DOD Endpoint Security Strategy and Evolution of Continuous Monitoring and Risk Scoring

May 8, 2025

Brian Hennigan/J.C. Wilson

DISA PEO-CYBER, ENDPOINT SECURITY DIVISION (ID3)

Agenda

- Endpoint Security Landscape
- Evolving Continuous Monitoring and Risk Scoring to a New Reality
- CMRS Today
- Microsoft Defender for Endpoint (MDE) Challenge – Secure Endpoint Data Reporting (SEDR)
- Evolving CMRS

Endpoint Security Landscape

Fewer Dictated Tools, More Choice

- The DoD CIO Endpoint Security Framework seeks to shift from a singular mission specific enterprise solutions to a data-centric capability to modernize endpoint security.

Data and Functional Requirements

- As the Department moves towards a data-centric model for defending the DODIN, and a decentralized approach for procuring endpoint security capabilities, it is imperative to address functional requirements, data standards for publishing data, an implementation plan, and a roadmap.

Disparate and Changing Tools are a Challenge to Achieving a Complete Endpoint Data Picture

- DISA and DoD CIO seek to provide a roadmap for enabling greater interoperability and component choice of solutions while providing operational flexibility to enable agile, interoperable, and resilient endpoint defenses.

Endpoint Security Minimum Data Standards

DOD CIO CS released “Endpoint Security Minimum Data Standards” 7 Sep 23 with updated Master Data Endpoint Record (MDER)

The MDER is comprised of 180+ data elements broken down in seven categories:

- Network (32)
- Hardware Configuration (50)
- Software Configuration (19)
- Organization Context (20)
- Vulnerability Compliance (24)
- User Data (20)
- Security Products (17)

What is Continuous Monitoring and Risk Scoring ?

CMRS

Historically aggregates data from DoD endpoint tools (ESS, ACAS, C2C, MDE+, Thunderdome) for near real-time risk assessment and continuous monitoring of DoD assets' security including JFHQ-DODIN's mission to secure and defend the DODIN mission area (NCAS, CORA) and automates support for DCIO's Congressional reports (FISMA, FITARA)

