ARMY SOSSEC
PM-DCO CYBER TALK

McAfee and Advanced Cyber Threat Defense (ACTD)

Patrick Greer | Solutions Architect, McAfee
Agenda

• Overview
• Advanced Cyber Threat Defense (ACTD)
  • Components Explained
  • Product Integrations
  • Security Connected Ecosystem
  • Portability and Adaptability
• Data Exchange Layer (DXL)
• Journey to Cloud
  • Hybrid and Cloud Edge
• Comprehensive ZeroTrust Coverage
• Wrap Up
A view of the customer’s former operating environment

- Ten independent contracts
- Multiple siloed teams & contractors
- Exposure to existing and future threats
- Significant opex to manage outdated and fragile environment
- High exposure to aging infrastructure failures
- No consolidated dashboard view of threats
- No advanced analytics
- Incapable of achieving real-time protection
Limited visibility and situational awareness; inability to share threat IoC’s

Siloed security tools; limited focus and functionality

Exposure to existing and future threats

Significant opex to manage outdated and fragile environment

No consolidated dashboard view of threats

Alert fatigue; outpaced by current and emerging threats

No advanced analytics

Incapable of achieving real-time protection

Limited visibility and situational awareness; inability to share threat IoC’s
The McAfee Approach

**Modernize:** Replace outdated technology with resilient endpoint architecture

**Simplify:** Deploy a security-connected threat defense ecosystem

**Scale:** Migrate efficiently and remain up-to-date seamlessly on latest technology
Integrated network and endpoint security

Implemented global threat intelligence platform

Cloud-enabled technologies

Bridged network visibility and network security

Created an open threat intelligence fabric for the enterprise

Delivered DCO machine-learning capabilities

Extensible for cloud workloads

Implemented global threat intelligence platform

Driving Innovation
Unified endpoint security

Created an open threat intelligence fabric for the enterprise

Delivered DCO machine-learning capabilities

Delivered common architecture to facilitate a security-connected ecosystem

Created an open threat intelligence fabric for the enterprise

Extensible for cloud workloads

Delivered DCO machine-learning capabilities

Implemented global threat intelligence platform

Cloud-ready technologies

Orchestration and Automation enabled
The Customer Outcomes

- One contract with consistent SLAs
- Reduced cost by $79M
- Migrated 550K endpoints under centralized management in one year
- Reduced staff by 73%
- 99.9% system availability
- Automated cyber scorecard provides real-time awareness
- Advanced capabilities to 100K endpoints already finding new risks
- Robust, modernized endpoint architecture continuously updated
Automated cyber scorecard provides real-time awareness.

Robust, modernized self-learning endpoint architecture.

Integrated, non-siloed collaborative defenses.

Inter-service and inter-agency indicator sharing.

750K endpoints under centralized management and growing.

99.9% system availability.

Integrated, non-siloed collaborative defenses.

Automated cyber scorecard provides real-time awareness.

Mission-centric outcomes.

Analytics-based security.

Integrated, non-siloed collaborative defenses.

99.9% system availability.

Inter-service and inter-agency indicator sharing.

750K endpoints under centralized management and growing.
Advanced Cyber Threat Defense (ACTD)

Core Analyst Benefits

- Allows cyber operators to focus on **real** threats, advanced forensics, and **proactive** protection strategies

- ACTD enables SOC & DCO Analysts to increase endpoint intelligence, drive enterprise-wide automation, and share threat intelligence.

| Shift focus of SOC from tactical firefighting to a strategic lifecycle threat defense; empower analysts to do more and investigate more effectively |
| Threat IOC’s share instantly across all network and host sensors to inoculate all connected cyber systems with new defensive countermeasures |
| Automated, self-learning system continually evaluates environment and adapts to new zero-day and advanced persistent attacks |
| Leadership command and control of cyber environment based on all source intelligence; advanced CND situational awareness |
| Continually evolve defenses with a modular, extensible threat defense fabric that can easily integrate new technologies as missions change |
| Minimizes the amount of time it takes to get to the root of an attack. |
McAfee Advanced Cyber Threat Defense (ACTD) provides an open, shared threat intelligence platform which delivers adaptive, real-time threat detection and response capabilities against today's advanced threats - from device-to-cloud.
Threat Intelligence Approach

