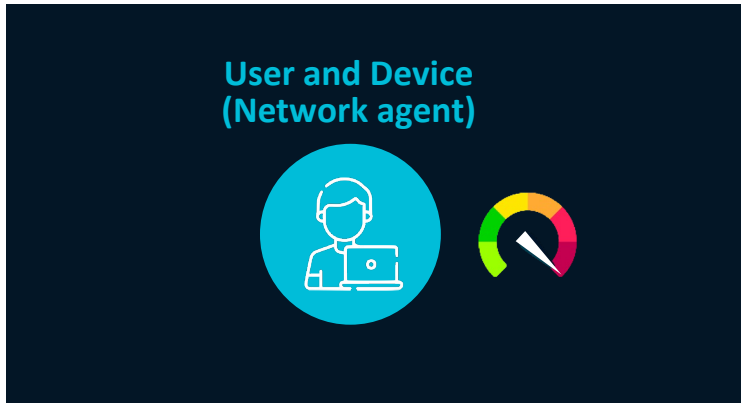
Example: Hashicorp Boundary



Technical building blocks (ZTNA)

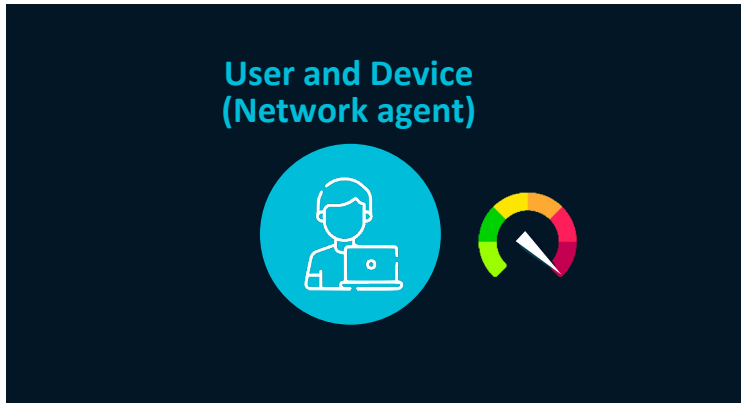


Technical building blocks – User & Device



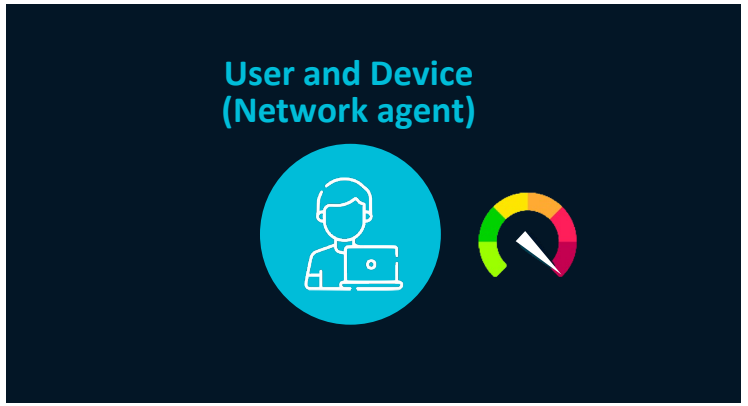
- Network Agent
  - Comprised of user & device
  - Network agent must be authorized access in ZTA

Technical building blocks – User



- Establishing User Trust
  - Unified Identity & Access Management (IAM)
    - SSO
  - Multifactor
  - Passwordless
  - Roles

