ECS

ECS XDR
SOLUTION GUIDE

Cybersecurity threats confront every area of your business. Real threats take time to identify. False positives create distractions. Limited time and resources, alert fatigue, and a lack of the right tools prevent you from handling these threats as best you can.

That’s where extended detection and response (XDR) comes in. XDR provides a high-level view of the most important and urgent threats facing your enterprise. A level up from the maturity of endpoint detection and response (EDR) and managed detection and response (MDR), XDR integrates multiple sources of data, revealing connections that empower you to take on the most pressing cyber threats.

Plus, investing in XDR doesn’t mean buying all new systems. ECS will work with you to build onto your existing technology investments. When you’re looking for an enhanced level of security, ECS’ XDR solution will help you achieve it.

VISIBILITY

CHALLENGE: Disparate cybersecurity data and alerts take time to correlate, limiting your visibility into threats.

SOLUTION: XDR consolidates all your security alerts into one view of your environment. We aggregate data from endpoint and non-endpoint sources including cloud apps, cloud services, network traffic, and security information and event management (SIEM). By automatically correlating and validating alerts, our XDR solution gives analysts a centralized view of every incident, enabling your team to respond more quickly and efficiently to real cyber threats.

FOCUS

CHALLENGE: Alert fatigue prevents your team from quickly distinguishing real threats from false positives.

SOLUTION: By converting a stream of alerts into a manageable number of incidents, ECS' XDR solution enables your team to focus your efforts on valid alerts and actionable intelligence. Our single-pane view cancels out the extra noise from unnecessary or irrelevant alerts so that we can quickly provide you with actionable intelligence that distinguishes real threats from false positives.

RESPONSE

CHALLENGE: Validating the full scope of an incident and quickly taking action is hard without the right tools and automation.

SOLUTION: With ECS' XDR solution, when threats are identified, we provide you with actionable recommendations and a plan of response. Centralizing your alert data in one place enables our experts to provide expedient risk mitigation and light incident response, delivering the ability to not only take action on endpoints but other security tools in your environment as well.

EFFICIENCY

CHALLENGE: Your team lacks the people, resources, or expertise to implement an XDR system.

SOLUTION: ECS provides a fully managed 24/7/365 XDR solution, enabling your team to focus on the most important thing: responding to real threats quickly. Because we hold certifications like ISO and SOC 1-2 and store your data as a single tenant, you can rest assured that our tools and processes are vetted for your security. ECS **ARC Intelligence** provides a threat analytics stack, threat intelligence platform, advanced threat feeds, case management, and orchestration to minimize the time it takes to detect and mitigate threats.

Interested in learning more about ECS' XDR solution?
Reach out and **talk to an expert** about our custom, U.S.-based solutions.

ECS is a leading information technology provider delivering solutions in cloud, cybersecurity, software development, IT modernization, and science and engineering. The organization's highly skilled teams 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.