ACTD provides an open, shared threat intelligence platform which delivers adaptive, real-time threat detection and response capabilities against today’s advanced threats (from device-to-cloud)

- Shared threat intelligence and actionable forensics utilizing an open-architecture threat sharing environment
- Full interoperability and integration of all cyber defenses promote automated and collaborative actions to emerging threats
- Machine-Learning, Application Containment, and malware sandboxing functionality for zero-day behavioral detection and prevention of signature-less threats
- Global connected security fabric – autonomous, self-learning environment that will provide defensive persistence and resiliency to the network
- Ideal for DIL environments with limited or no outside connectivity
Connected, Threat Sharing Environment

Shared Cyber Threat Intelligence “Our Guiding Principles”

- All Enterprise Security Products Investments Should Work Together
- Advanced Capabilities Should Exist on the Endpoint but Requires “Off Box” Integrations to Minimize Endpoint Performance and Increase Effectiveness
- Known Good / Known Bad Indicators of Compromise Should be Stored and Shared Instantly Across the DoDIN
- In-depth Analysis and Hunting Should be Focused on Unknown Threats and Integrated into a Common Threat Intelligence Platform
Platform Flexibility

A customizable, portable solution that can be tailored to the unique requirements of Tactical, DDIL and POR

**Key Features**

- Behavior-based detections; machine learning and application containment capabilities reduce dependencies on security updates or signatures

- ACTD can function as a portable, isolated system within disconnected enclaves. Deeply customizable and flexible to satisfy dynamic mission requirements.

- Solution created to specifically address the “unknowns” in an environment; identify and remediate malicious files that have no prior reputation
ACTD in the Army
Foundation of the Army Endpoint Security Solution (AESS)

Recognized as ARMY’s Endpoint

- Army AESS is the enterprise, managed solution for endpoint security
- AESS is a complete replacement of the legacy HBSS tool set with significant capabilities that can be tailored to the unique requirements of Tactical, DDIL and POR
- The Army has already invested in these AESS capabilities, including Endpoint Detection and Response (EDR), application containment, application control (whitelisting), data loss prevention, and AI that learns the environment and responds on behaviors not signatures

Enterprise IT as a Service (EITaaS)

- Adaptable to support all three lines of effort on EITaaS – compute and storage, network as a service, end user services

Partner Integrations

- ACTD Platform allows for rapid integration of new technologies and partners to support ARMY’s dynamic mission requirements
# ACTD in the Army (cont'd)

Foundation of the Army Endpoint Security Solution (AESS) Ecosystem

## Data Exchange Layer

### DoD Mandated Endpoint Security Modules
- McAfee ePolicy Orchestrator
- McAfee Agent
- Policy Auditor
- Host Intrusion Prevention
- Virus Scan
- Device Control Module
- Assets Publishing Service
- Asset Configuration Compliance Module
- Operational Attributes Manager
- Rogue System Detection

Delivered by ECS as a managed service on the ACTD platform, AESS is a turnkey solution that includes all hardware, software, maintenance, and operations.

### Endpoint Security Platform
- Real-Protect Machine Learning
- Signature-less Malware Detection
- Dynamic Application Containment
- Efficient on-host performance/Zero-Impact Scanning

### Threat Intelligence Fabric (DXL)
- Operationalizes threat intelligence
- Automated response orchestration
- Sources threats from sensors (endpoints, IPS, firewalls, etc.), global sources (e.g. GTI, US Cert, VirusTotal, etc.), and local

### Malware Sandbox
- Detects zero-day malware and provides in-depth analysis/reporting
- Combines AV signatures, reputation, and real-time emulation defenses with static code and dynamic analysis (sandboxing)

### Analytics & Reporting Services
- Actionable alerts and integrations to prioritize and respond to threats
- Consolidates threat data and reputation feeds, delivers global view of systems, data, risks, and activities

