BeyondTrust

Identity Empowering Air Force Cybersecurity Priorities



An introductory overview of utilizing Privileged Access Management to secure sensitive data and operations within the military's distributed and interconnected environments.

Josh Brodbent
RVP, Solutions Engineering
BeyondTrust

Josh has more than 25 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.

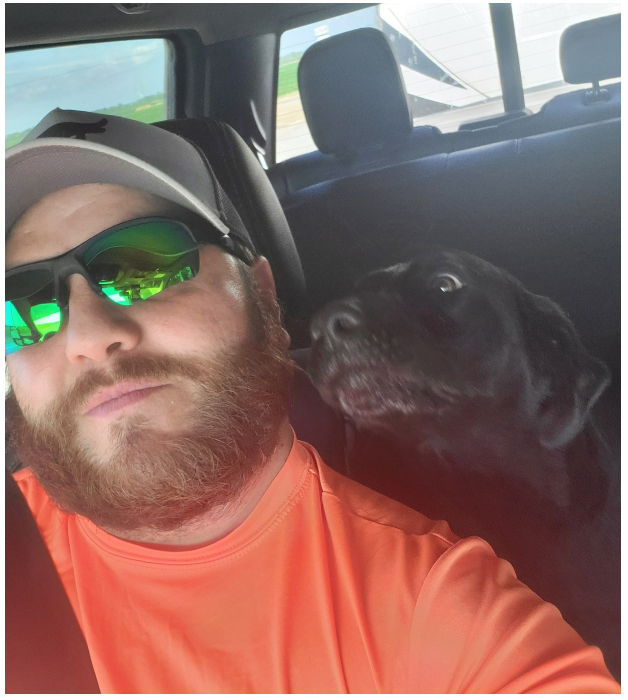






JACKSON
HOLE, WY





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

1 Get Your Definitions Right and Educate the Organization



Zero Trust Definitions

1. Zero Trust is a collection of concepts centered around validating and authenticating everything

2. Zero Trust Architecture (ZTA) is a cybersecurity plan applying zero trust principles and encompasses component relationships, workflow planning, and access policies