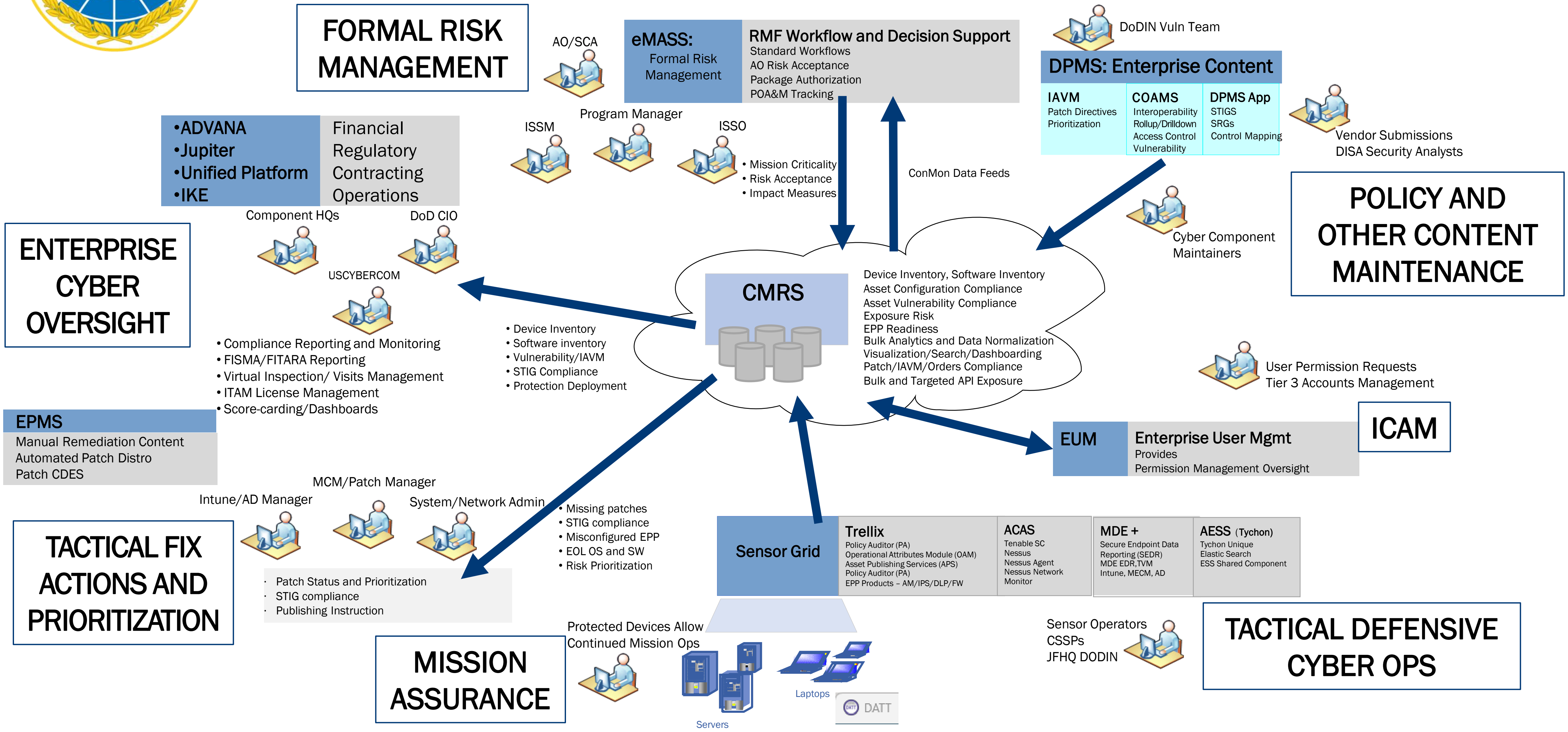
Operational Value

- DoD requires understanding of cybersecurity risk from an asset vulnerability and configuration perspective
- System owners require visibility into asset vulnerabilities and configuration that enables prioritized remediation

CMRS 1.0 Limitations

- Inefficient data brokerage
- 2–4 month development/testing cycle for new toolsets
- Large server footprint and maintenance costs
- Legacy Government Off The Shelf (GOTS)

Today’s CMRS Operational View



FORMAL RISK MANAGEMENT

AO/SCA

eMASS: Formal Risk Management

RMF Workflow and Decision Support
Standard Workflows
AO Risk Acceptance
Package Authorization
POA&M Tracking

ISSM

Program Manager

ISSO

- Mission Criticality
- Risk Acceptance
- Impact Measures

ConMon Data Feeds

DoDIN Vuln Team

DPMS: Enterprise Content

IAVM	COAMS	DPMS App
Patch Directives Prioritization	Interoperability Rollup/Drilldown Access Control Vulnerability	STIGS SRGs Control Mapping

Vendor Submissions
DISA Security Analysts

POLICY AND OTHER CONTENT MAINTENANCE

Cyber Component Maintainers

- ADVANA
- Jupiter
- Unified Platform
- IKE

Financial
Regulatory
Contracting
Operations

Component HQs

DoD CIO

USCYBERCOM

ENTERPRISE CYBER OVERSIGHT

- Compliance Reporting and Monitoring
- FISMA/FITARA Reporting
- Virtual Inspection/ Visits Management
- ITAM License Management
- Score-carding/Dashboards

- Device Inventory
- Software inventory
- Vulnerability/IAVM
- STIG Compliance
- Protection Deployment

CMRS

Device Inventory, Software Inventory
Asset Configuration Compliance
Asset Vulnerability Compliance
Exposure Risk
EPP Readiness
Bulk Analytics and Data Normalization
Visualization/Search/Dashboarding
Patch/IAVM/Orders Compliance
Bulk and Targeted API Exposure

User Permission Requests
Tier 3 Accounts Management

ICAM

EUM

Enterprise User Mgmt
Provides
Permission Management Oversight

EPMS
Manual Remediation Content
Automated Patch Distro
Patch CDES

MCM/Patch Manager

Intune/AD Manager

System/Network Admin

TACTICAL FIX ACTIONS AND PRIORITIZATION

- Missing patches
- STIG compliance
- Misconfigured EPP
- EOL OS and SW
- Risk Prioritization

- Patch Status and Prioritization
- STIG compliance
- Publishing Instruction

Sensor Grid

Trellix	ACAS	MDE +	AESS (Tychon)
Policy Auditor (PA) Operational Attributes Module (OAM) Asset Publishing Services (APS) Policy Auditor (PA) EPP Products – AM/IPS/DLP/FW	Tenable SC Nessus Nessus Agent Nessus Network Monitor	Secure Endpoint Data Reporting (SEDR) MDE EDR,TVM Intune, MECM, AD	Tychon Unique Elastic Search ESS Shared Component

