



OUR SERVICES

Expel MDR Premium

Industry-Leading Managed Detection and Response

Your challenge

Security operations teams are suffering from exhaustion, triaging an endless stream of alerts, wasting time on false positives, and losing time for the more strategic work that delivers results. Simultaneously, security leaders continue to face challenges in hiring, training, and retaining talent, which leads to even more overwhelm for the team. Despite the constant burn out, the SOC still needs to ensure all of their attack surfaces are secure, 24/7.

To combat this strain, many organizations seek outside help from a managed detection and response (MDR) service so that they can keep up with the work without accidentally missing threats. Unfortunately, most MDRs are complex to onboard and configure, lack comprehensive detection and threat intelligence, and provide little visibility into the investigation process. This often leaves customers unsure what work is being done, ultimately creating more work and more alerts to triage.

How we help

Expel Managed Detection and Response (Expel MDR) is the industry-leading MDR provider that delivers rapid detection and response, and helps you build cyber resilience. Our technology-driven approach to MDR leverages automation and AI to deliver best-in-class managed services.

Expel MDR takes work off your plate by quickly detecting risks across your tech environment and collaborating with your team to verify the threat, take critical remediation actions, and provide a detailed report of what happened, where, when and why in real-time through our Expel Workbench™ platform. This reduces the strain on your internal teams, provides confidence that your environment is secure 24/7, and gives you time back for those important projects.

Expel MDR Premium Benefits

Expel Workbench is constantly leveraging the insights from every customer to deliver improved security outcomes.

24/7 World-Class Service Delivery

Get up and running quickly with seamless onboarding and support, direct contact with our SOC during incidents, full transparency, and assurance that you're covered 24/7.

Industry-Leading Protection

Our technology-powered SOC delivers unrivaled security outcomes across every metric, tailored to you. Expel keeps you safer, more informed, and better prepared.

Automation and AI to Improve Outcomes

Expel Workbench automation and AI accelerate triage, investigation, and remediation, reducing false positives, adding context, and driving faster resolution times.

Improve Cyber Resilience

We help you get the most from your technology stack with continuous resilience recommendations from our SOC, so you can stay ahead of the latest threats while reducing your exposure.

WHY EXPEL

23

minutes mean-time-to-respond (MTTR)

1.7

minutes mean-time-to-detect (MTTD)

120+

technology integrations

2.6

minutes mean-time-to-touch

What you get with Expel MDR Premium

		MDR PREMIUM with pro support
24/7 SOC Monitoring	Real-time alert investigation and triage	✓
	Direct SOC-to-customer alert/incident communications (via Slack/MSFT Teams, virtual conference)	✓
AI & Automation-Powered Detection Coverage	Comprehensive, multi-layer detections mapped to MITRE ATT&CK®	✓
	Detection, context, tuning, prioritization and correlation - powered by Josie and Ruxie™	✓
	Coverage for all listed attack surfaces: cloud, identity, SaaS, endpoint, network	✓
Expert remediation guidance & response	Remediation and resilience recommendations	✓
	Automated remediation	Multi-surface auto-remediation + manual fallback where possible
Threat Research	Threat bulletins	✓
	On-demand SOC access	72 hours, +
Platform & Technology	Expel Workbench™ user interface	✓
	Active technology device integrations (maximum)	Unlimited
	Expel Workbench API	✓
Metrics & Reporting	Detailed status & visibility on every alert	✓
	Self-service dashboarding and reports	✓
SIEM Coverage	SIEM utilization for investigative context	✓
	Out-of-the-box SIEM rules coverage	✓
	Coverage and tuning of custom rules*	✓
Concierge Service Delivery	Onboarding	White glove, human-assisted onboarding and training
	Ongoing touchpoints	Named resource for recurring business and executive reviews with custom metrics
	Technical and advanced functionality support	Via Zendesk, Workbench, Email or Slack/Teams + Zoom Follow up upon request
Additional Managed Services	Expel Threat Hunting (hypothesis-based)	+
	Expel Vulnerability Prioritization	+
	Expel Phishing	+



Learn more at expel.com