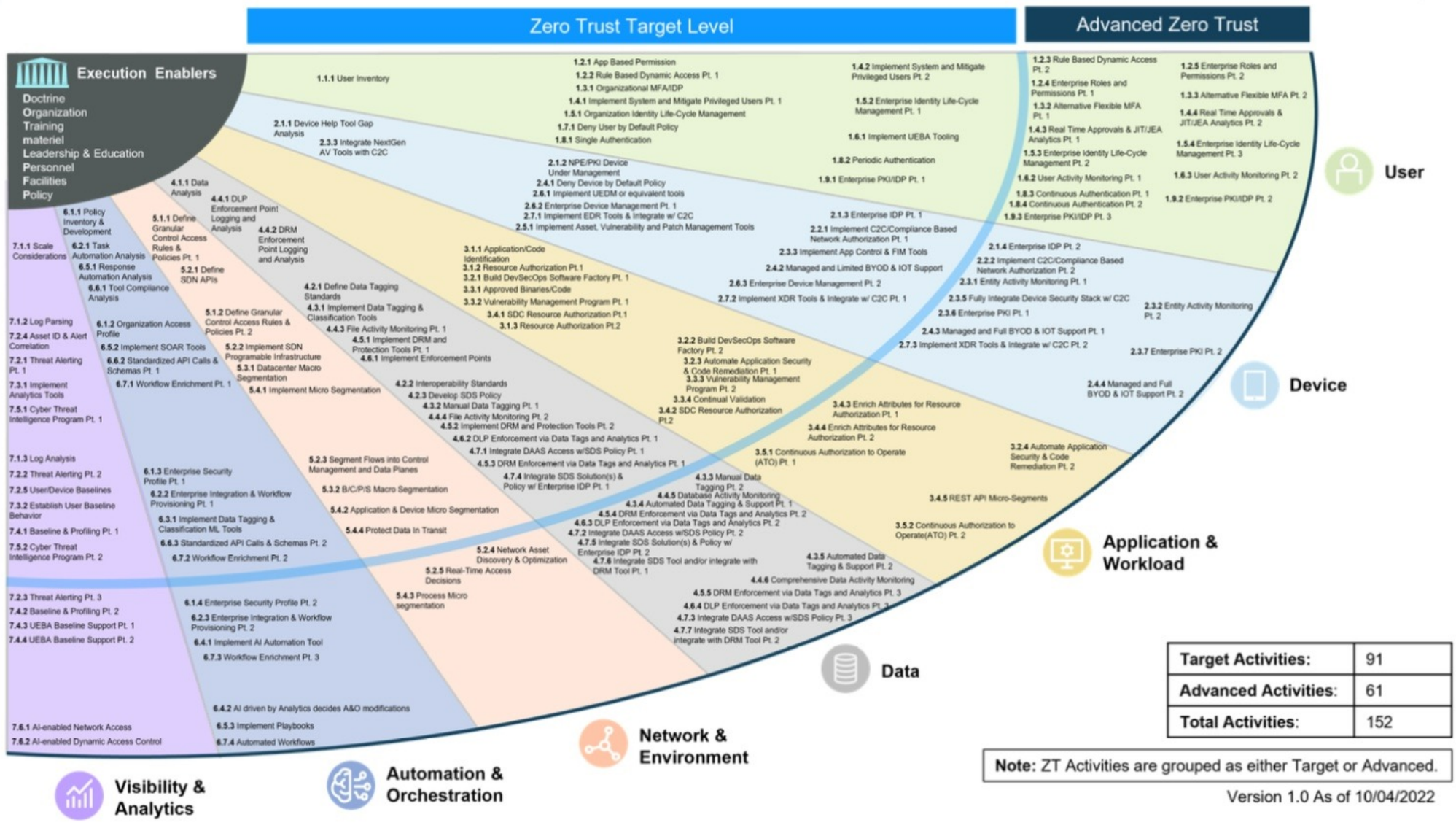


MAIN GOAL

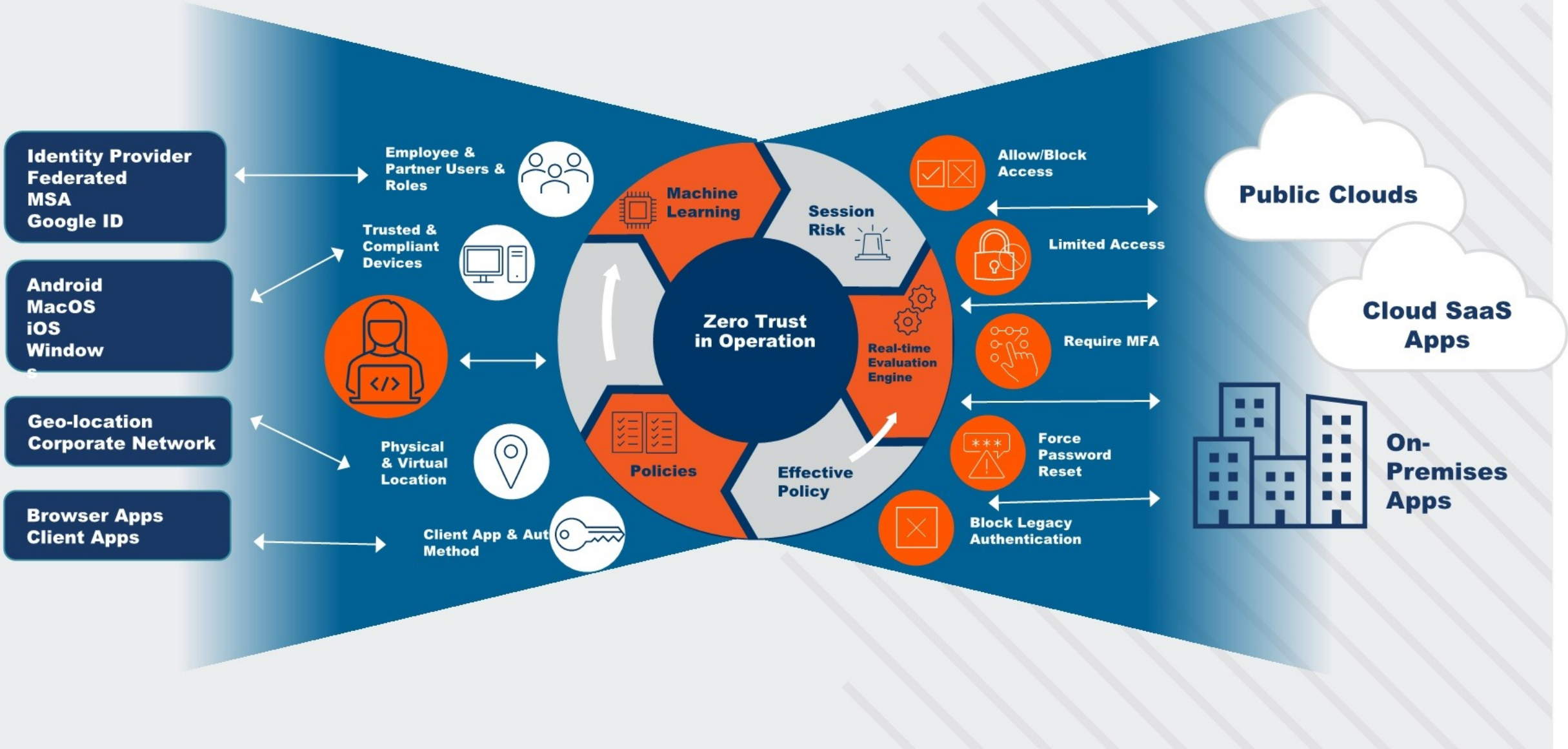
"Prevent unauthorized access to data and services, coupled with making the access control enforcement as granular as possible"

