Managed Extended Detection and Response

CONTAIN CRITICAL THREATS IN MINUTES, NOT DAYS

Enterprise-grade security, delivered as a seamless extension of your team

NIST National Institute of Standards and Technology

Response process
NIST 800-61

What Makes Us Different

Our co-managed security operations model allows you to retain ownership, visibility, and authority over your environment. We manage the operational burden.

You keep administrative access to the XDR platform.

- You see the same alerts, investigations, and outcomes our SOC sees.
- We handle 24x7 monitoring, triage, and response so your team doesn't have to. This "glass box" model ensures transparency, trust, and alignment—without outsourcing accountability.

To learn more about Managed Extended Detection and Response, contact your Connection Account Team today!

1.800.998.0067
www.connection.com/services

The Challenge: Alert Overload and the Skill Gap

Building a full, 24x7 security operations center (SOC) is often complex and cost prohibitive. The cybersecurity landscape presents a constant barrage of alerts that can overwhelm even the most capable IT teams.

- 86% of organizations identified a shortage of skilled cybersecurity professionals as a major challenge. The talent gap is a critical threat vector.*
- 86% of organizations say they have experienced AI-related security incidents. Modern threats are evolving faster than teams can track them.*
- 4% of organizations reached the Mature stage of cybersecurity readiness. Most organizations are highly exposed to risk.*

Managed Extended Detection and Response Services: Your 24x7 Co-managed SOC

Managed XDR delivers 24x7 threat detection and response as a co-managed service, combining industry-leading XDR platforms with expert human analysts who actively investigate and contain threats on your behalf. We work with your team, not around it, providing enterprise-grade security outcomes without forcing you to surrender control or build an in-house SOC. We reduce noise, accelerate response, and stop threats before they become incidents.

Our Approach to Managed XDR

Managed XDR is built to reduce noise, accelerate response, and close security gaps without adding operational burden to your team. Our delivery model combines prevention, unified visibility, expert-led integration, and active response to stop threats before they escalate.

- **Prevention-first Mindset**—Our onboarding begins with a deep dive security health check, tuning endpoint, firewall, and identity controls to dramatically reduce background noise so real threats stand out.
- **24x7 Monitoring and Intelligent Correlation**—Our security operations team monitors your environment around the clock, correlating weak signals across endpoint, network, and cloud into high fidelity incidents that demand action.
- **Human-led Investigation**—Automation accelerates detection, but context matters. Every critical alert is reviewed by a certified security analyst to confirm the threat is real before escalation or response.
- **Active Containment and Response**—This is the difference between monitoring and management. When a threat is confirmed, we execute pre-approved response playbooks—isolating hosts, revoking access, and blocking malicious activity—to stop incidents before they become breaches.

* Cisco Cybersecurity Readiness Index 2025