BeyondTrust



# Aligning ICAM, the Executive Order & Zero Trust for the Defense Department

# Josh Brodbent
# RVP, Solutions Engineering
# BeyondTrust

Josh has more than 20 years in IT experience and has architected identity and privilege access management solutions for over 3 million user accounts.

He joined BeyondTrust in 2018 as a Senior Solutions Engineer and was quickly selected to lead the team. Prior to BeyondTrust, he was a senior Solutions architect for Quest Software.

He began his career by founding a managed service provider (MSP) at 12. He held multiple industry certifications by 14, making him the youngest in the nation to do so. That MSP went on to become successful, and ultimately his launching point into Public Sector architecture and support.

BeyondTrust

**1,250+** Employees

**18** Countries

**2003** Founded

**Market Leader**

Ranked as a PAM leader by Gartner, Forrester, and KuppingerCole

**Global Presence**

~20k customers in 100+ countries and extensive partner network

**Integrated Platform**

Unified platform with seamless third-party integrations

**Broadest Portfolio**

Best-in-class identity and privileged access solutions

**Customer Driven**

90%+ gross retention and exceptional customer support and success

**Technology Pioneers**

Heritage of innovation with 75+ patents and commitment to R&D

# Company Overview

| | |
|---|---|
| **Headquarters** | **Atlanta, GA \| USA** |
| **Global Offices** | **Americas, EMEIA, APJ** |
| **Privately Held** | **Francisco Partners & Clearlake Capital** |

