MDR VENDOR EVALUATION · EXPEL VS. RELIAQUEST

Six questions to ask ReliaQuest

Bring these to your next vendor call. The answers will tell you everything you need to know.

Use these questions in your evaluation—then see how Expel answers each one.

01	INVESTIGATION OWNERSHIP **When a threat is confirmed in my environment, who owns the investigation—your SOC or my team?**	EXPEL Our SOC owns investigation and remediation end to end, visible in real time through Expel Workbench™. Nothing gets handed back for your team to finish.
02	AFTER-HOURS ACCESS **If my team has a critical incident at 3am, who do I talk to—a SOC analyst directly, or a customer success manager?**	EXPEL Direct 24×7 access to SOC analysts via Slack or Teams. Not a customer success manager—an analyst who already knows your environment.
03	HUMAN JUDGMENT VS. AUTOMATION **Your platform is AI-first and agentic. What happens when a sophisticated threat needs the kind of human judgment automated triage might miss?**	EXPEL Ruxie™ AI surfaces context-based recommendations—analysts make the final call on every incident. Human-led, AI-powered, never autonomous.
04	MARKET RECOGNITION AND CATEGORY **Gartner doesn't include you in their MDR market guide. How do you define your service category, and how does that shape what's actually included in your coverage and response commitments?**	EXPEL Expel is named a Representative Vendor in the Gartner® Market Guide for MDR and a Leader in the Forrester Wave™ for MDR Services, Q1 2025—recognized as an MDR provider, not a platform vendor.
05	RESPONSE SLA **What's your SLA for beginning investigation of a critical alert? Does "beginning investigation" mean an automated triage step, or an analyst actively reviewing the incident?**	EXPEL Expel publishes a 15-minute SLA for response to critical events—and that's an analyst on the incident, not an automated triage step. We go further: our mean time to remediate (MTTR) is 14 minutes.
06	INTEGRATION DEPTH **How many of your data sources connect through direct API versus indirect SIEM syslog forwarding—and what does that mean for data fidelity and response speed?**	EXPEL Most of our 160+ coverage areas connect through direct, bi-directional API—no SIEM required. By Expel's own analysis, about 81% of ReliaQuest's connections route through indirect syslog paths, which adds latency and reduces fidelity.

ASK US QUESTIONS LIVE

Join a group demo to see the Expel difference in real life.

expel.com/democast