Source: NIST SP 800-207, Zero Trust Architecture, August 2020

US Dept of Defense 152 Controls Defined

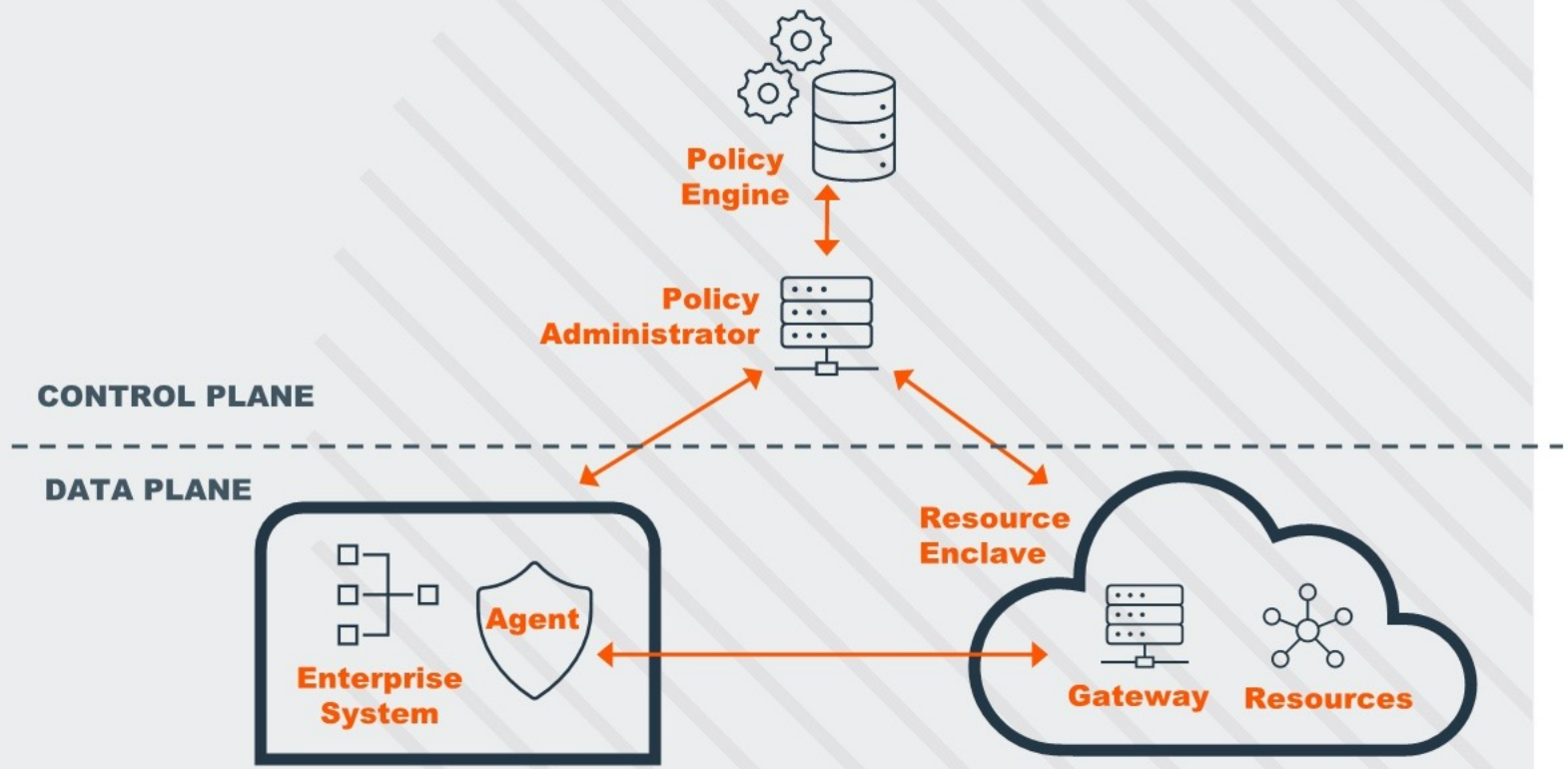


https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf


Identity Provider
Federated
MSA
Google ID
Android
MacOS
iOS
Window
s
Geo-location
Corporate Network
Browser Apps
Client Apps
Employee &
Partner Users &
Roles
Trusted &
Compliant
Devices
Physical
& Virtual
Location
Client App & Aut
Method
Machine
Learning
Session
Risk
Zero Trust
in Operation
Real-time
Evaluation
Engine
Policies
Effective
Policy
Allow/Block
Access
Limited Access
Require MFA
Force
Password
Reset
Block Legacy
Authentication
Public Clouds
Cloud SaaS
Apps
On-
Premises
Apps

Zero Trust Theoretical

- Control Plane
- Data Plane
- Subject
- Policy Engine
- Policy Administrator
- Policy Enforcement Point
