ECS

ECS MCAFEE XDR
SOLUTION GUIDE

Dangerous and disruptive cybersecurity threats are targeting enterprises at breakneck speed. Major ransomware and critical infrastructure threats are becoming more pervasive and discrete by the day. Enterprise organizations must defend their networks and data from a wide range of modern attacks.

Every organization must adopt a proactive cybersecurity posture, maintain security operations center (SOC) requirements, and implement refinements and updates before criminals have the opportunity to exploit vulnerabilities. It is vital to monitor suspicious behavior across the entire digital landscape.

Make no mistake: tracking and preventing modern threats is a race against time.

Enterprises that leverage current technology investments with advanced security solutions can achieve an advanced level of efficacy.

ECS MCAFEE XDR

The ECS and McAfee Extended Detection and Response (XDR) platform represents the next iteration of cybersecurity empowerment. The platform builds upon your current technology investments to establish a robust SOC environment that improves protection, increases personnel productivity, and lowers the total cost of ownership (TCO).

It drives threat prioritization, predictive threat assessment, and proactive response processes. Go beyond typical and under-optimized detective controls. Monitor a cohesive, simple view of threats. Analyze real-time information and deploy better, faster outcomes.

XDR leverages cloud-native solutions that unify multiple data sources from the endpoint and non-endpoint sources such as cloud apps, cloud services, network traffic, and SIEM. Enhanced threat intelligence presents a view of the entire landscape in a single view and enables ECS to deliver expedient risk mitigation and a deeper level of managed detection and response (MDR).

With the XDR platform, ECS lowers TCO for threat response by providing increased global threat intelligence and enhanced telemetry architecture.

Threat detection capabilities include:

- Native support for behavior analysis of users and technology assets
- Threat intelligence including shared local threat intelligence coupled with externally acquired threat intelligence sources
- Reducing the need to chase false positives by automatically correlating and confirming alerts
- Integrating relevant data for faster, more accurate incident triage
- Centralized configuration and hardening capability with weighted guidance to help prioritize activities
- Comprehensive analytic

NEXT LEVEL MDR

In a recent Forrester report, 36 percent of IT decision-makers noted that the alerts surfaced by their current EDR solutions were false positives and did not require investigation. In addition, 35 percent claimed that junior staff members lacked the skills to triage and investigate alerts without supervision from senior staff

Alert fatigue, false positives, inexperienced staff, and a lack of defined processes are real-world problems that exacerbate an already dangerous digital environment. XDR can alleviate these challenges.

XDR optimizes response processes with advanced context by providing enhanced threat detection and response capabilities, including:

- Converting a large stream of alerts into a manageable number of incidents for manual investigation
- Providing integrated incident response options that have the necessary context from all security components to resolve alerts quickly
- Providing response options that go beyond infrastructure control points, including network and endpoints
- Providing automation capabilities for repetitive tasks
- Reducing training and up-leveling tier-1 support by providing a standard management and workflow experience across security components
- Providing usable and high-quality detection content with little-to-no tuning required

MAXIMIZE ROI

Comprehensive, scalable, customized, and integrated for information technology and security operations – the ECS McAfee XDR platform is delivered as a full-service solution.

The platform is built to maximize ROI by combining your existing toolset with industry-leading technology. In addition, ECS focuses on continuous improvement. We'll meet your current IT and security needs and work together to modernize your security program.

ECS will introduce dedicated resources across various IT and security-related functionalities. That includes IT help desk support, networking engineering, e-mail and cloud application management, security engineering, and threat analysis.

