CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM ICAM UPDATE

ROSS FOARD
CISA ARCHITECTURE AND ENGINEERING
CENTER OF EXCELLENCE

Presenter

- Over 20 years of public sector and commercial cybersecurity and identity and access management experience
- Supports DHS' Cybersecurity and Infrastructure Security Agency (CISA) as a senior engineer in the Architecture and Engineering Center of Excellence (A&E COE)
- Ross is responsible for architecture and technical integration of Identity and Access Management, Cryptography, Data Protection and Zero Trust Architectures
- Co-lead on the Federal Mobility Group (FMG) Derived PIV Working Group (DPIVWG)

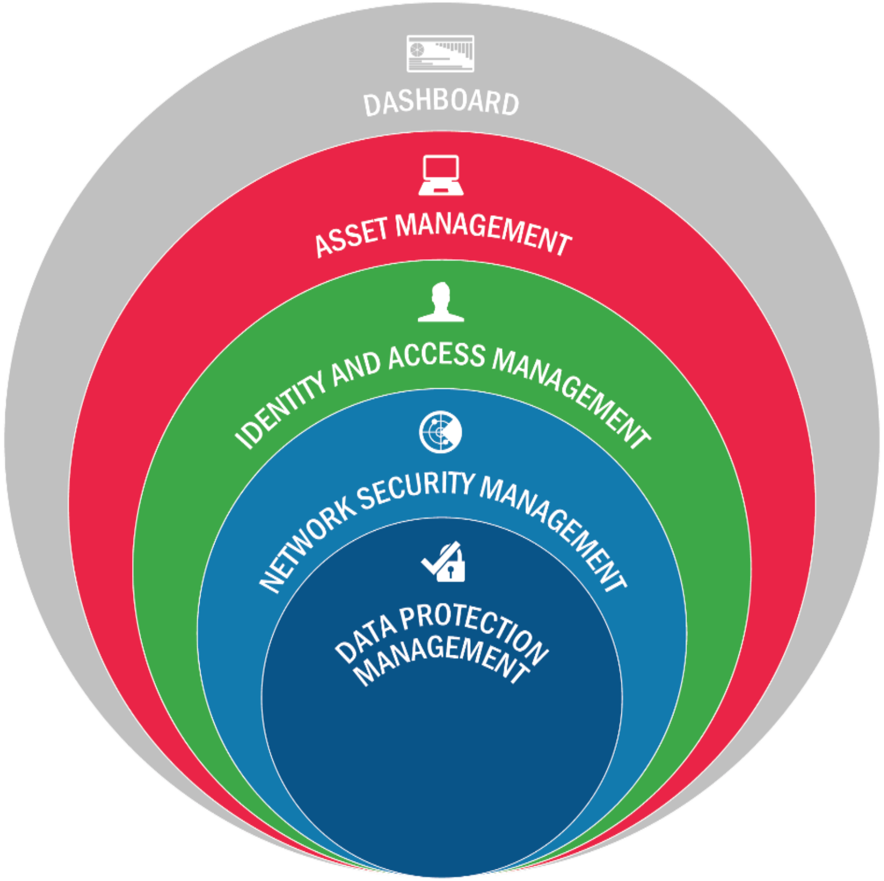
Ross Foard
IT Specialist (INFOSEC)
CISA

Agenda

- About me
- Review where we were when we last spoke FedID 2019
- The CDM Program ICAM Capabilities current
- Where ICAM needs to go under EO 14028 – Zero Trust Architecture
- What is Zero Trust and how does it differ from Perimeter-based security?
- How is Federal Identity, Credential, and Access Management (FICAM) changing to support ZTA?
- Strengthening MFA as the Architecture and Technologies Evolve
- For Many Agencies a Hybrid Solution Architecture Next
- Notional Identity-centric Zero Trust Architecture
- Contact Information

2019 Introduced CDM ICAM

- **FedID 2019** – A cross-agency panel discussed CDM and Federal ICAM partnership
- **Agency and Federal Dashboards** – Provide risk information about the .gov space
- **Asset Management** – Hardware, software, vulnerabilities and configurations
- **Identity and Access Management** – Users Accounts and associated vetting and privileges
- **Network Security Management** – Incident response, ongoing assessments and authorization, boundary protections and building in security
- **Data Protection Management** – Future implementations will provide security to data assets