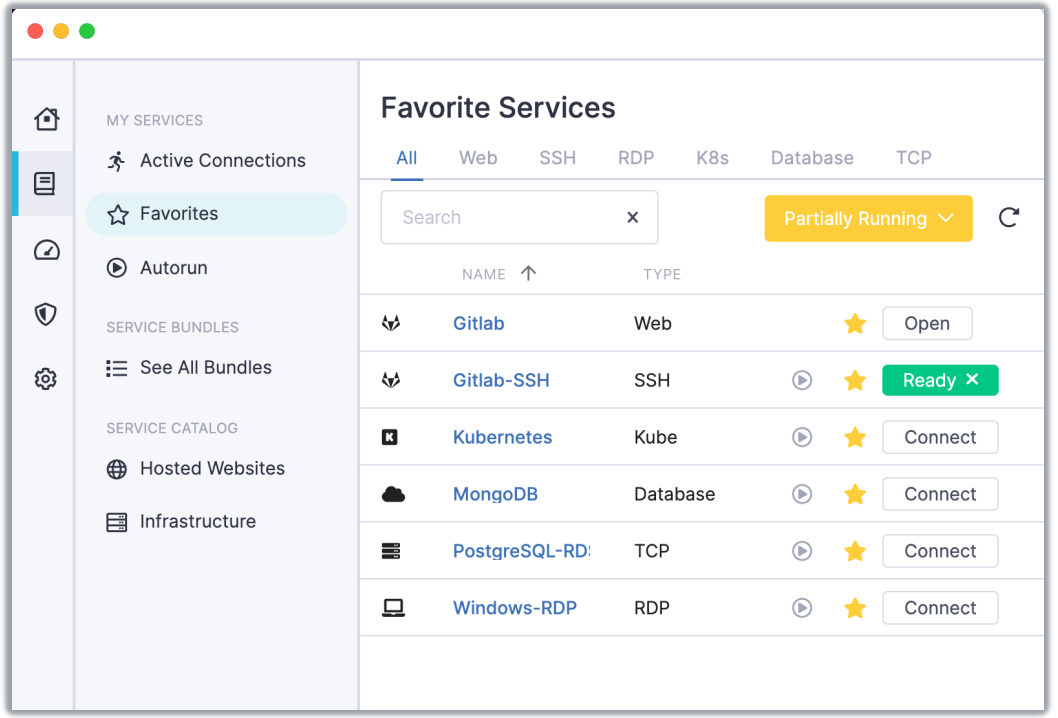
Technical building blocks – Device



- Establishing Device Trust
  - Device Identity
    - Registration (device inventory database)
    - Device certs
  - Validating device posture
    - Validating trust factors/signals (software versions, required apps, compromised state)
    - Corporate-managed (UEM) vs. BYO

Technical building blocks – Endpoint (ZTNA)

- Endpoint component enables user access to services while validating the user/device and enforcing policy
- Support existing tools and methods (CLI) that engineers are familiar with
- App catalog of available logical services/hosts
- Typically requires a local host agent which can surface user validation and ensures policy enforcement with the gateway
- Provides explainability for self-remediation



Technical building blocks – Access Gateway

- Proxy component enables user access to services while validating the user/device and enforcing policy
- Policy enforcement, via communication with Policy Engine for granular access
- Can support a variety of protocols
- Continuous authorization
- Can scale and be deployed/distributed across multiple VPCs/AWS accounts/subnets

Technical building blocks – Policy Engine

- Policy engine components evaluates access control policy to grant/deny access
- Integrates with enterprise tooling to establish User Trust and Device Trust
- Easy-to-use admin interface to configure policies
- APIs to enable automation

Core concepts

- Role
  - Maps users & devices to a set of permission grants
- Service Catalog
  - List of resources available
- Policy
  - Which Roles can access specific Services in the Catalog
- Workflows
  - Publishing services
  - Managing policies
  - Integrating with SSO

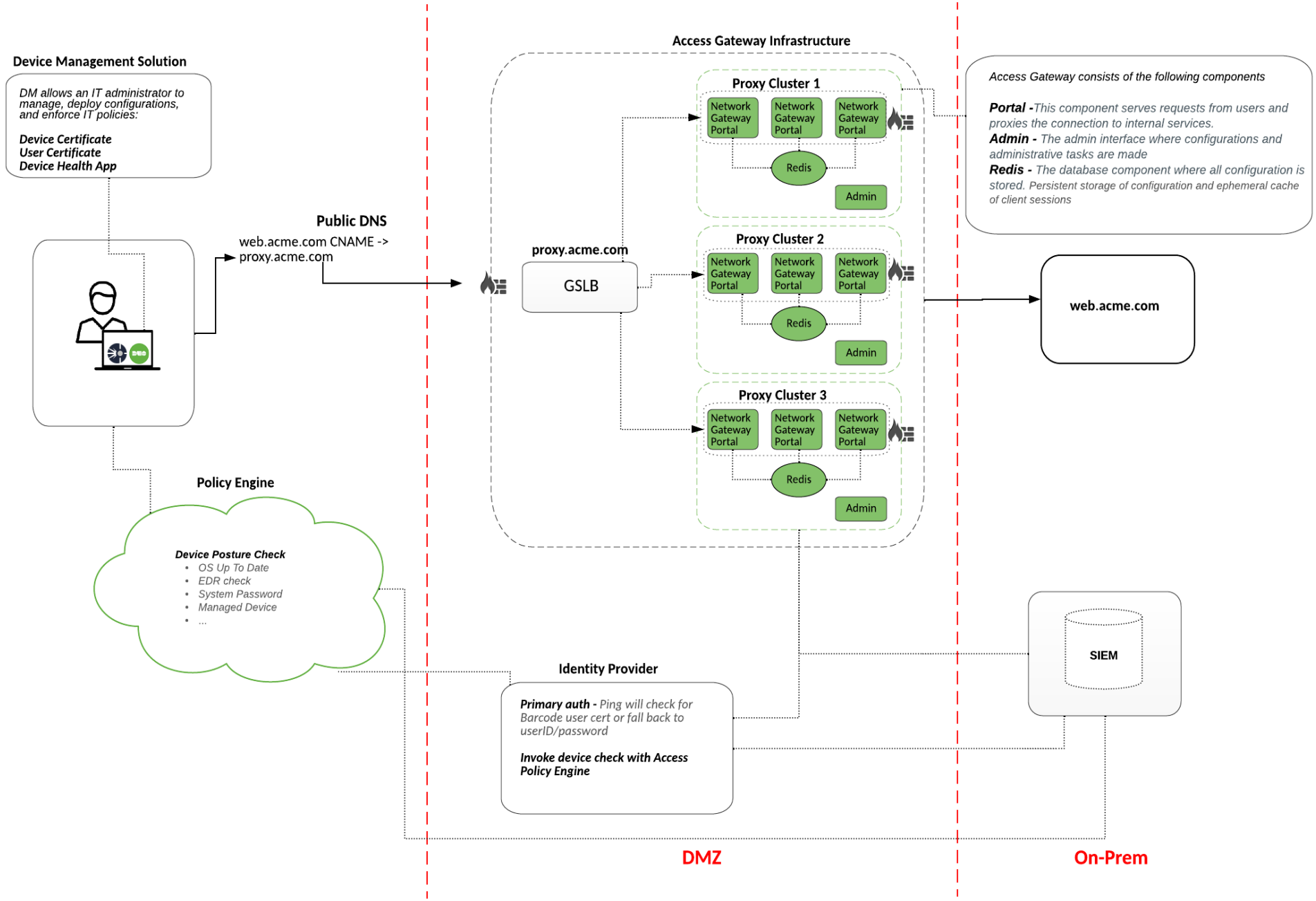
Additional Components

- Device Management
  - Corporate Assets
  - Seamlessly deploy configurations
- SIEM
- External Trust Signals
  - EDR
  - DM/UEM
  - SOAR
  - UEBA

