Innovative Utilization of ICAM and PAM in DDIL Environments

Bryan Rosensteel
US Federal CTO
Ping Identity

BeyondTrust

Ping Identity

ICAM
&
Zero Trust

BeyondTrust

Ping Identity

What is ICAM?

(Identity, Credential & Access Management)

BeyondTrust

Ping Identity

What is PAM?

BeyondTrust

Ping Identity

What is Zero Trust?

BeyondTrust

Ping Identity

"ICAM is the set of tools, policies, and systems that an agency uses to enable the right individual to access the right resource, at the right time, for the right reason in support of federal business objectives."

IDManagement.gov, Federal ICAM Architecture Introduction

BeyondTrust

Ping Identity

"Privileged access management (PAM) consists of the cybersecurity strategies and technologies for exerting control over the elevated ("privileged") access and permissions for users, accounts, processes, and systems across an IT environment."

IDManagement.gov, Federal ICAM Architecture Introduction

BeyondTrust

Ping Identity

"Zero trust 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."

CISA.gov, Zero Trust Maturity Model

BeyondTrust

Ping Identity

How important are ICAM and MFA to the successful implementation of Zero Trust?

BeyondTrust

Ping Identity

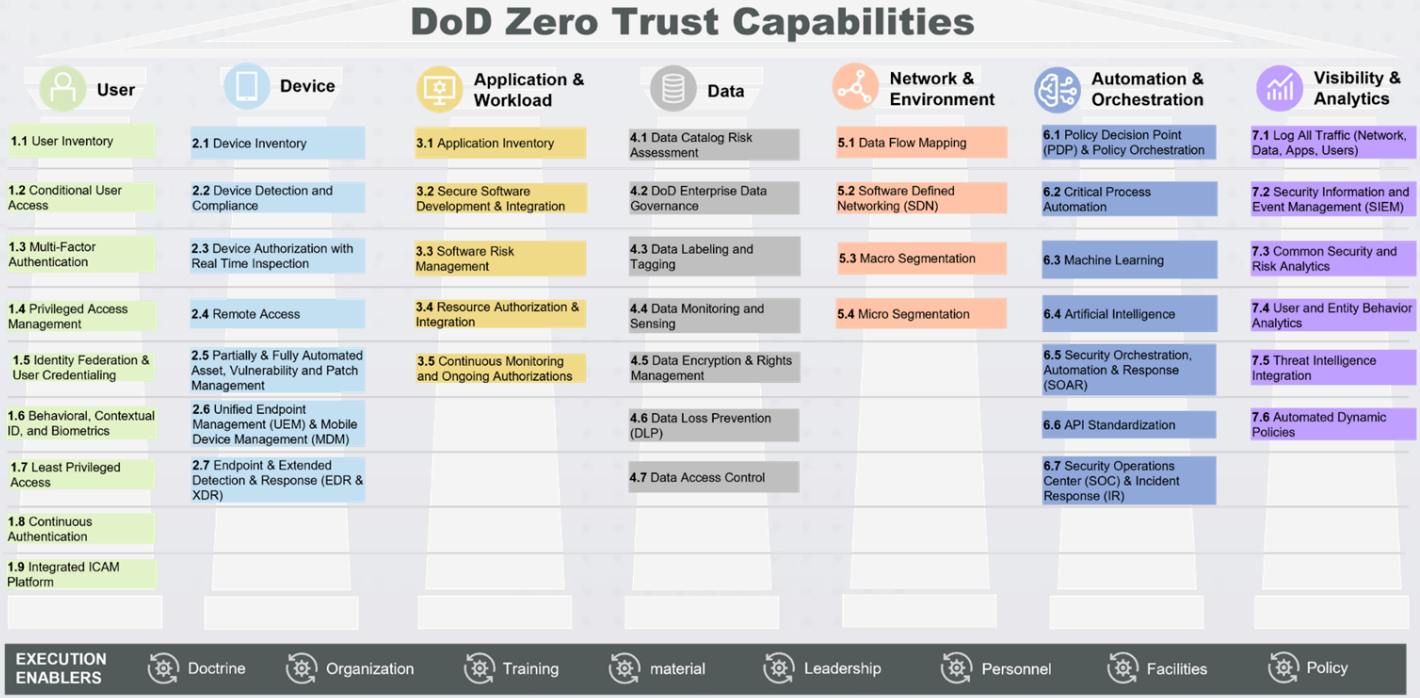


Figure 5, DOD Zero Trust Strategy, DOD Zero Trust Strategy

BeyondTrust

Ping Identity

Three fundamentals of zero trust:

1. **Who** has access to **what**?
2. **Should** they have **that** access?
3. **What** are they doing with that access?

