Connection
we solve IT®

Managed Cisco Extended Detection and Response

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.
  (Source: Cisco Cybersecurity Readiness Index 2025)

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

Managed Cisco XDR delivers 24x7 threat detection and response as a co-sourced service, combining Cisco's industry-leading XDR platform 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 Cisco XDR

Managed Cisco 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, using Cisco XDR to correlate 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.

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

1.800.998.0067 ■ www.connection.com/services

CISCO
Partner

CONTAIN CRITICAL THREATS IN MINUTES, NOT DAYS

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

NIST
National Institute of
Standards and Technology

Response process
NIST 800-61

The Connection Advantage

Connection has been a Top Tier Cisco Partner since 2008, with specializations in XDR, SASE, and Secure Networking.

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 Cisco XDR

- 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.