3 Take-Aways for the DoD Zero-Trust Reference Architecture

Thomas Lintemuth

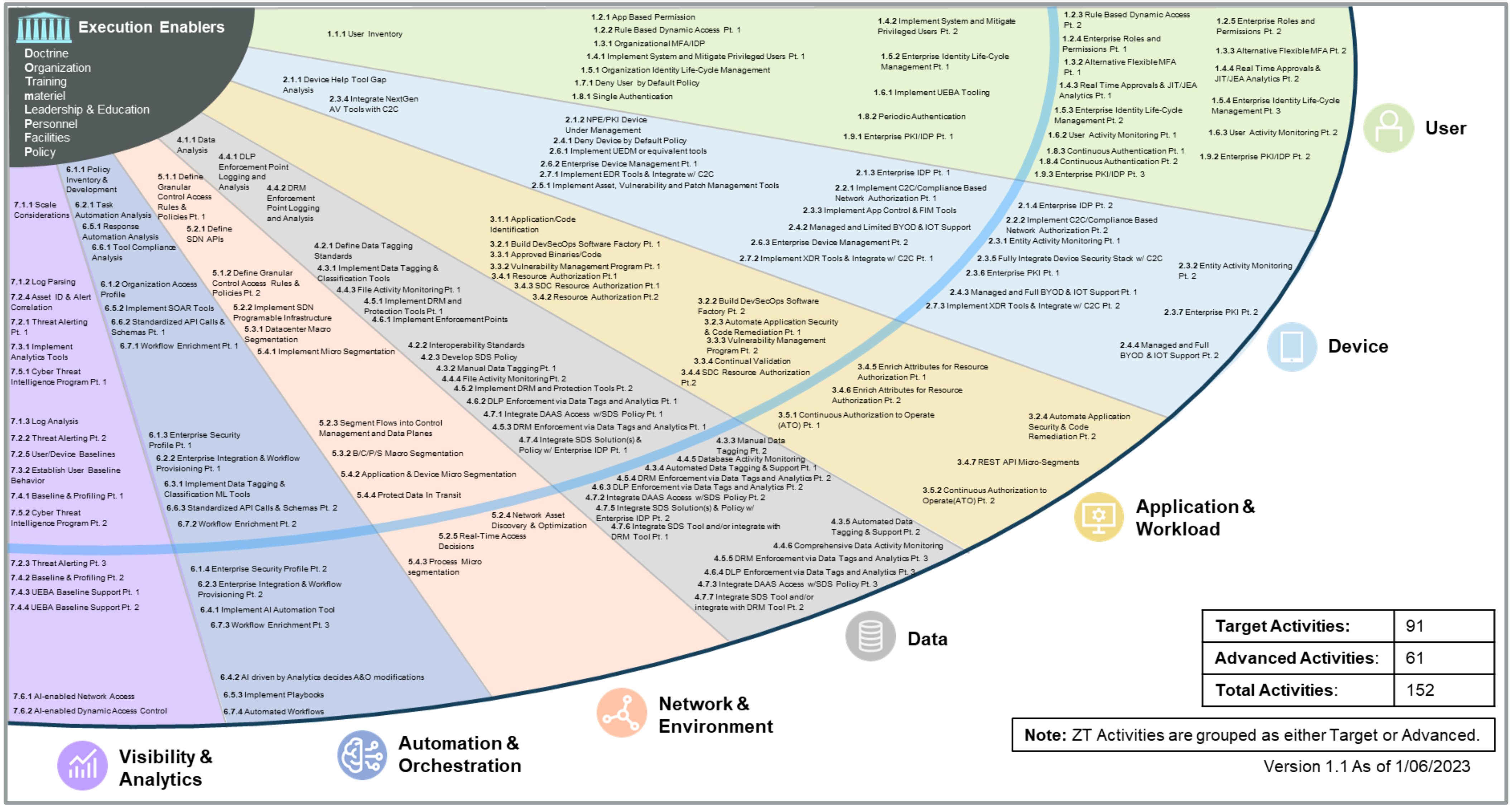
Zero Trust According to DoD

User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
1.1 User Inventory	**2.1** Device Inventory	**3.1** Application Inventory	**4.1** Data Catalog Risk Assessment	**5.1** Data Flow Mapping	**6.1** Policy Decision Point (PDP) & Policy Orchestration	**7.1** Log All Traffic (Network, Data, Apps, Users)
1.2 Conditional User Access	**2.2** Device Detection and Compliance	**3.2** Secure Software Development & Integration	**4.2** DoD Enterprise Data Governance	**5.2** Software Defined Networking (SDN)	**6.2** Critical Process Automation	**7.2** Security Information and Event Management (SIEM)
1.3 Multi-Factor Authentication	**2.3** Device Authorization with Real Time Inspection	**3.3** Software Risk Management	**4.3** Data Labeling and Tagging	**5.3** Macro Segmentation	**6.3** Machine Learning	**7.3** Common Security and Risk Analytics
1.4 Privileged Access Management	**2.4** Remote Access	**3.4** Resource Authorization & Integration	**4.4** Data Monitoring and Sensing	**5.4** Micro Segmentation	**6.4** Artificial Intelligence	**7.4** User and Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	**2.5** Partially & Fully Automated Asset, Vulnerability and Patch Management	**3.5** Continuous Monitoring and Ongoing Authorizations	**4.5** Data Encryption & Rights Management		**6.5** Security Orchestration, Automation & Response (SOAR)	**7.5** Threat Intelligence Integration
1.6 Behavioral, Contextual ID, and Biometrics	**2.6** Unified Endpoint Management (UEM) & Mobile Device Management (MDM)		**4.6** Data Loss Prevention (DLP)		**6.6** API Standardization	**7.6** Automated Dynamic Policies
1.7 Least Privileged Access	**2.7** Endpoint & Extended Detection & Response (EDR & XDR)		**4.7** Data Access Control		**6.7** Security Operations Center (SOC) & Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

EXECUTION ENABLERS Doctrine · Organization · Training · material · Leadership · Personnel · Facilities · Policy

Source: United States Department of Defense

DoD Target Levels



Execution Enablers

Doctrine
Organization
Training
materiel
Leadership & Education
Personnel
Facilities
Policy