BeyondTrust

Ping Identity

Evolution of Zero Trust in Government

The Catalyst

NIST SP 800-207 (Zero Trust Architecture) published in response to the Office of Personnel Management breach.

BeyondTrust

Ping Identity

Evolution of Zero Trust in Government

From Guidance to Policy

Biden Administration EO 14028 directs OMB (Office of Management and Budget) to create policy implementing NIST SP 800-207

BeyondTrust

Ping Identity

Evolution of Zero Trust in Government

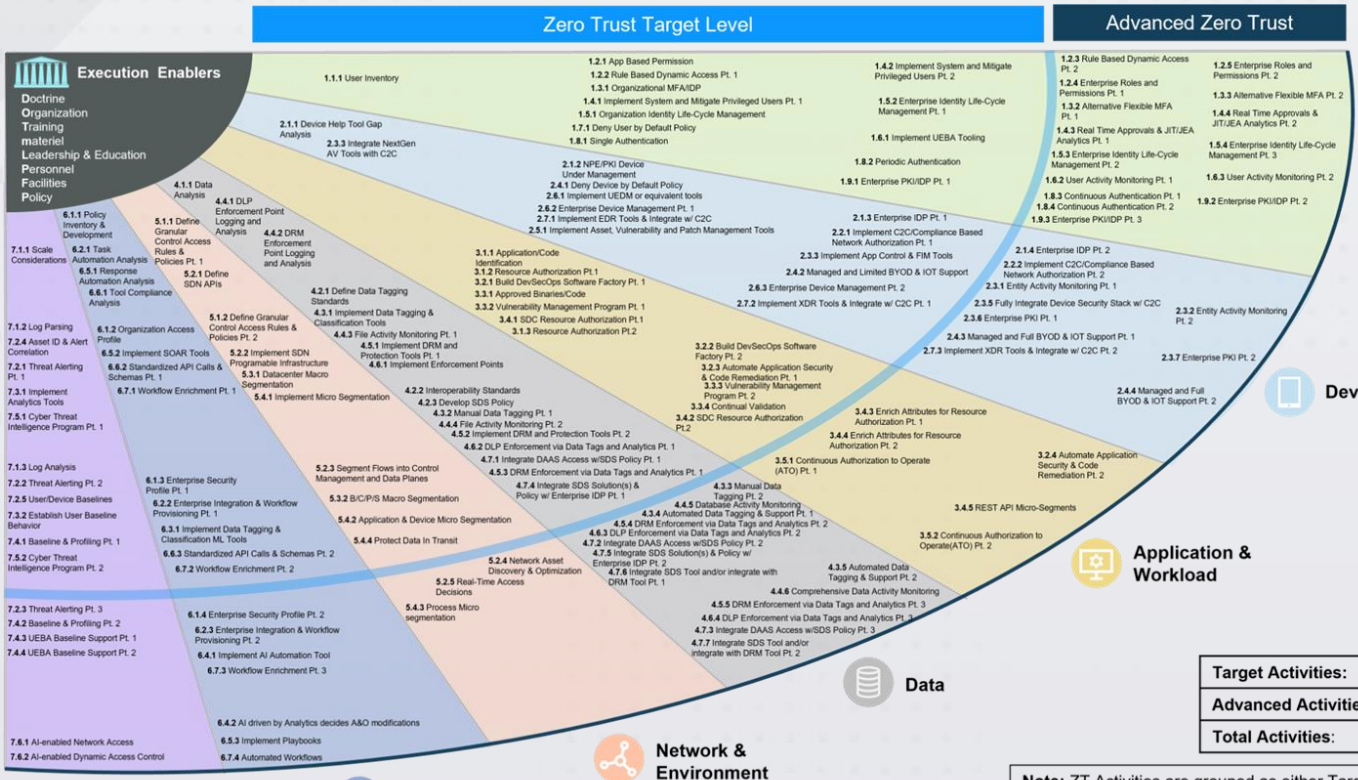
Action Taken

Following the release of EO 14028, the DOD Zero Trust Strategy is released with 91 target and 61 advanced controls to implement Zero Trust.