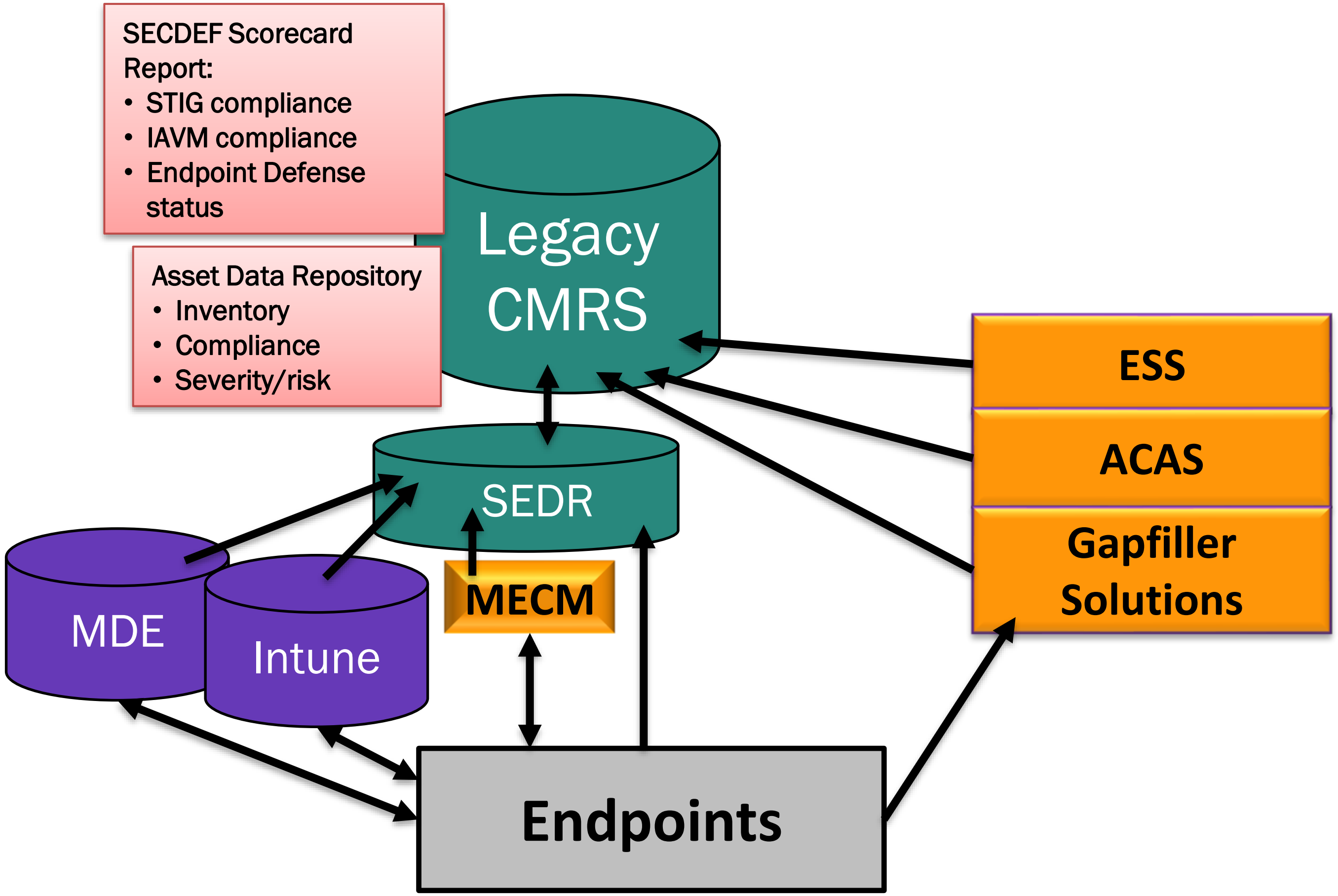
MISSION ASSURANCE

Protected Devices Allow
Continued Mission Ops

Sensor Operators
CSSPs
JFHQ DODIN

TACTICAL DEFENSIVE CYBER OPS

CHALLENGE #1 – Microsoft Defender for Endpoint



Legend

Purple: Cloud Native Applications

Light Green: GOTS Applications

Gold: Commercial Products

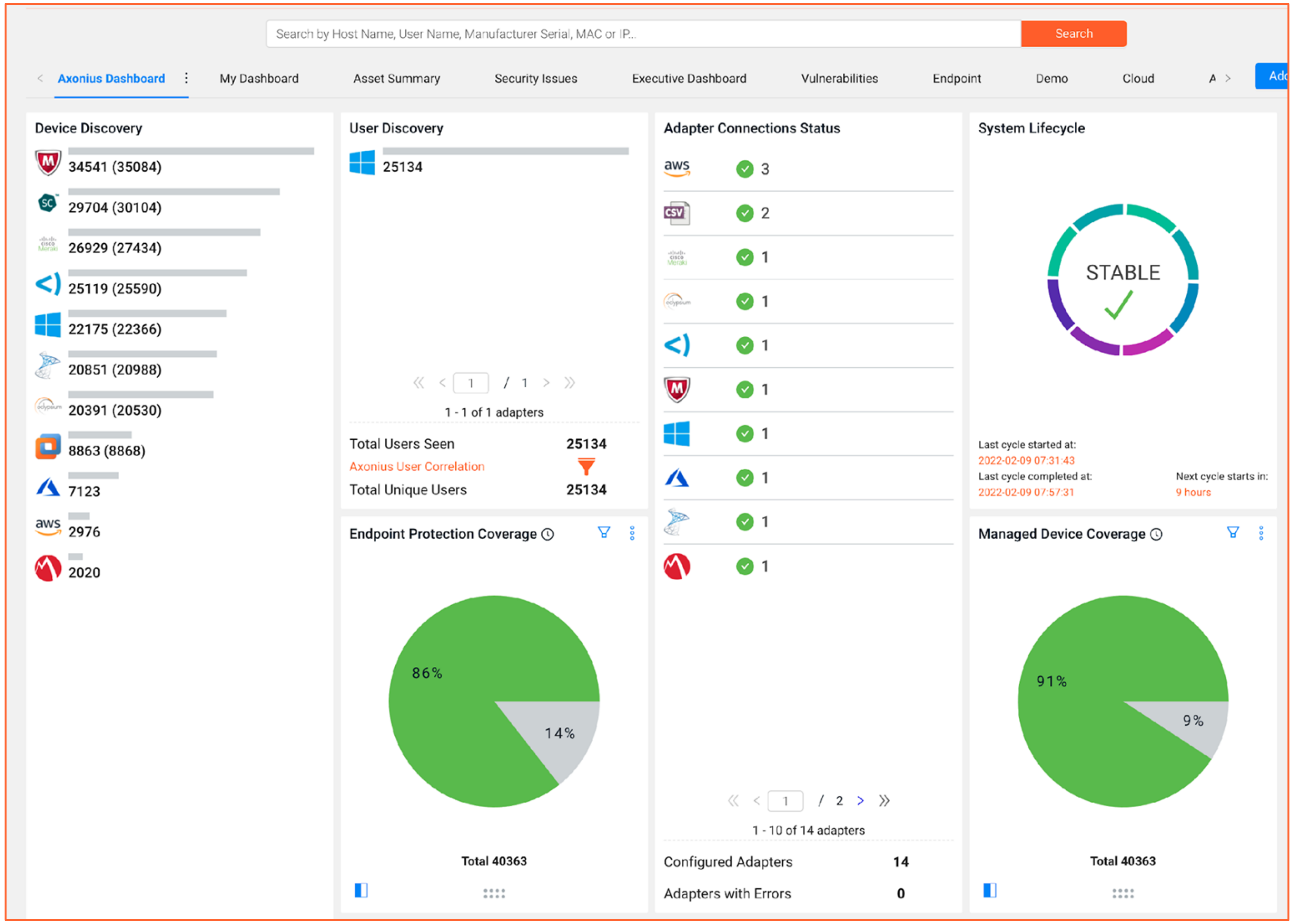
Gray: Managed Systems

Pink: User Interfaces

CMRS Modernization Approach

Leverage a modern tool to connect 1000+ data sources that enable customers to:

- Get a credible, comprehensive inventory of all devices, users, cloud assets, and SaaS apps
- Discover coverage gaps and risk
- Validate and enforce policies



Device Discovery

34541 (35084)
29704 (30104)
26929 (27434)
25119 (25590)
22175 (22366)
20851 (20988)
20391 (20530)
8863 (8868)
7123
2976
2020

User Discovery

25134

1 / 1

1 - 1 of 1 adapters

Total Users Seen	25134
Axonius User Correlation	
Total Unique Users	25134

Adapter Connections Status

aws	3
CSV	2
	1
	1
	1
	1
	1
	1
	1
	1

1 / 2

1 - 10 of 14 adapters

Configured Adapters	14
Adapters with Errors	0

System Lifecycle

Last cycle started at:
2022-02-09 07:31:43
Last cycle completed at:
2022-02-09 07:57:31
Next cycle starts in:
9 hours