User

1.1.1 User Inventory
1.2.1 App Based Permission
1.2.2 Rule Based Dynamic Access Pt. 1
1.3.1 Organizational MFA/IDP
1.4.1 Implement System and Mitigate Privileged Users Pt. 1
1.5.1 Organization Identity Life-Cycle Management
1.7.1 Deny User by Default Policy
1.8.1 Single Authentication
1.4.2 Implement System and Mitigate Privileged Users Pt. 2
1.5.2 Enterprise Identity Life-Cycle Management Pt. 1
1.6.1 Implement UEBA Tooling
1.8.2 Periodic Authentication
1.9.1 Enterprise PKI/IDP Pt. 1
1.2.3 Rule Based Dynamic Access Pt. 2
1.2.4 Enterprise Roles and Permissions Pt. 1
1.3.2 Alternative Flexible MFA Pt. 1
1.4.3 Real Time Approvals & JIT/JEA Analytics Pt. 1
1.5.3 Enterprise Identity Life-Cycle Management Pt. 2
1.6.2 User Activity Monitoring Pt. 1
1.8.3 Continuous Authentication Pt. 1
1.8.4 Continuous Authentication Pt. 2
1.9.3 Enterprise PKI/IDP Pt. 3
1.2.5 Enterprise Roles and Permissions Pt. 2
1.3.3 Alternative Flexible MFA Pt. 2
1.4.4 Real Time Approvals & JIT/JEA Analytics Pt. 2
1.5.4 Enterprise Identity Life-Cycle Management Pt. 3
1.6.3 User Activity Monitoring Pt. 2
1.9.2 Enterprise PKI/IDP Pt. 2

Device

2.1.1 Device Help Tool Gap Analysis
2.3.4 Integrate NextGen AV Tools with C2C
2.1.2 NPE/PKI Device Under Management
2.4.1 Deny Device by Default Policy
2.6.1 Implement UEDM or equivalent tools
2.6.2 Enterprise Device Management Pt. 1
2.7.1 Implement EDR Tools & Integrate w/ C2C
2.5.1 Implement Asset, Vulnerability and Patch Management Tools
2.1.3 Enterprise IDP Pt. 1
2.2.1 Implement C2C/Compliance Based Network Authorization Pt. 1
2.3.3 Implement App Control & FIM Tools
2.4.2 Managed and Limited BYOD & IOT Support
2.6.3 Enterprise Device Management Pt. 2
2.7.2 Implement XDR Tools & Integrate w/ C2C Pt. 1
2.1.4 Enterprise IDP Pt. 2
2.2.2 Implement C2C/Compliance Based Network Authorization Pt. 2
2.3.1 Entity Activity Monitoring Pt. 1
2.3.5 Fully Integrate Device Security Stack w/ C2C
2.3.6 Enterprise PKI Pt. 1
2.4.3 Managed and Full BYOD & IOT Support Pt. 1
2.7.3 Implement XDR Tools & Integrate w/ C2C Pt. 2
2.3.2 Entity Activity Monitoring Pt. 2
2.3.7 Enterprise PKI Pt. 2
2.4.4 Managed and Full BYOD & IOT Support Pt. 2

Application & Workload

3.1.1 Application/Code Identification
3.2.1 Build DevSecOps Software Factory Pt. 1
3.3.1 Approved Binaries/Code
3.3.2 Vulnerability Management Program Pt. 1
3.4.1 Resource Authorization Pt.1
3.4.3 SDC Resource Authorization Pt.1
3.4.2 Resource Authorization Pt.2
3.2.2 Build DevSecOps Software Factory Pt. 2
3.2.3 Automate Application Security & Code Remediation Pt. 1
3.3.3 Vulnerability Management Program Pt. 2
3.3.4 Continual Validation
3.4.4 SDC Resource Authorization Pt.2
3.4.5 Enrich Attributes for Resource Authorization Pt. 1
3.4.6 Enrich Attributes for Resource Authorization Pt. 2
3.5.1 Continuous Authorization to Operate (ATO) Pt. 1
3.2.4 Automate Application Security & Code Remediation Pt. 2
3.4.7 REST API Micro-Segments
3.5.2 Continuous Authorization to Operate(ATO) Pt. 2

Data

4.1.1 Data Analysis
4.4.1 DLP Enforcement Point Logging and Analysis
4.4.2 DRM Enforcement Point Logging and Analysis
4.2.1 Define Data Tagging Standards
4.3.1 Implement Data Tagging & Classification Tools
4.4.3 File Activity Monitoring Pt. 1
4.5.1 Implement DRM and Protection Tools Pt. 1
4.6.1 Implement Enforcement Points
4.2.2 Interoperability Standards
4.2.3 Develop SDS Policy
4.3.2 Manual Data Tagging Pt. 1
4.4.4 File Activity Monitoring Pt. 2
4.5.2 Implement DRM and Protection Tools Pt. 2
4.6.2 DLP Enforcement via Data Tags and Analytics Pt. 1
4.7.1 Integrate DAAS Access w/SDS Policy Pt. 1
4.5.3 DRM Enforcement via Data Tags and Analytics Pt. 1
4.7.4 Integrate SDS Solution(s) & Policy w/ Enterprise IDP Pt. 1
4.3.3 Manual Data Tagging Pt. 2
4.4.5 Database Activity Monitoring
4.3.4 Automated Data Tagging & Support Pt. 1
4.5.4 DRM Enforcement via Data Tags and Analytics Pt. 2
4.6.3 DLP Enforcement via Data Tags and Analytics Pt. 2
4.7.2 Integrate DAAS Access w/SDS Policy Pt. 2
4.7.5 Integrate SDS Solution(s) & Policy w/ Enterprise IDP Pt. 2
4.7.6 Integrate SDS Tool and/or integrate with DRM Tool Pt. 1
4.3.5 Automated Data Tagging & Support Pt. 2
4.4.6 Comprehensive Data Activity Monitoring
4.5.5 DRM Enforcement via Data Tags and Analytics Pt. 3
4.6.4 DLP Enforcement via Data Tags and Analytics Pt. 3
4.7.3 Integrate DAAS Access w/SDS Policy Pt. 3
4.7.7 Integrate SDS Tool and/or integrate with DRM Tool Pt. 2

Network & Environment

5.1.1 Define Granular Control Access Rules & Policies Pt. 1
5.2.1 Define SDN APIs
5.1.2 Define Granular Control Access Rules & Policies Pt. 2
5.2.2 Implement SDN Programable Infrastructure
5.3.1 Datacenter Macro Segmentation
5.4.1 Implement Micro Segmentation
5.2.3 Segment Flows into Control Management and Data Planes
5.3.2 B/C/P/S Macro Segmentation
5.4.2 Application & Device Micro Segmentation
5.4.4 Protect Data In Transit
5.2.4 Network Asset Discovery & Optimization
5.2.5 Real-Time Access Decisions
5.4.3 Process Micro segmentation

Automation & Orchestration

6.1.1 Policy Inventory & Development
6.2.1 Task Automation Analysis
6.5.1 Response Automation Analysis
6.6.1 Tool Compliance Analysis
6.1.2 Organization Access Profile
6.5.2 Implement SOAR Tools
6.6.2 Standardized API Calls & Schemas Pt. 1
6.7.1 Workflow Enrichment Pt. 1
6.1.3 Enterprise Security Profile Pt. 1
6.2.2 Enterprise Integration & Workflow Provisioning Pt. 1
6.3.1 Implement Data Tagging & Classification ML Tools
6.6.3 Standardized API Calls & Schemas Pt. 2
6.7.2 Workflow Enrichment Pt. 2
6.1.4 Enterprise Security Profile Pt. 2
6.2.3 Enterprise Integration & Workflow Provisioning Pt. 2
6.4.1 Implement AI Automation Tool
6.7.3 Workflow Enrichment Pt. 3
6.4.2 AI driven by Analytics decides A&O modifications
6.5.3 Implement Playbooks
6.7.4 Automated Workflows

