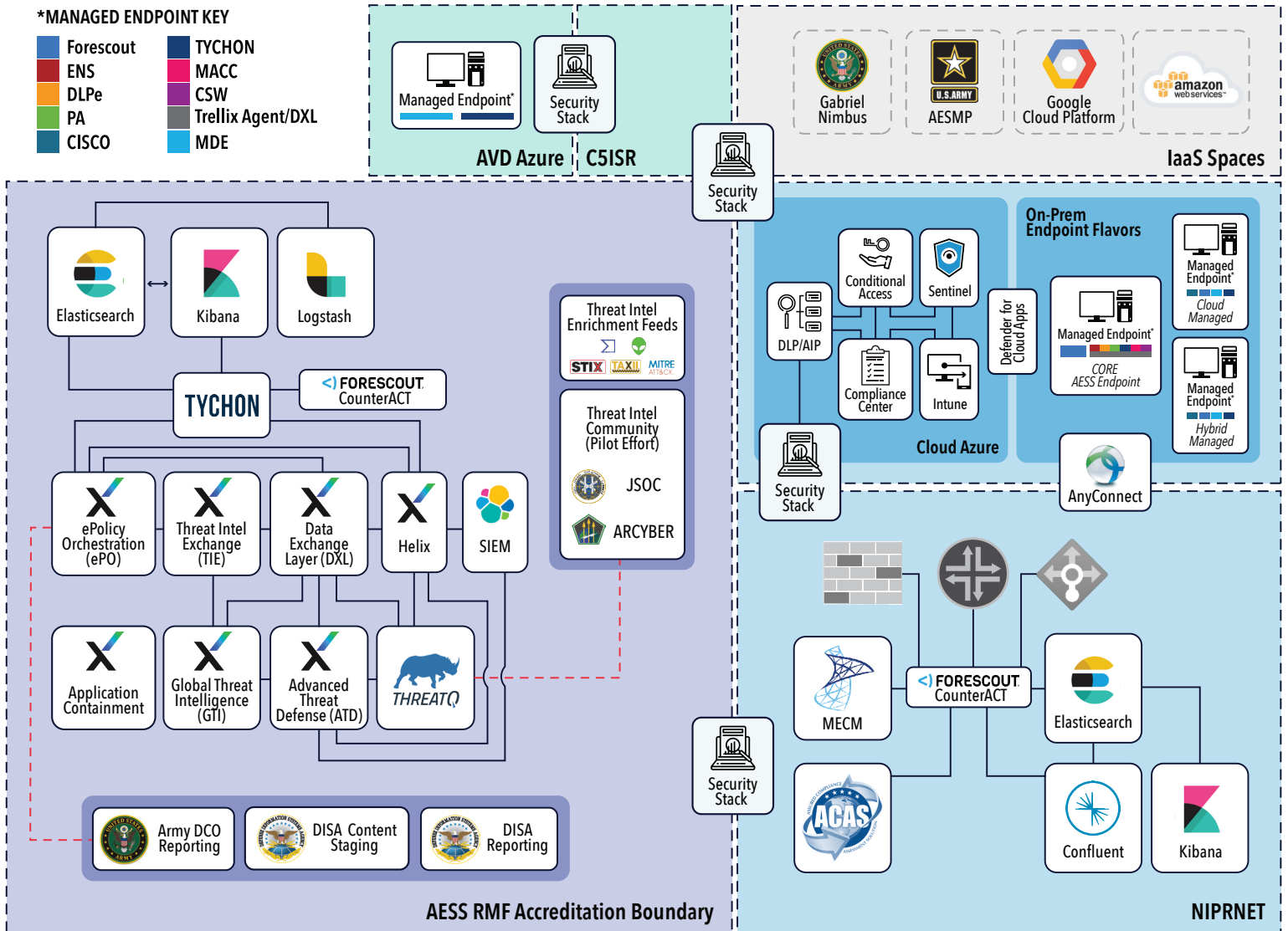# ECS

ARMY ENDPOINT SECURITY SOLUTION 2.0
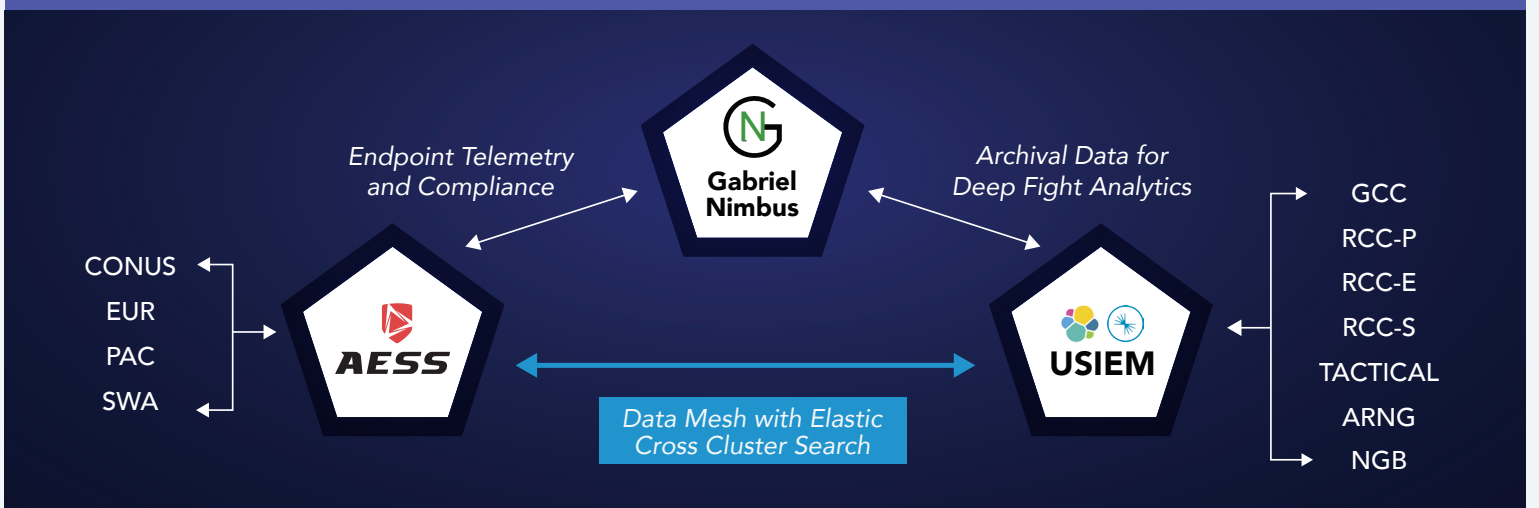
AESS

HYBRID MULTI-CLOUD SECURITY AND ZERO TRUST ARCHITECTURE

ECS' ZTA solution provides a unified and integrated platform to provide security of assets and data in a hybrid multi-cloud environment. The architecture provides endpoint security, visibility, and remediation for on-prem, cloud, and virtual endpoints across the DODIN-A

AESS HYBRID-MANAGED ARCHITECTURE

*MANAGED ENDPOINT KEY

- ■ Forescout
- ■ ENS
- ■ DLPe
- ■ PA
- ■ CISCO
- ■ TYCHON
- ■ MACC
- ■ CSW
- ■ Trellix Agent/DXL
- ■ MDE

AVD Azure | C5ISR

- Managed Endpoint*
- Security Stack

IaaS Spaces

- Gabriel Nimbus
- AESMP
- Google Cloud Platform
- amazon web services™

Security Stack

AESS RMF Accreditation Boundary

- Elasticsearch
- Kibana
- Logstash
- TYCHON
- FORESCOUT CounterACT
- ePolicy Orchestration (ePO)
- Threat Intel Exchange (TIE)
- Data Exchange Layer (DXL)
- Helix
- SIEM
- Application Containment
- Global Threat Intelligence (GTI)
- Advanced Threat Defense (ATD)
- THREATQ