- Access Policy
- Gateway
- Resource Enclave
- Enterprise System
- Agents

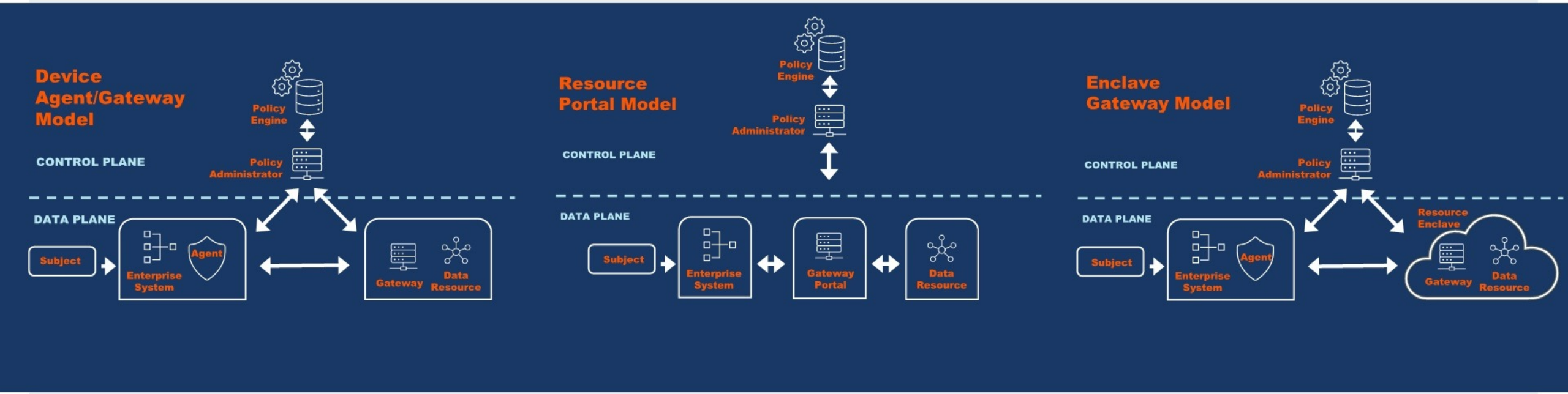


2 Beware of Buzzword Bingo During Your Design

Relevant…
Don’t solve a problem that does not need fixing

B	I	N	G	O
Zero Trust	Cloud Washing	Future Proof	Infinitely Scalable	Unhackable
Imposter Syndrome	CI/CD Pipeline Protection	API Protection	Data Security	Serverless
Attack Monitoring	Continuous Monitoring		Codeless Integration	Vendor Agnostic
Data Privacy	Regulatory Compliant	Five Nine’s	Digital Transformation	Just in Time
Shadow IT	Cloud Agnostic	Identity Based Segmentation	XaaS	Artificial Intelligence

Zero Trust Architectures



Unique PAM Integration in DDIL

- **Manage Privileged Accounts**

  Implement least privilege model. Enforce multi-factor authentication for privileged accounts.