Visibility & Analytics

7.1.1 Scale Considerations
7.1.2 Log Parsing
7.2.4 Asset ID & Alert Correlation
7.2.1 Threat Alerting Pt. 1
7.3.1 Implement Analytics Tools
7.5.1 Cyber Threat Intelligence Program Pt. 1
7.1.3 Log Analysis
7.2.2 Threat Alerting Pt. 2
7.2.5 User/Device Baselines
7.3.2 Establish User Baseline Behavior
7.4.1 Baseline & Profiling Pt. 1
7.5.2 Cyber Threat Intelligence Program Pt. 2
7.2.3 Threat Alerting Pt. 3
7.4.2 Baseline & Profiling Pt. 2
7.4.3 UEBA Baseline Support Pt. 1
7.4.4 UEBA Baseline Support Pt. 2
7.6.1 AI-enabled Network Access
7.6.2 AI-enabled Dynamic Access Control

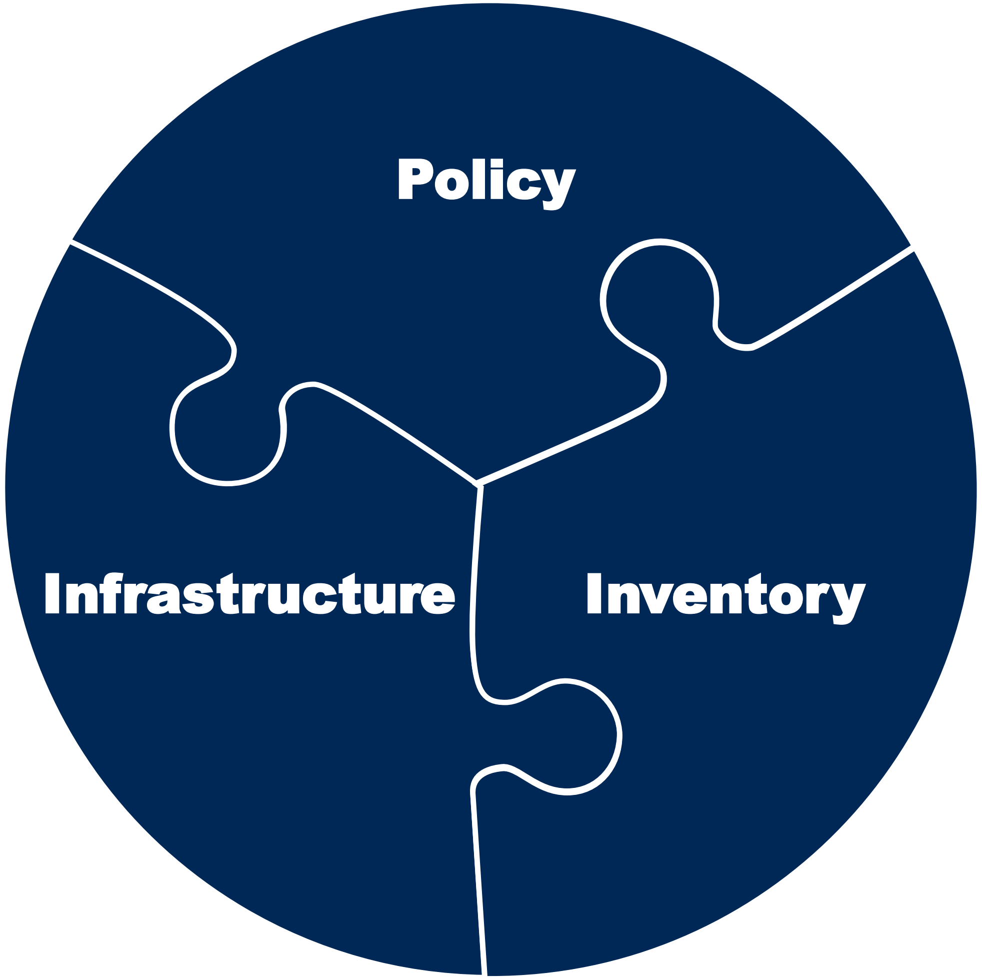
Target Activities:	91
Advanced Activities:	61
Total Activities:	152