DASHBOARD
ASSET MANAGEMENT
IDENTITY AND ACCESS MANAGEMENT
NETWORK SECURITY MANAGEMENT
DATA PROTECTION MANAGEMENT

2023 CDM Program Capabilities look very similar

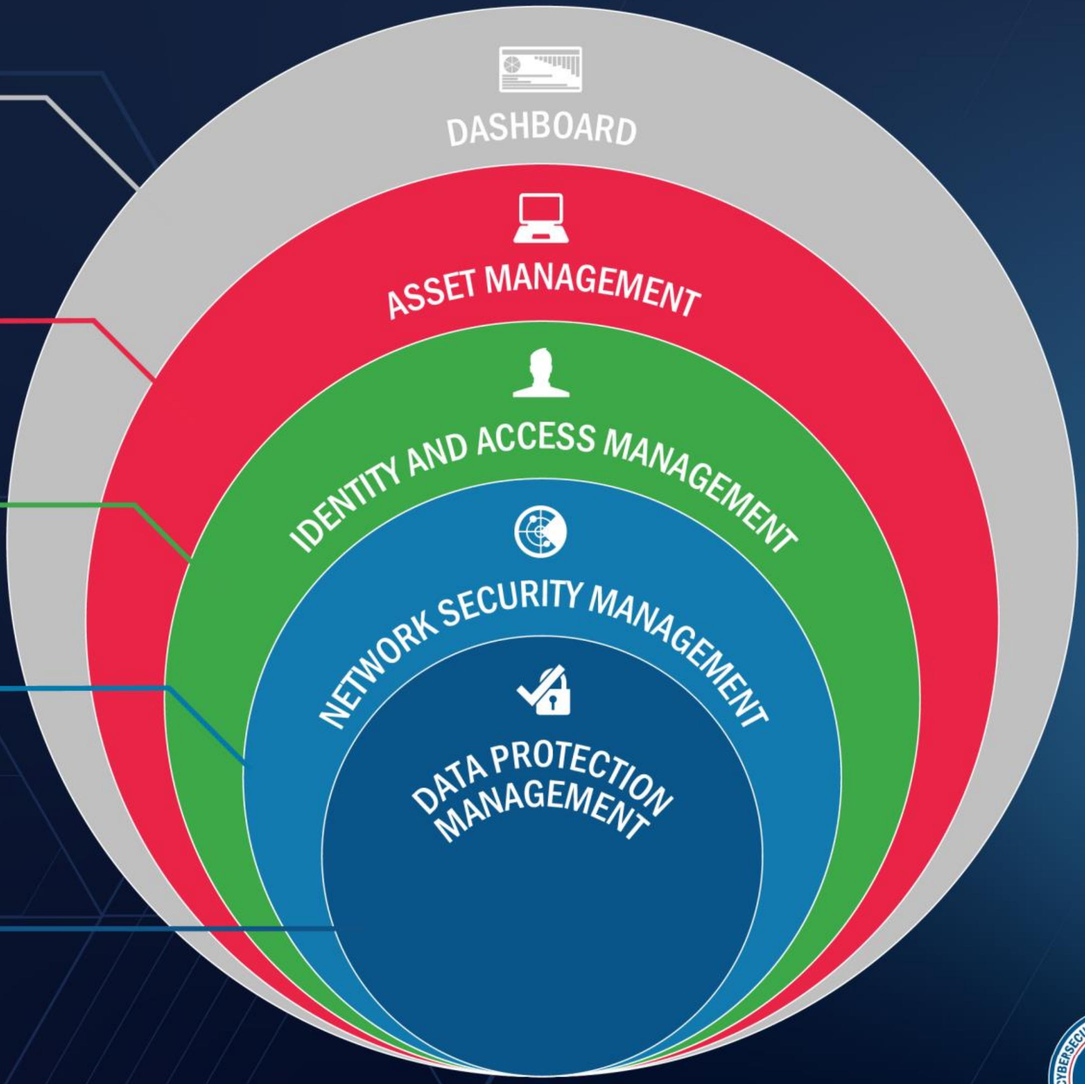
Agency and Federal Dashboards
Visualization tool to better understand, prioritize, and mitigate cyber risks.

Asset Management
What is on the network?

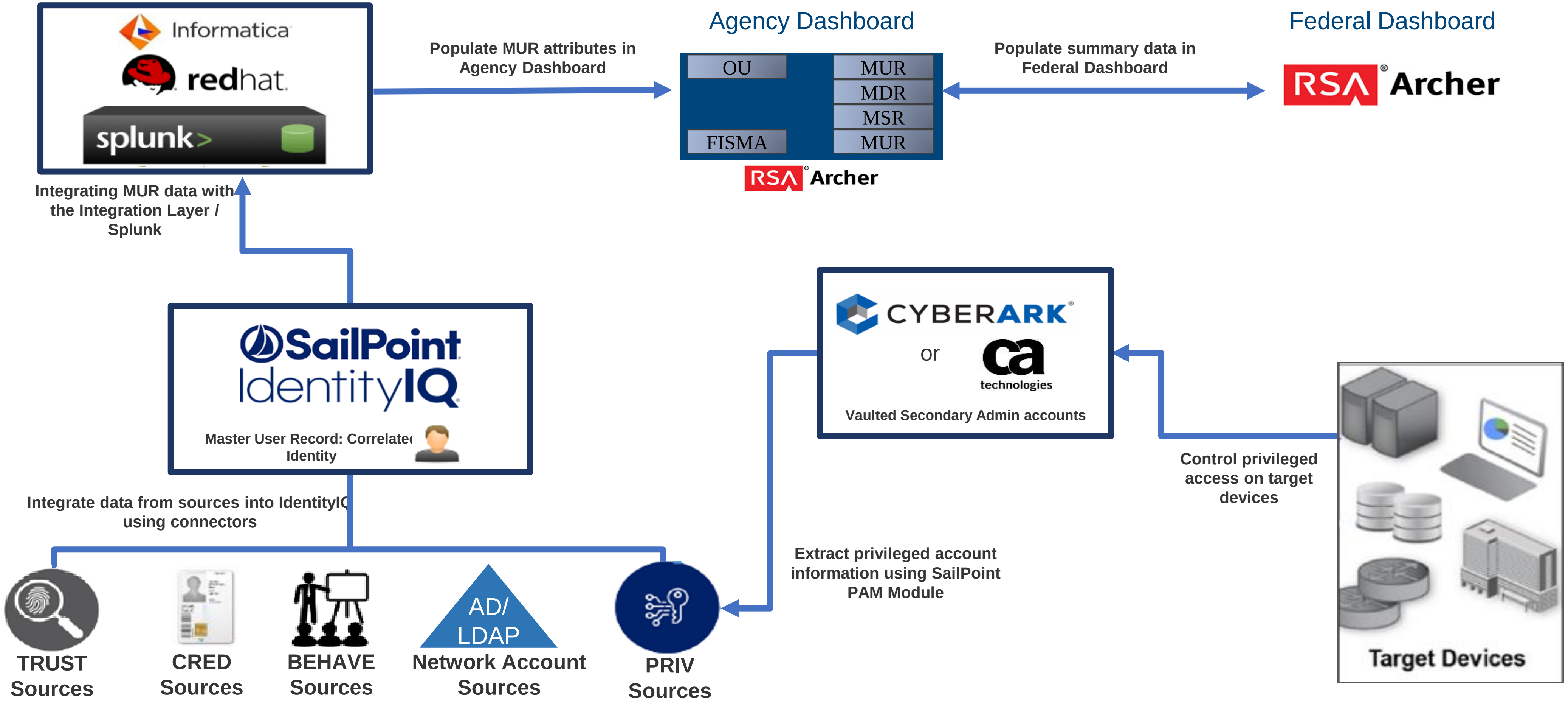
Identity and Access Management
Who is on the network?

Network Security Management
What is happening on the network?
How is the network protected?

Data Protection Management
How is data protected?