Threat Intel Enrichment Feeds
- STIX TAXII MITRE ATT&CK

Threat Intel Community (Pilot Effort)
- JSOC
- ARCYBER

- Army DCO Reporting
- DISA Content Staging
- DISA Reporting

Cloud Azure

On-Prem Endpoint Flavors

- DLP/AIP
- Conditional Access
- Sentinel
- Compliance Center
- Intune
- Defender for Cloud Apps
- Managed Endpoint* *CORE AESS Endpoint*
- Managed Endpoint* *Cloud Managed*
- Managed Endpoint* *Hybrid Managed*
- Security Stack
- AnyConnect

NIPRNET

- Security Stack
- MECM
- ACAS
- FORESCOUT CounterACT
- Elasticsearch
- Confluent
- Kibana

Data Mesh and Unified SIEM

- CONUS
- EUR
- PAC
- SWA

AESS

Endpoint Telemetry and Compliance

Gabriel Nimbus

Archival Data for Deep Fight Analytics

USIEM

Data Mesh with Elastic Cross Cluster Search

- GCC
- RCC-P
- RCC-E
- RCC-S
- TACTICAL
- ARNG
- NGB

ARMY ENDPOINT SECURITY SOLUTION
ZERO TRUST HYBRID CLOUD REFERENCE ARCHITECTURE

AESS is the only deployed cybersecurity solution to offer all endpoint security and management capabilities required by Joint Forces HQ DoDIN/DISA.

Real-Time Automation	AESS Continuous Innovation	Capability Requirement	Framework	NIST
	TYCHON · elastic	CMRS BDP · Vulnerability Management	Enterprise Visiblity SIEM	**IDENTIFY**
	THREATQUOTIENT™	Intelligence Feeds · Analyst Workbench	Threat Intelligence Platform (TIP)	
BLOCK	Cloud Access Security Broker · Secure Access Service Edge	Shadow IT · Discovery · Remediation · Sanctioned Services	Cloud Security Platform CASB	
BLOCK	‹› FORESCOUT	Zero Trust · Authentication	Comply to Connect	**RESPOND**
BLOCK	Trellix	Alert Correlation · Orchestration Automation Incident Response	SOAR	
BLOCK	Trellix	Zero Day IOC Gen. · Dynamic Analysis · Static Analysis	Sandbox	
BLOCK	Trellix	Application Containment · Application Control	App Containment	**PROTECT AND DETECT**
BLOCK	Trellix	Insider Threat Device Control · Data Loss Prevention	Exfiltration	
BLOCK	elastic · Microsoft Defender · Trellix	AI / ML Behavior · Signatureless Detection · Memory Attacks · Zero Day	Modernized Endpoint Protection Platform	
BLOCK	opentext™ | EnCase™	Quarantine/Kill · Delete/Uninstall · Asset Mgmt. · Risk Score · Hunt · Compliance	Forensics	**RECOVER**
BLOCK	elastic · Microsoft Defender · TYCHON	Quarantine/Kill · Delete/Uninstall · Asset Mgmt. · Risk Score · Hunt · Compliance	EDR	

SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE

DATA EXCHANGE LAYER

Advanced Endpoint Security

- **Microsoft Defender for Endpoint:** Integrated protection, detection, and response.
- **Extended Detection & Response (XDR):** Correlated analytics across endpoints and users.
- **Comply-to-Connect (C2C):** Enforces secure access by compliant devices only.
- **Forensic Investigation & O&M:** Deep endpoint forensics with full lifecycle support.

