ECS

ARMY ENDPOINT SECURITY SOLUTION


ADVANCED CYBER THREAT DEFENSE (ACTD)

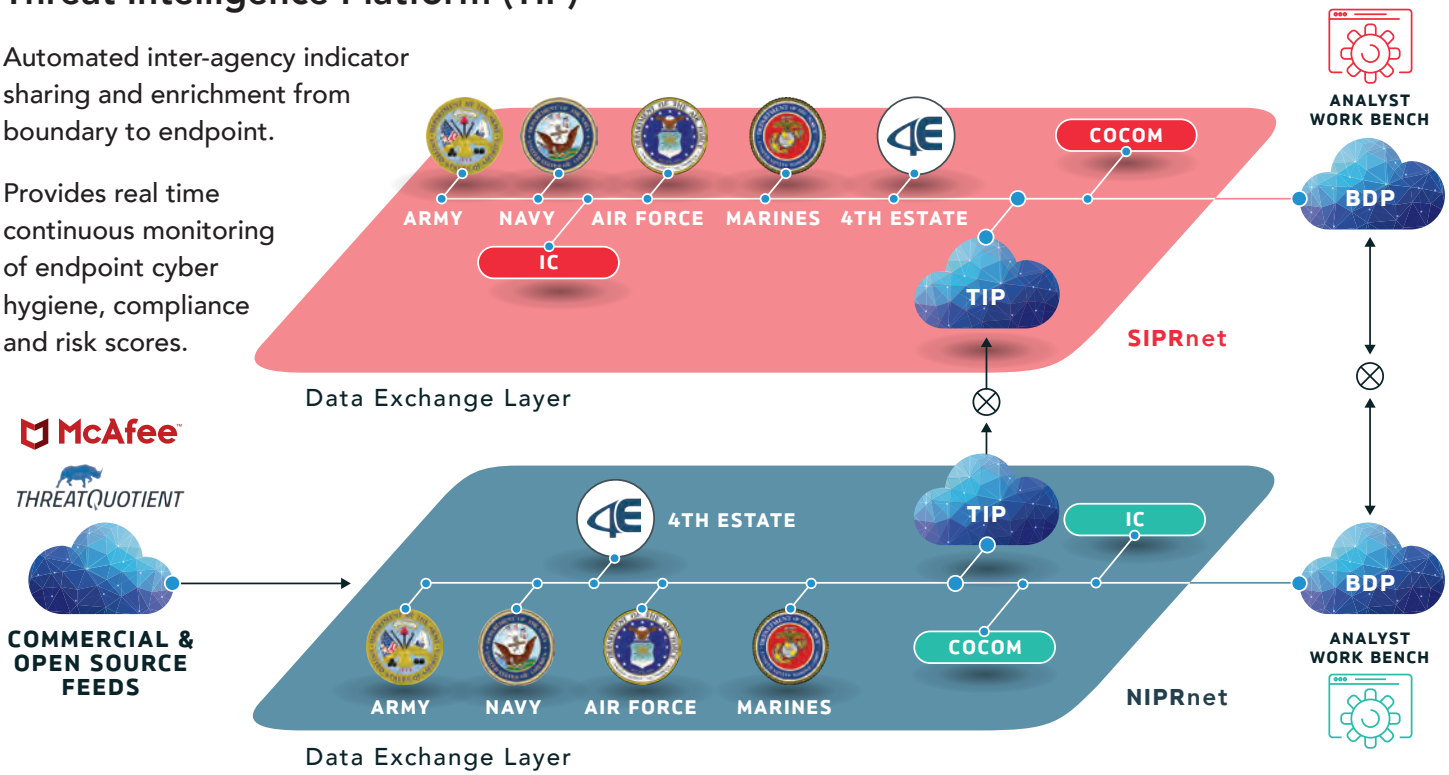
# ADVANCED CYBER THREAT DEFENSE (ACTD)

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.

## Threat Intelligence Platform (TIP)

Automated inter-agency indicator sharing and enrichment from boundary to endpoint.

Provides real time continuous monitoring of endpoint cyber hygiene, compliance and risk scores.