DASHBOARD
ASSET MANAGEMENT
IDENTITY AND ACCESS MANAGEMENT
NETWORK SECURITY MANAGEMENT
DATA PROTECTION MANAGEMENT

2019 CDM IAM Notional Architecture



Agency Dashboard

Federal Dashboard

Populate MUR attributes in Agency Dashboard

Populate summary data in Federal Dashboard

Integrating MUR data with the Integration Layer / Splunk

Master User Record: Correlated Identity

or

Vaulted Secondary Admin accounts

Control privileged access on target devices

Integrate data from sources into IdentityIQ using connectors

Extract privileged account information using SailPoint PAM Module

TRUST Sources

CRED Sources

BEHAVE Sources

Network Account Sources

PRIV Sources

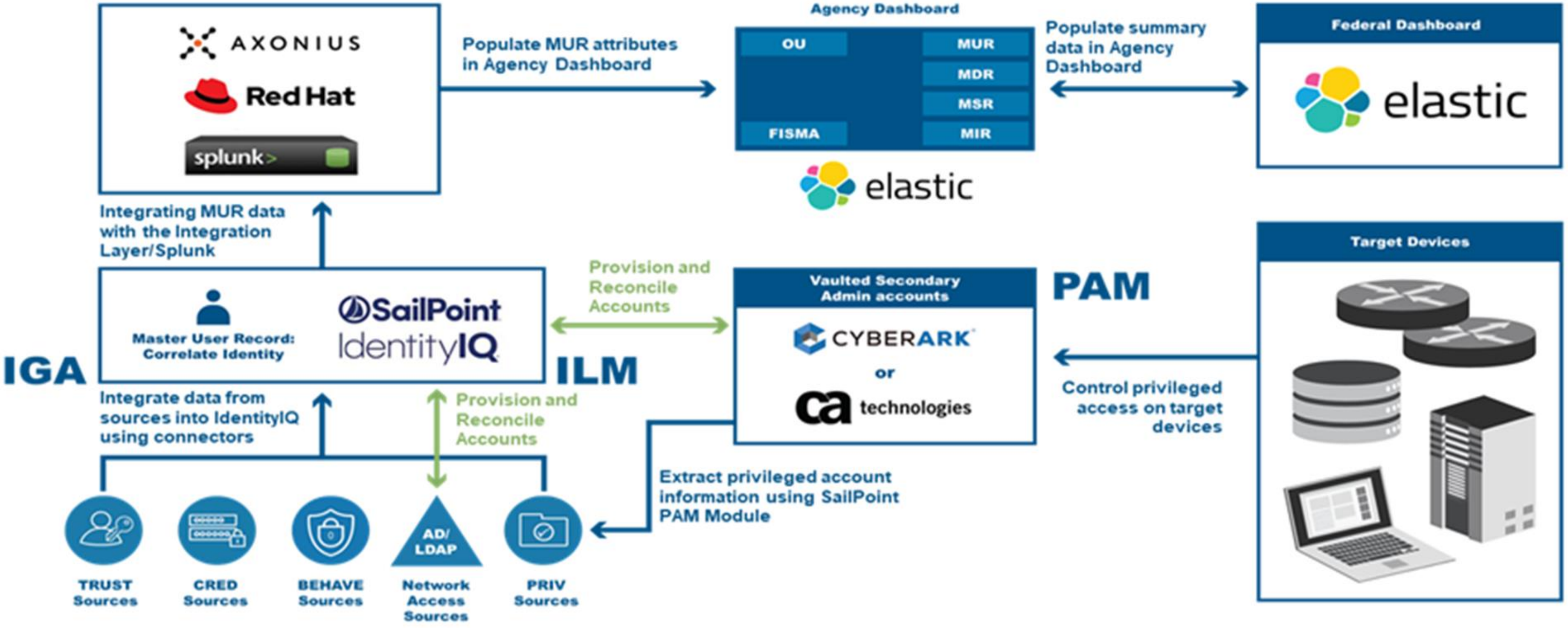
Target Devices

Current CDM ICAM – Expanded PAM, ILM and Dashboard

MUR information is available in the CDM Dashboards – Now in the Elastic Stack

CISA has helped Agencies establish a Master User Record (MUR) and manage Lifecycle of users

CRED enumerates the authenticators users have


AXONIUS
Red Hat
splunk>
Populate MUR attributes in Agency Dashboard
Agency Dashboard
OU
MUR
MDR
MSR
FISMA
MIR
elastic
Populate summary data in Agency Dashboard
Federal Dashboard
elastic
Integrating MUR data with the Integration Layer/Splunk
Master User Record: Correlate Identity
SailPoint IdentityIQ
IGA
ILM
Provision and Reconcile Accounts
Vaulted Secondary Admin accounts
CYBERARK
or
ca technologies
PAM
Target Devices
Control privileged access on target devices
Integrate data from sources into IdentityIQ using connectors
Provision and Reconcile Accounts
Extract privileged account information using SailPoint PAM Module
TRUST Sources
CRED Sources
BEHAVE Sources
AD/ LDAP
Network Access Sources
PRIV Sources

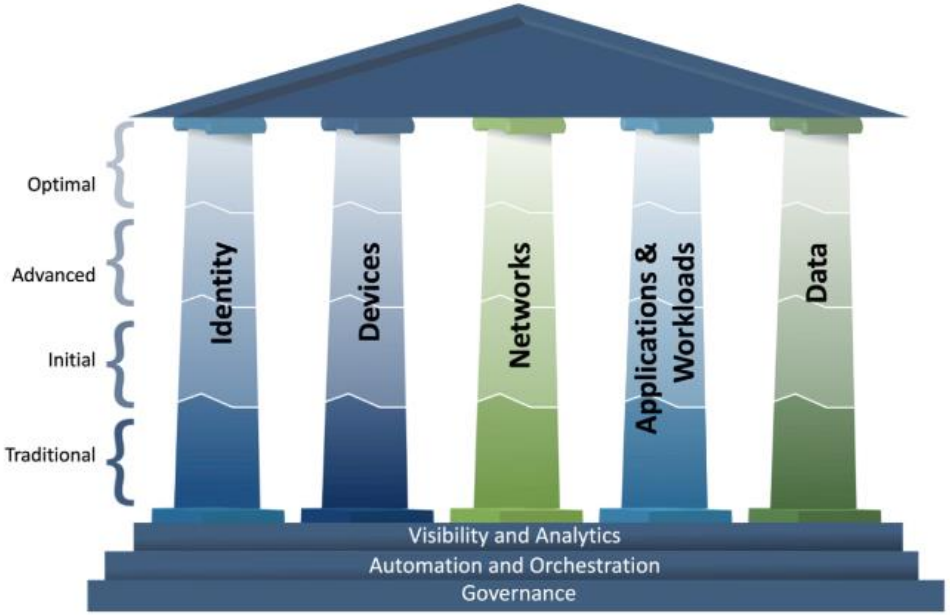
Increased focus on Identity Lifecycle Management of users

