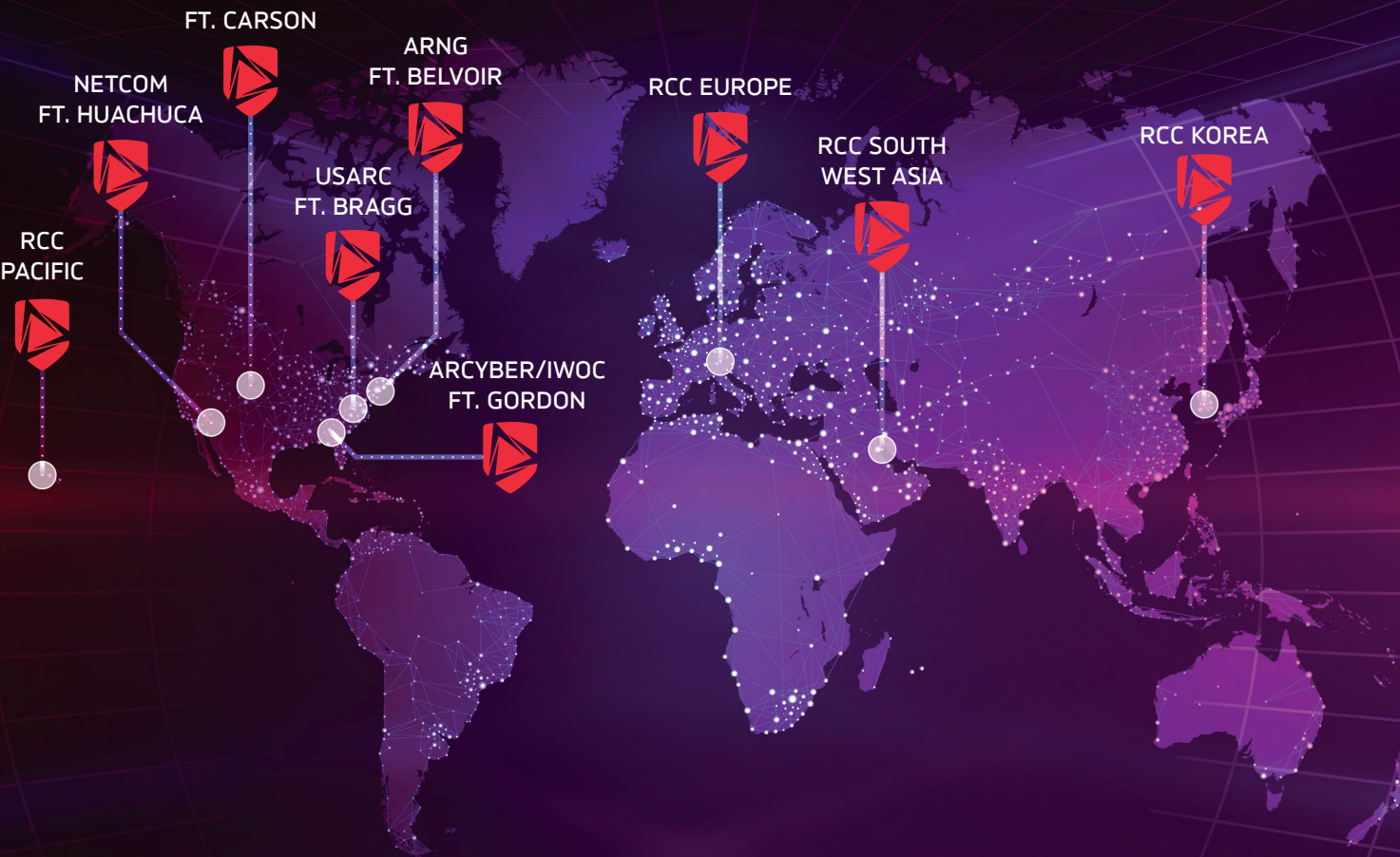## OPERATING WORLDWIDE TODAY

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
ARNG FT. BELVOIR
NETCOM FT. HUACHUCA
RCC EUROPE
USARC FT. BRAGG
RCC SOUTH WEST ASIA
RCC KOREA
RCC PACIFIC
ARCYBER/IWOC FT. GORDON

Project Highlights

>700K
Endpoints managed (Desktops/Servers/VM)

400K+
Malicious events automatically contained

Global NIPR/SIPR migration to ACTD 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

DELIVERING COMPLETE ENDPOINT SECURITY TODAY

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

McAfee™ · TYCHON · THREATQUOTIENT · elastic · FORESCOUT · CORTEX XSOAR BY PALO ALTO NETWORKS · Attivo NETWORKS · opentext™ | EnCase™ · aws · Office 365 · Azure

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 McAfee partner with strategic experience and technical expertise in the deployment and management of McAfee 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.

