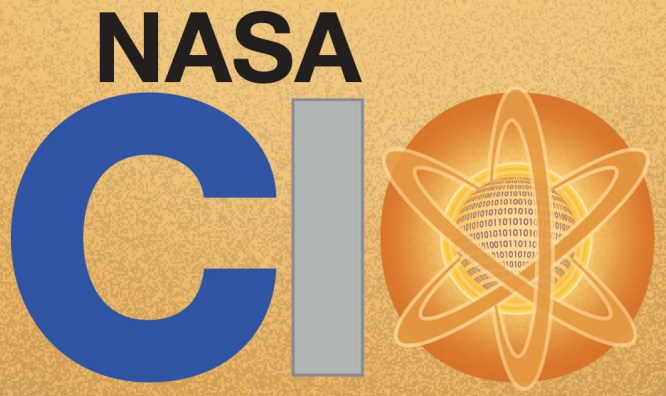
National Aeronautics and Space Administration

Planning for a Zero Trust Architecture Target State



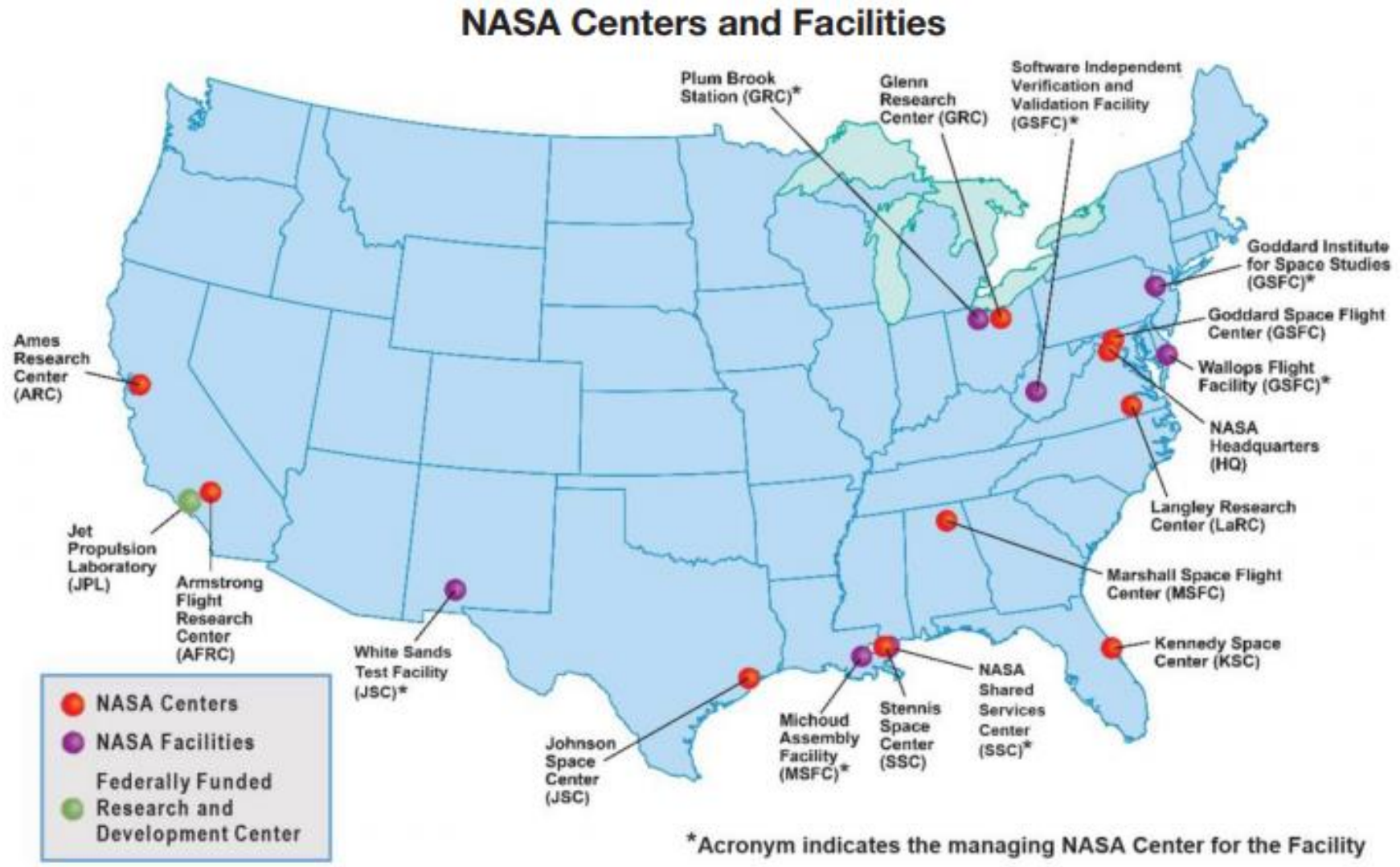
Dennis Kay
Cybersecurity Standards, Architecture and Engineering