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

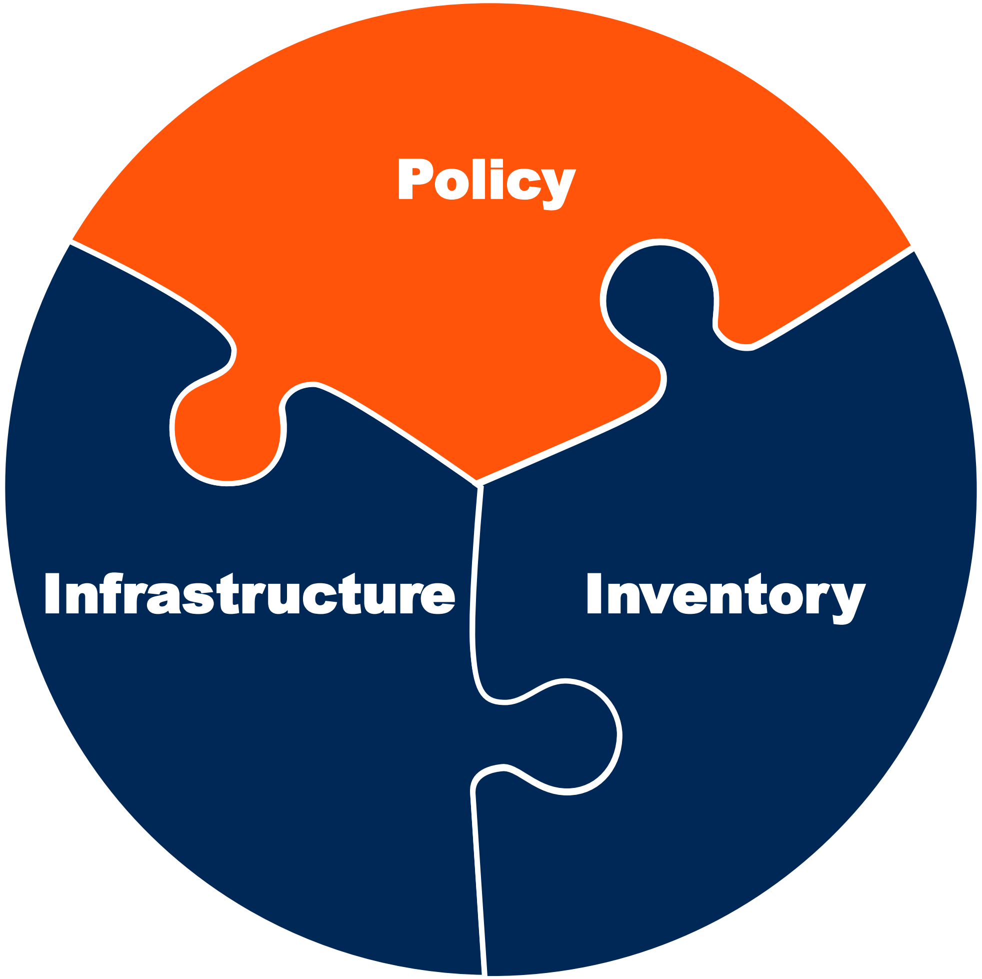
Version 1.1 As of 1/06/2023

Source: United States Department of Defense

Take-Aways From the DoD Architecture



Take-Away No. 1



Foundational Access Policy Decisions

Users

Authentication

Devices

Day

Time

Location

Advanced Access Policy Decisions

- Vulnerability
- Device posture
- Data restrictions
- Threat intelligence
- Need to know
- Real time events
- Next up

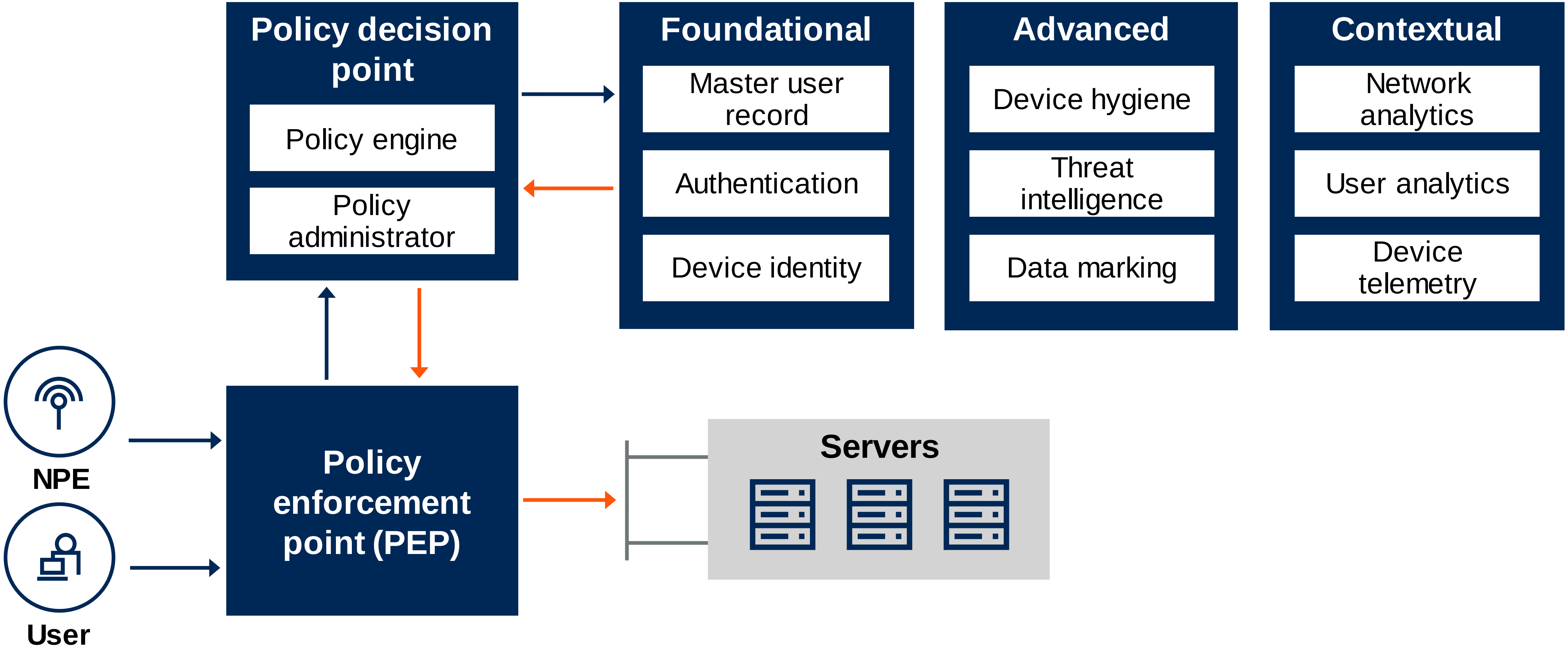
Contextual Access Policy Decisions

User analytics

Network analytics

Device telemetry

Zero-Trust Access Policy



Policy decision point

Policy engine

Policy administrator

Foundational

Master user record

Authentication

Device identity

Advanced

Device hygiene

Threat intelligence

Data marking

Contextual

Network analytics

User analytics

Device telemetry

NPE

User

Policy enforcement point (PEP)

Servers

Additional Security Policy Decisions

1. Privileged access management policies including JIT/JEA.
2. Procedure to automatically provision/deprovision users.
3. Standardize secure coding processes.
4. Process to transition to microservices using CI/CD process.
5. Data policy including DLP, DRM, Software Defined Storage, DaaS and which data tags to use.
6. Develop policy for API use.
7. Develop role profiles.