### Correlation Engine
- Identifies and scores threat events in real time, using both rule- and risk-based logic
- Delivers notifications if specific users, groups, applications, servers, or subnets are threatened

### Application Whitelisting
- Blocks unauthorized applications
- Groups binaries (EXEs, DLLs, drivers, and scripts) and intelligently classifies them as well-known, unknown, and known-bad applications

### Data Loss Prevention
- Monitors and prevents data loss
- Applies centrally managed security policies to control how users use and transfer sensitive data
- Generates detailed forensics reports

### Detection and Remediation
- Unifies security hygiene, asset, and endpoint systems management
- Automates DOD Cyber Scorecard Reporting and Remediation
- FuzzyHashing & Historic Host Journal

## ACTD in the Army (cont'd)

Foundation of the Army Endpoint Security Solution (AESS) Ecosystem

Delivered by ECS as a managed service on the ACTD platform, AESS is a turnkey solution that includes all hardware, software, maintenance, and operations.
Data Exchange Layer (DXL)

An expanding ecosystem for services and data integrations that embody “Together is Power”
Data Exchange Layer (DXL)

An open ecosystem for app integration and instant communication

- Open and flexible communications framework
- Secure, real-time way to unite data (any format) and actions across the enterprise
- Connects security products and solutions from multiple vendors for bi-directional security information sharing
  - Autonomous cyber - automate, adapt, and respond across all integrated cyber defense capabilities
- **OpenDXL** – Enables developers to leverage the DXL technology in order to connect products throughout security infrastructure

Create integrated security systems to automate the threat defense lifecycle to address **more threats, faster, with fewer resources**
The Future of ACTD

Expanding Capabilities, Adopting Cloud, and the Principles of ZeroTrust
McAfee Supports the Army Migration to Cloud

Cloud-ready solutions facilitate a phased journey to cloud providing a seamless transition and visibility over a diverse, hybrid environment

**On-Premises**

Traditional endpoint and network security

- CC/S/A manage and maintain on-premise hardware for cybersecurity administration
- Partial asset visibility and limited security controls
- ACTD architecture & real-time threat sharing (Army AESS)
- Global IoC data normalized and distributed via TIP across CC/S/A
- Endpoint Modernization

**Hybrid**

Seamless orchestration between on-premise and cloud platforms

- Full visibility across on-premises, mobile, and cloud services
- Custom Apps migrated to cloud; not redesigned
- Unified Cloud Edge (UCE) adoption
- Basic incident workflows
- Integrated partner ecosystem
- Threat intelligence sharing between cloud workloads and on-prem devices

**Multi-Cloud**

Iterate and improve foundation to efficiently manage and optimize workloads in the cloud

- Gain efficiencies and redesign cloud applications driven by API (Containers, DevSecOps)
- ZeroTrust alignment; data-driven and trust built into business strategies
- Insider Threat
- Strong workflows, processes, and threat intelligence sharing across multiple cloud providers
Secure Hybrid Cloud Environments

Cloud Workload Security (CWS) – Seamless orchestration between on-premise and cloud platforms

Automate Discovery & Deployment

Correct Anomalies
Segment patient zero without an agent using Security Groups

Micro-segmentation

NEW Auto-remediation

Defend Against Advanced Attack

Visualize & Detect Network Threats

Protect
Adapt
Detect
Correct
Discover and Monitor

Threat Prevention
Behavioral Detection
Intrusion Prevention
Application Whitelisting
Integrity Monitoring

Shared Threat Intelligence
Vulnerability Management
Quarantine Workloads
Micro & Nano-segmentation

Network flow logs

GuardDuty
Virtual NSP

GuardDuty
Virtual NSP
Zero Trust Models: Analyst, Government & Industry Voice

Zero Trust Architecture, Zero Trust Network Architecture, CARTA, Service Access Service Edge [SASE]
McAfee Unified Cloud Edge (UCE) Approach