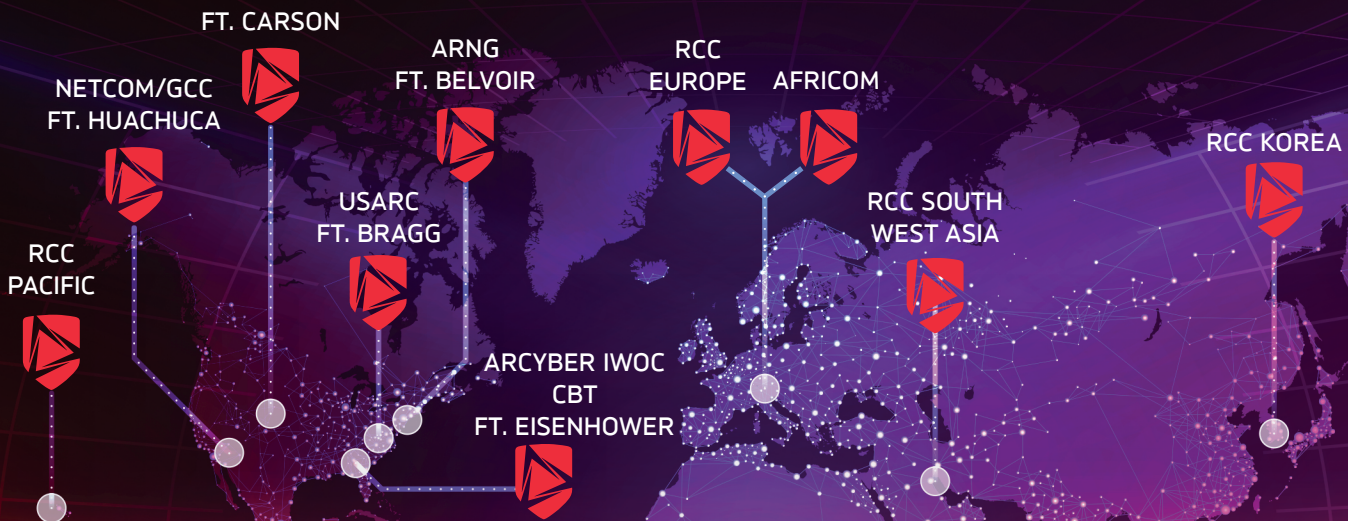## Visibility, Intelligence & Automation

- **Endpoint Visibility & Reporting:** Enterprise-wide endpoint health and activity insight.
- **Threat Intelligence Integration:** Enriched detection from classified and open-source feeds.
- **USIEM:** Unified monitoring and alerting across security systems.
- **Analysis of Alternatives (AoA):** Data-driven modernization and tech assessments.
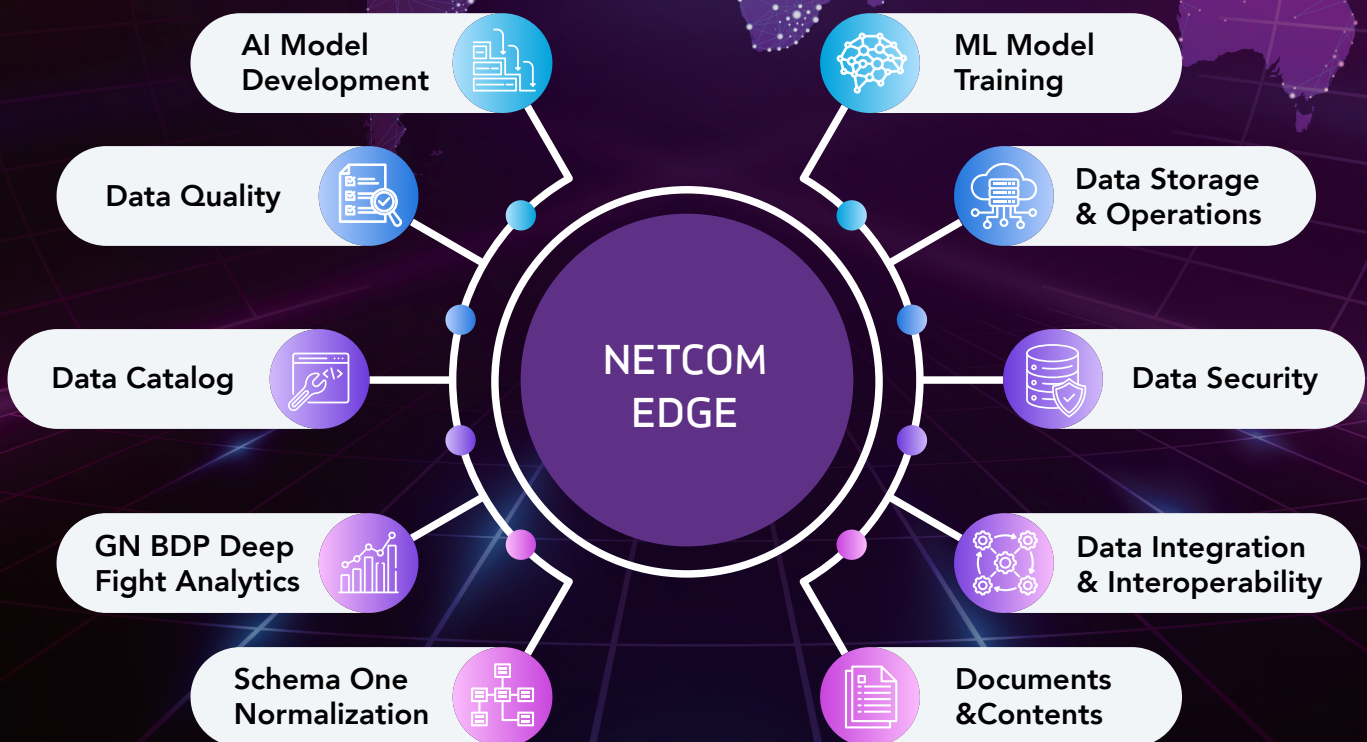
Global Mission Enablement