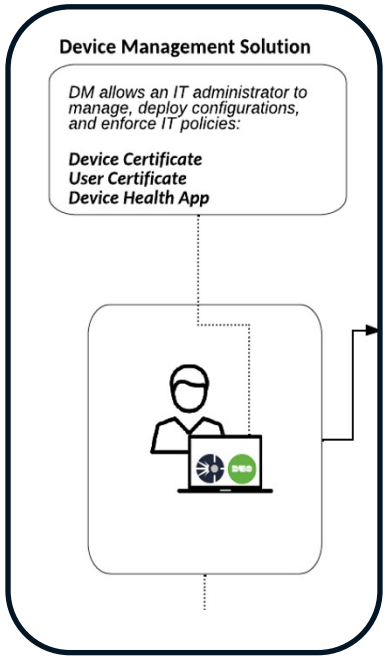
Lab

- Bring up all 4 modules (Network, Target, Controller, Worker)
- Bring up services

Example ZTNA Deployment

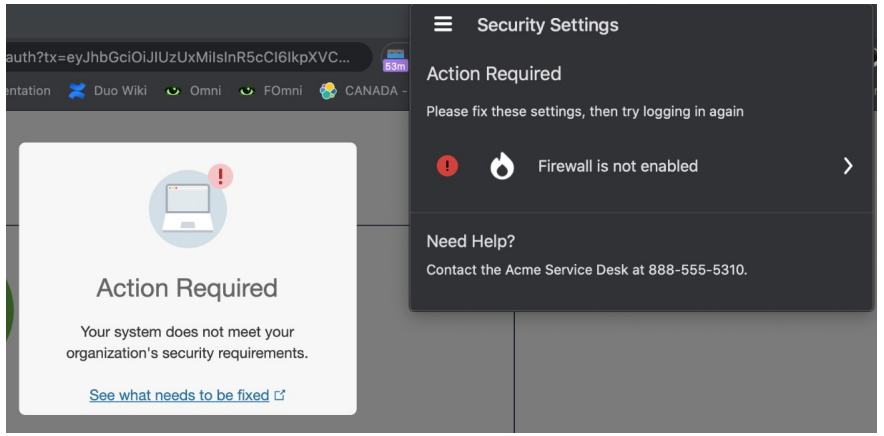


Example ZTNA Deployment (User & Device)



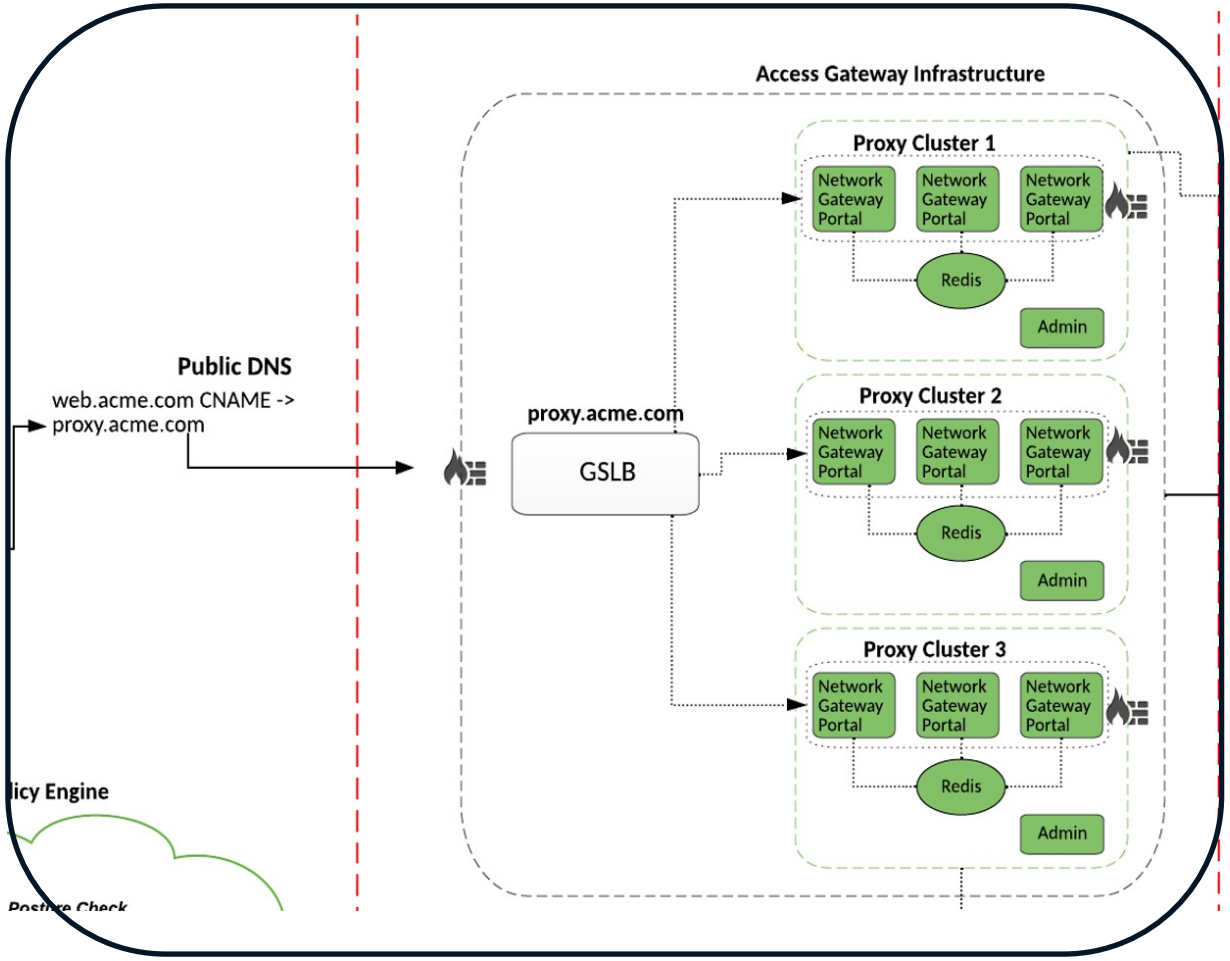
- Device Landscape
  - ~180k devices
  - MacOS/Win/Android/iOS
  - 3 Device Mgmt solutions
- Device Configurations
  - User Cert
  - Device Cert
  - Browser configs
  - Health App