Sample Role Profile

Role Profile:__________

Date:__________

Developed by:______________________________

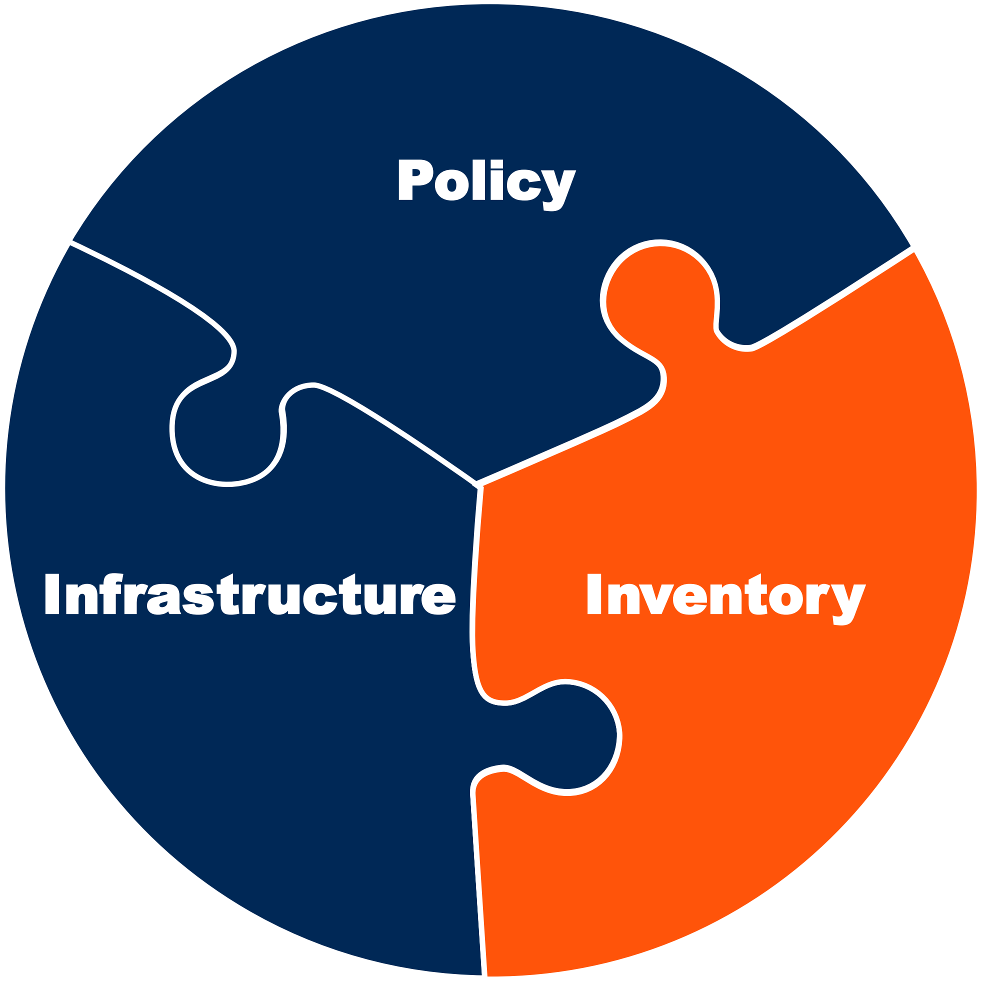
Approved by:______________________________

				Locations Allowed From		Endpoint Posture					Date / Time		Data
	BYOD Allowed	MFA Required	Identity Provider	Int'l	National	AV	Vulnerabilities	EDR Active	FW On	UEM Enrolled	Hours	Days	Data tags
Applicaton 1													
Applicaton 2													
Applicaton 3													
Applicaton 4													
.													
.													
.													
.													

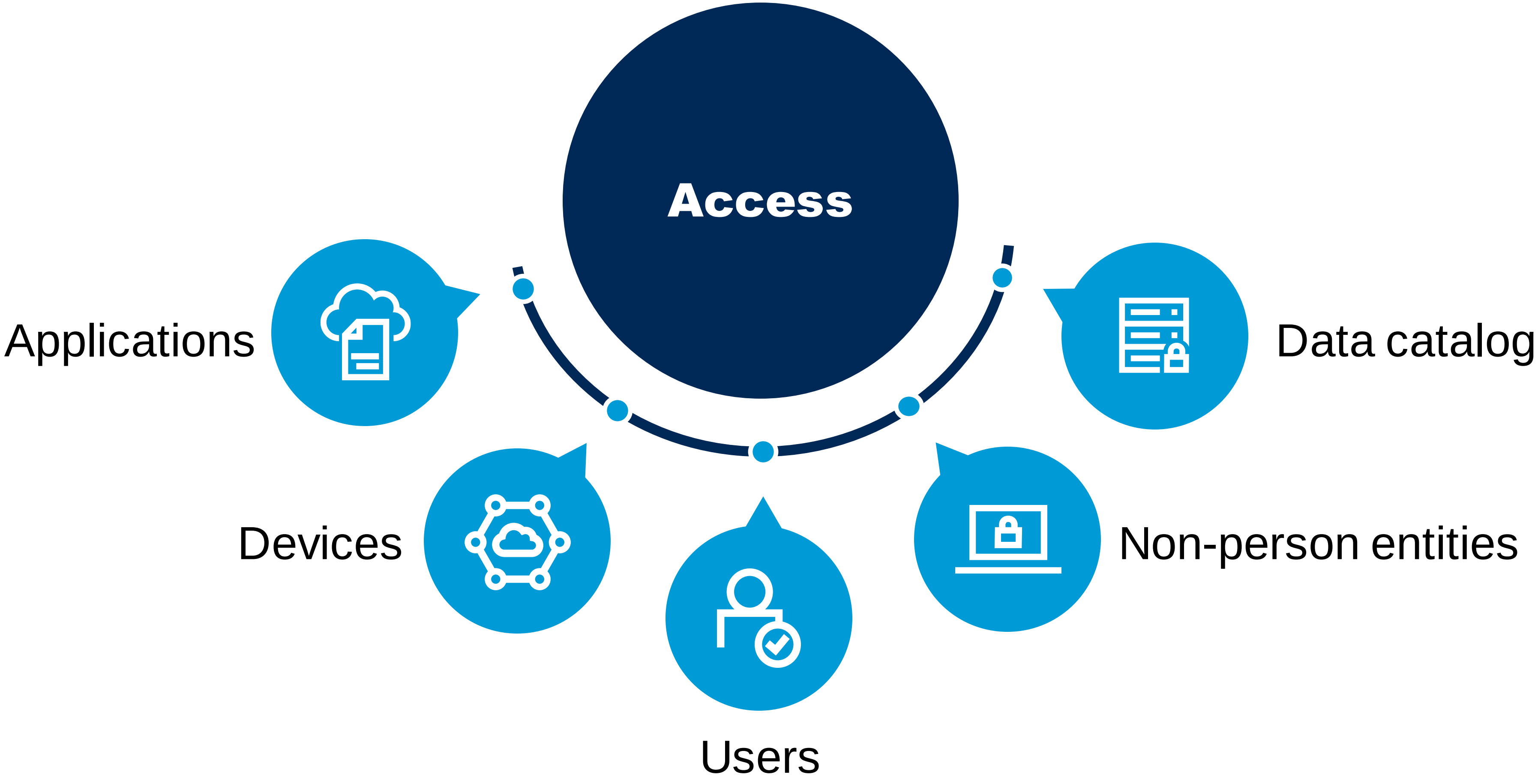
Key Issue Take-Away:

Well defined policy is the foundation of zero trust.

