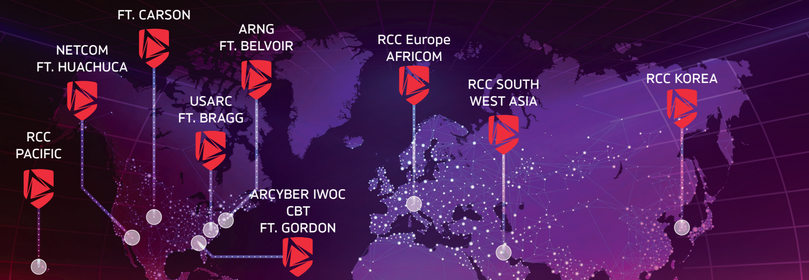
OPERATING WORLDWIDE TODAY

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.



AESS 2.0 ZERO TRUST CAPABILITIES MAPPING

User	Device	Network	Application & Workload	Data	Visibility & Analytics	Automation & Orchestration
User Authentication	Device Authentication	Software Defined Networking (SDN)	Software Defined Compute (SDC)	Software Defined Storage (SDS)	Discovery& Baselining	API Standard
User Authorization	Device Authorization	Macro Segmentation	DevSecOps (DSO)	Data Tagging	SIEM	Incident Response
Privileged Access Management (PAM)	Device Compliance		Software Supply Chain	Data Loss Prevention (DLP)	Machine Learning	SOAR
			Application Delivery	Data Rights Management (DRM)		Artificial Intelligence
			Micro Segmentation			Analytics

Core AESS Capability

Hybrid Cloud Integration

DELIVERING COMPLETE ENDPOINT SECURITY TODAY

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

Trellix · Microsoft Defender · elastic · TYCHON · aws · Office 365 Azure · THREATQUOTIENT · CORTEX XSOAR BY PALO ALTO NETWORKS · NetApp · FORESCOUT · opentext™ | EnCase™

Project Highlights

>700K 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)

Authority To Operate (ATO) 1/4/2019

CMMI DEV/3 · CMMI SVC/3 · ISO 20000-1:2011 · ISO 27001:2013

ECS delivers advanced solutions in cybersecurity, cloud, artificial intelligence (AI), machine learning (ML), application and IT modernization, science, and engineering. ECS is an award-winning partner with strategic experience and technical expertise in the deployment and management of cybersecurity products. We are committed to simplifying cybersecurity for every client and providing consulting, managed services, and resale to meet each organization's individual needs.

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

Updated January 2024

ECS

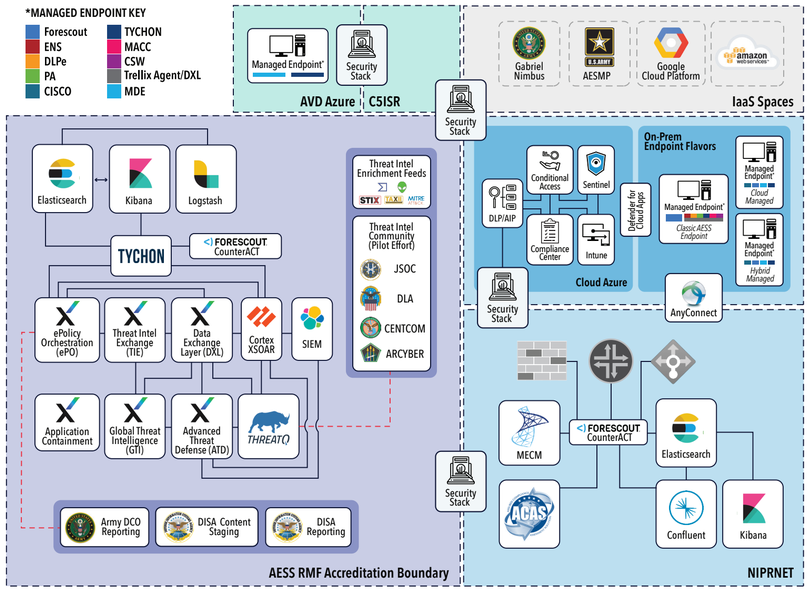
ARMY ENDPOINT SECURITY SOLUTION 2.0

AESS

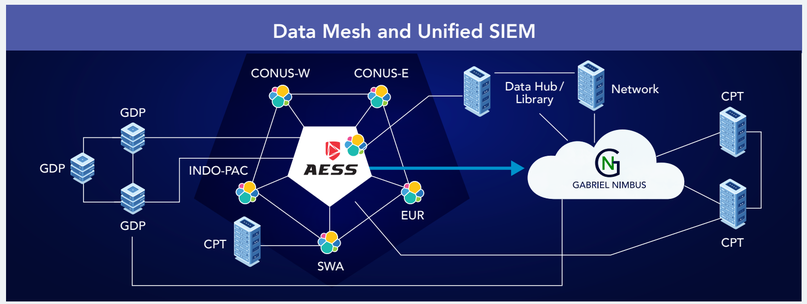
HYBRID MULTI-CLOUD SECURITY AND ZERO TRUST ARCHITECTURE

ECS's 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 Flow 1 (GFE on NIPRnet), Flow 2 (GFE on VPN) and Flow 3 (GFE not on VPN and BYOD).

AOA LAB ARCHITECTURE AND INFORMATION FLOWS



Data Mesh and Unified SIEM



ARMY ENDPOINT SECURITY SOLUTION
ZERO TRUST HYBRID CLOUD REFERENCE ARCHITECTURE

Real-Time Automation	AESS Continuous Innovation	Capability Requirement	Framework	NIST
SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE / DATA EXCHANGE LAYER	TYCHON elastic	CRMS 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	CORTEX	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 Asset Mgmt. Hunt · Delete/Uninstall Risk Score Compliance	Forensics	RECOVER
BLOCK	elastic Microsoft Defender TYCHON	Quarantine/Kill Asset Mgmt. Hunt · Delete/Uninstall Risk Score Compliance	EDR	

* *Completed Integration Testing in AESS Lab, not deployed*

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

Threat Detection and Protection:

- Moving from **detection to engagement in milliseconds** by convicting and blocking malicious activity at the lowest level in the stack
- **Isolating and process-recording suspicious activity** for additional analysis via sandboxing or by an analyst
- Automatic reversal of unauthorized endpoint changes`
- **Orchestration and response integration** to automate playbooks and analyst workflows
- Tailored thresholds determine automatic remediation or assignment to analysts for manual investigation

Asset Management and Maintenance:

- **Inventorying** all hardware and software for each endpoint; **journaling** all changes
- Collecting hygiene data from endpoint to enterprise in the **Automated Cyber Hygiene and Risk Scorecards**

Information Sharing and Reporting:

- Generating **indicators of compromise (IOC)** and instantaneously sharing them across the global **Data Exchange Layer**
- Sharing indicators and external data from the intelligence community, commercial databases, and third-party feeds on the **Threat Intelligence Platform**