- Posture Requirements
  - Minimum OS (N-2)
  - Passcode
  - Disk Encryption
  - Device Mgmt validation
  - EDR validation
  - Jailbroken/rooted



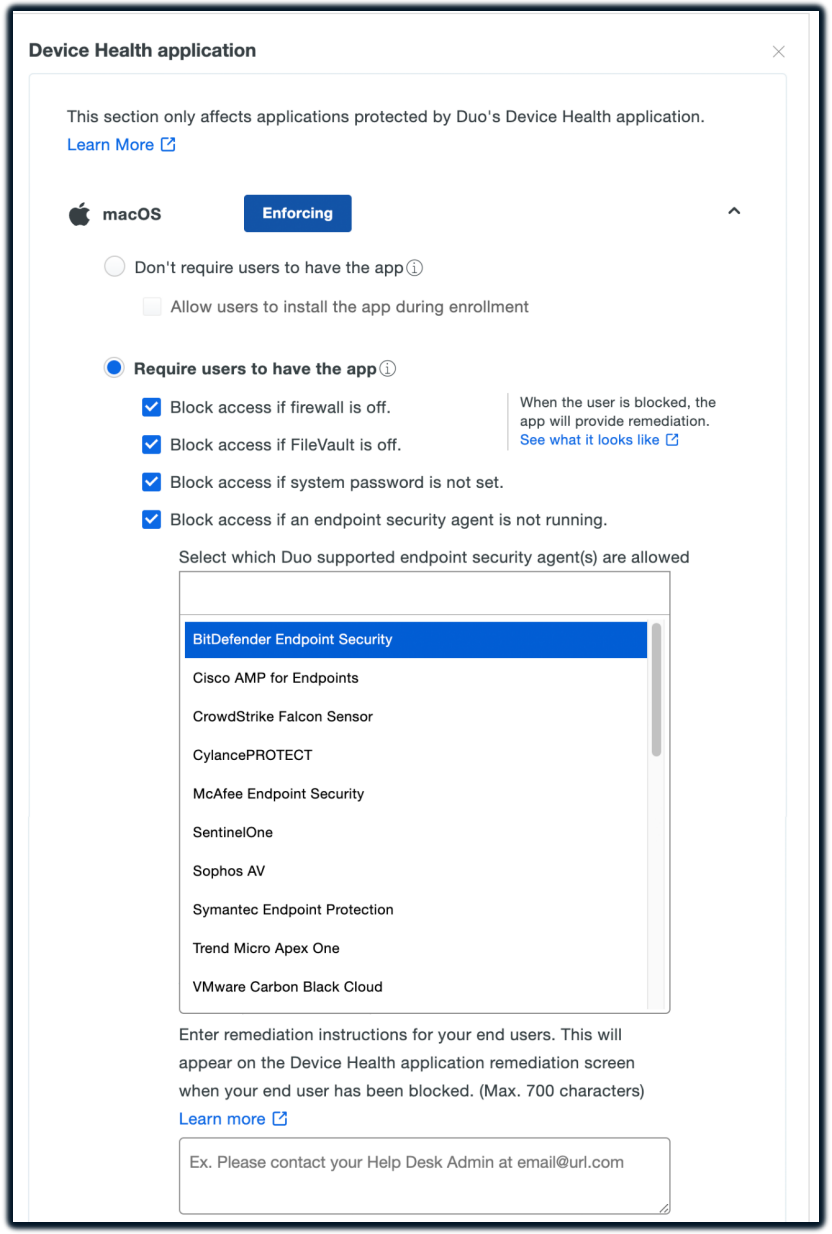
Example ZTNA Deployment (Access Gateway)

