PARTNER BRIEF

Secure your AWS environment with Expel MDR

Visibility gaps don't fix themselves

Moving workloads to AWS doesn't automatically make them secure. You've got logs to analyze, alerts to triage, and cloud expertise to maintain—all while your team is already stretched covering the rest of the environment. Cloud coverage gaps are real, and attackers know how to find them.

Expel Managed Detection and Response (MDR) for AWS is built for exactly this situation. We provide 24/7 monitoring and response with direct integrations into AWS GuardDuty, AWS CloudTrail, and now AWS Security Hub—so you get coverage that's actually tuned to your environment, not a generic ruleset that treats every finding as urgent.

Expel MDR: Built for your AWS environment

Expel is a recognized leader in the Forrester Wave™: Managed Detection and Response, Q1 2025. We've been doing cloud detection for 10+ years, which means we understand AWS, the architecture, the services, the attack patterns, well enough to tell you what actually warrants attention.

When Expel sends you an alert, it's been through our detection engineering and triage process. We filter the noise, surface what matters, and give you context and recommended actions, or take auto-remediation steps, so your team isn't starting from ground zero on every finding.

Our coverage spans cloud and Kubernetes environments, SaaS and identity applications, endpoints, networks, and SIEM technologies. Everything connects back to a single investigation surface so we can see the full picture, not just the AWS slice of it.

BY CHOOSING A PARTNER-DRIVEN APPROACH, EXPEL AND AWS PROVIDE YOU WITH:

Enhanced staffing resources

Expel and AWS analysts work as an extension of your team—covering the gaps you may not have the headcount to uncover.

Works with what you have

No rip-and-replace. Expel integrates with your existing AWS environment and security stack.

Cloud threat expertise

The Expel SOC has been doing cloud detection for 10+ years. We know which AWS threats are signal versus noise.

Stronger AWS capabilities

Tight feedback loop on detections and workflows means your team gets smarter about AWS over time.

Tailored delivery

Get 24/7 coverage with as much or as little involvement from your team as makes sense for your operations.

Expel MDR at a glance

Swift setup and real-time insights

- Onboard in hours, not weeks—unlike most MDR providers
- Direct integrations with AWS GuardDuty, CloudTrail, and Security Hub
- Real-time findings and recommendations from Expel SOC analysts

Rapid response times

- Mean time to remediate of 20 minutes for high/critical alerts with auto-remediation
- Faster response across every metric, not just the ones that look good in a pitch deck

Scalability and shared responsibility

- Scale threat coverage as your AWS footprint grows
- Reduce the cost and burden of running a full-time SOC
- Keep your team focused on building, not alert triage

Predictable budgeting

- No surprise costs—know what you're getting and what it costs
- Specialized cloud expertise without the full-time hire
- ROI you can measure from day one

What our customers say

"They showed us exactly what they were monitoring from a cloud security standpoint—and what they could get running immediately."

Jeremy Stinson
Principal Architect, Qlik

"Expel's approach felt more like a partnership—one where our two teams would work seamlessly together."

Lori Temples
VP, IT Security, GreenSky

Ready for AWS security that actually works?

Most security teams don't have a visibility problem—they have a prioritization problem. Expel turns those findings into action.

Contact your Expel or AWS sales representative to learn more, or email aws-sales@expel.com to get started.

CONTACT SALES