SUPERIOR SUPPORT

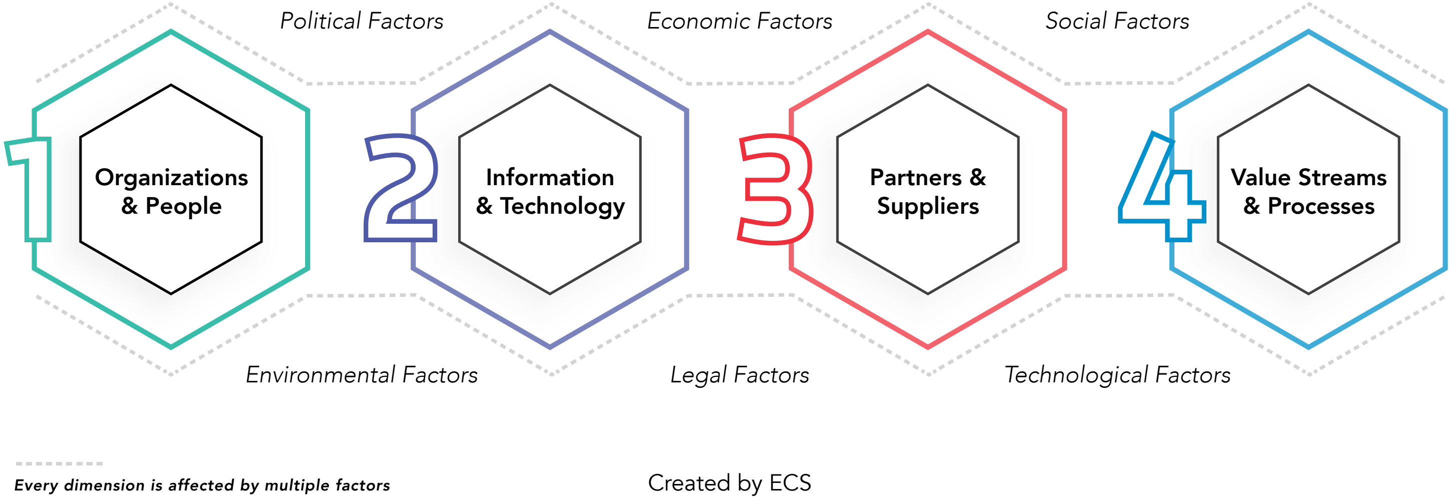
A dedicated program manager works with you hand-in-hand to deliver against mutually agreed upon use cases and requirements.

ECS also provides a 24x7x365 IT help desk/service desk, along with specialized IT support resources.

The support team is trained across all operating systems in various client environments and serves tier-1 support for security and IT troubleshooting.

ECS follows the IT Infrastructure Library (ITIL) framework for our service desk operations. The use of ITIL processes reduces trouble resolution and deployment times. We deploy, install, configure, debug, and maintain end-user computing systems throughout the lifecycle and ensure compliance with all standards.

ITIL Framework



Created by ECS

ECS uses enterprise tools for entering and tracking ticketing information through a proprietary process known as CARE2. CARE2 stands for Communicate and Coordinate, Assess and Assemble, Respond and Report, Evaluate and Evolve. CARE2 tracks all customer tickets and ensures consistent and accountable communication with stakeholders.

We strive for a constantly evolving support environment that drives customer satisfaction and process improvement through comprehensive reporting and evaluations. The methods by which we assess issues and assemble resources fully support our customers' unique needs and circumstances.

BENEFITS OF ECS MANAGED SOLUTIONS

- 24x7x365 access to a service portal to track activities, escalations, and threat reports
- Deep cybersecurity domain expertise, a long track record of success, and highly respected industry veterans
- Threat intelligence derived from multiple sources (150+), providing real-time analysis, indicators of compromise (IoCs), open-source intelligence (OSINT), and prioritized escalations and ticketing
- McAfee Labs' global threat intelligence feeds directly to your SIEM solution
- US-based McAfee security consultants and analysts
- Service built on a high-touch, core advisory services model
- Proven event detection and remediation methodology

ELITE CYBERSECURITY TALENT

ECS maintains a staff of experienced employees qualified to assist our customers with a broad range of IT, networking, and application requirements. We cultivate the expertise necessary to support legacy and current operating systems and platforms, large data center footprints, hybrid cloud environments, segmented network architectures, and more to deliver successful outcomes across a broad range of commercial and federal customers.

Engineering: The ECS engineering team is purpose-built and trained to offload the day-to-day management of our clients' IT and security tools. ECS engineers offer support in architecture, design, implementation, management, and troubleshooting with competencies covering the endpoint to the cloud.

Cloud: ECS provides premier consulting for several cloud providers, including AWS, Azure, and Google Cloud. As a managed service provider, we provide IaaS, PaaS, migration, 24x7 support, software development, and more.

Security Monitoring & Threat Analysis: Our analysts use a combination of your existing technology and additional cyber threat tools to build a state-of-the-art threat detection program customized for your enterprise.

ECS leverages log management tools to help capture activity and events from across your network.

We maintain the logs for compliance purposes and use them to establish a normalization baseline within your environment. Our analysts and engineers ensure we receive logs from all critical data sources, assisting with custom parsers or collection techniques as needed.

THREAT INTELLIGENCE

ECS analysts use a combination of tools and expertise to monitor and hunt for suspicious or anomalous activity across your environment. In addition to your SIEM tools, ECS implements our threat analytics stack, threat intelligence platform, advanced threat feeds, case management, and orchestration. This combination of tools streamlines operations and minimizes the time from threat detection to mitigation.

ECS' threat intelligence stack of over 63 threat intelligence feeds introduces world-class threat data from around the globe so our team can identify malicious and anomalous activity on your network.