- Infrastructure
  - Sizing requirements
  - Highly available and scale
  - Geo-dispersed
  - Prod/Nprd environment
- Configurations
  - SSL certs
  - DNS (split-brain)
  - IdP integration (Prod/Nprd)
  - ACLs
  - Administration
    - Onboarding new resources
    - Renew SSL certs
    - Session termination
    - Automation
      - CIRT playbook
- Requirements
  - Enforce TLS 1.2 (or greater)
  - Session duration



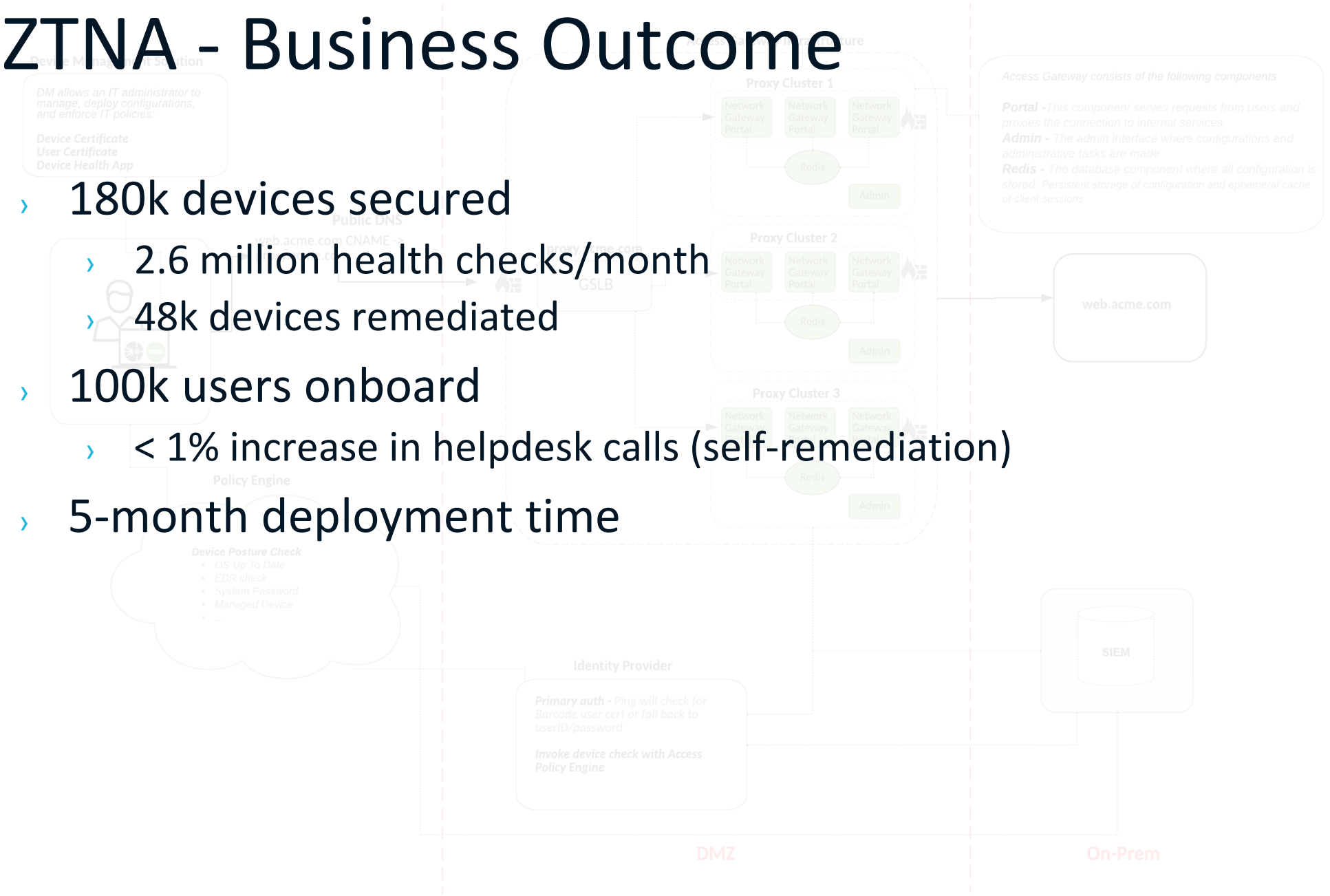
Example ZTNA Deployment (Policy Engine)

- Policy & Control
  - Device requirements (policies)
    - Via Access Gateway
  - Anonymous networks disabled
  - Regular employees