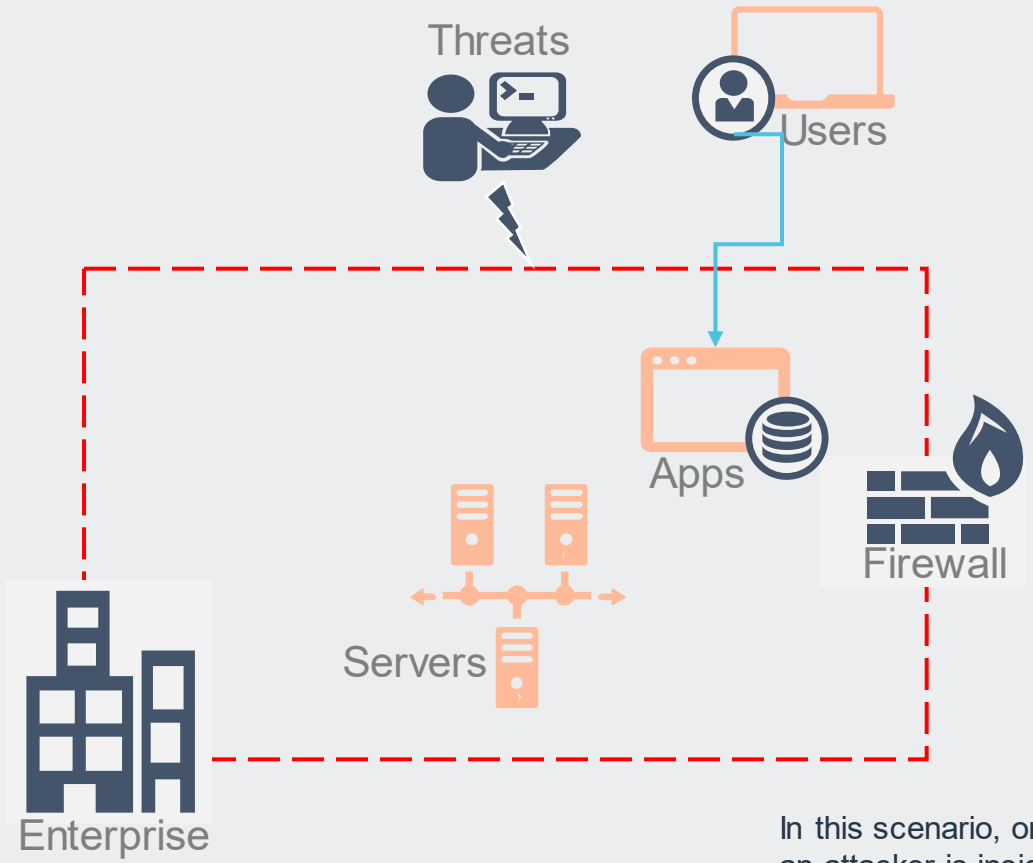
# Zero Trust Guidance

- **National Security Memorandum (NSM-8)**
  - DoD agencies must develop a plan to implement Zero Trust Architecture, which shall incorporate, as appropriate: NIST Special Publication 800-207 Guidance (Zero Trust Architecture

- **NIST 800-207/NIST Zero Trust Planning Guide for Federal Administrators**
  - Zero trust could be summarized as a set of principles used to plan and implement an IT architecture. NIST recommends agencies focus their ZT strategy on 3 areas: network identity, endpoint health, and data flows.

# Traditional Security vs. Zero Trust Security

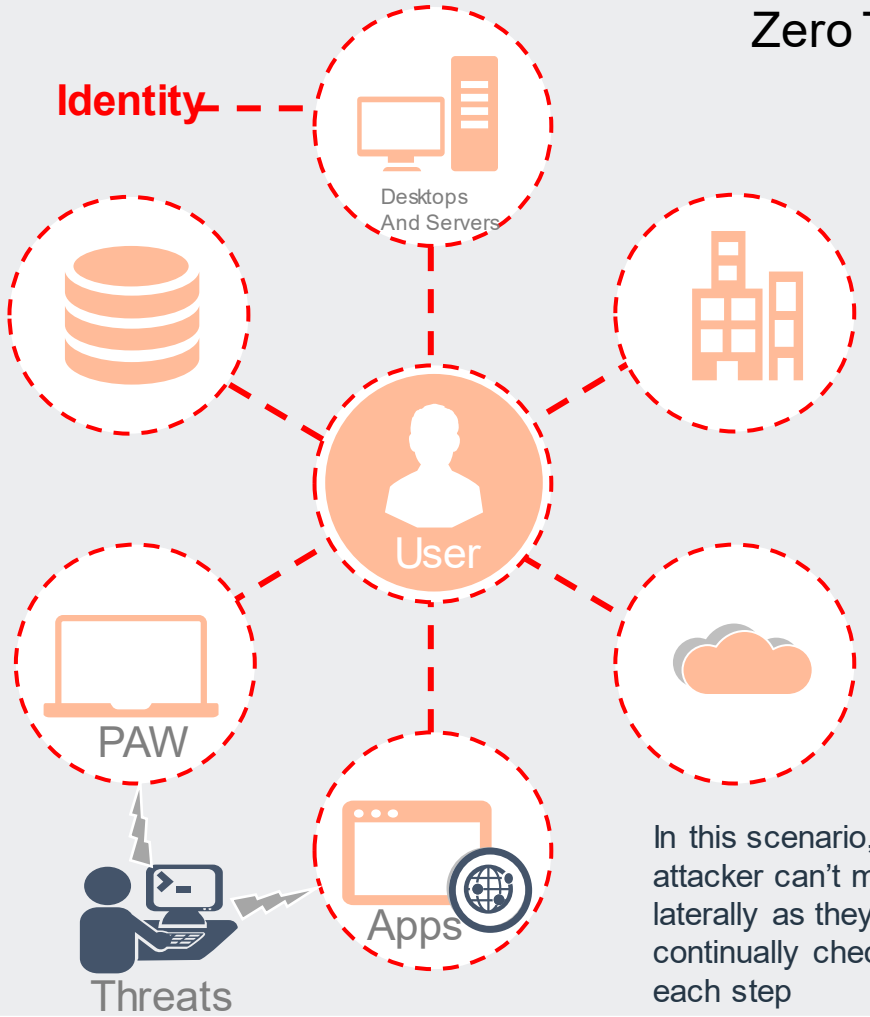
## Perimeter Based Security
Physical and Digital Barriers




