OUR SOLUTIONS

Expel MDR for Palo Alto Networks environments

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

Addressing security challenges with MDR

You know the drill—your team is drowning in alerts while sophisticated attacks keep evolving. Even with solid platforms like Palo Alto Networks in place, you're still dealing with alert fatigue, staffing gaps, and the constant pressure to catch threats that slip through the cracks.

That's where Expel MDR comes in. We plug directly into your existing Palo Alto Networks environment and handle the heavy lifting—triaging alerts, correlating data across your XDR, network, SIEM, and cloud/SaaS infrastructure, and adding our own detection logic on top of what you already have. Think of it as extending your SOC without the headcount or budget battles.

Maximize your Palo Alto Networks ROI

You've already invested in Palo Alto. Expel helps you get actual value out of it instead of letting alerts pile up in queues. We integrate directly via API, so onboarding is fast—we're talking days or hours, not months of implementation headaches.

Our analysts provide 24×7 coverage across your entire environment. The Expel Workbench™ platform uses AI and automation to cut through the noise, and our team delivers an average 14-minute mean time to remediate (MTTR) for critical/high alerts. Our customers typically see a 308% annual ROI[1] because we help them use their security tools effectively.

Continuous, intelligent monitoring for your Palo Alto environment.

Here's how it works: We take your native Palo Alto Networks alerts and correlate them with everything else in your environment. Our detection rules are built around MITRE ATT&CK tactics, so you're getting coverage that maps to real adversary tactics, with a focus on early identification in the attack lifecycle.

Our analysts don't just monitor and throw alerts over the fence—they investigate, provide remediation guidance, and can even take auto-containment actions when needed. We also feed threat intelligence from our entire customer base and external sources back into your environment, which means you benefit from attacks we've seen elsewhere.

Bottom line: We reduce Palo Alto alert noise by over 86% on average[2] through our AI and automation, so your team can focus on what actually matters instead of chasing false positives.

[1] Enterprise Strategy Group: Analyzing the Economic Benefits of Expel's Managed Detection and Response Services, April 2025

[2] Expel internal tracking of false positive reduction rate for Palo Alto, May 2025 - May 2026.

REAL-WORLD USE CASES

Suspicious network connections

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

Credential theft

Swiftly identify and respond to tactics like credential/process dumping, PowerShell cmdlet, and potential mimikatz and kereboasting attacks.

Living-off-the-land (LoL) attacks

Expel detections quickly identify execution, persistence, defense evasion, and other common LOL tactics, with host isolation actions for quick containment.

Malware

Protect your organization with 24×7 monitoring and response to detect and neutralize malware, and block bad hashes before they spread.

Abnormal API use

Quickly identify and remediate access keys for suspicious API calls across your network.

Expel provides coverage for the following Palo Alto technologies:

ENDPOINT/ XDR	SECURITY OPERATIONS/ SIEM/LOGGING/ IDENTITY	NETWORK	CLOUD & SAAS
paloalto NETWORKS **Palo Alto Networks Cortex XDR Pro**	paloalto NETWORKS **Palo Alto Networks Cortex XSIAM** **Palo Alto Networks Cortex XDR Pro** **Palo Alto Networks Strata**	paloalto NETWORKS **Palo Alto Networks Panorama** **Palo Alto Networks Next Gen Firewall**	paloalto NETWORKS **Palo Alto Networks SaaS Security (fka Prisma SaaS)** **Palo Alto Networks Prisma Cloud Compute** **Palo Alto Networks Strata**
• Malware and ransomware • Suspicious file activity • Registry modification • Suspicious code execution • Defense evasion • Credential access and dumping	• Credential access • Command and control • Data exfiltration • Suspicious network activity	• Data exfiltration • Suspicious network activity • Malware traffic • Suspicious ports	• Suspicious authentication • Credential access • Privilege escalation • Suspicious execution • Defense evasion

How you'll benefit with Expel MDR

Extend Palo Alto Networks protections

Expel MDR adds detection rules, threat intelligence, an expert SOC team, and machine learning to Palo Alto Networks' native detections for more extensive coverage and protection from attacks

Maximize ROI of existing tech stack

Expel integrates with Palo Alto Networks and 160+ other security tools, 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 for high/critical alerts. Benefit from synchronization within Palo Alto Networks Cortex XDR for complete visibility into the status of Expel actions and related Palo Alto Networks alerts.

Unburden your SecOps

Enhance your SOC with 24×7 monitoring and an extensive threat detection library. Reduce cyber strain with Expel alert status updates synced to your Palo Alto Networks Cortex XDR instance, avoiding console switching and manual work.

What our customers say

"Expel's remediation recommendations allowed us to make better decisions faster, especially at 2am. We put an incredible amount of trust in Expel to go through all of the alerts we receive, so we no longer have to worry at the end of every week about trying to track them all down."

SENIOR VP OF RISK AND INFORMATION SECURITY
FIA Tech

FIATECH

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

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

expel