Federal CIO Zero Trust Architecture Summit
November 13 2019

NASA Zero Trust Presentations Topics

- NASA Locations and Scope of Identity, Credentials and Assets
- Opportunity Space and Potential Benefits
- Zero Trust Architecture Concept Overview and
- Access Management Enhanced with Attribute Based Access Control
- Zero Trust Path Scoring and Evaluation
- Use Case and Gap Analysis
- Value Proposition for NASA
- Implementation Approach
- Required Support from OCIO Organizations
- Initial Development Areas
- Implementation Challenges and Summary

NASA US Locations



Current NASA Identity, Credential, Assets Scope

- Active Users – ~115,000
- Remote Partner Users – ~50,000
- Onboarding/offboarding (past month) - ~2,700/1,100
- NASA Issued PIV Smartcard – 72,700
- NASA Issues Agency Smartbadge – 4,700
- Registers Smartcards – 4,200
- On-Time Password Tokens – 23,200
- Active Assets – 9,900
- Weekly Assets Provisioning Requests – 11,550
- Web Apps Integrated with Central AuthN Services ~1,300
- Weekly Assets Provisioning Requests – 11,550

Zero Trust Opportunity Space for NASA

- Access is generally *binary* and based on black/white rulesets and limited factors
  - PIV access required or not
  - Behind the firewall or not (workstation in internal network or connecting via VPN access)
  - Required level of confidence or not
  - Authorized or unauthorized devices
  - Access from US or outside
- If a required factor is lost or not available, users cannot access required services
  - Loss of PIV card, temporary exemption processes
  - Inability to access VPN (example: cached credential corruption, insufficient VPN capacity)
  - Increased rigor for background checks to establish user level of confidence
  - Reprovisioning of replacements for lost or stolen devices
- Often requires **manual** intervention from enterprise or center level service providers and help desks

Potential Benefits for NASA

- Improved user experience - Dynamic access allows for the use of multiple factors and situational context to achieve the necessary trust score
  - Improves our ability to establish a viable partner access architecture
  - Allows for the potential to increase security with international partners collaboration
  - Establishes a framework to trust Internet of Things (IoT) to further secure asset access
- Simplifies integration for asset owners
  - Applications only need to integrate with the proxy passing on the risk score(s)
  - Risk values can be coded into metadata for data access
  - Allows for more options for physical access controls
- Effective Risk Management
  - Provides a consistent evaluation of risk and ensures only authorized users can access valued assets
  - Improved protection from existing and evolving threats
  - Reduced impact from breaches
  - Potential cost reduction from reduced incidents
- Provide architectural alignment of mission support program areas with strategies for implementing and maintaining OMB FISMA and DHS CDM DEFEND compliance

Zero Trust Architecture Concept

Static Factors are assigned trust values and weights

Credential

Level of Confidence

Device Trust

Network

Physical Location

Biometrics

Device Orientation and Peripherals

Dynamic Factors are assessed and scored at time of access

Threat Intelligence

Geovelocity

GPS Coordinates

***Users* have various roles and are *entitled to access* various assets.** *Types of users can be: NASA workers, Federal Partners, External Contractors and Commercial Partners, Affiliates, Foreign Nationals, Devices/IoT*

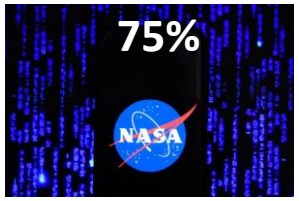
Assets/Applications have level of risk scores – *thresholds that must be exceeded for access to be permitted. In general, the security plan categorization determines asset level or risk.*