BeyondTrust

Ping Identity

TechNet indo-pacific
ACCELERATE INDO-PACIFIC INNOVATION
November 7–9, 2023 • Honolulu, HI



Target Activities:	91
Advanced Activities:	61
Total Activities:	152

Note: ZT Activities are grouped as either Target or Advanced.

Version 1.0 As of 10/04/2022

BeyondTrust

Ping Identity

DDIL & TICAM Environments

BeyondTrust

Ping Identity

DDIL
Denied, Distributed, Intermittent and Limited Impact

TICAM
Tactical Identity, Credential & Access Management

BeyondTrust

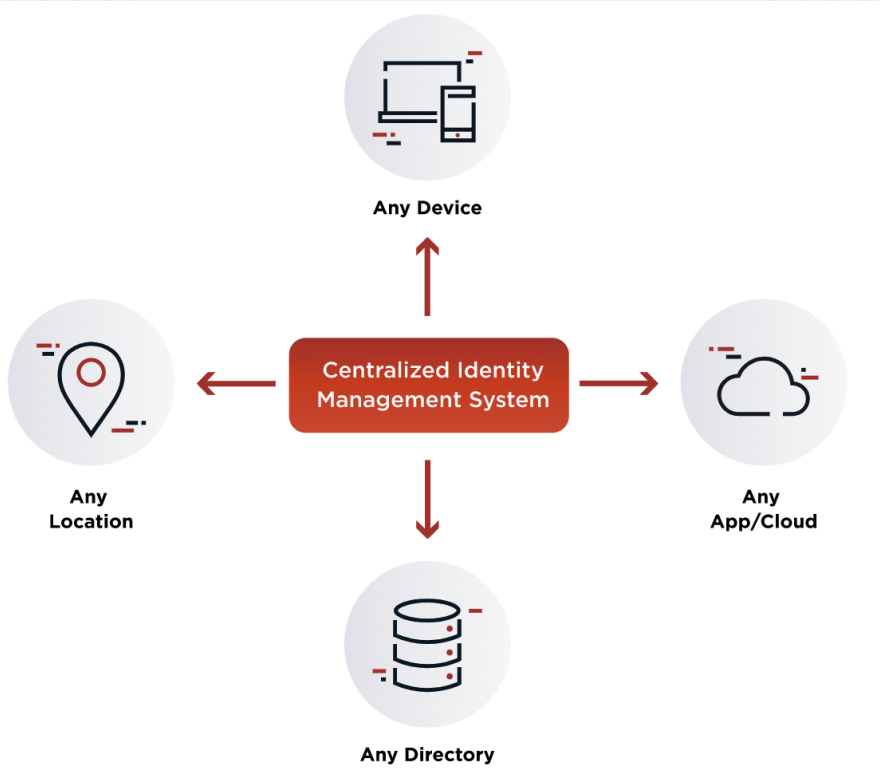
Ping Identity

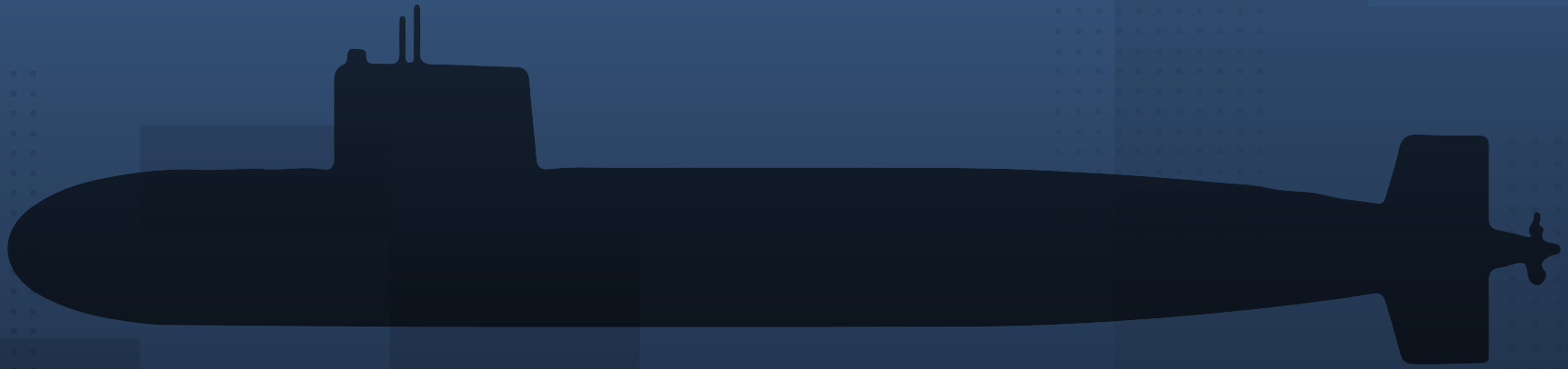
What are some considerations for implementing Zero Trust framework in a DDIL Environment?

BeyondTrust

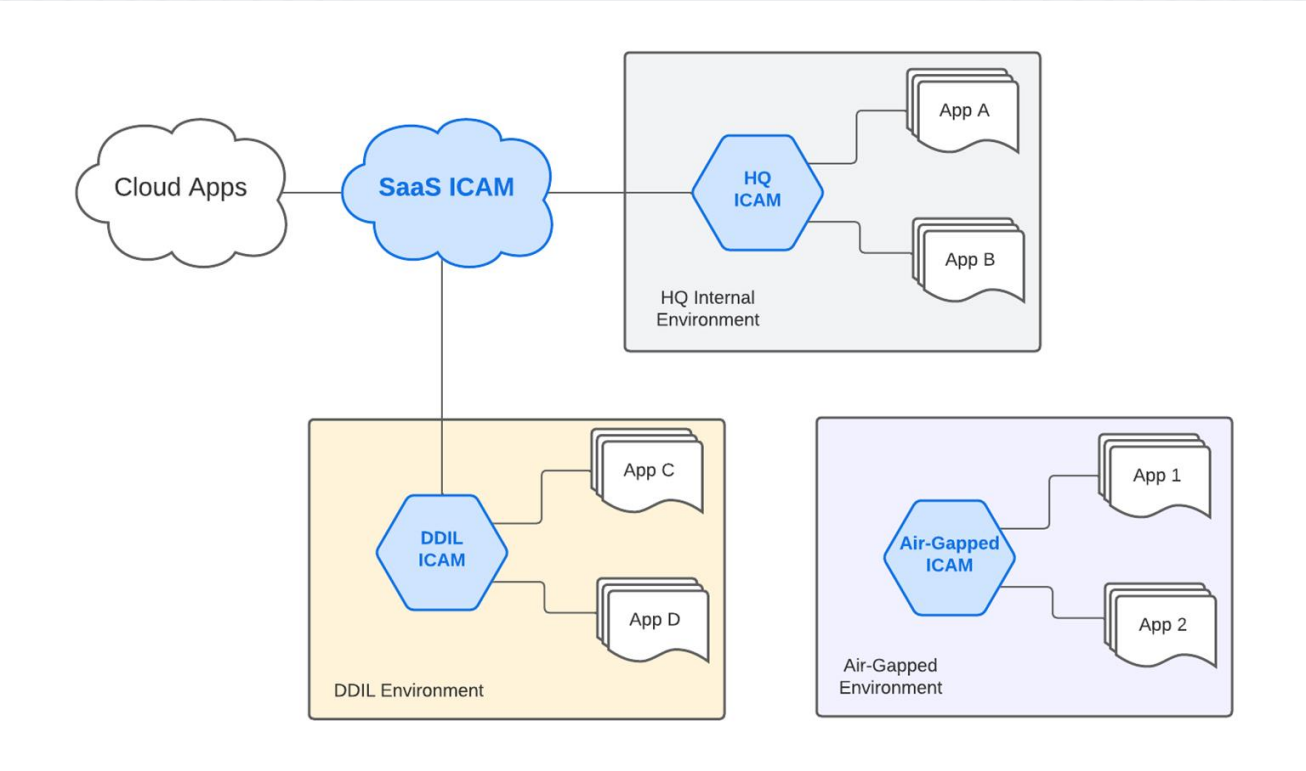
Ping Identity

Idealized Identity Policy





Likely Identity Policy



What are some of the primary requirements to implementing a Zero Trust framework and how do we go about achieving these capabilities?