- **COCOM Support – AFRICOM:** Forward-deployed endpoint security and visibility.
- **AFRICOM Storage Expansion:** Scalable storage to support regional ops.
- **Collaborative Dev Environment:** Secure, agile space for rapid prototyping and integration.

OPERATING WORLDWIDE TODAY

Deployed worldwide on NIPRnet and SIPRnet, the Army Endpoint Security Solution (AESS) provides Regional Cybersecurity Centers (RCC) with the most advanced tools and discovery capabilities for comprehensive cybersecurity protection, detection, and remediation. ECS delivers a managed service with 24/7/365 Tier 2 and 3 support, analyst/DCO training and all Operations and Maintenance.

FT. CARSON

NETCOM/GCC
FT. HUACHUCA

ARNG
FT. BELVOIR

RCC
EUROPE   AFRICOM

RCC KOREA

USARC
FT. BRAGG

RCC SOUTH
WEST ASIA

RCC
PACIFIC

ARCYBER IWOC
CBT
FT. EISENHOWER

DATA GOVERNANCE

AI Model Development

ML Model Training

Data Quality

Data Storage & Operations

Data Catalog

NETCOM EDGE

Data Security

GN BDP Deep Fight Analytics

Data Integration & Interoperability

Schema One Normalization

Documents &Contents

Powered by Advana

DELIVERING COMPLETE ENDPOINT SECURITY TODAY

Contractor-owned/operated managed service ▪ Contractual SLAs/KPIs ▪ Continuous innovation

Microsoft Defender ▪ Trellix ▪ elastic

TYCHON ▪ aws ▪ Office 365 ▪ Azure

THREATQUOTIENT ▪ GitLab ▪ NetApp™

FORESCOUT ▪ HPE GreenLake ▪ opentext™ | EnCase™

PROJECT HIGHLIGHTS

750K
Endpoints managed
(Desktops/Servers/VM)

1.5M
Malicious events
blocked every month

Global NIPR/SIPR migration to AESS platform within 7 months of ATO

Global NIPR/SIPR infrastructure deployed and operational within 10 months

2 million new file reputations created

Hybrid-Cloud ready (AWS, Azure, Google Cloud Platform, IBM Cloud)

Continuously Maintained Authority to Operate (ATO) since 1/4/2019

From the boardroom to the battlefield, ECS empowers your mission, amplifies your impact, and drives lasting results with frontier technology solutions. Our highly skilled teams bring the best of innovation to urgent mission needs across the U.S. public sector, defense and intel, and commercial industries, with a focus on efficiency and impact. ECS maintains partnerships with leading AI, cloud, and cybersecurity technology providers and holds specialized certifications in their technologies.

cyber@ecstech.com ▪ www.ecstech.com/aess