Trust Score: 70%

Trust Score *is a combination of factors and are used to continually provide identity assurance. Trust Score determines level of access as required by the Level of Risk value of the asset being accessed.*

Applications

Data

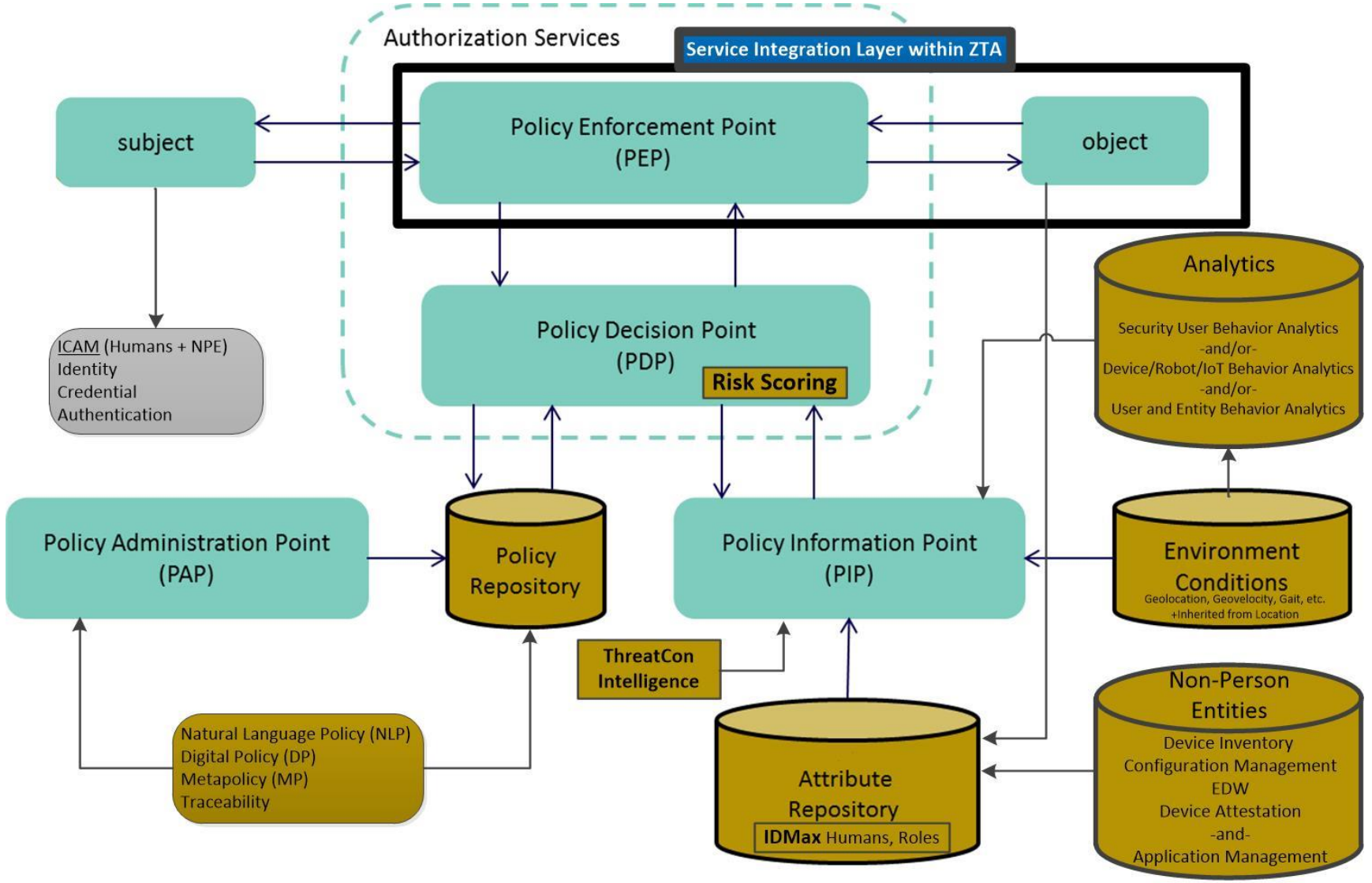


Network Segments