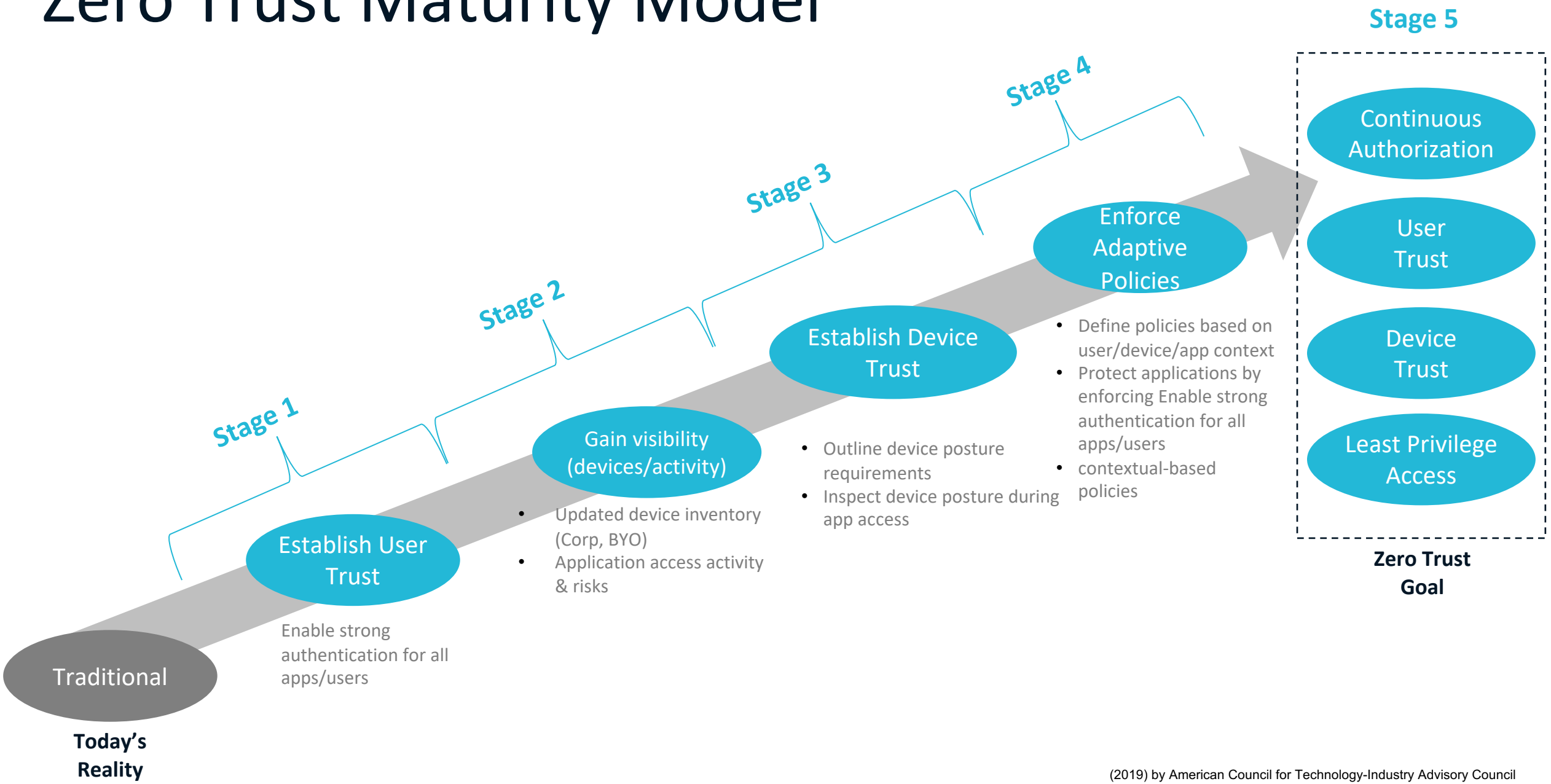


ZTNA - Business Outcome

- 180k devices secured
  - 2.6 million health checks/month
  - 48k devices remediated
- 100k users onboard
  - < 1% increase in helpdesk calls (self-remediation)
- 5-month deployment time



Zero Trust Maturity Model



Challenges/Opportunities

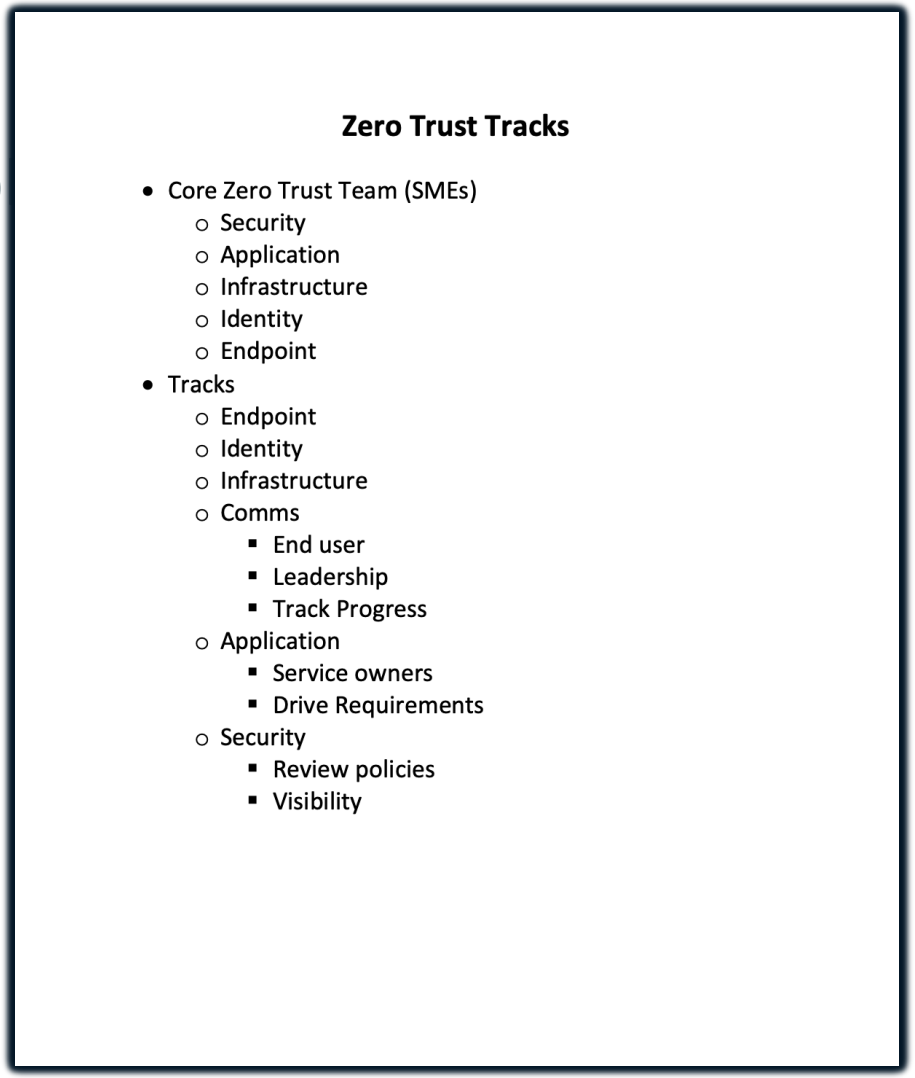
- Applications
  - Security Requirements
  - Application dependencies
- Endpoint
  - Asset inventory
  - ZTA surfaces issue
  - Seamless UX for diverse workforce
- Workforce
  - Adopting new method of access
  - Unclear steps to self-remediate
- Requires cross-functional alignment
  - Aligning priorities