Take Away No. 2



Who Is the Who, What Is the What



Access

Applications

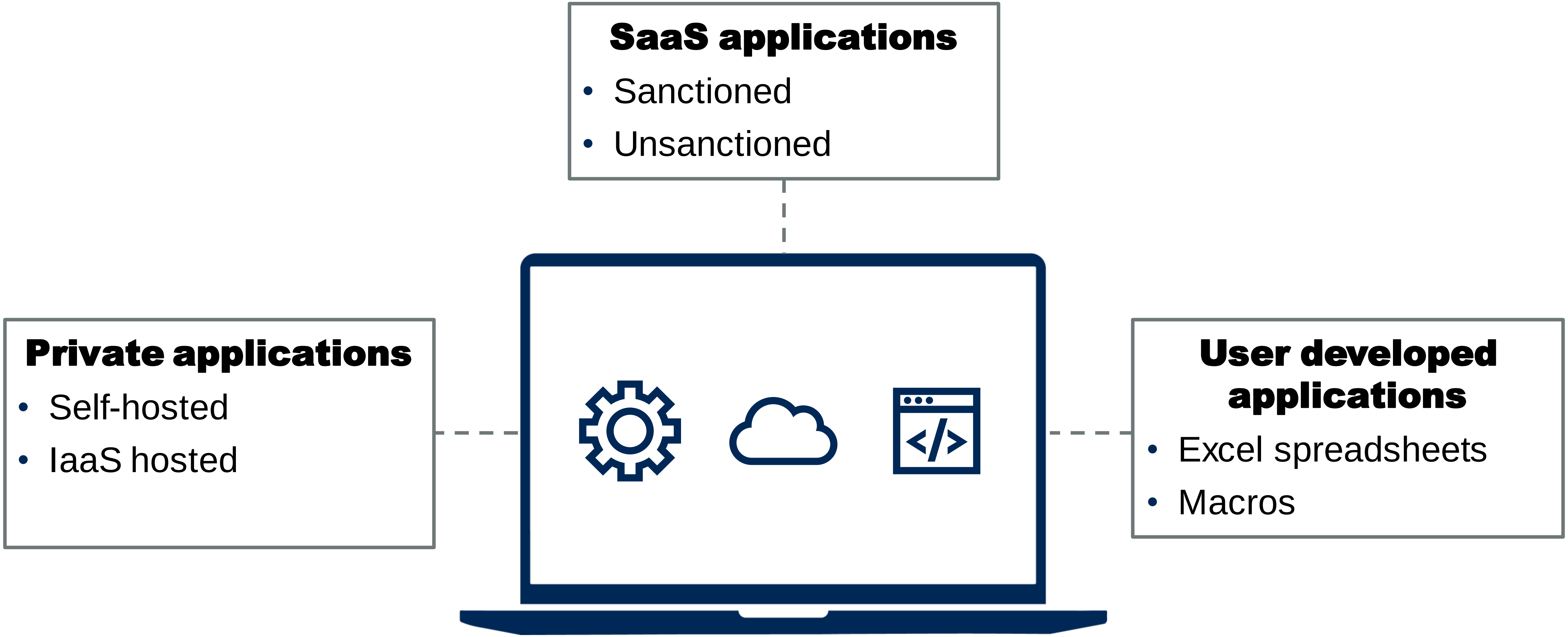
Devices

Users

Non-person entities

Data catalog

Application Catalog



SaaS applications

- Sanctioned
- Unsanctioned

Private applications

- Self-hosted
- IaaS hosted

User developed applications

- Excel spreadsheets
- Macros

Users: Varied and Dynamic

Internal

Contingent

Contract

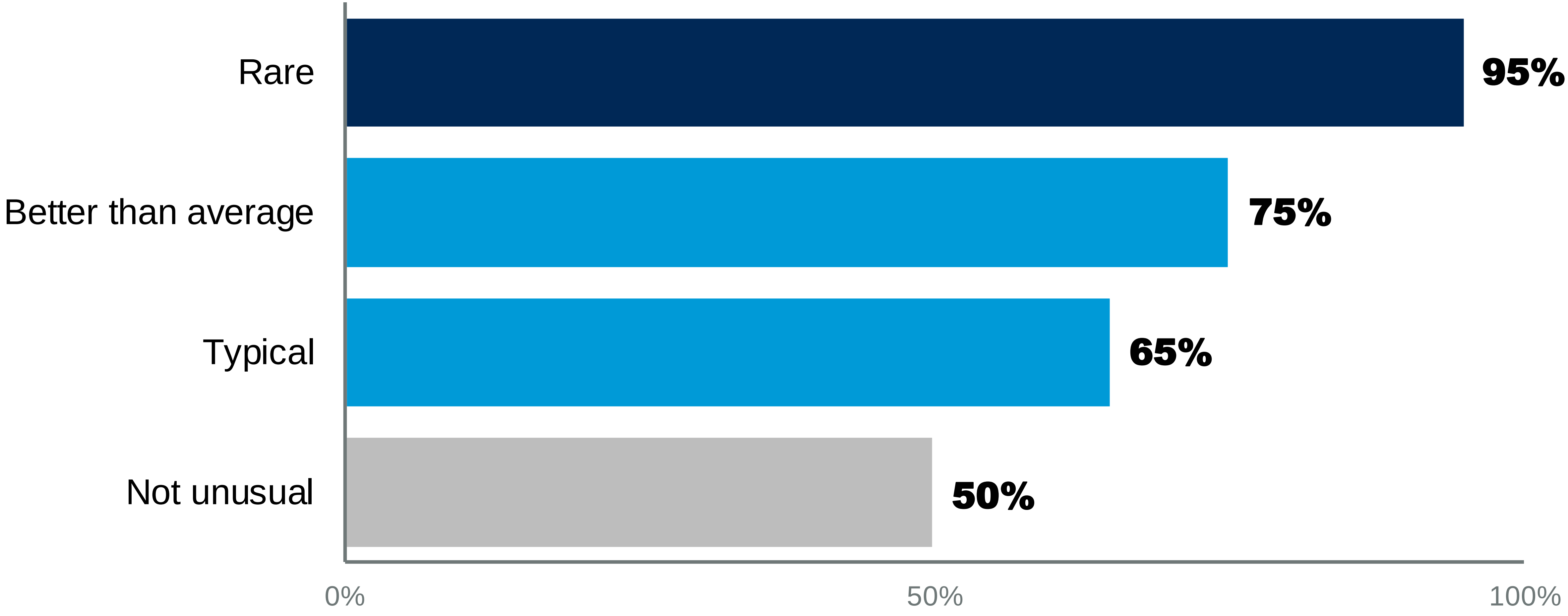
External partners

Customers

Devices

- End user
- Non-person entities
  - IOT
  - OT
  - CPS
- Servers

How Accurate Is Your Asset Database?