Physical Access

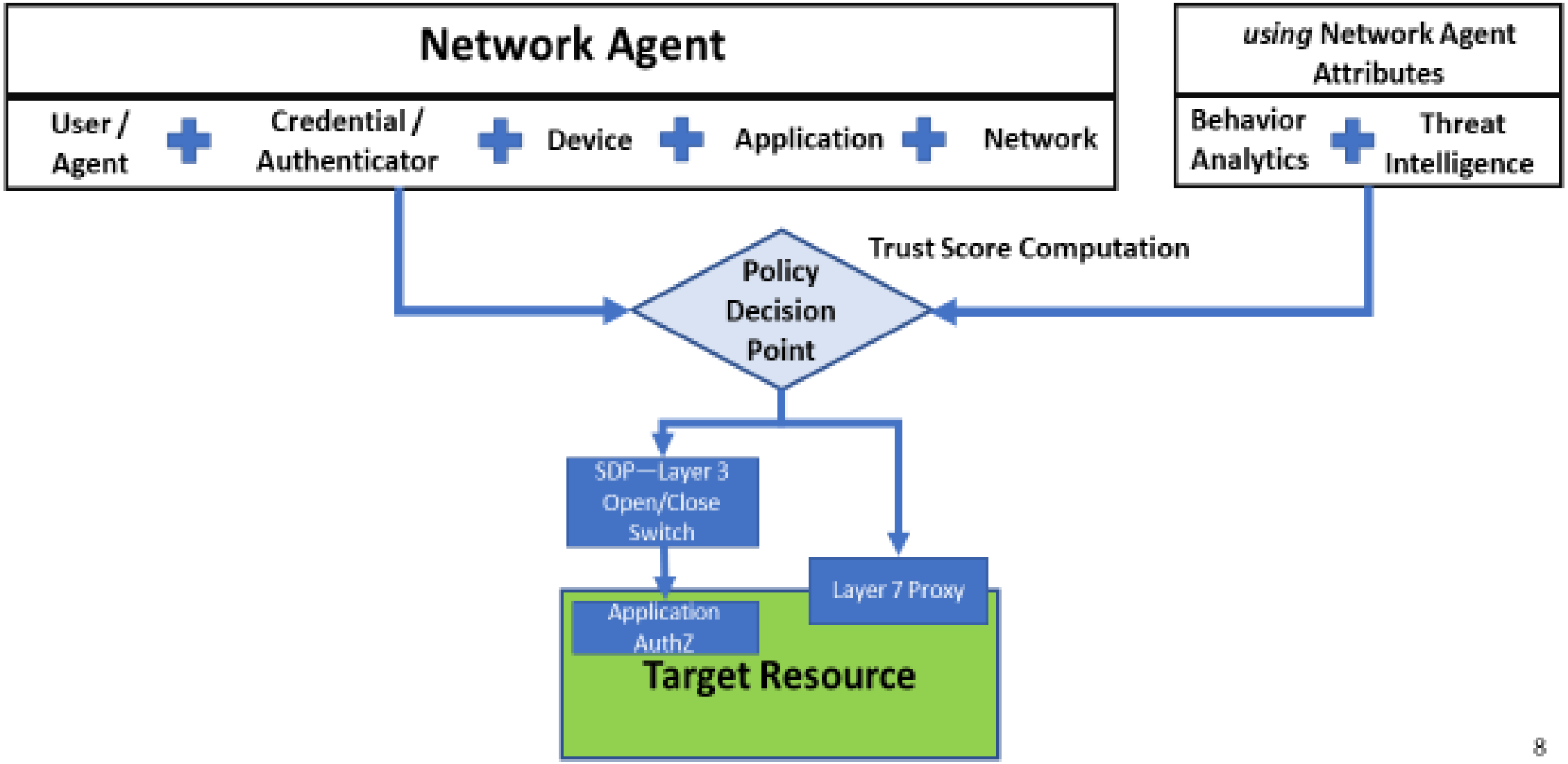
TRUST SCORE + USER ENTITLEMENT = AUTHORIZATION FOR ACCESS

Access Management Enhanced with Attribute Based Access Control



NIST SP 800-162 Figure 5 ABAC Access Control Mechanism
With ZTA Additions and Service Integration Layer