Tips for getting started

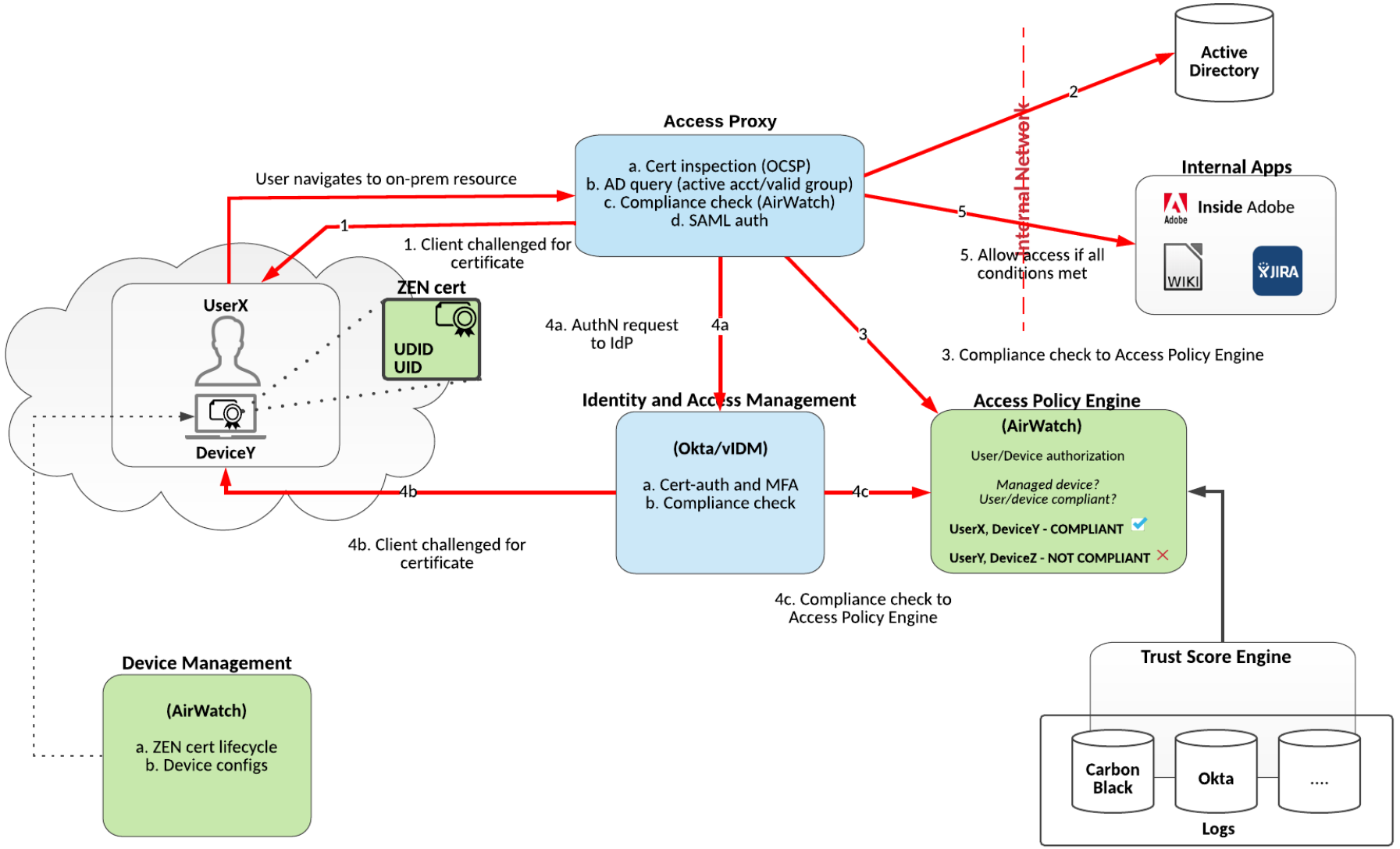
- Sell the vision, people, process, and technology
  - Leadership buy-in
    - ‘Air Cover’ enables team to move quickly
  - Share benefits to the workforce
- Start small, gain experience, expand
- Find a concrete use case
  - M&A
  - Vendor/Contractor
  - Top X apps
- Small cross-functional core team
- Evaluate existing investments
- Actively communicate