BeyondTrust

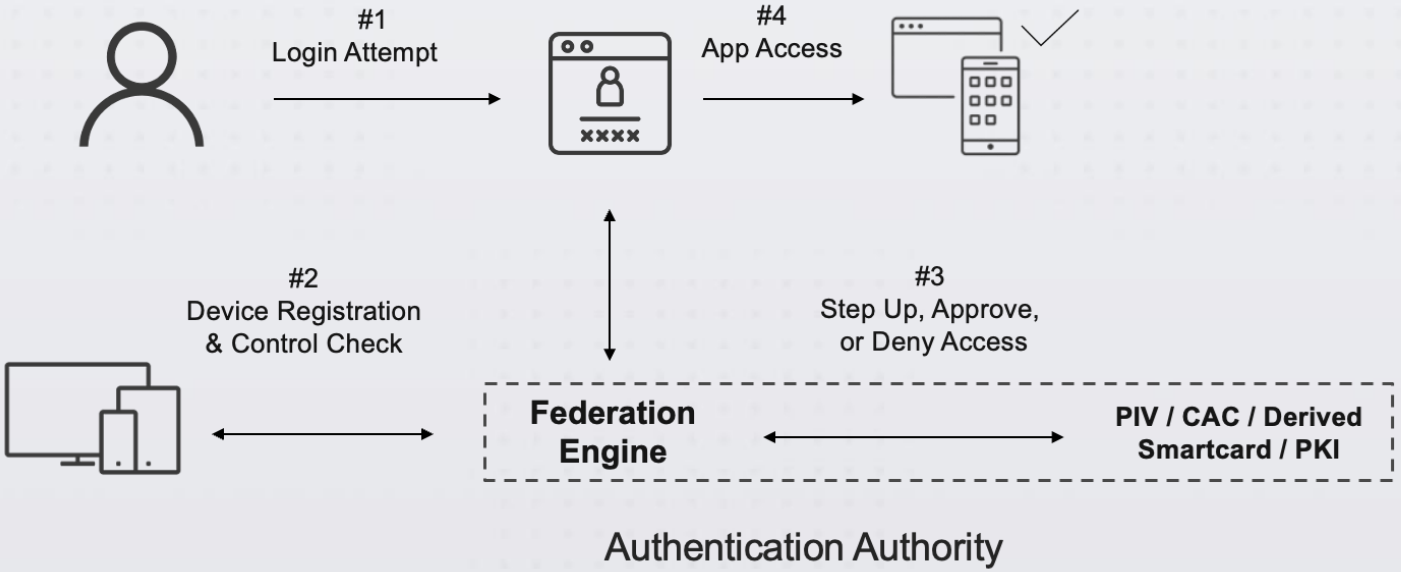
Ping Identity

Authentication vs. Authorization

BeyondTrust

Ping Identity

Adaptive Authentication



BUT…