Zero Trust Path Scoring And Evaluation



ZTA Scoring Path

	Network Agent Instantiated construct at authorization time, after authentication					*Using Network Agent Attributes*		Evaluation	Target
	User (or agent)	**Credential or Authenticator**	**Device**	**Application**	**Network**	**Behavior Analytics**	**Threat Intelligence**	**Policy Decision Point**	**Resource**

Authenticated PRINCIPAL	• UUPIC
	• IAL (IAL static/possibly dynamic for Federation)
	• LOC
	• Security Group Memberships (NED or NCAD)
	• Role
	• Relevant Attributes, source IdMAX, from NED or NCAD
		• AAL
		• Federation:FAL
		• Federation:IdP
			• Managed by:
			  ○ GFE
			  ○ PFE (assumed)
			  ○ Contractor
			  ○ Partner
			• Device health
			  ○ OS version
			  ○ Patch status
			  ○ Virus scan
			  ○ DAR status
			  ○ …other
			• Jamf, Intune, Ansible, MaaS360 (Provide device information continuously, not just while device on NASA network)
			• Geolocation
			• PAW Tier Level
				On Mobile <or> Agents on Hosts/Endpoints
				• Application identity
				• Attestation of integrity
					<end point source>
					• Micro-perimeter network (higher score)
					• Trusted NASA network (higher score)
					• Corporate network
					• Internet at large (lower score)
					• Trusted Partner Network
					• IoT/OT Network
						SUBA/UEBA
						• Is the user /network agent behavior typical? (macro, high score, n.n std dev)
						• Is the user behaving as the user has historically behaved? (micro, high score)
						• Is the user exhibiting a new behavior pattern?(low score or access control exception)
						• Geovelocity Computation
							• Force Protection Conditions (FPCON)
							NORMAL
							ALPHA
							BRAVO
							CHARLIE
							DELTA
							• Known urgent risk with specific source network, hardware, software, or user community (macro)
							• APT case definition, e.g., [Windows Admin; Windows 7; ASB] (micro)
							• Targeted case definition, e.g., [C-Level; Macintosh; non-NASA source network, Financials] (micro)
								• Performs overall additive scoring
								• Applies case specific filtering
								• Provides dynamic remediation processing
									Supplies and/or inherits risk policy for access control
									• Policy (ies)
									• Policy Traceability
									• Security Categorization
									• Logical Level of Risk (LOR)

Use Case Problem Space

User Affiliation
Vetted NASA/Contractor
Vetted Federal/DoD Employee/Contractor
Commercial Partner (under Agreement)
Universities/Research Entity (under Agreement)
Int'l Space Entity (under Agreement)
Int'l Research Entity (under Agreement)
Public

User/Level Of Confidence
20
30
35
40
45
50
60
65
70
75

Citizenship
US
OK Countries
Designated Bad Countries

Credential (Authenticator)
NASA PIV
NASA ASB
NASA Token OTP
NASA Derived Credential
Registered PIV/CAC (AAL3)
Registered PIV-I (AAL TDB)
NASA Password/AAL1
NASA Guest Password
Federated Identity Cred (AALx)
Federated Identity Cred - Social Login
NASA Yubikey (AAL2/3)
Registered Derived Credential
Generic AAL1
Generic AAL2
Generic AAL3