Source: Analyst Client Inquiry

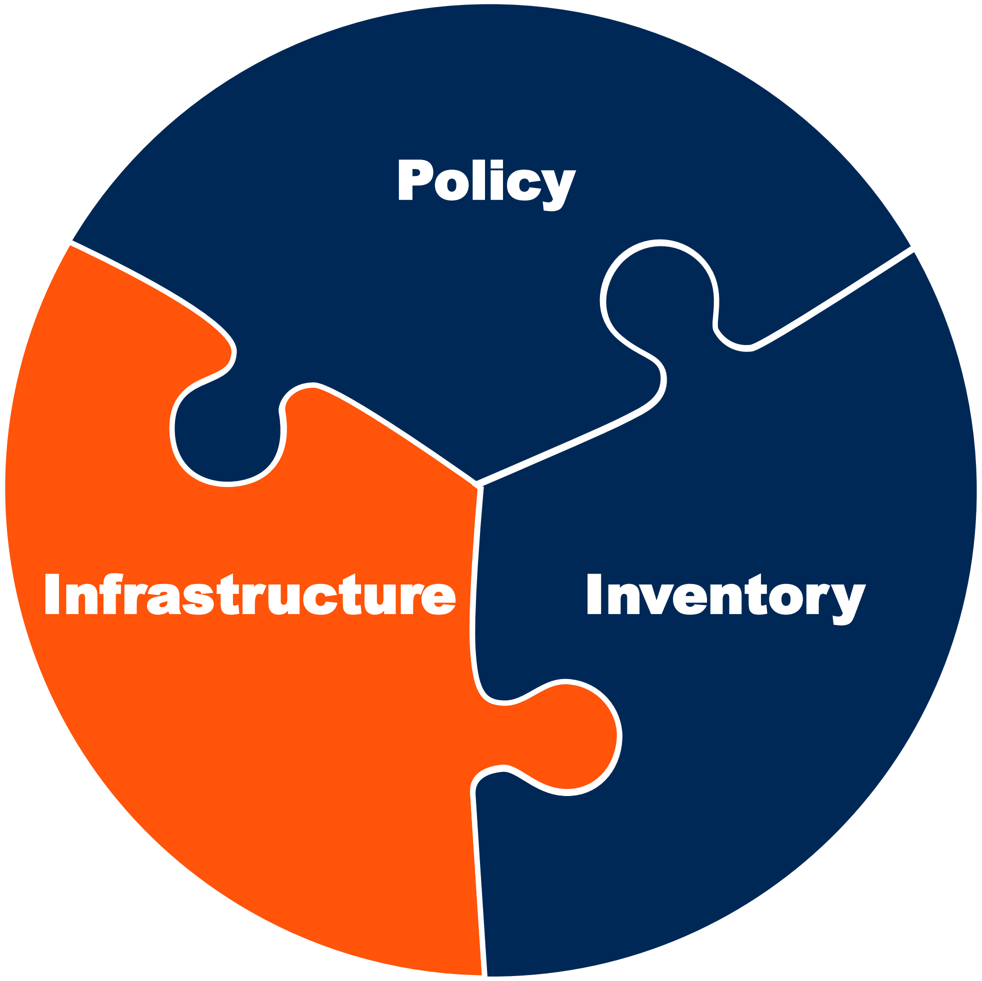
Data Catalog

Dataset identifier	Dataset name	Dataset description	Dataset owner	Application supported	Curator	Criticality	Category	Tag
A unique identifier of the data asset.	A name given to the resource.	Free-text account of the resource.	Business owner of the data	Applications that use the data	Associate or Role responsible for the data	Importance of the data to the organization	Rating of the data based on internal classification nomenclature	A keyword or tag describing the resource

Key Issue Take-Away:

Know your who's and your what's.

Take Away No. 3



Infrastructure Required

- API gateway
- Cloud security posture mgmt.
- Database activity monitoring
- Data loss prevention
- Digital rights management
- Endpoint detection and response
- File integrity monitoring
- Multifactor authentication
- Network access control
- Network detection and response
- Privileged access management
- Policy enforcement point
- Public key infrastructure
- Software defined networking
- Software defined storage
- SOAR
- User entity behavioral analysis
- Unified endpoint management
- Vulnerability threat management
- Extended detection and response

Infrastructure Required

- API gateway
- Cloud security posture mgmt.
- Database activity monitoring
- Network detection and response
- Digital rights management
- File integrity monitoring
- Software defined networking
- Policy enforcement point
- Extended detection and response
- Software defined storage
- Privileged access management
- User entity behavioral analysis