Tips for getting started

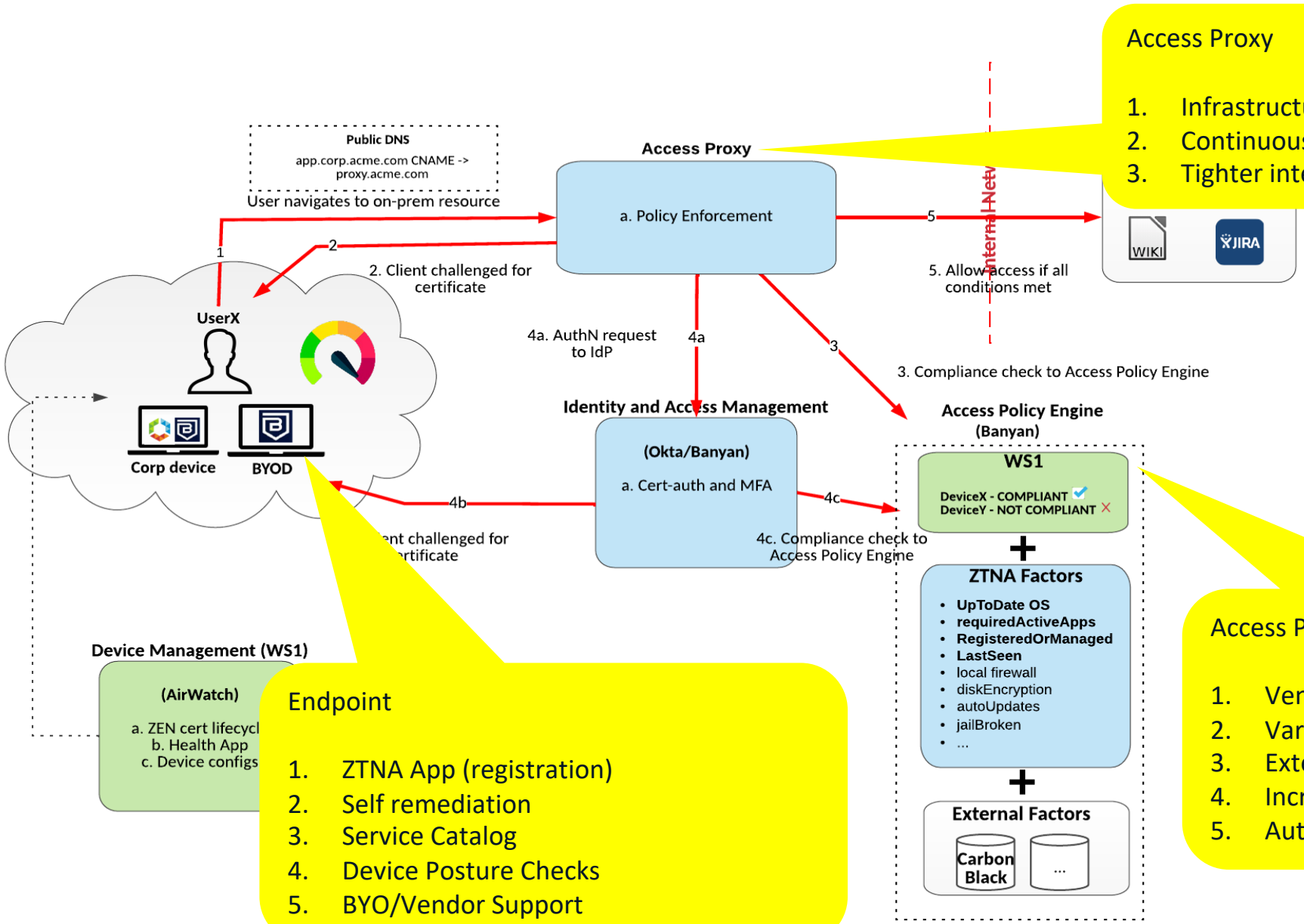
- Sell the vision, people, process, and techno
  - Leadership buy-in
    - ‘Air Cover’ enables team to move quickly
  - Share benefits to the workforce
- Start small, gain experience, expand
- Find a concrete use case
  - M&A
  - Vendor/Contractor
  - Top X apps
- Small cross-functional core team
- Evaluate existing investments
- Actively communicate



Example ZTNA Deployment (Initial phase)



Example ZTNA Deployment (Phase 2)



Access Proxy

1. Infrastructure support (SSH/RDP/K8s)
2. Continuous AuthZ
3. Tighter integration w/ Control Plan

Endpoint

1. ZTNA App (registration)
2. Self remediation
3. Service Catalog
4. Device Posture Checks
5. BYO/Vendor Support

Access Policy Engine

1. Vendor/BYO support
2. Variable trust
3. Extended policy options
4. Increase device posture capabilities
5. Automation

Thank you