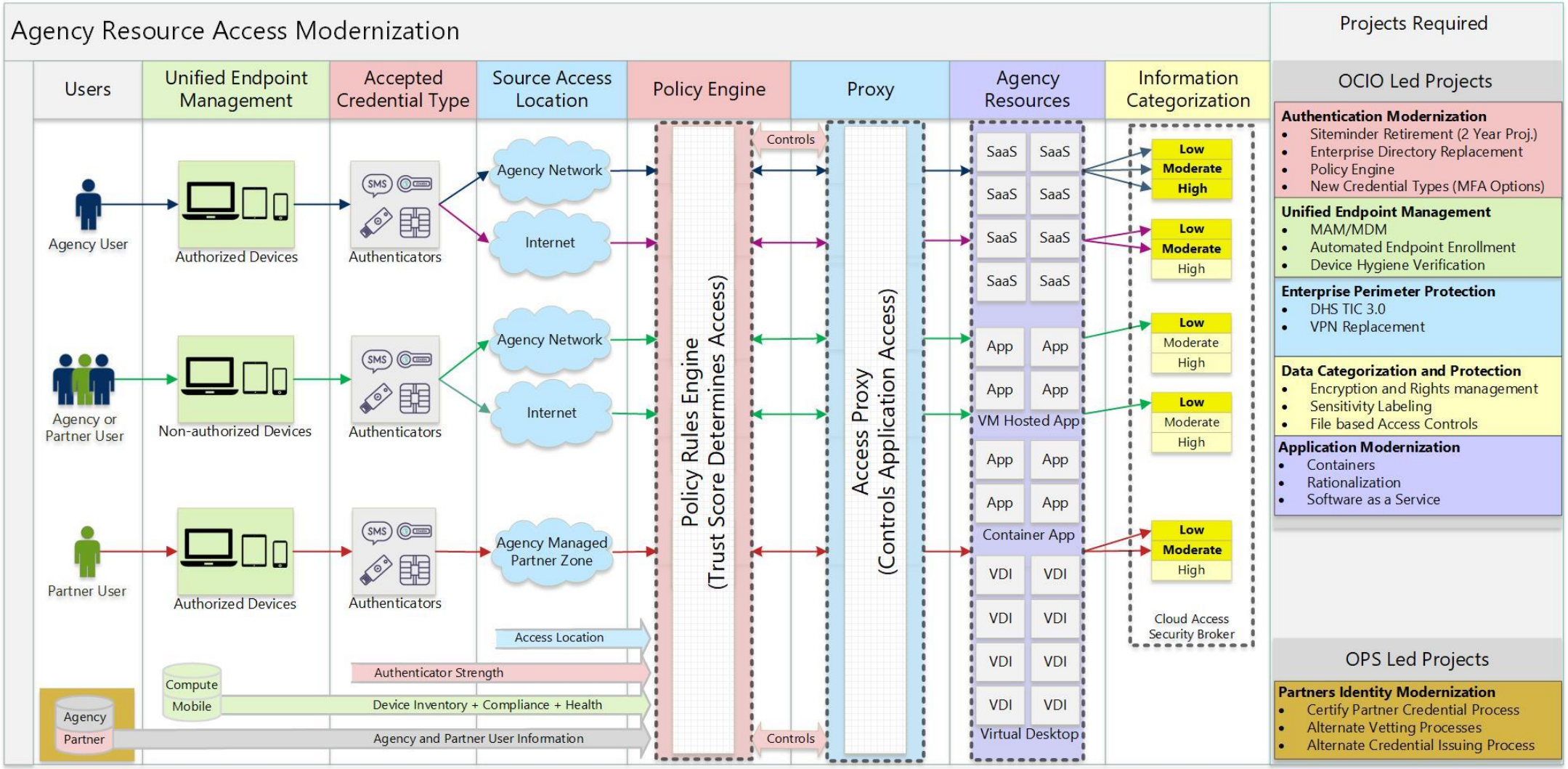
Device
NASA GFE
NASA Hygiene verified
Non-NASA Gov GFE
Unknown Hygiene
Non-NASA Hygiene Verified
Partner Provided
NASA VDS
NASA PAW

Network (Device Source Connection)
Direct Internal NASA Network
NASA Provided Partner Network (Zone)
NASA Provided Guest
Untrusted Domestic US
Untrusted World
Proxied via Software Defined Perimeter
Bridged / Dedicated Connection to Partner Network

Resource Types
File Shares
Collaboration Tools
Chat/IM
Web Applications
Code Repository
Large Data Sets
Drawings/Design
HVA
Mutual SaaS