Policy Enforcement Point Examples

ZTNA

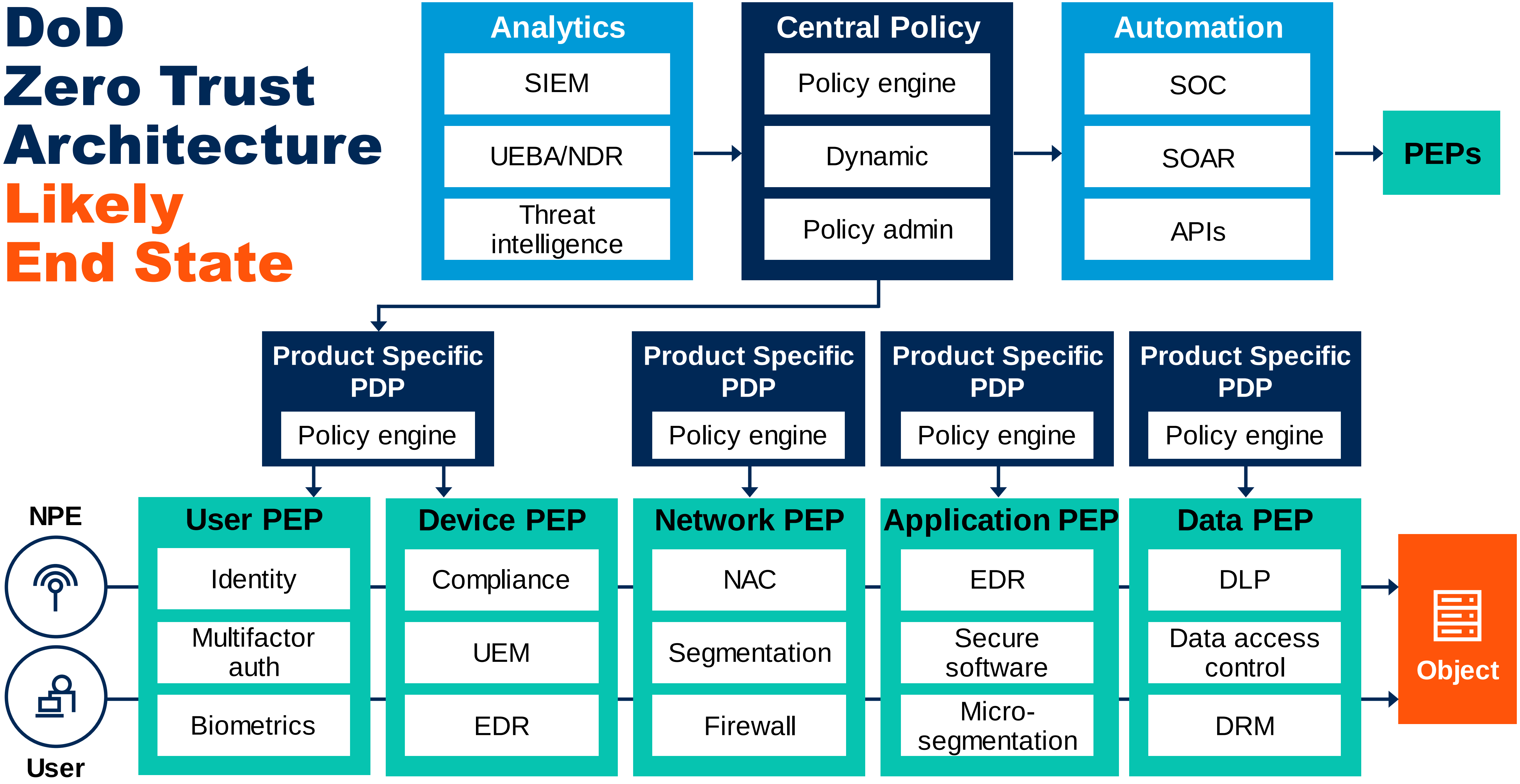
Enterprise firewall

Identity aware proxy

Micro-segmentation

Software defined networking

DoD Zero Trust Architecture **Likely End State**



Analytics
- SIEM
- UEBA/NDR
- Threat intelligence

→ **Central Policy**
- Policy engine
- Dynamic
- Policy admin

→ **Automation**
- SOC
- SOAR
- APIs

→ **PEPs**

Product Specific PDP — Policy engine → User PEP, Device PEP

Product Specific PDP — Policy engine → Network PEP

Product Specific PDP — Policy engine → Application PEP

Product Specific PDP — Policy engine → Data PEP

NPE

User

User PEP
- Identity
- Multifactor auth
- Biometrics

Device PEP
- Compliance
- UEM
- EDR

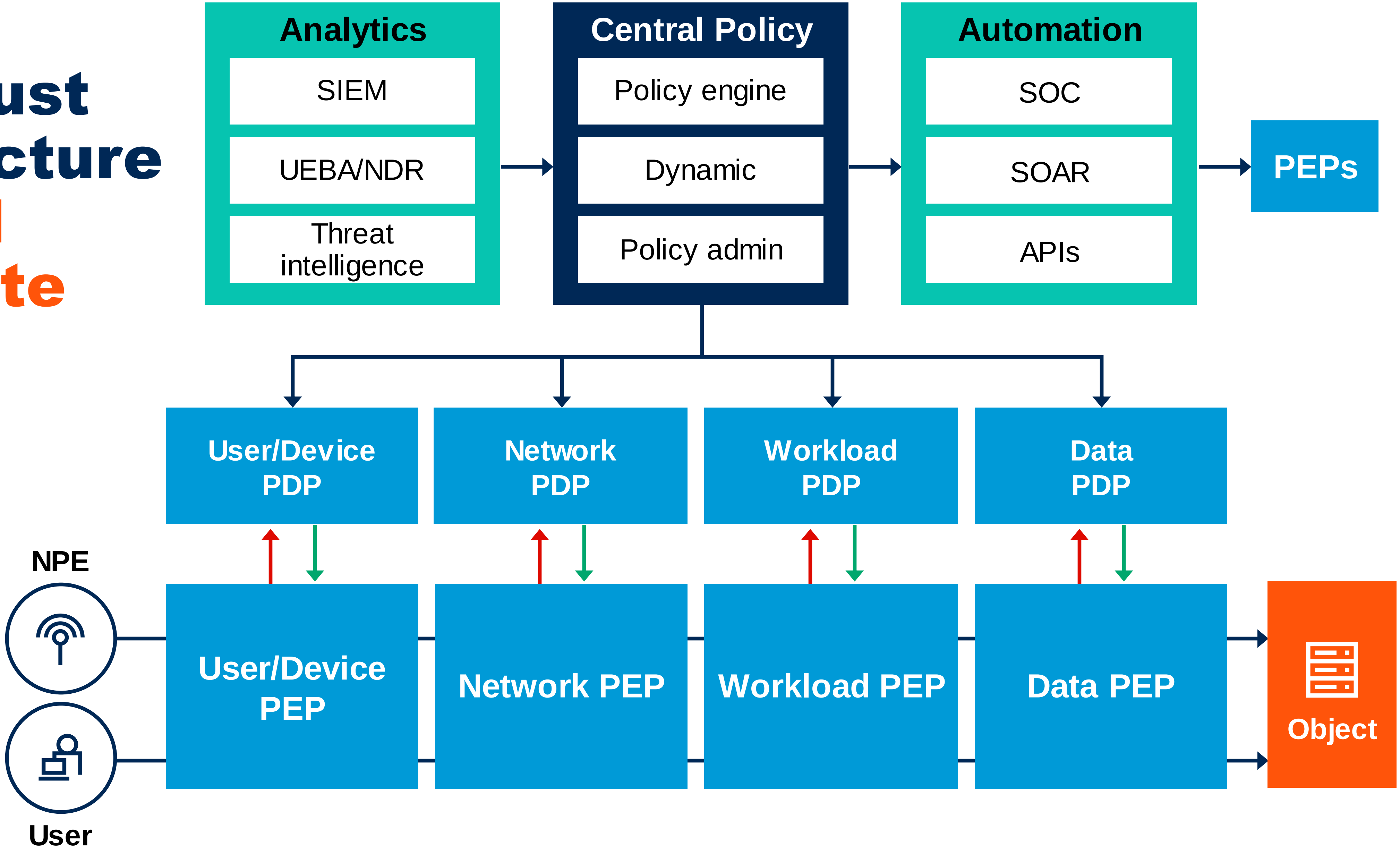
Network PEP
- NAC
- Segmentation
- Firewall

Application PEP
- EDR
- Secure software
- Micro-segmentation

Data PEP
- DLP
- Data access control
- DRM

→ **Object**

DoD Zero Trust Architecture Optimal End State



Key Issue Take-Away:

Design for the optimal. Start with the likely.

Recommendations

- Ensure you specific policies and all your security policies are up to date.
- Consolidate user repositories and establish granular role based entitlements.
- Verify your IT asset management system is trustworthy.
- Build an application catalog.
- Find and categorize your data.

Recommended Gartner Research

To learn more about access to Gartner research, expert analyst insight, and peer communities, contact your Gartner representative or click on “Become A Client” on gartner.com to speak with one of our specialists.

- **Market Guide for Zero Trust Network Access**
  Aaron McQuaid, Neil MacDonald, John Watts and Rajpreet Kaur
- **Use the U.S. DoD Model for Your Zero Trust Approach: User Pillar**
  Ant Allan and Thomas Lintemuth
- **Use the U.S. DoD Model for Your Zero Trust Approach: Network & Environment Pillar**
  Thomas Lintemuth
- **Infographic: 4 Essential Stages on the Journey to Zero Trust**
  Thomas Lintemuth

Access to Gartner research is subject to individual subscription type and product entitlements.