- **Secure Remote Access**

  Control and monitor privileged remote access sessions. Enforce privileged access policies.

- **Monitor Privileged Activities**

  Log and audit all privileged user activities. Detect anomalous behavior.

“Security and usability are not a tradeoff - they can and should coexist harmoniously. With thoughtful design, you can have both.”

DDIL Landscape Overview



Distributed systems

Analyze the security challenges posed by distributed and decentralized systems across multiple locations



Remote access

Evaluate the risks of providing remote access to systems and data from various endpoints



Interconnectivity

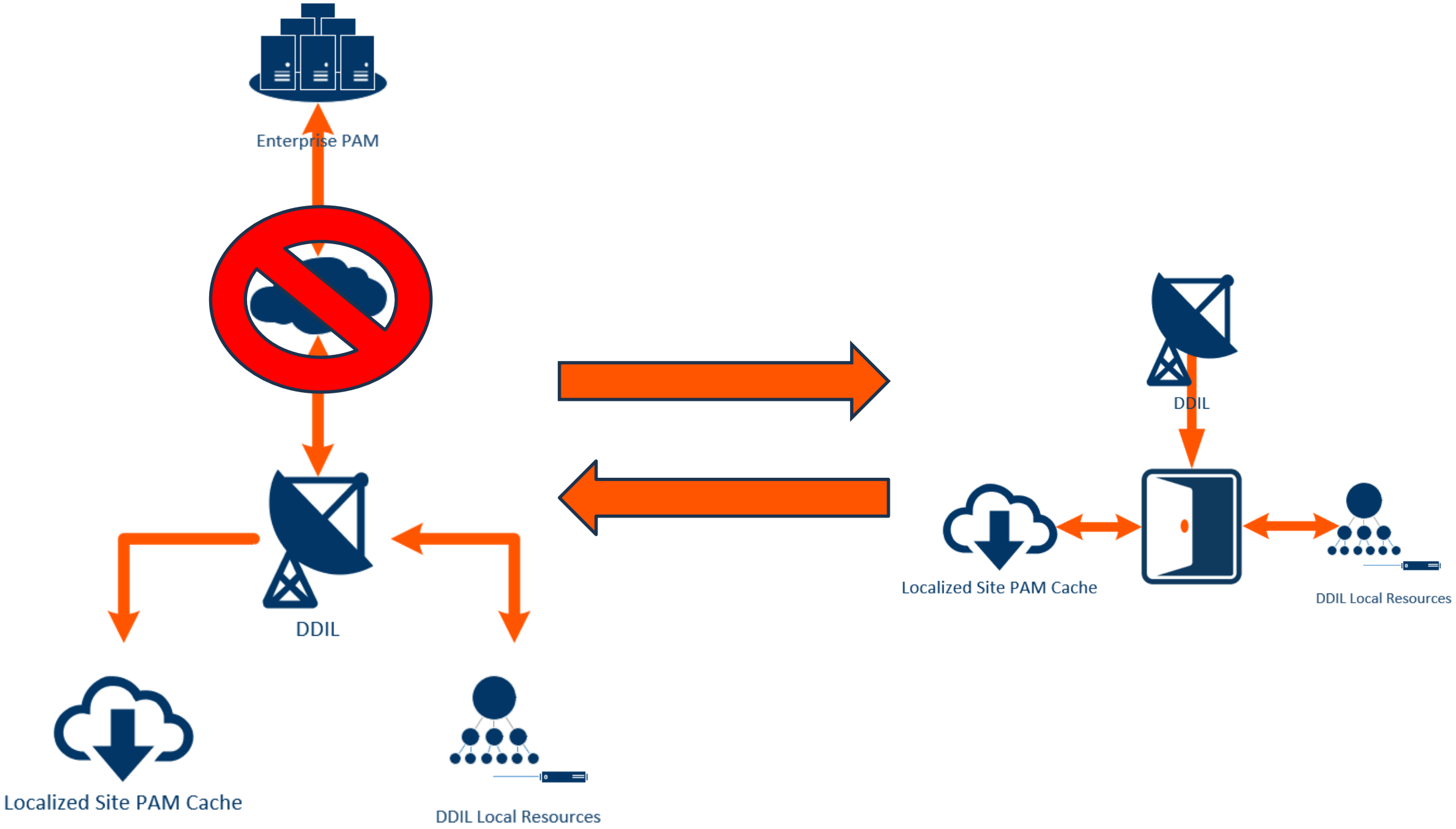
Examine the vulnerabilities introduced through interconnected systems and data flows



