expel

BUYER'S GUIDE

10 questions to ask before you trust AI with your security

AI is the hardest claim to check in a security evaluation. Ask for the specifics: where their AI acts alone, who reviews its calls, and how much of the AI you've deployed they actually cover.

The AI running your security operations

01 Where does AI act without human review?

Red flag: "Everywhere," or "fully autonomous." Or "human in the loop" with no detail about which loop.

Ruxie triages and closes high-confidence benign alerts. Analysts make the consequential calls.

02 Can you show me the reasoning behind one AI decision?

Red flag: An audit log of actions with no reasoning. Or the model's calls aren't exposed to customers.

Every step Ruxie takes is visible to customers in Expel Workbench™.

03 When your AI escalates, who do I talk to?

Red flag: A success manager, a portal ticket, or a voicemail after hours.

Reach a named Expel analyst in Slack or Teams, 24x7, included in the service.

04 Are your response times a contractual SLA?

Red flag: "We aim for." A time-to-acknowledge sold as a response time. Or no number at all.

Expel averages a 14-minute mean-time-to-remediate on high and critical incidents.

05 What happens when we add a tool it hasn't seen?

Red flag: It routes through their SIEM first, or it's a services engagement with months of tuning.

Expel is bring-your-own-tech (BYOT), agentless and API-first, across 160+ coverage options.

Coverage for the AI you've deployed

06 Can you detect attackers using AI, or only employees?

Red flag: A dashboard of which AI apps employees visited, presented as threat detection.

Expel detects both. Attacker AI use and employee AI exposure are separate detection sets.

07 Do you see prompt-level signal, or only activity logs?

Red flag: Coverage stops at "user accessed AI service."

Expel reads prompt-level signal, so you see intent behind the action.

08 What about the AI systems we build ourselves?

Red flag: Commercial AI tools only. Or visibility into usage, with no detection behind it.

Expel covers the AI you build, including prompt injection.

09 What framework maps your AI coverage?

Red flag: No framework, or a claim of complete coverage of a two-year-old threat surface.

Expel's AI-specific detections map to 13 of the 16 MITRE ATLAS tactics.

10 Is this included, or a separate line item?

Red flag: A new SKU, a new console, a new onboarding project, and a different team.

Included in Expel MDR. Same team, same platform, same place as everything else.

We just answered all ten. Watch us back it up.

See Ruxie work in our next Democast, 30 minutes with live Q&A.

expel.com/democast