CISA has helped Agencies manage Privileged Users through Privileged Access Management tools

Where ICAM Needs to Go – Zero Trust Architecture

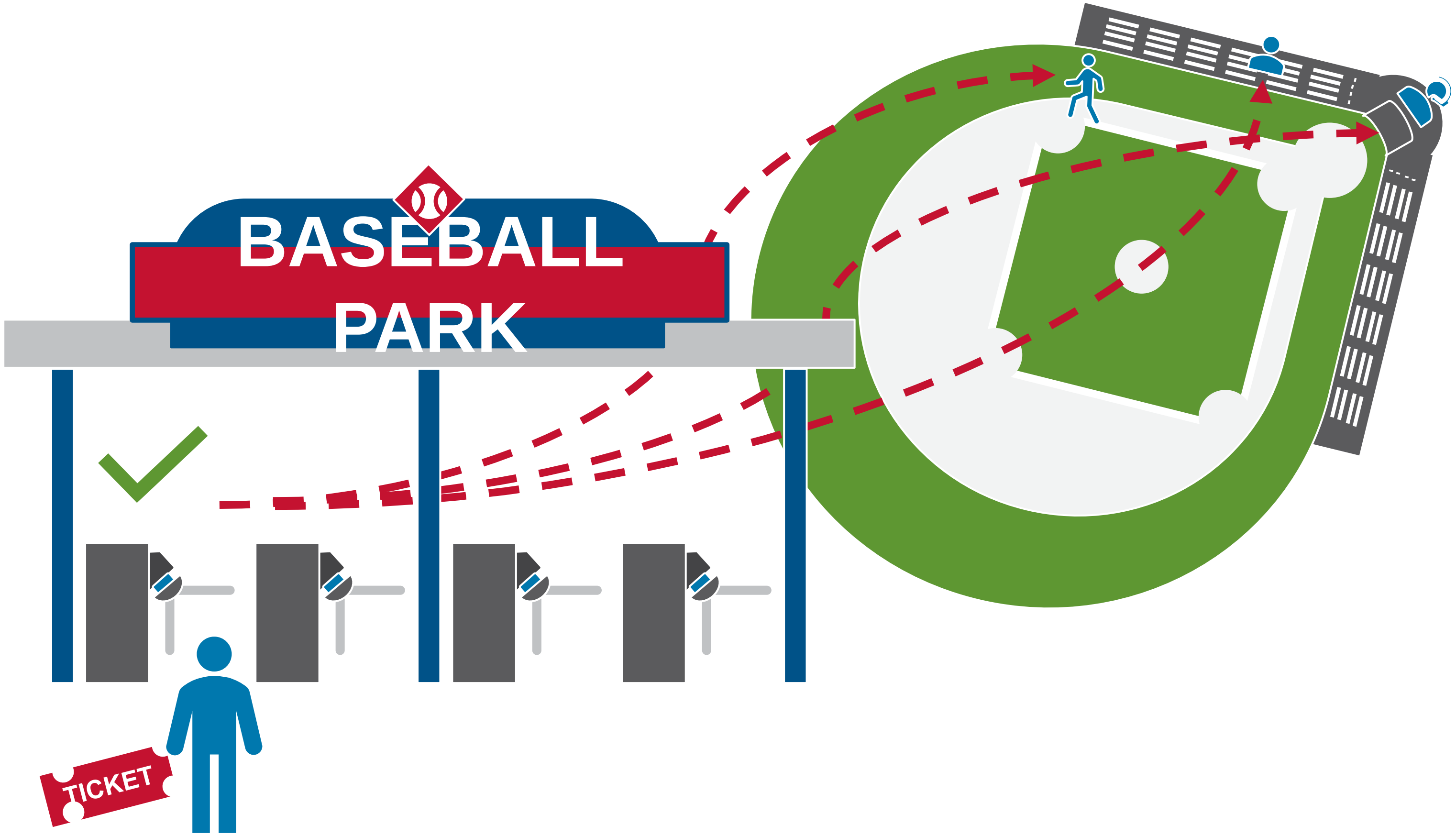
CISA and the Office of Management and Budget (OMB) supports this strategy through OMB memos M-19-17, M-22-09, and by conducting CyberStat meetings with agencies and publishing guidance.

- Published at zerotrust.cyber.gov and www.cisa.gov/resources-tools
  - CISA developed and updated the Zero Trust Maturity Model
  - CISA developed Cloud Security Technical Reference Architecture (TRA)
  - CISA developed the SCUBA Hybrid Identity Solutions Architecture