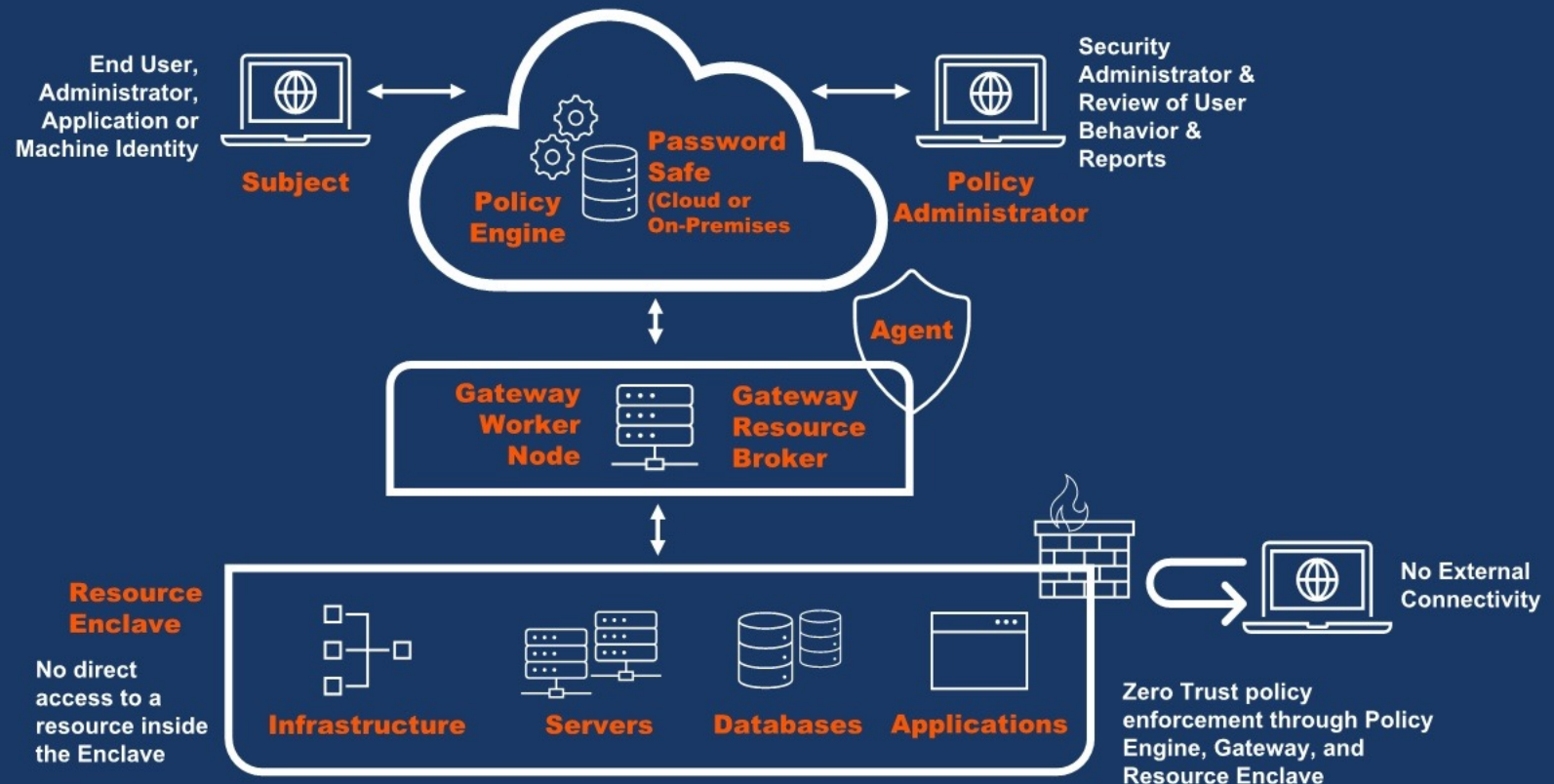
Security requirements

Outline the stringent security and compliance requirements for classified data and operations

The DDIL landscape presents unique security challenges that require innovative cybersecurity solutions for PAM implementations.