CMMIDEV/3 · CMMISVC/3 · ISO 20000-1:2011 · ISO 27001:2013

cyber@ecstech.com · www.ecstech.com/cyber
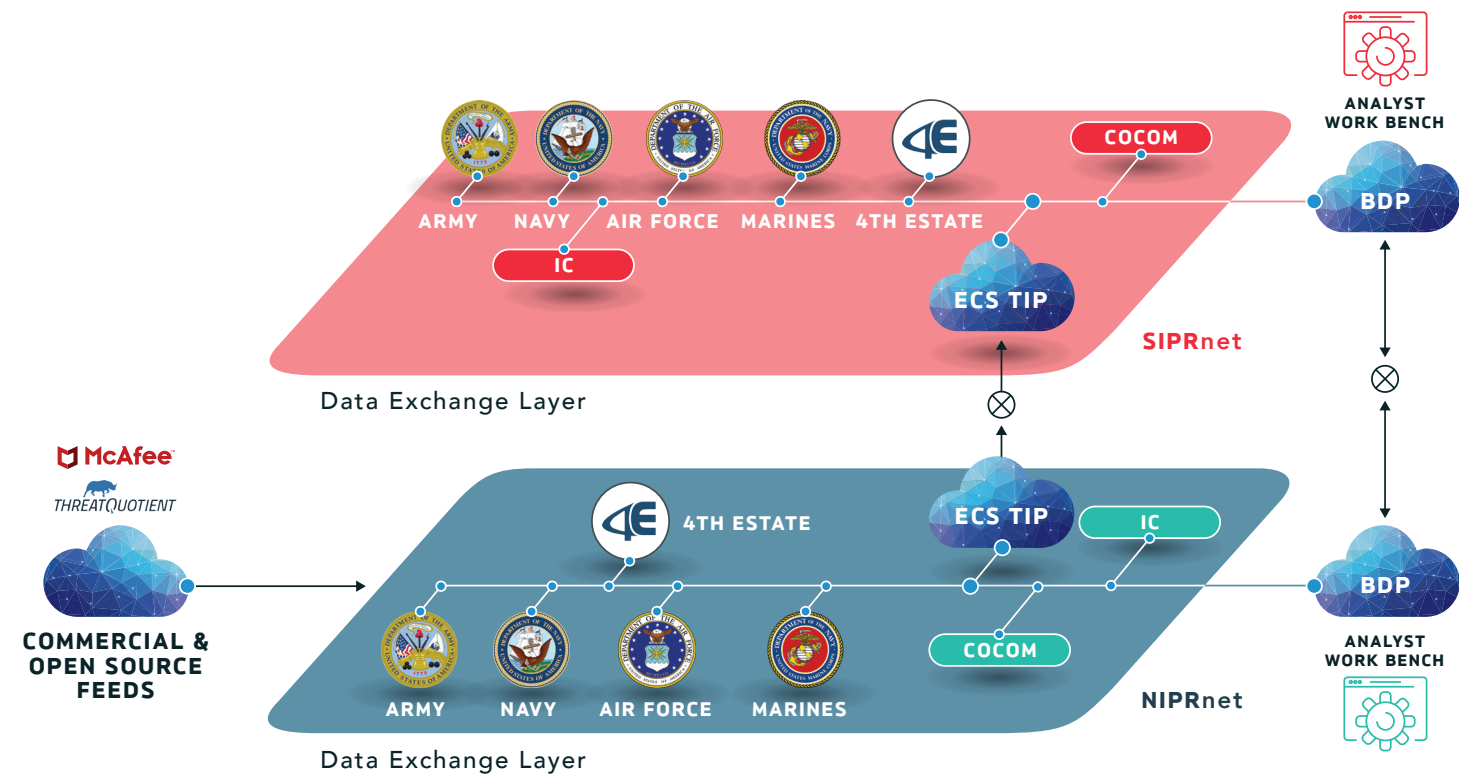

ARMY ENDPOINT SECURITY SOLUTION

AESS

ADVANCED CYBER THREAT DEFENSE (ACTD)

ECS

ECS

ADVANCED CYBER THREAT DEFENSE (ACTD)

ECS's AESS solution integrates the most advanced cybersecurity technologies from McAfee and other Innovation Alliance partners into the Advanced Cyber Threat Defense (ACTD) platform, providing endpoint security, visibility, remediation, orchestration, and management capabilities as a service.

COCOM
ANALYST WORK BENCH
BDP
ARMY NAVY AIR FORCE MARINES 4TH ESTATE
IC
ECS TIP
SIPRnet
Data Exchange Layer

McAfee
THREATQUOTIENT
COMMERCIAL & OPEN SOURCE FEEDS

4TH ESTATE
ECS TIP
IC
COCOM
BDP
ANALYST WORK BENCH
ARMY NAVY AIR FORCE MARINES
NIPRnet
Data Exchange Layer

Current Adopters of the ACTD Platform

U.S. Department of the Army	Joint Special Ops Command (JSOC)	Defense Logistics Agency (DLA)	U.S. Central Command (CENTCOM)	Missile Defense Agency (MDA)	U.S. Air Forces Central Command (AFCENT)

Real Time IOC Sharing Participants

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.

NIST

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	IDENTIFY
		GTI TIE DXL — THREATQUOTIENT	Intelligence Feeds	Analyst Workbench	Threat Intelligence Platform (TIP)	
		CASB MVision — MVISION *	Shadow IT · Discovery Remediation Sanctioned Services		Cloud Security Platform CASB	
		FORESCOUT · APPGATE *	Zero Trust	Authentication	Comply to Connect	RESPOND
		elastic · CORTEX	Alert Correlation	Orchestration Automation Incident Response	SOAR SIEM	
		Automated Sandboxing — McAfee	Zero Day IOC Generation	Dynamic Analysis Static Analysis	Sandbox	
		Attivo NETWORKS *	Counter Infiltration Threat Emulation		Threat Deception	
		McAfee	Application Containment Application Control		App Containment	PROTECT AND PREVENT
		DLP — McAfee	Insider Threat Device Control	Data Loss Prevention	Exfiltration	
		ENS Real Protect ATP — McAfee	AI / ML Behavior Signatureless Detection Memory Attacks · Zero Day		Modernized Endpoint Protection Platform	
		TYCHON opentext EnCase *	Quarantine/Kill Asset Mgmt. Hunt	Delete/Uninstall Risk Score Compliance	EDR Forensics	RECOVER

minutes · seconds · milliseconds (labels on SOAR column)
BLOCK (labels on multiple rows)

* Completed Integration Testing in AESS Lab, not deployed

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**