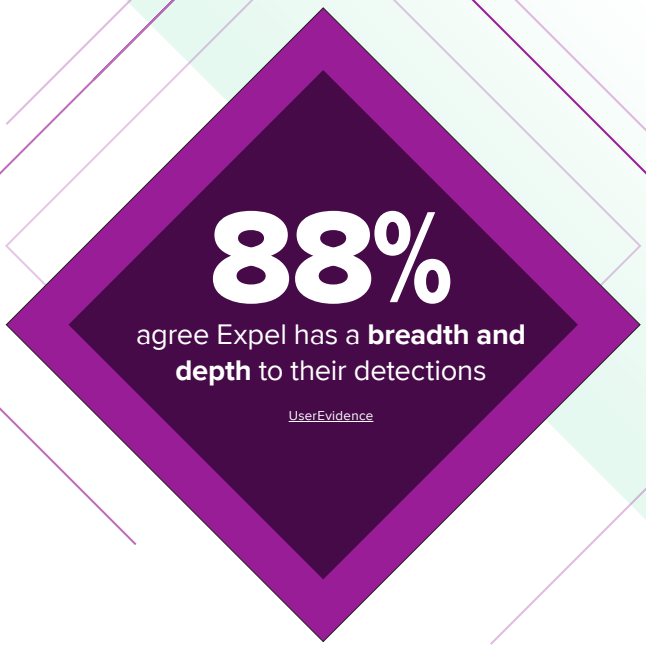
Uplevel your MITRE coverage

Comprehensive detections align to MITRE to easily track and improve threat coverage



YOUR CHALLENGE

Finding and remediating attacks as early as possible is still the most effective way to protect your organization from a constantly evolving threat landscape.

But it's nearly impossible to anticipate every infiltration, and every tactic, every time.

To do so, you must think like an adversary, keeping up with the latest techniques and constantly evolving your approach. The problem is that attackers never stop innovating with new ways to breach your defenses. Many security teams align their defensive strategies with industry frameworks like MITRE ATT&CK®, which can help you prepare for the most common and successful methods of attack.

However, ensuring you have threat detection coverage across all stages of the attack lifecycle requires ongoing threat research, detection engineering effort, and tuning, all of which adds more work to the team. Lacking coverage at any point in the attack lifecycle exposes the business to serious threats.

HOW WE HELP

Expel maps to the MITRE ATT&CK® framework to provide world-class detections that instantly improve your overall coverage across every stage of the attack lifecycle.

We help you understand what your MITRE coverage is—both with and without our detections—to provide you with the visibility to gradually improve your detection program.

Our detections identify high-fidelity events early, all while taking the detection engineering lift off your team. We provide full transparency, showing you exactly how Expel-written and your own detections align to each MITRE ATT&CK tactic, so you know exactly where you're covered. Using telemetry and learnings from our global customer base, we up-level these insights, continuously writing new detections and tuning existing ones to identify events that vendor technologies cannot detect on their own.

Expel detections are written at both the product and technology-type level to evolve with your tech stack. Expel's alignment to widely used industry frameworks makes it easy to map and consistently improve your coverage and your cyber resilience.

WHY EXPEL

At Expel, we can help improve your overall MITRE ATT&CK® coverage. Here's how we do it:

Industry leading protection

Continuous and timely detection analysis is key to accelerate your metrics—from mean-time-to-detect, -triage, or -respond—our technology-powered SOC delivers unheard of results and SLA/SLOs.

World-class detection and threat intelligence

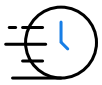
Our industry leading detection engine and AI-assisted investigation capabilities weed out false positives, and allow our analysts to get you answers fast with clear actions to remediate threats.

Unrivaled visibility, context, and personalization

We provide 100% transparency, so you can see every step of our investigations in our security operations platform, Expel Workbench™, or only be alerted when we need your feedback—the choice is entirely yours.

Proactive risk, resilience, and posture analysis

We'll constantly recommend what you should be doing to minimize exposure, save money, and improve efficiency. We identify next steps and assist with the quantification of the impact so that you can easily solve for your top security challenges.



Fast time-to-value

You can opt to either onboard almost completely independently, or take advantage of full-concierge style onboarding

WHAT OUR CUSTOMERS SAY

"Expel was the only vendor we evaluated that wrote its own meaningful cloud detections."

Learn more at expel.com

Awards and Recognition

4.8/5 Stars
on G2 Peer Review

CUSTOMER NPS
75+