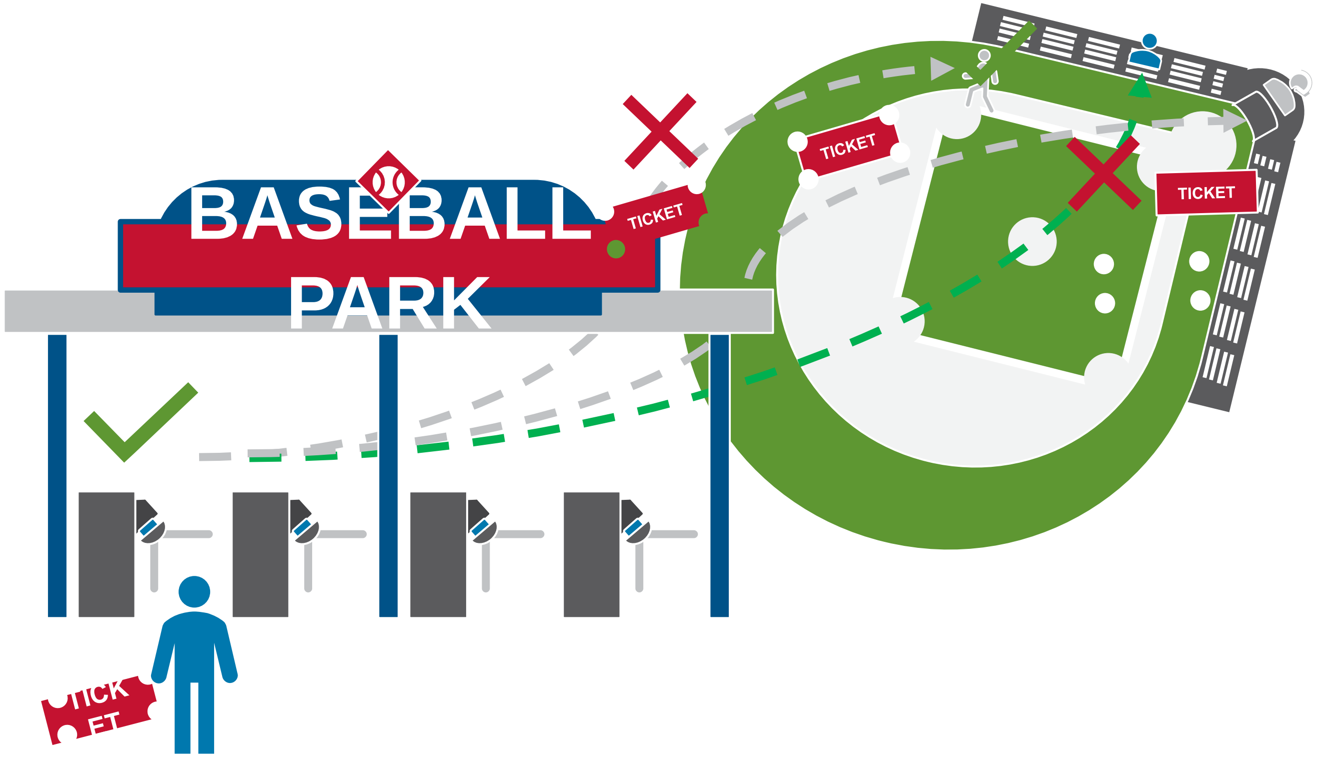
Traditional Perimeter-Based Security

- Only show your ticket once
- No other validation to ensure you only go where you're allowed
- Trust is implicit



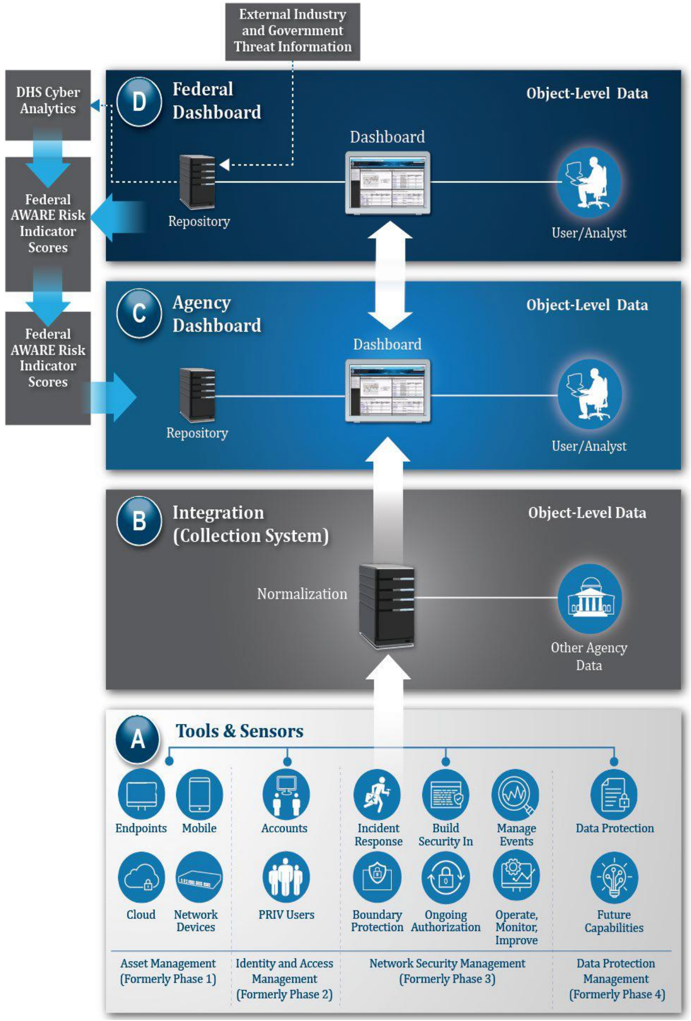
Zero Trust at the Ballpark

- Several checkpoints throughout the park for validation
- Integrated security
- Trust must be verified at each access
- More granular access controls