Data Types
Low
Moderate
High
ITAR
EAR
SBU
Classified

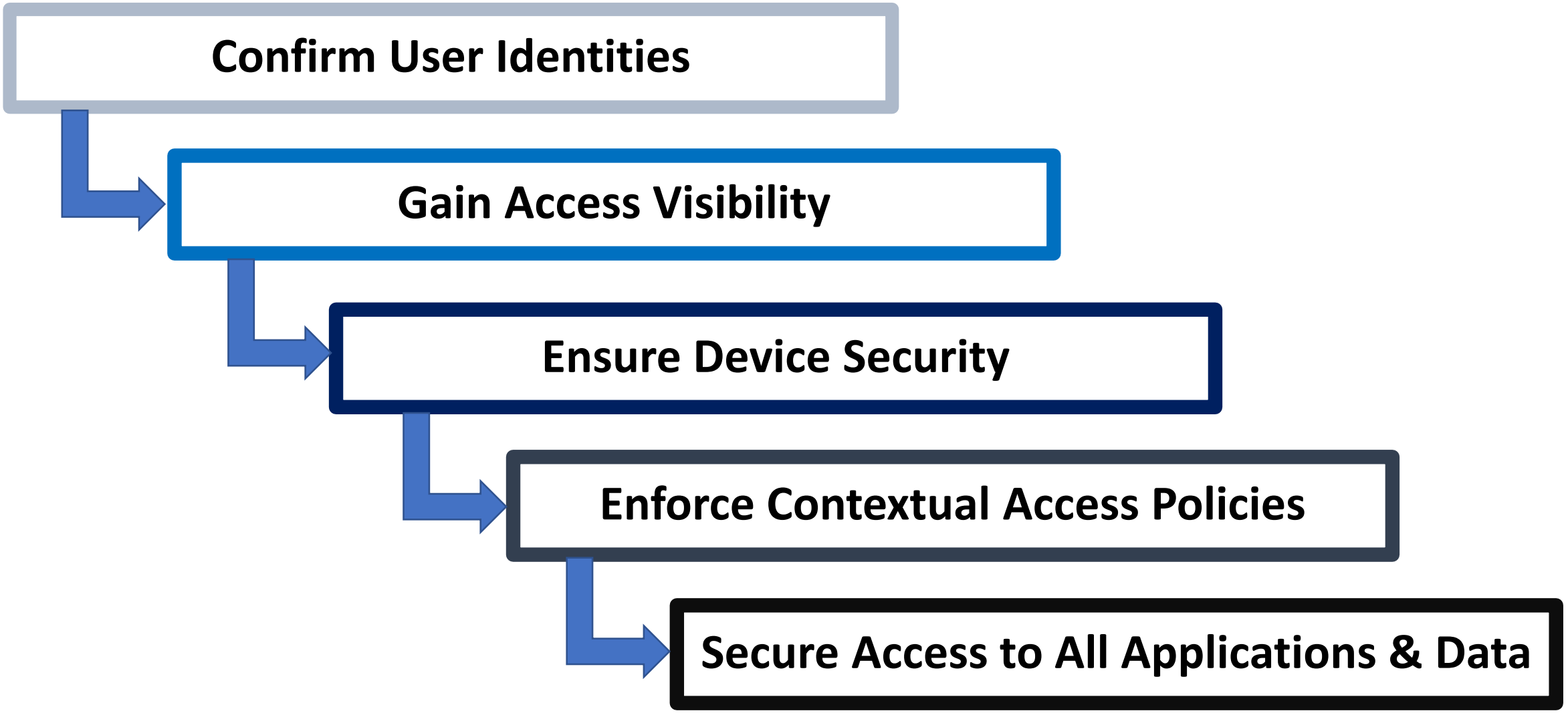
User and External Partner Use Case Flows



Value Proposition for NASA

- Alignment with NASA Strategic Plan regarding partner access, external collaboration and risk management
  - The Plan references “partner” 104+ times
  - Can effectively provides Partner Access Architecture/Standardization for secure collaboration
- Utilize strong NASA’s Identity Management program
- Holistic Risk-Based Access Management
  - Risk managed approach for authorizing access
  - Data centric approach with device (agnostic) trust scoring
- Support cybersecurity objectives for risk managed authorization of trusted devices
- Leverage NAC capabilities and incorporating Software Defined Network/Access
- Alignment with CDM DEFEND leveraging proposed NAC, identity and access management functionalities
- Considerations for program and mission support realignment objectives

