

Seven questions to ask Rapid7

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

DEPLOYMENT TIMELINE

How long does deployment take from signed contract to full monitoring coverage, and what does “full coverage” include on day one?

EXPEL

Agentless onboarding with direct, bi-directional API connections—no proprietary agents. Operational in hours, not months.

02

MONITORING DEPTH

Which of my existing tools will your SOC actively monitor, and which ones do you only ingest for investigation context after the fact?

EXPEL

We monitor every connected tool in your stack, and help build and monitor custom detections tailored to your environment.

03

SIEM DEPENDENCY

Do I need InsightIDR as my SIEM for this to work, or can you connect directly to the tools I already run?

EXPEL

No SIEM required. Direct API connections to the tools you already run pull richer data faster than log or SIEM-based ingestion.

04

AUTO REMEDIATION

If I want you to quarantine a user or an endpoint, what else do I have to license to make that happen?

EXPEL

Nothing. Automated response across cloud, endpoint, identity, network, and SaaS is included in the service—no separate SOAR product.

05

AFTER-HOURS ACCESS

When I have a critical incident at 2am, do I reach a SOC analyst directly, or does everything route through my Customer Advisor and the portal?

EXPEL

Direct 24x7 access to SOC analysts via Slack or Teams. Not a relay through an advisor—the analysts who live in your environment.

06

CLOUD COVERAGE

Do you cover cloud security tools like Wiz, Orca, or FortiCNAPP, or is cloud coverage limited to AWS, Azure, and Google Cloud workloads?

EXPEL

160+ coverage areas across endpoint, cloud, identity, SaaS, and network, including cloud-native security platforms.

07

RESPONSE SLA

What is your response process, and what are the SLAs tied to it?

EXPEL

Expel averages a 5-minute MTTT and 14-minute MTTR, backed by a guaranteed 15-minute MTTT SLA for critical events and 30 minutes for high-severity events.

ASK US QUESTIONS LIVE

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

expel.com/democast