OUR SOLUTIONS

Expel MDR for Microsoft environments

24x7 monitoring across your attack surfaces

Addressing security challenges with MDR

The pressure is on. You're facing a relentless barrage of cyber threats and the resulting alert fatigue is overwhelming your already stretched security team. The skills gap only compounds the problem. It's no surprise you're exploring managed detection and response (MDR) providers. You need 24×7 expert monitoring, threat hunting, and rapid incident response to stay ahead of sophisticated attacks. However, navigating this landscape requires careful consideration. You also need a partner that integrates seamlessly with your existing tools, not one that demands costly replacements or a new SIEM investment.

Many IT and security teams, likely including yours, are consolidating their security stacks around platform vendors like Microsoft. This strategic consolidation aims to streamline operations, reduce complexity, and ultimately, lower costs and simplify security management. Now, you just need an MDR partner who can support your Microsoft environment.

Augment your Microsoft investment

Expel MDR provides an additional layer of security expertise for organizations like yours who need help identifying and responding to cyber threats, maximizing existing security investments, solving security talent gaps, and preventing business disruption. Expel's unique approach enables your organization to utilize your existing Microsoft investment to its full potential with direct API connections and fast, flexible onboarding that delivers value within days (or hours). No matter which enterprise license (E3, E5, etc.) you've invested in, Expel MDR is ready to support your Microsoft infrastructure.

Expel's 24×7 coverage spans the widest breadth of attack surfaces from endpoint to cloud, including over 160+ security technology integrations. With world-class security practitioners, multi-surface managed response, and an AI-driven platform (Expel Workbench™), you get fast, measurable results, including a 14-minute mean time to remediate (MTTR) for high/critical alerts.

24x7 monitoring for your Microsoft infrastructure

Expel MDR processes native alerts from your security tools, enhancing them with proprietary detection rules that align with the MITRE ATT&CK framework. Our expert detection engineering team continuously analyzes and develops new rules and analytics tailored to your specific attack surfaces and Microsoft technology footprint. Moreover, we incorporate threat intelligence from our customer base and external sources to refine alerts, minimize noise, and extract maximum security insights. With the combined power of our SOC expertise and technology, Expel is able to reduce the noise from your Microsoft alerts by over 66% on average.

REAL-WORLD USE CASES

Identity & account compromise

Continuous monitoring of user activity and behaviors helps detect anomalies, so you can quickly identify and remediate compromised accounts.

Malware

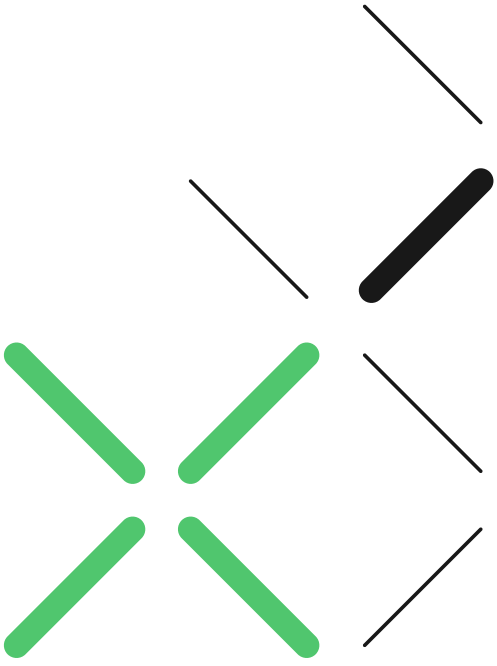
Protect your organization with 24×7 monitoring and response to detect and neutralize malware before it spreads.

Discovery & lateral movement

Identify enumeration activity, suspicious role and policy changes, and unexpected user and API activity that indicates that an attacker is attempting to discover and exploit cloud resources.

Data exfiltration

Protect against unauthorized use and transmission of data with full investigative support and rapid response to restore systems and prevent future attacks.



Expel supports the following Microsoft technologies with direct API integrations:

MICROSOFT TECHNOLOGY	ATTACK SURFACE	USE CASES
• Microsoft Azure • Microsoft Azure Log Analytics • Microsoft Azure Kubernetes Service (AKS) • Microsoft Azure Monitor Activity Log • Microsoft Defender for Cloud Apps • Microsoft Defender XDR	CLOUD	• Suspicious user activity • Suspicious API calls • Risky policy changes • Enumeration • Cryptomining
• Microsoft Defender for Endpoint • Microsoft Defender for Endpoint with Intune	ENDPOINT	• Malware and ransomware • Suspicious file activity • Registry key modification • Suspicious code execution • Defense evasion
• Microsoft Entra ID Protection	IDENTITY & ACCESS	• Suspicious authentication
• Microsoft 365 • Microsoft Teams	SaaS	• Anomalous login activity • Suspicious role changes • Data exfiltration • Lateral movement
• Microsoft Sentinel	SECURITY OPERATIONS & SIEM	• Credential access • Command and control • Data exfiltration • Suspicious network activity

How you'll benefit with Expel MDR

Maximize ROI on your Microsoft investment
With over 160+ integrations with Microsoft and other security tech, there's no need to rip and replace. Expel works with your existing infrastructure, helping you make the most of your current investments and enabling you to grow with any new ones.

Holistic visibility and coverage
Expel maintains comprehensive visibility across your environment and multiple attack surfaces, ensuring gaps are covered and conducting root cause analysis when incidents arise.

Unburden your SecOps
Enhance your SOC with 24×7 coverage, multi-surface managed response, and an extensive detection library, reducing the burden on detection engineering. Expel AI and automations reduce false positive noise from Microsoft alerts by up to 66%, alleviating the strain on your team.

Simplify SIEM management
Extract more value from your Sentinel configuration with Expel's onboarding and rule optimization assistance, and get the most from your investment with ongoing support for your custom and out-of-the-box rules.

WHAT OUR CUSTOMERS SAY

"Folding our SIEM into Expel Workbench gives us a more comprehensive view of our Microsoft 365, Defender, and Azure Active Directory ID security events and alerts. Together, they enable faster and more accurate incident response. And with more streamlined workflows and less manual effort, we gain back valuable time to address other security needs."

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 our website expel.com.

expel