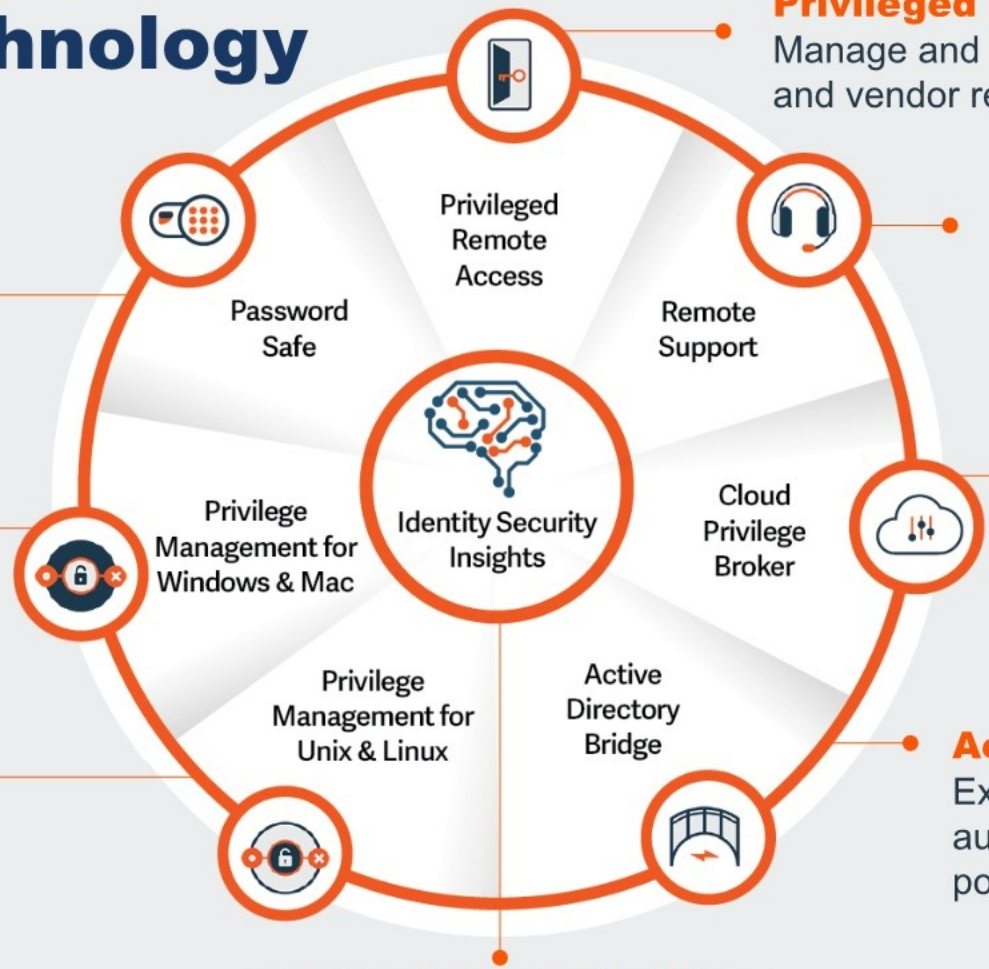

Enterprise PAM
DDIL
Localized Site PAM Cache
DDIL Local Resources
DDIL
Localized Site PAM Cache
DDIL Local Resources

NIST 1800-35(x)
Product Implementation Examples



- Different versions covering architecture to vendors (x)
- Zero trust architectures based on vendor feedback
- Real world implementations
- Vendor specific recommendations
- Considerations when deploying
- Definitions for every component from every vendor

