expel

VENDOR COMPARISON SHEET

# Expel MDR for Cloud

## Expel was **the only MDR vendor** named by Forrester with a **perfect score** in **cloud threat detection**.

| Scores for Detection Surface: Cloud<br>The Forrester Wave™: Managed Detection and Response Services, Q1 2025 | |
|---|---|
| **VENDOR** | **SCORE** |
| **Arctic Wolf** | 1.00 |
| **Binary Defense** | 3.00 |
| **CrowdStrike** | 3.00 |
| **eSentire** | 3.00 |
| **Expel** | **5.00** |
| **Rapid7** | 1.00 |
| **Red Canary** | 3.00 |
| **ReliaQuest** | 3.00 |
| **Secureworks** | 3.00 |
| **SentinelOne** | 3.00 |

## Expel vs. the other guys

| | Expel | Other MDRs |
|---|---|---|
| **COVERAGE** — Kubernetes and Workloads | We provide granular Kubernetes security by analyzing configurations and runtime application behavior, so we can stop threats others typically miss. | Only a handful of MDR providers support Kubernetes in a meaningful way, and those that do tend to offer more generic cloud security with less specific Kubernetes expertise. |
| **COVERAGE** — Control Plane | Expel is built for multi-cloud flexibility, and covers AWS, Google Cloud, Azure, and is the only MDR with coverage for Oracle Cloud Infrastructure. | Other MDR providers cover only the top 2–3 cloud vendors, and none support Oracle Cloud Infrastructure. |

| | Expel | Other MDRs |
|---|---|---|
| **COVERAGE** — CNAPP | Covers the most CNAPP solutions (Wiz, Orca, Lacework, Palo Alto, etc.), allowing you to increase the value of your current investments. | Offer spot coverage or push you to adapt to their platform and preferred tech ecosystem. |
| **COVERAGE** — SaaS and applications | Directly integrates with more leading SaaS technologies than other MDR providers, including: Workday, Box, Dropbox, GitHub, GitLab, Slack, Salesforce, and more. | Offer spot coverage, and very few have direct integrations with many of the major SaaS providers. They also often require you to have a SIEM to gain this telemetry. |
| **DETECTIONS** | Maintains custom Expel-written detections (500+ for cloud alone), spanning an extensive integration ecosystem, leading to high-fidelity alerts. | Many leverage noisy, out-of-the-box detections and primarily focus on basic IAM telemetry, missing holistic context. |
| | Automatically pulls relevant information to contextualize cloud alerts with other telemetry sources across your entire tech stack, not just the cloud. | Other MDR providers take the alerts and look primarily at basic IAM telemetry. Most don't look at holistic telemetry. |
| **RESPONSE** | Our SOC analysts provide swift, human-led, cloud-specific incident response with clear, actionable remediation guidance. | Provide alerts without clear cloud-specific response capabilities, relying on automation or pushing remediation back to you. |
| | Provides clear, actionable remediation steps tailored to your specific cloud environment. | Offer generic advice or push the burden of remediation entirely on your own security team. |
| | Our analysts proactively hunt for emerging threats unique to cloud environments, identifying risks before they trigger alerts. | Hyper-focus on EDR and are primarily reactive. They typically wait for alerts, rather than actively searching for new attack vectors in cloud infrastructure. |
| **TRANSPARENCY** | Provides a transparent 'glass-box' MDR with real-time visibility and direct communication with you on Slack, Teams, etc. | Leverage AI and chatbots for communication, or route you through an account manager. |
| **EXPERTISE** | We were built cloud-native, with 9+ years experience delivering high-fidelity cloud alerts, and were the first in the industry to support Kubernetes environments. | Many popular MDR providers in the market began as an EDR and are playing catch up–so their cloud and Kubernetes detections lack depth. |
| | Happy analysts stick around. We remove friction and manual processes for our analysts, resulting in a 91% retention rate over 2 years. | Experience high analyst turnover because they are unable to keep pace with customer growth. |

# **How we secure your cloud** (better than our competitors)

1.  Expel ingests signal from your cloud logs and alerting tools via **direct integrations**.

2.  We apply a **detection methodology** that takes advantage of the alerting capabilities you already have.

3.  We augment your capabilities with hundreds of **proprietary Expel detection rules**, ensuring we don't miss security-relevant activity.

4.  Our platform **enriches and prioritizes alerts** based on severity, configuration, and your unique business context, allowing analysts to determine which alerts require attention.

5.  We provide **clear, detailed remediation recommendations or use automation** to perform them on your behalf.

07/15/25

## Protect your entire cloud environment with ease, from the application layer to the control plane, backed by 24x7 expert coverage.

**Watch a demo: expel.com/on-demand-mdr-demo**

expel