Supporting the journey to a ZeroTrust architecture

**UCE Priorities by Customer Challenges**

<table>
<thead>
<tr>
<th>Data is everywhere</th>
<th>Web and Cloud Threats</th>
<th>Remote users to cloud</th>
<th>Remote sites to cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example Features</td>
<td>Example Features</td>
<td>Example Features</td>
<td>Example Features</td>
</tr>
<tr>
<td>• Unified DLP/CASB Classifications</td>
<td>• Risk-based Policies</td>
<td>• MVC Managed MCP</td>
<td>• Dynamic IPSec for remote site tunnels</td>
</tr>
<tr>
<td>• Unified Incidents</td>
<td>• Unified Shadow Policies</td>
<td>• MMCS for iOS/Android devices</td>
<td>• SD-WAN integration guides</td>
</tr>
</tbody>
</table>

**Example Features**

- MVC Managed MCP
- MMCS for iOS/Android devices
- Dynamic IPSec for remote site tunnels
- SD-WAN integration guides

**Cloud architecture scale and resiliency**

- 99.999% service availability
- Low latency architecture

**Threat efficacy**

- GTI, GAM, Insights
UCE High-level Solution Architecture

**Unmanaged Users**
- Limited Access
- Based on policy
- Unmanaged Endpoints

**Remote Users (no VPN)**
- Managed Endpoints
- McAfee Endpoint Security
- McAfee Client Proxy
- McAfee Encryption

**On-Base Users**
- Managed Endpoints
- McAfee Endpoint Security
- McAfee Client Proxy
- McAfee Encryption

**Unified Cloud Edge (UCE)**
- Full Access
- Activity Monitoring (UEBA)
- DLP
- Shadow IT/Risk
- Service Groups
- Sanctioned SaaS Applications

**Cloud Access Security Broker (CASB)**
- DLP
- Web Gateway

**DoD Custom Applications**

1. UCE offers visibility and control over data and threats across SaaS, PaaS and IaaS environments for all users.
2. UCE performs Data Loss Protection for all network traffic and is tightly integrated into MVISION Cloud.
3. MVISION Cloud performs Shadow IT analysis of all cloud services accessed by agency end-users.
4. UCE ensures compliance by protecting sensitive data from the endpoint to the cloud and within the cloud.
DevOps to DevSecOps

Make Everyone Responsible for Security

DevSecOps

- Focus on building security into application development from end-to-end
- A “Shift-Left” strategy makes continuous and integrated security an integral part of the application lifecycle
- Focus on built-in security; not security functioning as a perimeter around applications and data

- DevOps Security must adapt to meet demands of cloud-native technologies such as containers, microservices, and Zero-Trust principles
- Static security policies and checks often do not apply to cloud-native technologies
IaaS Security Layers

1. Detect and correct security misconfigurations
2. Detect and secure Workloads and Containers
3. Protect the data in the apps
Securing Containers

Securing ever-changing container workloads and the infrastructure on which they depend

Am I at risk due to misconfigurations?
Validate Container Orchestration System Config (CSPM)

Are my containers vulnerable?
Vulnerability Assessment for container components (Vulnerability Management)

Is my runtime secure?
App Level Visibility and Control (Zero Trust Security Model)
Reduced Complexity at the Endpoint and Beyond

Single Agent, Unified Console, Expansive Ecosystem

Single Agent

Endpoint Security

Unified Security Console

Remote Sandboxing

Cloud Workloads

Data Protection

Container Security

Expansive Integrated Ecosystem

Open
Industry's largest
universal command
fabric

Partners
100+
pre-integrated
partners

McAfee
Endpoint, SOC
Analytics, SIEM,
Network

McAfee Confidential
Our Brand Promise

We believe that no one person, product, or organization alone can secure the digital world.

It’s why we rebuilt McAfee around the idea of working together: People working together. Products working together. Organizations and industries working together.

We aim to inspire collaboration among our customers, partners—even our competitors—to make the connected world a safer place.

McAfee. Together is power.

McAfee. The device-to-cloud cybersecurity company.