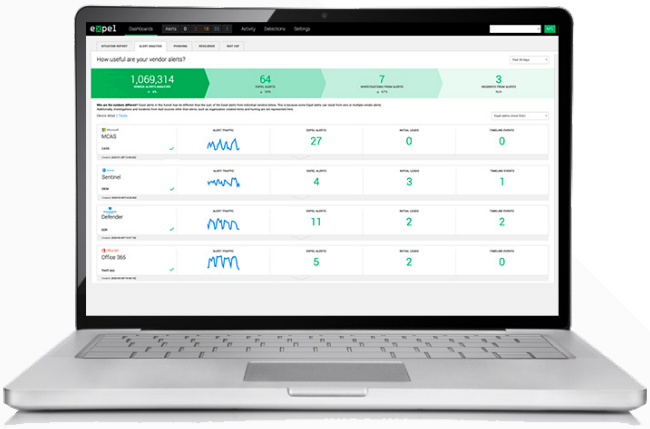
Expel for Microsoft

24x7 Managed detection and response

You're heavily invested in Microsoft and its security tools, now it's time you get the most value out of it.

With so many tools out there it can be tough to know where to start and what to look for. At Expel, we ingest signal from your Microsoft stack via API and apply our detection strategy for each tool to catch suspicious activity before the damage is done.



What does Expel for Microsoft include?

- 24x7 monitoring of Azure, O365, Defender for Endpoint, Sentinel, MCAS and more
- Detections written by Expel for an added layer of security where it's need most (we're looking at you, cloud)
- Response actions for each incident so you know what happened and what you need to do about it (written in plain English)

What you get

Make your Microsoft investments work harder for you. Expel's 24x7 managed detection and response protects your full Microsoft environment across email, endpoint, SIEM and cloud.

Automate security operations across your Microsoft stack to speed up time-to-detect and time-to-fix

Boost visibility with comprehensive monitoring of Microsoft's tools and apps across on-prem, cloud and everywhere in between

Optimize signal get the most out of the Microsoft investments you already made with metrics to prove it

www.expel.io

Why Expel?

With Expel you get answers, not alerts. We cut through the 'white noise' of alerts by layering our experience on top of Microsoft's tools and collaborate with you in real-time so nothing falls through the cracks.

Detections for Microsoft provide an added layer of alerting based on Microsoft-specific features that attackers are known to exploit

Collaborate on Teams with our analysts (and bots) for quick messaging when things looks suspicious

Get full transparency so you can see exactly what our analysts are doing for you 24x7... as it's happening

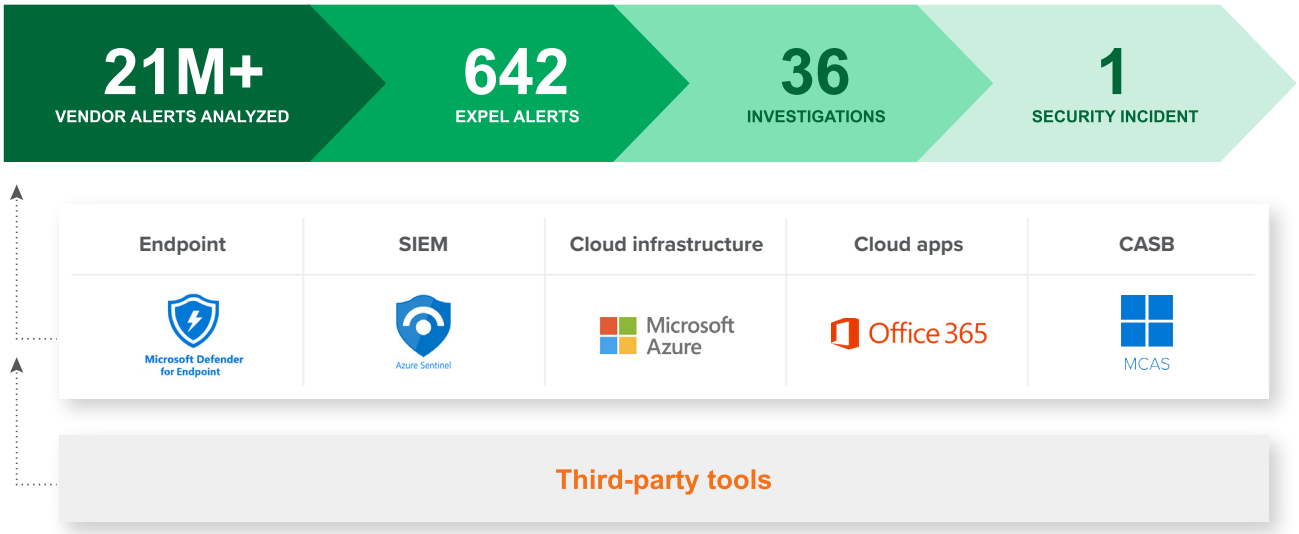
Ivanhoé Cambridge

Ivanhoe Cambridge, a real estate investment firm, relies on Expel to monitor the organization's many security signals, including Microsoft Azure, Microsoft Defender for Endpoint and Office 365.

"Expel built a platform that ingests alerts across our vast network, evaluates and weeds out millions of false positives, and then automates the investigative steps so Expel analysts can recommend the right next actions to our team. That's what Expel does for us; their approach just makes sense,"

–Patrick Gilbert, head of security at Ivanhoé Cambridge

It all starts with your Microsoft security signal



Expel's a managed detection and response (MDR) provider whose mission is to make great security as accessible as the internet. The company's SOC-as-a-service capability offers 24x7 security monitoring and response for cloud, hybrid and on-premises environments.

Learn more at www.expel.io.