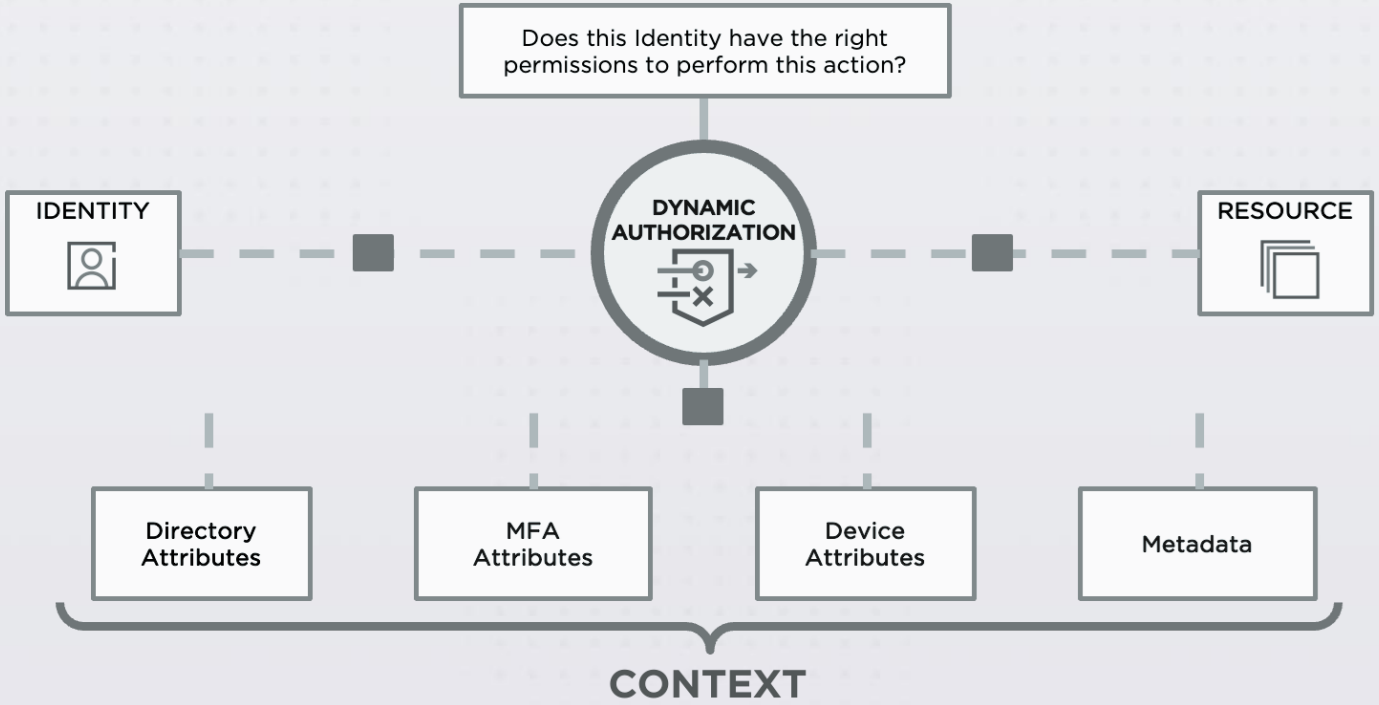
MFA isn’t enough to secure resources against today’s threat landscape. You need authorization to do so.

Authentication is merely the enabler of authorization.