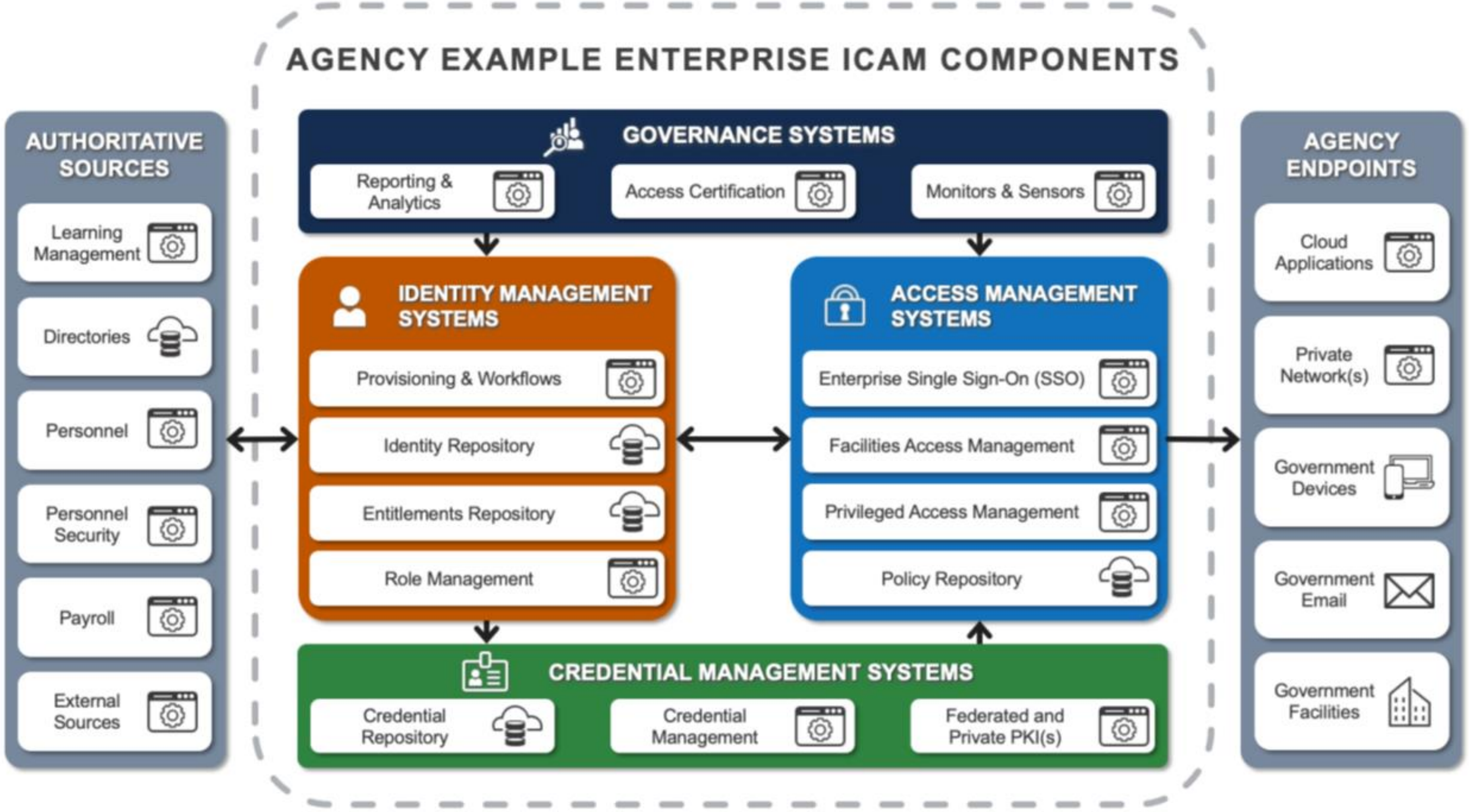
CDM Future – A “New era” for CDM

- CDM’s DEFEND task orders are nearing completion
- CDM has updated Technical Requirements in Version 2.5
  - Critical Asset Management requirements identified.
  - Updates to IDAM and EDR.
  - OMI and OAS removed as unique CDM Layer A functions
  - Data Protection Management (DPM) updated



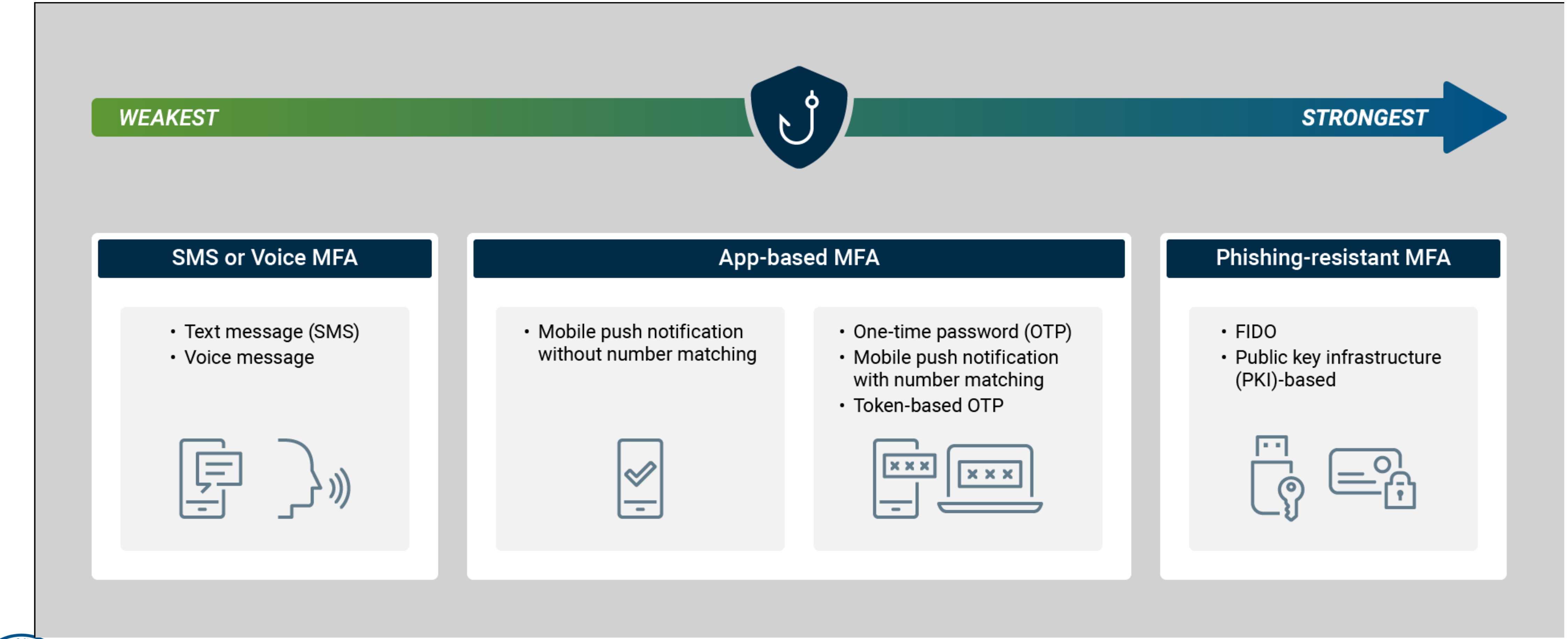
Federal ICAM – Essential to Zero Trust

Federal ICAM has always been about ensuring the right user has access to the right resource at the right time and only that necessary to perform the mission



https://playbooks.idmanagement.gov/

CISA helps Agencies understand MFA options



WEAKEST → STRONGEST

SMS or Voice MFA

- Text message (SMS)
- Voice message

App-based MFA

- Mobile push notification without number matching

- One-time password (OTP)
- Mobile push notification with number matching
- Token-based OTP