POWERFUL THREAT INTELLIGENCE CAPABILITIES

- Our leading intelligence analysts combine technical and strategic capabilities to provide the information you need from the executive level to the SOC
- Analysts work closely with our SOC team to glean intelligence from our MDR offering to customers with the latest observations
- ECS has a window into different industries and provides unique observations tailored to your specific industry
- Our analysts are available to answer questions about IOCs, intel reports, and the latest trends in the threat landscape
- We track 150+ sophisticated actors, including financially motivated cybercriminals, hacktivists, and nation-states from across the globe

The XDR platform leverages data from the endpoint, network, cloud infrastructure, and cloud application environments to get ahead of adversaries, drive faster and better decisions, gain unified visibility and control, and orchestrate efficient SOC workflows.

Let us help you leverage your current technology investments to make faster, more decisive decisions.

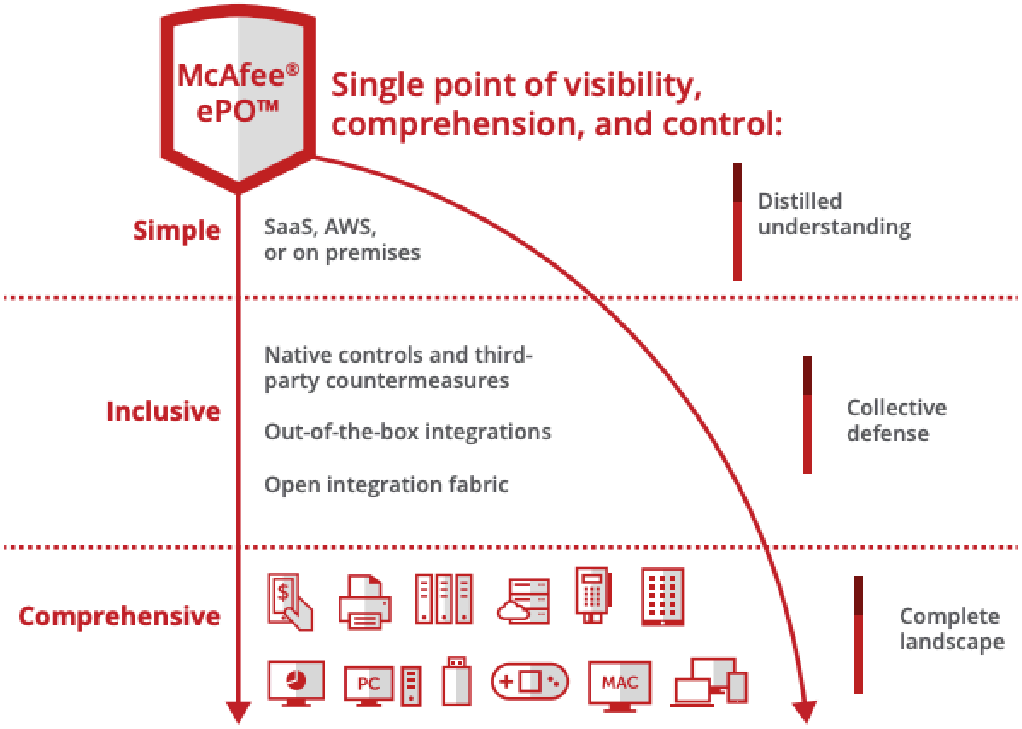

McAfee® ePO™
Single point of visibility, comprehension, and control:
Simple
SaaS, AWS, or on premises
Distilled understanding
Inclusive
Native controls and third-party countermeasures
Out-of-the-box integrations
Open integration fabric
Collective defense
Comprehensive
PC
MAC
Complete landscape

Figure 1: XDR delivers next-generation SOC capabilities at a highly competitive price.

NEXT STEPS

The ECS team is ready to help secure your environment, customers, and data. If you recognize that today's most dangerous threats require a dynamic cybersecurity response, here's what to do:

- Review this Solution Guide with your team
- Schedule an XDR meeting with our team of experts
- Get back to driving business forward, confident that your organization can defend against today's most dangerous threats

Interested in learning more about the ECS McAfee XDR platform?
Reach out and **speak to an expert today.**

ECS is a leading information technology provider delivering solutions in cloud, cybersecurity, software development, IT modernization, and science and engineering. The company's highly skilled teams approach and solve critical, complex challenges for customers across the U.S. public sector, defense, and commercial industries. ECS maintains partnerships with leading cloud and cybersecurity technology providers and holds specialized certifications in their technologies.

SCHEDULE A MEETING