expel

OUR PRODUCTS

# Expel Managed Detection and Response

24/7 detection and response across attack surfaces

## Your challenge

Managing multiple attack surfaces is no easy task. Ensuring your on-premises resources are secure is challenging enough, but then throw in cloud—including SaaS apps and Kubernetes—and things get complex quickly.

Also, you don't just need security, you also need visibility into your environments to know what's working, what's not, and what improvements you can make to your security posture long term.

## Our solution

Expel Managed Detection and Response® (MDR) provides answers, not alerts. We integrate with the tech you already have—across attack surfaces—to maximize your existing tech investments. Our platform automates analysis for your vendor alerts to filter out false positives. We'll enrich the alerts that matter with context so we can resolve them with an average alert-to-fix of 22 minutes for critical alerts.

You choose the attack surface you'd like us to monitor and we'll:

- Prioritize detections based on your key assets
- Reduce alert-to-response to minutes
- Automatically stop threats from spreading
- Arm you with metrics to strengthen your security

## How you'll benefit

✓ **100+ integrations**

Connect your tech to our platform without agents. We'll apply custom detections and learnings to gain deeper insight and improve ROI.

✓ **The right automation at the right time**

We automate log ingestion and alerting, and provide remediation recommendations—or use automation to perform remediation on your behalf.

✓ **Transparency all day, every day**

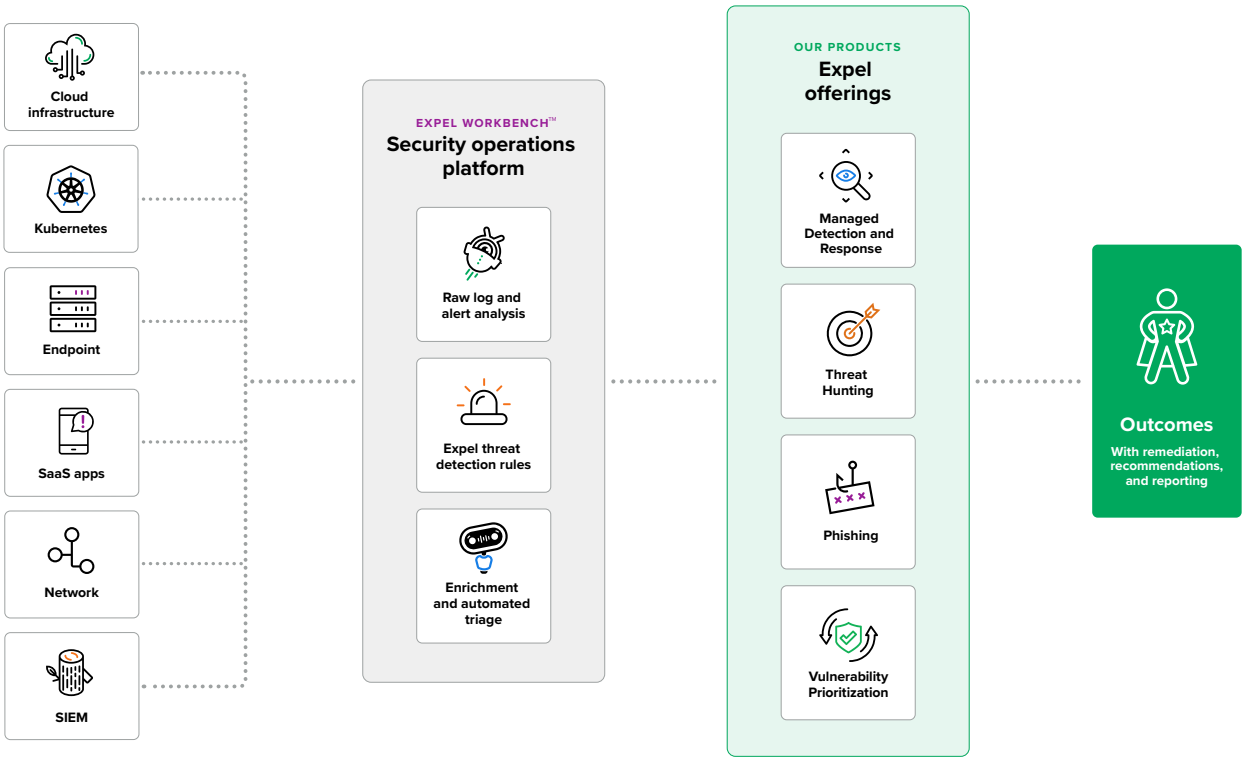
Get complete visibility into the investigation process through real-time alerts when incidents arise, plus intuitive reporting for a full picture of your risks and how to prevent them in the future.

✓ **Less noise, more context**

Our security operations center team investigates only the suspicious events that require further analysis, so you get immediate answers to the alerts that matter the most.

# How Expel MDR works

Expel MDR is powered by our security operations platform, Expel Workbench™, which integrates with your tech, digests your alerts, adds context, enriches alerts with intel, and assesses the risk. We then use automation to remediate or send to an analyst for further investigation.




# Why Expel

**Expel-written detection rules**
We boost your security with rules based on simulated and real-life attacks to continuously improve your time-to-respond.

**Threat-specific reporting**
Expel Workbench provides attack diagrams, maps, and timelines specific to different threats.

**Response details**
After our analysts investigate, Expel Workbench gives you detailed reports with clear actions.

**Resilience recommendations**
Get clear guidance on how to improve and diagnose the root cause of repeated incidents.

CORVUS

**"Everyone at Expel—from its leadership to our account team—understands the mindset of attackers and how to bring technology to bear to solve these challenges. No other company approaches the problem of security the way that Expel does."**

**Jason Rebholz,** CISO, Corvus Insurance

**Visit www.expel.com to learn more**
about Expel Managed Detection and Response.

expel

863GE70FR-08/10/23