Phishing-resistant MFA

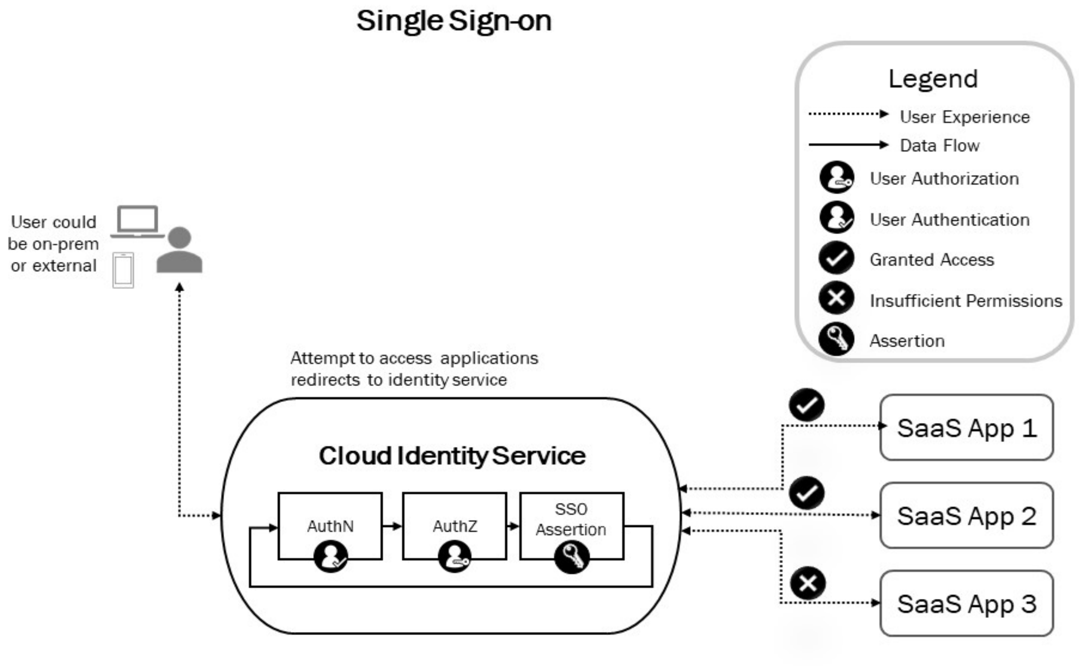
- FIDO
- Public key infrastructure (PKI)-based

MFA are most valuable in Single Sign-On Services

- Modern Single Sign-On services enable enforcement of a strong phishing-resistant multi-factor authenticator

- Modern protocols SAML and OIDConnect are the most widely used protocols supporting SSO

- User authorization decisions are made based upon the policy regarding the user’s role in the agency, and other context