In this scenario, once an attacker is inside, they can move laterally

## Identity Defined Security
Continuous Verification

Zero Trust




In this scenario, an attacker can't move laterally as they are continually checked at each step

# Why Zero Trust, Why Now?

## The Shift to Zero Trust

### TRADITIONAL
"Moat & Castle"

**Automatically Trust Users Because They Have Presented A Set Of Acceptable Credentials**

- Attackers only had to find a way inside the network (stealing user credentials, unprotected remote access, or certificate/key compromise, etc.)
- Once inside - largely free to roam networks and compromise more assets
- Attackers could persist undetected for years, while siphoning IP, valuable data, and compromising critical assets

### ZERO TRUST
"Perimeter-less"

**Continuously Authenticate And Verify Users, Devices, And Applications**

- Assume breach
- Always verify, never trust
- Attackers have a much harder time establishing a foothold in the IT environment; also protects against lateral movement & privilege escalation
- Concepts such as least privilege, continuous authentication, and micro-segmentation reflect the new realities of an evolving IT environment.

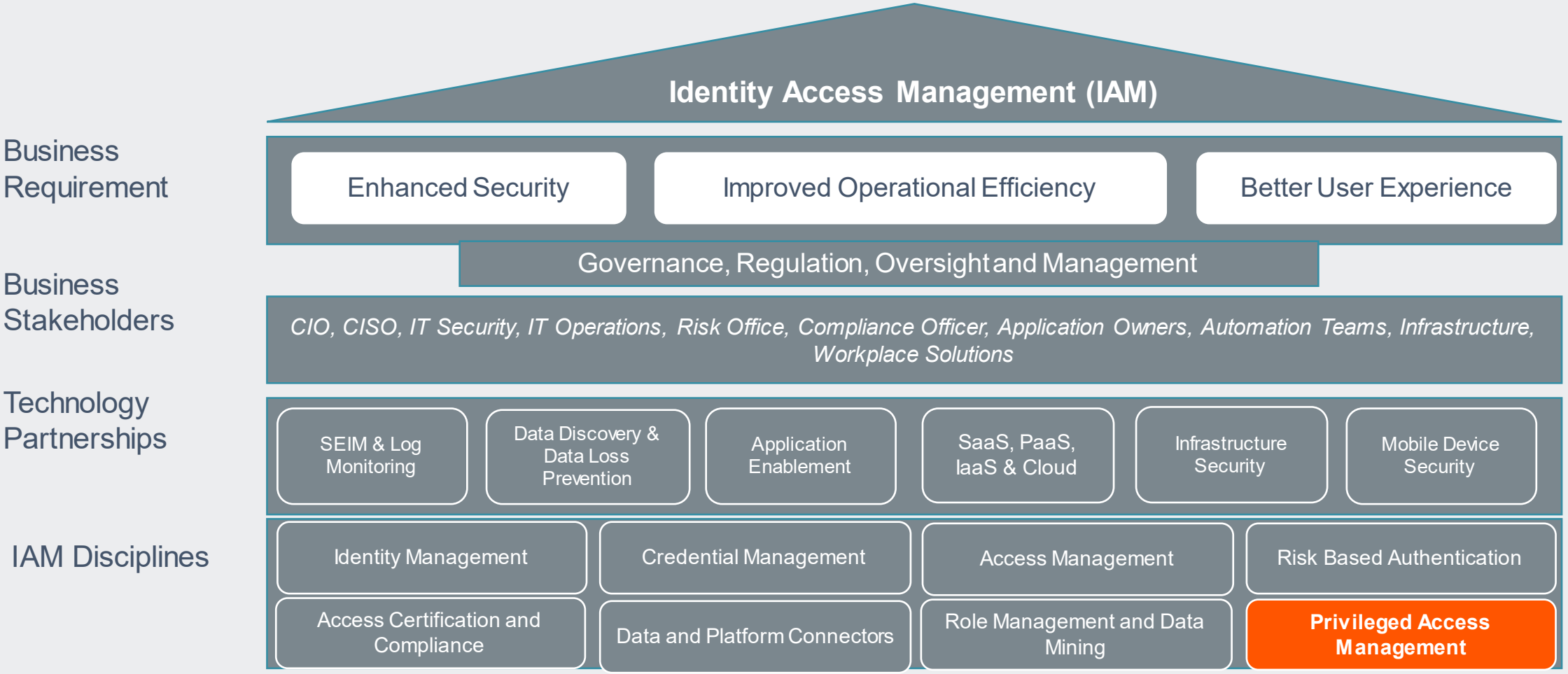