Zero Trust Maturity Approach



Implementation Approach

- Zero Trust Architecture implemented through an integrated roadmap with phases synchronized access component areas
- Leverage the Agency's existing strong Identity Management capabilities for strong user identity verification & access management
  - Level of Confidence; develop LoC inference
  - High assurance credentials – PIV and ASB, looking support for issuing and accepting additional multi-factor (AAL2 and AAL3) authenticator types
  - Access Management/Entitlement management enhancements
  - Authentication Infrastructure Enhancements - Risk-Adaptable Access Control (RAdAC) and Conditional Access
- Gain visibility into device trust, usage and activity
  - Inspect devices for integrity & trust inference, establish trust criteria
  - Leverage Hardware and Application Resource inventory explore CDM DEFEND offerings
- Define adaptive rules and policies
- Enhance endpoint configuration management and device trust inference capabilities

Requires Support of all CIO Organizations

Communication/Network Services

- Internal Border Network Access Control
- External Perimeter/Software Defined Perimeter/TIC 3.0
- Network Macro and Micro Segmentation
- Software Defined Network/Access (SD-N/SD-A)

Computing Services

- Cloud Access Security Broker for IaaS
- Cloud Privileged Access Management
- Enterprise Device Configuration Management

Information Services

- Data Standards/Categorization
- Data Centric Security
- Data Tagging
- Sensitive Data Identification

Operational Technology / Internet of Things

- Identity of Things (physical protection, cameras, etc.)
- Mission Facility Infrastructure
- Robots, Space Probes, Drones, Rovers

End User Services/Endpoint Devices

- Strong Authentication
- Device Attestation
- Enterprise Device Configuration Management
- Virtual Desktop Services

Applications

- Containerization
- Application Access Policy
- Secure PaaS and SaaS

Cybersecurity and Privacy

- Identity, Credential and Access Management Services – Central Web AuthN Services, Device Certs, RAdAC, new credential types
- Agency Security Configuration Standards
- Continuous Diagnostics and Mitigation – HWAM & SWAM
- Trust Inference Engines, Heuristic analysis/feedback loops
- Device Trust Scoring and Access Authorization Rules
- Breach Detection/Data Loss Prevention
- Endpoint Threat Detection and Response
- Splunk User and Entity Behavior Analytics

Proposed Initial Development Areas

- Privileged Access
  - Privileged Access Workstations
  - Privileged Access Network Segmentation
  - High Value Assets
- Software Defined Access – Attribute-based network micro-segmentation
- Software Defined Perimeter based access
- Mobile Devices – GFE, Partner Furnished, Personally Owned with enterprise mobile applications management
- Device Trust Inference, Measurement, Calibration and Algorithms
- User Level of Trust Inference – Security User Behavior Analytics (SUBA)
- Develop requirements/user stories for Authentication Infrastructure Modernization
- Develop continuous Multi-Factor Authentication capabilities
- Develop a proof of concept lab for Zero Trust technology evaluation
  - Create extended lab environment between ICAM Services, Cybersecurity Engineering, Communications Services and Cloud Services Offices.

Implementation Challenges

- NASA cybersecurity implementations has had a heavy emphasis on network layer based controls vs. overall security architecture with identity-based access control
- VPN mandate will continue to be an obstacle for partner access and external collaboration
- SSL content inspection breaks traffic flow and impacts many transaction patterns
- Strategically implement TIC point requirements – must align DHS TIC 3.0 and Cloud Smart with Zero Trust defined target state
- Test Bed/Proof of Concept dependency on evolving production capabilities
- Agency ICAM engineering and development resources are overburdened with a large backlog due to continually having to address gaps in other OCIO service domains
- External Partner user identity data and vetting; additional complexity with agreements

Summary

- Zero Trust is a broader access management strategy that the initial emphasis on network access
- Agency ICAM Services provides significant portion of the required identity and access management services and infrastructure
- Emphasis is on **trust** of people and devices for identity-based/risk-managed access to data and applications
- Software Defined Networking/Access is supportive of a Zero Trust Architecture, but only a portion of the complete infrastructure and services design
- Recommendations
  - Do not pick a solutions/vendors too early
  - Do not get locked into a single vendor solution for the overall implementation
  - Focus on developing support for mobile device and external partner access to provide more immediate benefits
  - Align strategic investment decisions with an evolving Zero Trust Architecture

Questions and Comments