Single Sign-on

Legend

User Experience

Data Flow

User Authorization

User Authentication

Granted Access

Insufficient Permissions

Assertion

User could be on-prem or external

Attempt to access applications redirects to identity service

Cloud Identity Service

AuthN

AuthZ

SSO Assertion

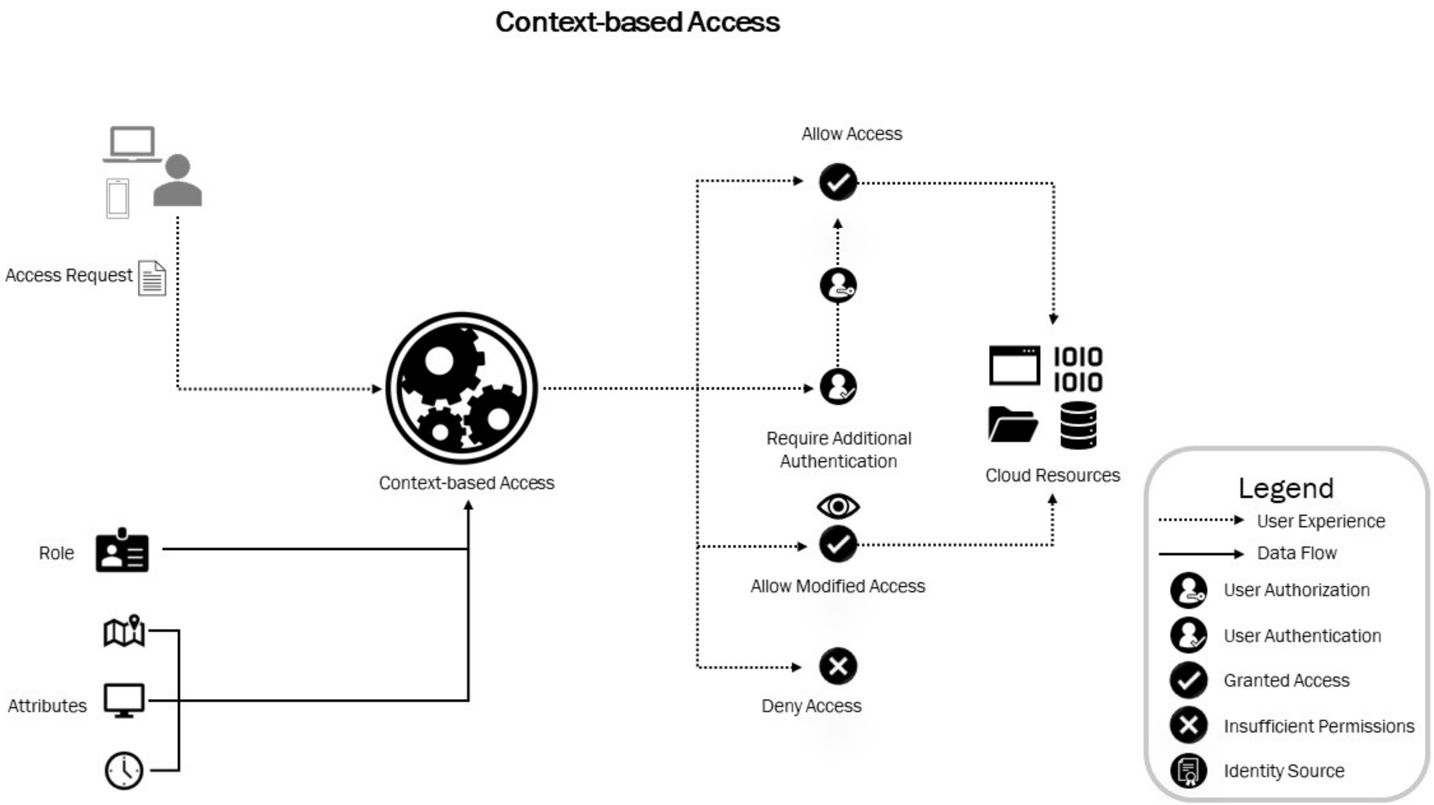
SaaS App 1

SaaS App 2

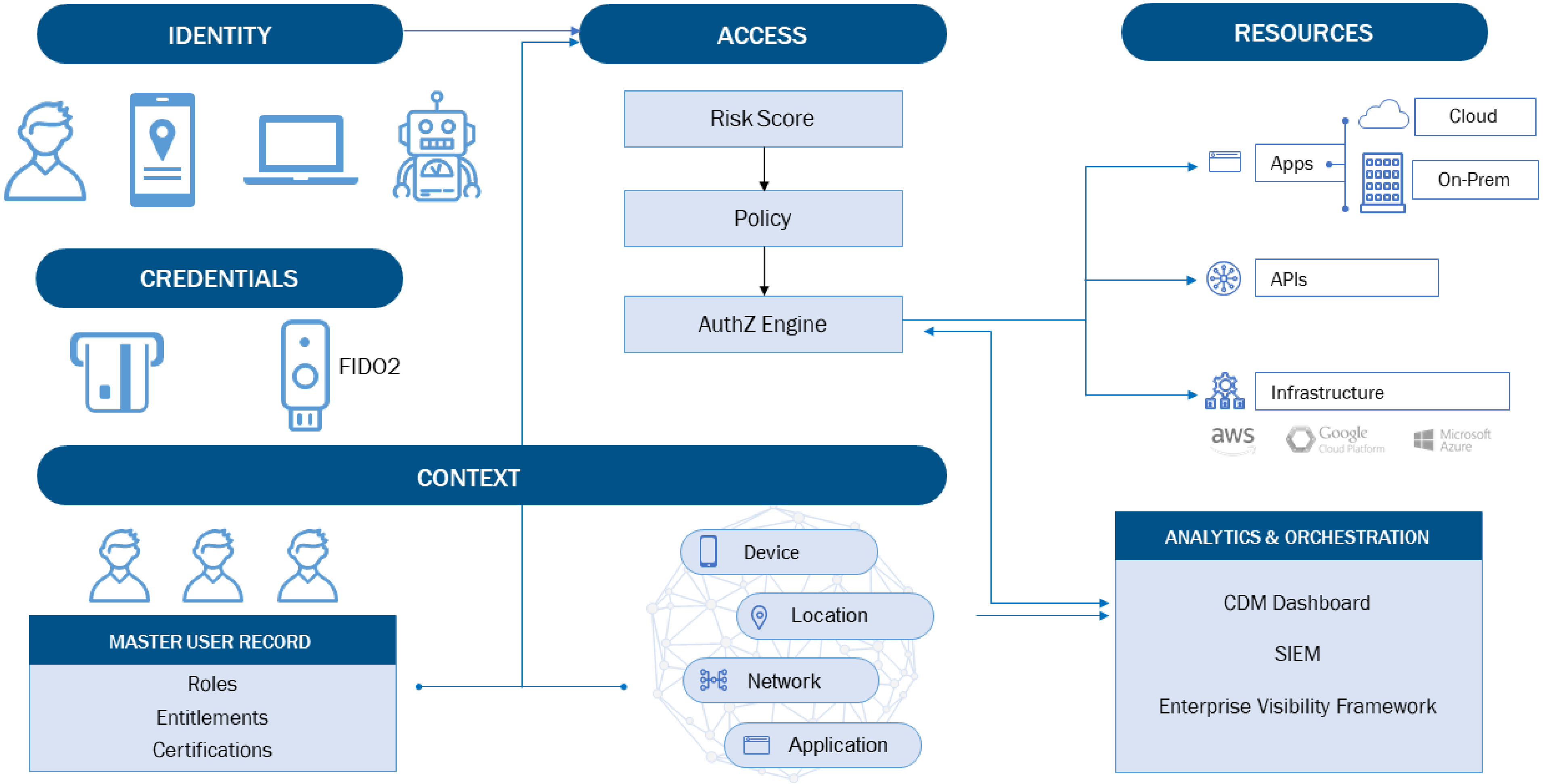
SaaS App 3

CISA SCUBA Hybrid Identity Solutions Architecture

Context-based access control (CBAC) is a method of access control that combines features of role-based access control (RBAC) and attribute-based access control (ABAC) to apply dynamic access policies using device-level signals as cues.



Identity Centric Zero Trust Architecture



IDENTITY

CREDENTIALS

FIDO2

CONTEXT

MASTER USER RECORD

Roles

Entitlements

Certifications

Device

Location

Network

Application

ACCESS

Risk Score

Policy

AuthZ Engine

RESOURCES

Apps

Cloud

On-Prem

APIs

Infrastructure

ANALYTICS & ORCHESTRATION

CDM Dashboard

SIEM

Enterprise Visibility Framework

Information

- For more information:
  - ross.foard@cisa.dhs.gov
    (ICAM and Zero Trust SME)
  - www.cisa.gov/cdm
    (Program Information)
  - www.gsa.gov/cdm
    (Acquisition Information)
  - www.us-cert.gov/cdm/training
    (Training Information)
  - https://community.max.gov/pages/viewpage.action?pageId=1086358530
    (Program Information on OMB MAX)

- For questions:
  - CDM@cisa.dhs.gov
    (CDM Program Questions)
  - CSD_CB_AcqBudg@cisa.dhs.gov
    (CDM Acquisition Questions)
  - CyberInsights@hq.dhs.gov
    (CDM Training Questions)
  - ICAM@gsa.gov
  - Identity Assurance and Trusted Access Division

Thank You!