# The Role of PAM

Applying the granularity of Privileged Access Management (PAM) to achieve Zero Trust objectives ensures all access is appropriate, managed, and documented, regardless of how the perimeter has been redefined

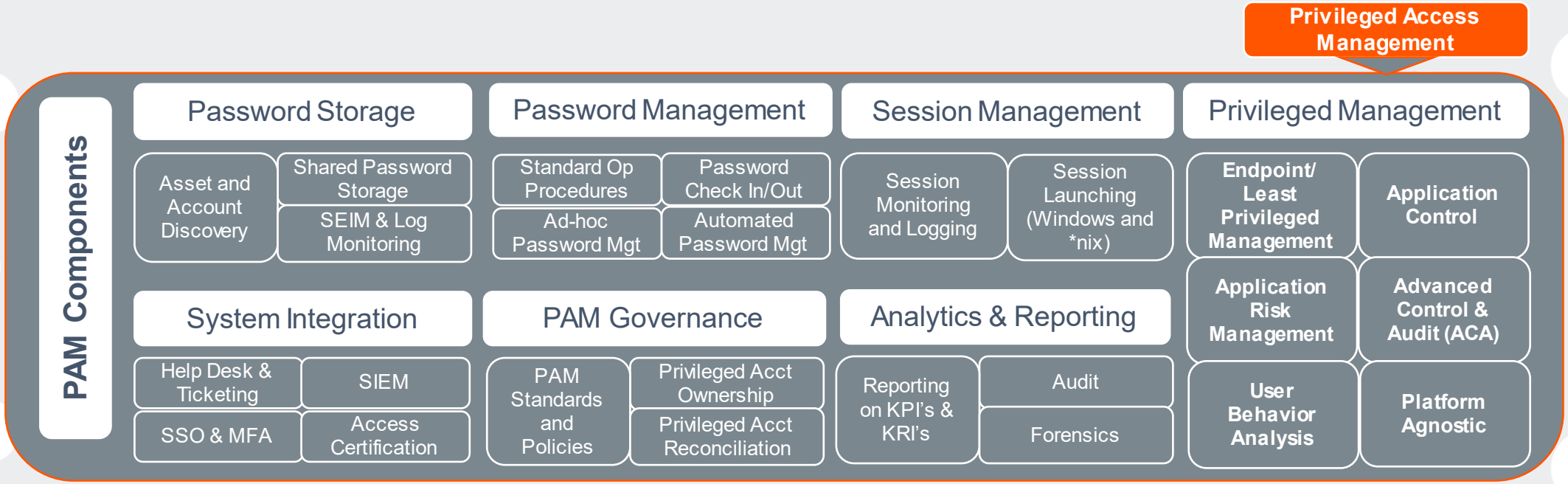
# 8 Ways PAM Enables Zero Trust

1. **Discovers, inventories, and smartly groups** all privileged assets to eliminate blind spots, illuminate shadow IT, and control access points
2. **Continuously enforces** adaptive and just-in-time access controls based on context
3. **Manages and enforces** credential security best practices for all privileged passwords, secrets, and keys for accounts
4. **Applies least privilege controls** for every identity and account - human, application, machine, employee, vendor, etc.
5. **Implements** segmentation and microsegmentation to isolate various assets, resources, and users to restrict lateral movement
6. **Secures remote access** with granular least privilege and adaptive capabilities well beyond that of VPNs, RDP, and other common remote access technologies
7. **Secures access to control planes** (cloud, virtual, DevOps) and sensitive applications
8. **Continuously monitors, manages, & audits** every privileged session that touches the enterprise