BeyondTrust Platform:
Applying Zero Trust to BeyondTrust Technology



Privileged Remote Access
Manage and audit employee and vendor remote access

Remote Support
Securely access and support any device or system in the world

Password Safe
Gain visibility and control of privileged credentials and secrets

Cloud Privilege Broker
Visualize and right-size entitlements across clouds

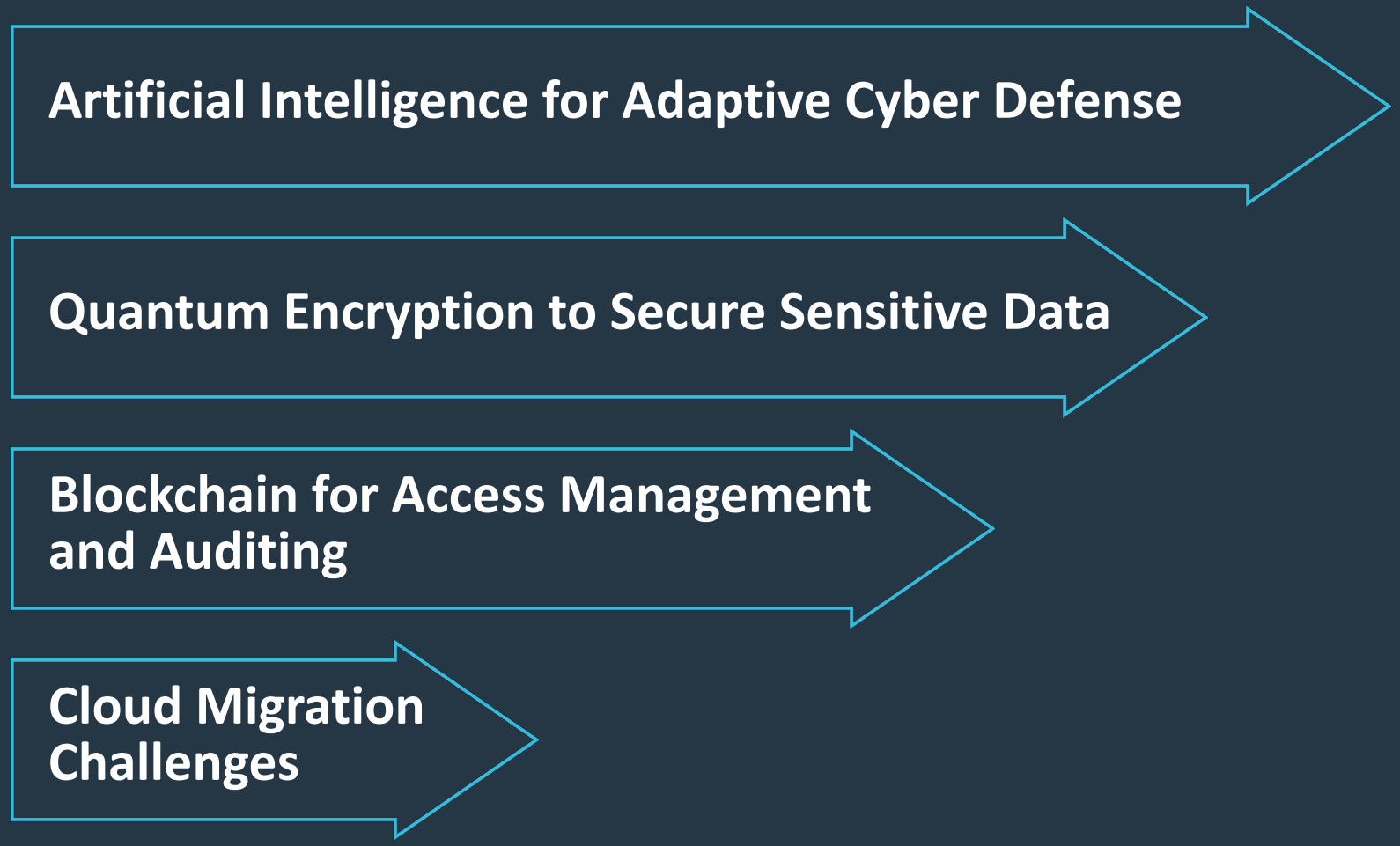
Privilege Management for Windows & Mac
Enforce least privilege and control applications

Active Directory Bridge
Extend and manage Unix/Linux authentication and group policies

Privilege Management for Unix & Linux
Implement unmatched privilege access security

Identity Security Insights
Gain one holistic view of identities and access across your IT estate from a single interface

Future Prospects



Key Takeaways

Strategic Role of PAM

Understand how PAM strategically fortifies security in complex DDIL environments.

PAM Application Insights

Gain actionable insights into creative application of PAM solutions for maximized security and operational efficiency.

Inspiration for Innovation

Be inspired to adapt and innovate PAM implementations tailored to your organization's unique DDIL landscape and security requirements.

Reinforced Cyber Defenses

Strengthen your cyber defense capabilities by unlocking PAM's full potential within your dynamic and interconnected systems.

Thank you and Next Steps

Stop by our BeyondTrust booth #517 to learn how we can partner to achieve Zero Trust objectives while supporting DDIL missions.

Reach out with additional questions:

Josh Brodbent

jbrodbent@beyondtrust.com



Attend our Tech Talk Webinar on Sept 12th!

Badge scan for follow-up link.