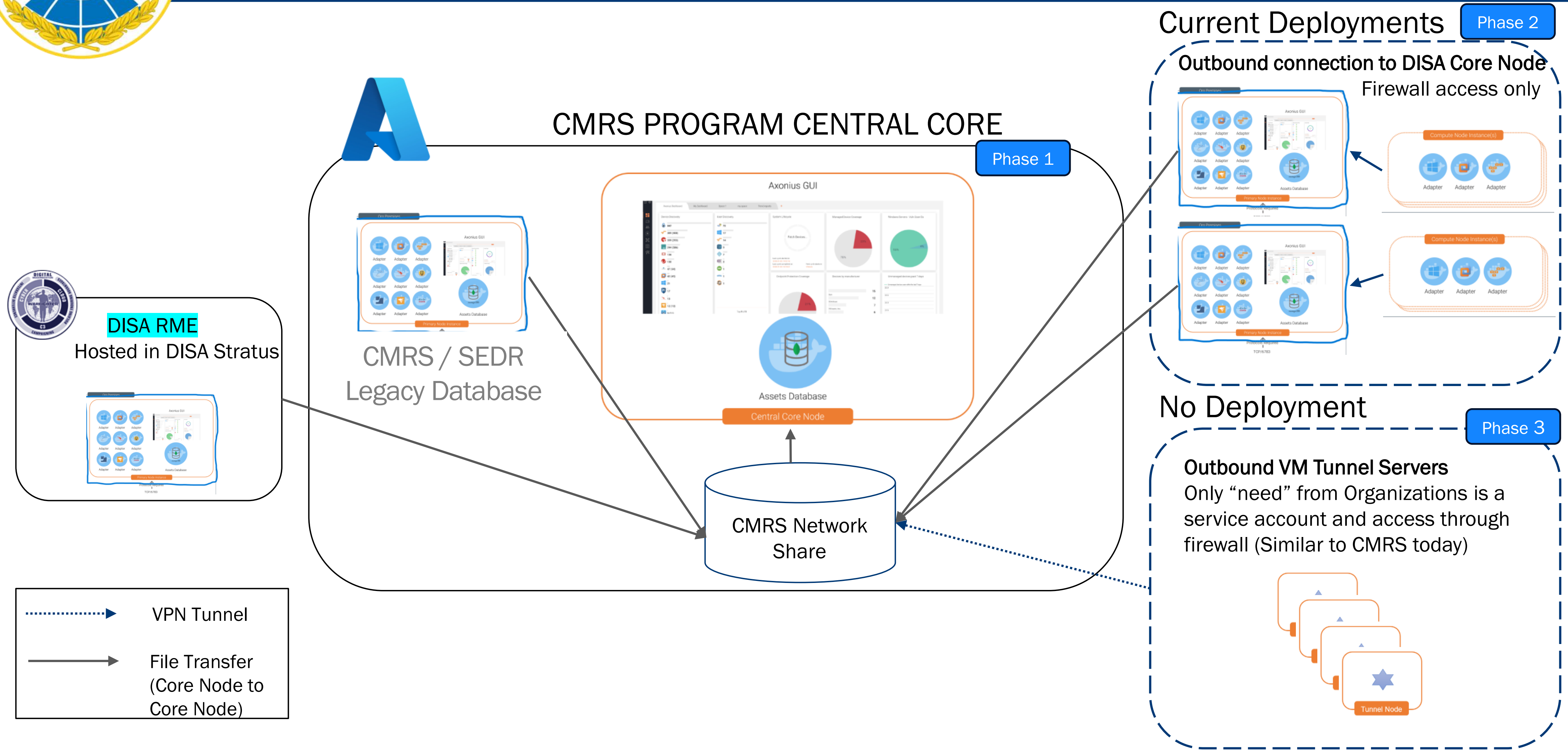
Endpoint Protection Coverage

Total 40363

Managed Device Coverage

Total 40363

Endpoint Security CMRS Modernization



Current Deployments

Phase 2

Outbound connection to DISA Core Node

Firewall access only

CMRS PROGRAM CENTRAL CORE

Phase 1

CMRS / SEDR Legacy Database

Axonius GUI

Assets Database

Central Core Node

DISA RME

Hosted in DISA Stratus

CMRS Network Share

No Deployment

Phase 3

Outbound VM Tunnel Servers

Only “need” from Organizations is a service account and access through firewall (Similar to CMRS today)

VPN Tunnel

File Transfer (Core Node to Core Node)

Way Forward

1) **Migrate SEDR to new hosting environment:** OCT 2025

2) **CMRS 2.0 Deployment:** JAN 2026

3) **Deploy connector nodes across DoD to publish into Core Node:** FEB 2026

    - Coordinate with DoD stakeholders and JFHQ DODIN to publish operational guidance

DEFENSE INFORMATION SYSTEMS AGENCY

DISA: The premier IT and telecommunications provider for the US military

in /DISA   X @USDISA   f /USDISA   DISA.mil