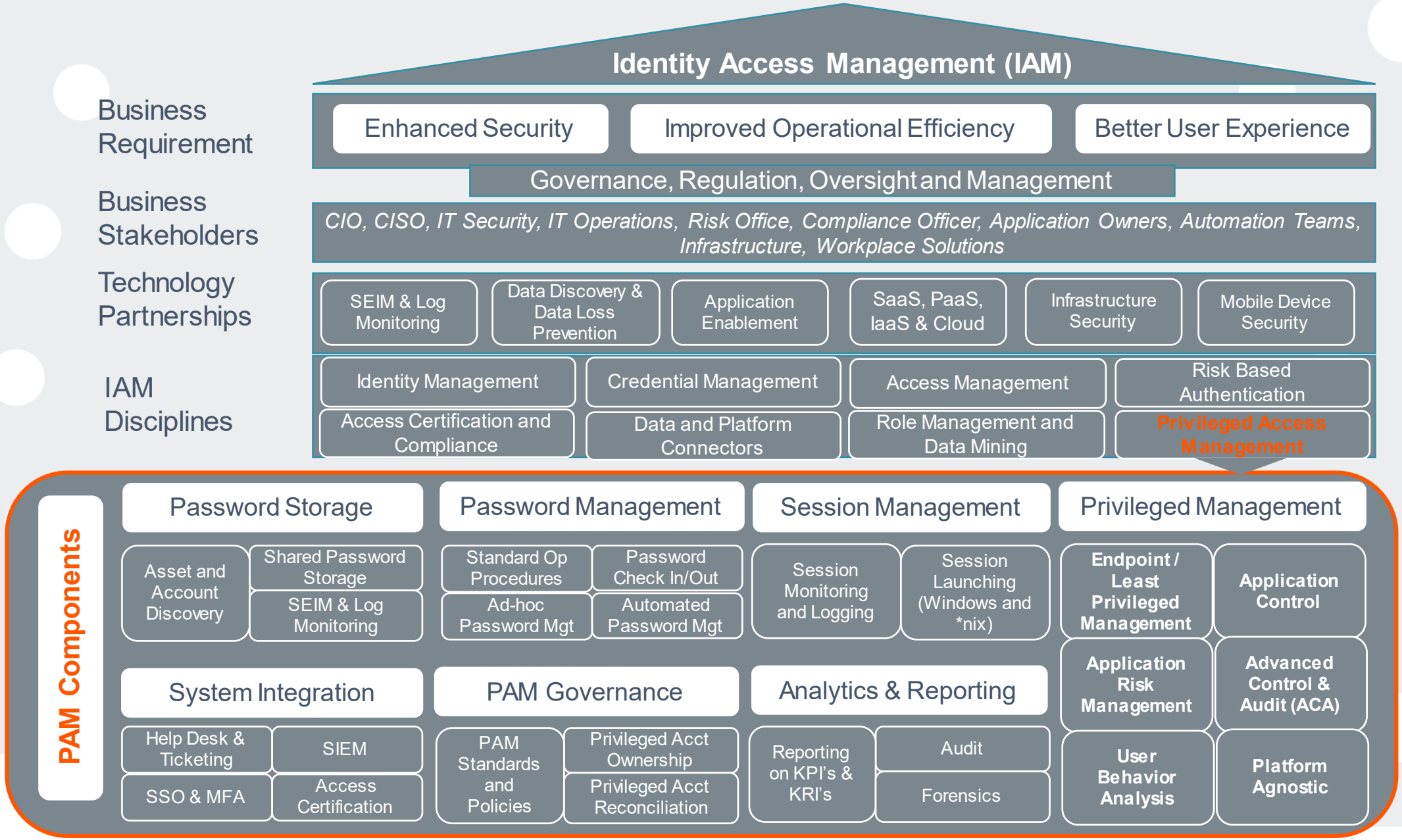
# The Universe of Identity Governance



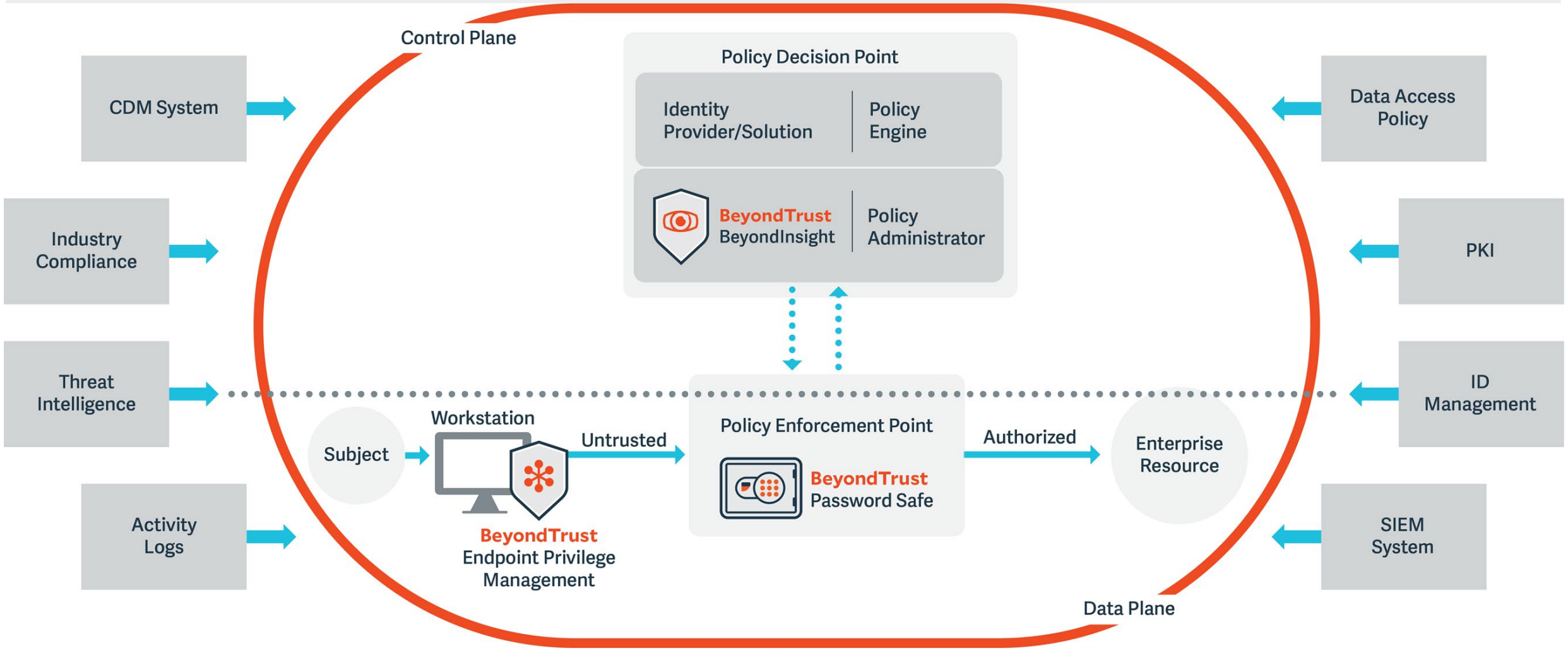
# Defining Privilege Access Management

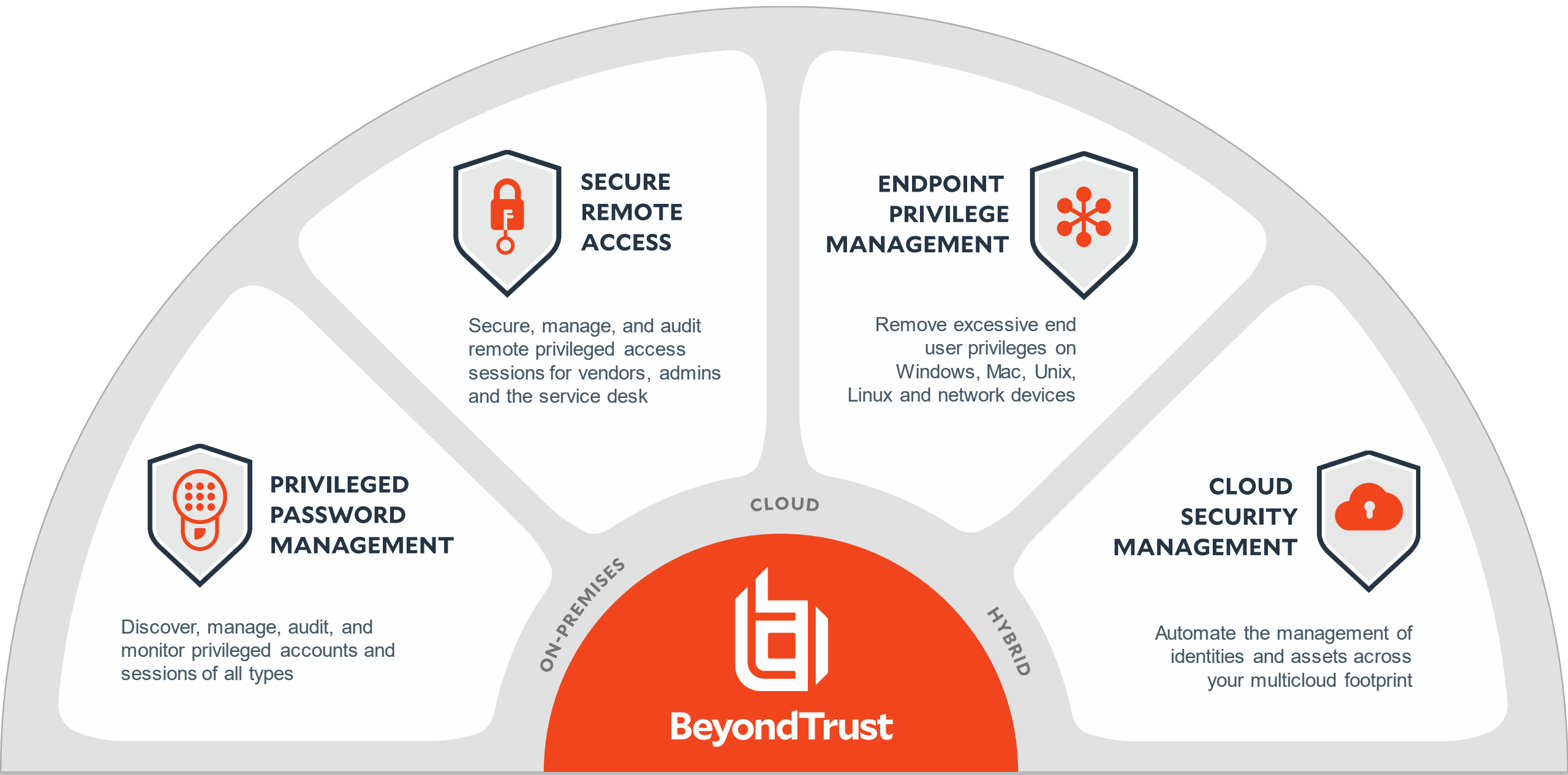


# Complete Identity Governance Model



# NIST SP 800-207 ZTA diagram, overlayed with BeyondTrust solutions






BEYONDINSIGHT Discovery | Reporting | Threat Analytics | Connectors | Central Policy & Management

# Thank You & Next Steps

**Stop by BeyondTrust booth #414 to understand how PAM will improve your cyber defenses.**

**Related Content:**

- Mapping BeyondTrust Capabilities to NIST Zero Trust (SP 800-207)
- Privileged Access Management is Essential to Zero Trust: A Candid Discussion with Government Cybersecurity Experts
- Zero Trust Identity Security for Public Sector Agencies

BeyondTrust