OUR SOLUTIONS

Expel MDR for CrowdStrike environments

24x7 monitoring across your endpoint, SIEM, and identity surfaces

Addressing security challenges with MDR

Cybersecurity is more challenging than ever, with a relentless barrage of sophisticated attacks overwhelming security teams and contributing to widespread alert fatigue. Even with organizations investing in robust security platforms like CrowdStrike, the sheer volume and complexity of threats can stretch internal resources thin, especially when compounded by the persistent cybersecurity skills gap.

An external managed detection and response (MDR) provider offers a vital layer of supplementary protection for your CrowdStrike environment, helping you manage incoming alerts and correlate data across your identity, endpoint, SaaS, and cloud environments. By adding its own unique detection methods and threat intelligence, an external MDR can significantly enhance protection beyond CrowdStrike's built-in features and help detect and respond to threats that might otherwise go unnoticed.

Augment your CrowdStrike investment

Expel Managed Detection and Response (MDR) enhances your security posture by providing expert threat detection and response, helping you get the most out of your current security tools, address staffing shortages, and avoid business interruptions. Our service allows you to fully leverage your CrowdStrike investment through direct API integrations and a swift, adaptable onboarding process that delivers rapid value (often within days, hours, or even minutes, as you can see in this demo).

Expel offers 24×7 coverage across endpoints, cloud, and more with complete transparency. Our expert security team, multi-surface managed response actions, and AI-powered Expel Workbench™ platform deliver rapid, quantifiable outcomes, including a 17-minute MTTR for critical alerts and a 308% annual ROI.*

24x7 monitoring for your CrowdStrike infrastructure

Expel MDR processes and correlates native alerts from across your security tools and cloud environments and enhances them with proprietary detection rules that align with the MITRE ATT&CK framework. Our expert team provides always-on monitoring of your incoming alerts, and full correlation and investigation across your full technology stack, as well as remediation guidance and actions to contain those threats. Moreover, we incorporate threat intelligence from our customer base and external sources to refine alerts, minimize noise, and extract maximum security insights. With our built-in AI and automations, Expel is able to reduce the noise from your CrowdStrike alerts by over 91% on average.**

* Enterprise Strategy Group: Analyzing the Economic Benefits of Expel's Managed Detection and Response Services, April 2025
** Expel internal tracking of false positive reduction rate for CrowdStrike technologies, May 2024 - May 2025.

REAL-WORLD USE CASES

Malware
Protect your organization with 24×7 monitoring and response to detect and neutralize malware before it spreads.

Living-off-the-land (LoL) attacks
Expel rapidly identifies threats using its detection engine, behavioral library, and expertise, with kill process and host isolation actions for quick containment.

Credential theft
Swiftly identify and respond to credential theft tactics like stolen credentials, hashes, and kerberoasting attacks with auto-response actions.

Suspicious network connections
Contain threats quickly by identifying suspicious and unexpected inbound/outbound connections from the endpoint, paired with remediation guidance and auto-response actions.

Expel supports the following CrowdStrike technologies with direct API integrations.

ON-PREM AND CLOUD ENDPOINTS	SECURITY OPERATIONS & SIEM	IDENTITY & ACCESS
CROWDSTRIKE **CrowdStrike Falcon**	CROWDSTRIKE **CrowdStrike Falcon Logscale** **CrowdStrike Falcon Data Replicator**	CROWDSTRIKE **CrowdStrike Falcon Identity**
• Malware and ransomware • Suspicious file activity • Registry modification • Suspicious code execution • Defense evasion • Credential access and credential dumping	• Credential access • Command and control • Data exfiltration • Suspicious network activity	• Detect passwords included in known leaks

How you'll benefit with Expel MDR

Extend CrowdStrike protections with Expel's expertise

Expel MDR provides an additional layer of protection, adding our detection rules, threat intelligence, expert SOC team, and machine learning capabilities to CrowdStrike's native detections for more extensive coverage and protection from attacks.

Maximize ROI of existing tech stack

Expel integrates with CrowdStrike and over 160+ other security tools across various environments, providing full visibility and coverage. We maximize current investments and support future growth—without forcing you to replace existing systems.

Get transparent and fast response

Expel delivers managed response across multiple surfaces with a 14 -minute average remediation time. Benefit from synchronization with your CrowdStrike tools for complete visibility into the status of Expel actions and related CrowdStrike alerts.

Unburden your SecOps

Enhance your SOC with 24/7 monitoring and an extensive threat detection library. Reduce strain with Expel alert status updates synced to your Falcon environment, avoiding console switching and manual work.

What our customers say

"We were looking for a trusted partner relationship. We weren't viewing this search as simply getting a point solution, but rather bringing in a company that could grow alongside us, and help us to improve and learn. We wanted to transition from making fear-based security decisions to making risk-based ones."

LEWIS MCINTYRE

Director of Cybersecurity and Incident Response

MARKEL

Don't settle for less; work with the leader in MDR.

Contact an Expel sales representative to learn more or visit expel.com.

expel