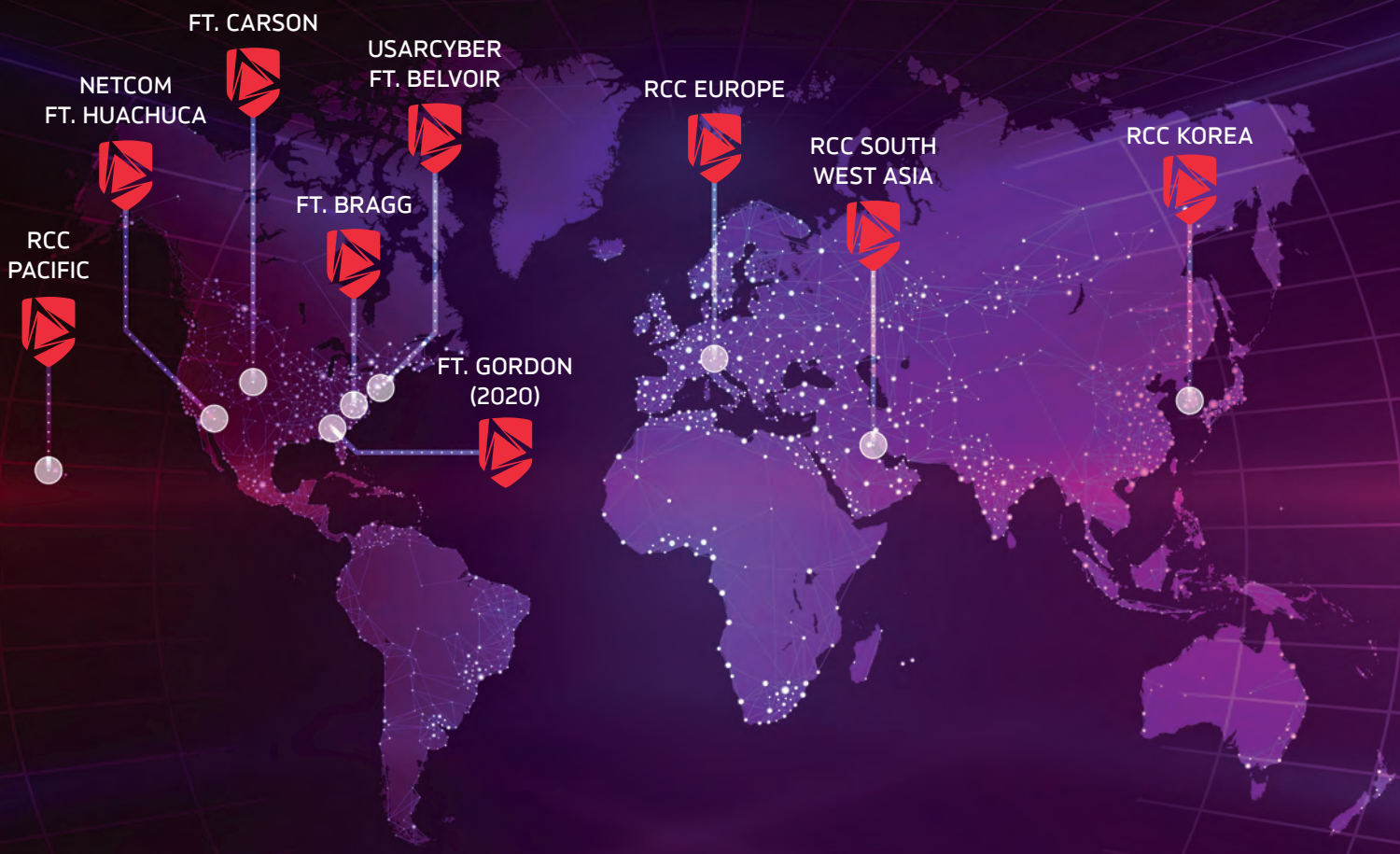

## Current Adopters of the ACTD Platform

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

TIP Participants

## 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.




## Project Highlights

**650K**
Endpoints managed
(Desktops/Servers/VM)

**1.3M+ PER MONTH**
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

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

Authority To Operate (ATO) 1/4/2019

# ARMY ENDPOINT SECURITY SOLUTION REFERENCE ARCHITECTURE


* *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**

## DELIVERING COMPLETE ENDPOINT SECURITY TODAY

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

McAfee™ | TYCHON

elastic | THREATQUOTIENT

Attivo NETWORKS. | Bromium®

DEMISTO | aws | Azure

FORESCOUT | CISCO

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