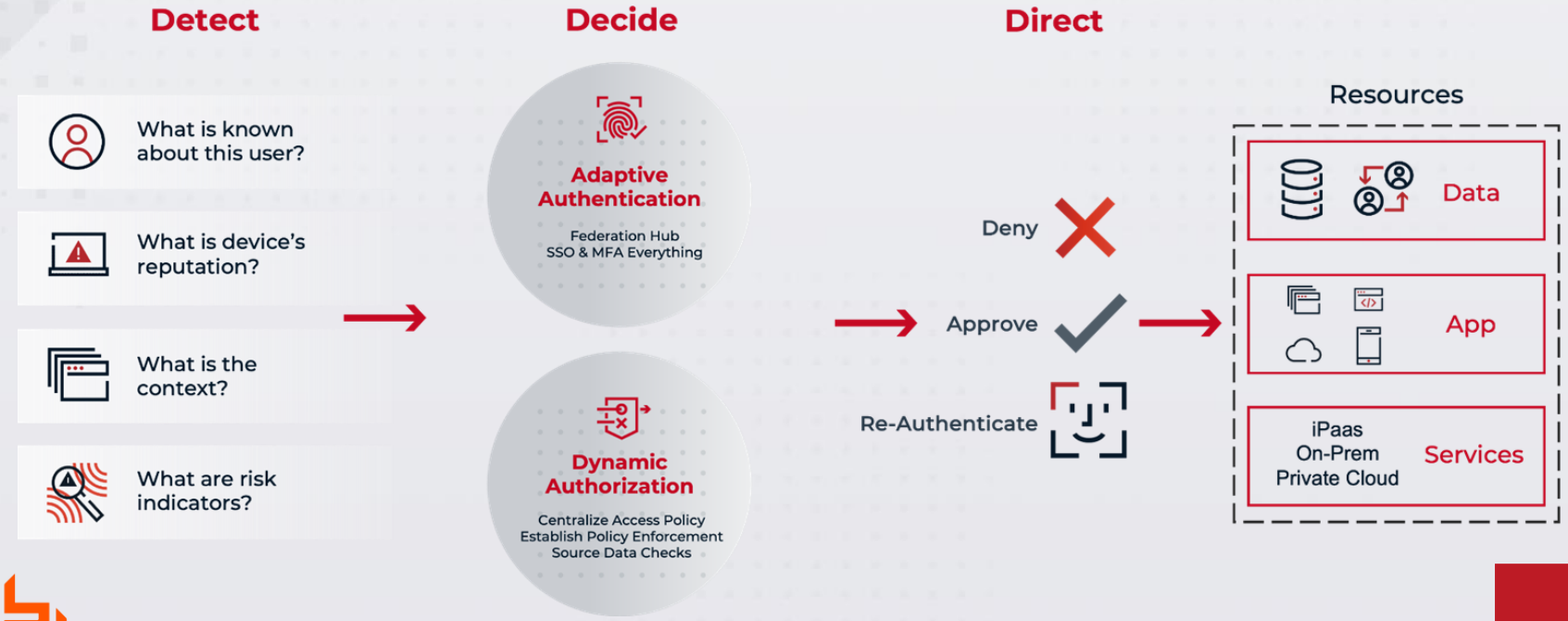
BeyondTrust

Ping Identity

Dynamic Authorization



Determining Trust: Zero Trust Orchestration



BeyondTrust

Ping Identity

Common PAM Use Cases

Discover All Accounts

- Discover all accounts across the estate
- Leverage automation to bring under management

Store & Manage Privileged and Non-Privileged Credentials

- Store credentials in secure vault and manage them per established policies / best practices
- Broker access to credentials and DevOps secrets for human users, services and applications
- Securely store secrets (certificates, tokens, API keys), and admin credentials for cloud consoles
- Securely store and manage employee business application passwords with audit support
- Manage all accounts centrally, even if asset is disconnected from corporate network

Manage & Monitor Access to Resources

- Assign temporary access privileges based on pre-determined attributes such as day, time, location
- Establish sessions without revealing passwords
- Document session activity

BeyondTrust

Ping Identity

Device Signaling

BeyondTrust

Ping Identity

What are “other” persons and “things” with privileged roles that are not so obvious? How can we control when and where they have access?

BeyondTrust

Ping Identity

RBAC vs. ABAC

BeyondTrust

Ping Identity

Role-Based Access Control (RBAC) is No Longer Enough

- RBAC employs static, simple logic
- Relies on applications to make access decisions
- Doesn’t take real-time context into consideration

BeyondTrust

Ping Identity

Get Granular with Attribute-Based Access Control (ABAC)

- Look at as many attributes as possible
- Use attributes to determine risk of each access attempt
- Adjust access permissions as needed

BeyondTrust

Ping Identity

Levels of Authorization

3 **Fine Grained**

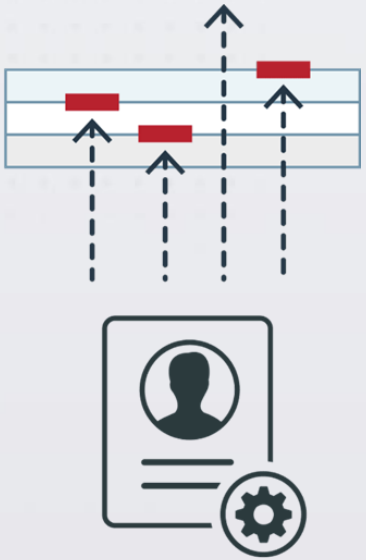
- Condition & Contextual

2 **Medium Grained**

- URL-Based

1 **Course Grained**

- Application Based



BeyondTrust

Ping Identity

Thank You

pingidentity.com | fedgov@pingidentity.com
beyondtrust.com | federalsales@beyondtrust.com