# MDR provider switch check:

What that cheaper deal doesn't tell you

## Smart security decisions start with full context

This framework gives you the questions and criteria you need to evaluate any MDR provider—whether you're considering Expel or comparing us to a lower-cost option. We'll help you surface the hidden trade-offs, uncover operational impact, and clarify the real cost of switching because we know it's never that easy and "bargain" alternatives can end up costing way more in downtime, team burnout, and missed threats.

### Justifying your Expel MDR investment against cost-cutting pressures

What can you do when your security budget is under a microscope because executives can't quantify the value of protecting your org against attacks that haven't happened yet?

Leadership keeps asking for ROI on security spending but doesn't understand you're preventing disasters they can't see.

Ultimately, they want to know why you can't just use "cheaper alternatives" or "bundle everything with one vendor because it's viewed as 'good enough'."

This framework provides questions to ask both Expel and other providers to prove why staying with Expel likely makes the most sense, from both a security and financial lens.


## Section 1 - True cost discovery of alternate provider

### That "cheaper" MDR option might cost you more than you think.

Before you chase budget savings, get clear on what's really included — and what'll hit your budget later under "surprise fees." Add-ons, migration headaches, renewal increases, and shadow costs are real. This section helps you uncover the things vendors don't advertise, but you should assess to get the full picture.

#### What's really included vs. what costs extra?

- ☐ Are data ingestion fees included or charged separately per source?
- ☐ Do you need a SIEM to collect telemetry? (If the answer is yes, then there are likely storage fees involved for the collection of that telemetry, along with the associated costs of maintaining a SIEM.)
- ☐ What's covered under "incident response" vs. what triggers consulting fees?
- ☐ Are custom integrations included or billed as professional services?
- ☐ Do user licenses scale with your team or cost extra per person?
- ☐ What compliance reporting is automated vs. manual (and billable)?

## Section 1 - True cost discovery of alternate provider

### What are the hidden switching costs?

- ☐ Who handles the technical migration—your team or theirs?
- ☐ How long will you pay both vendors during the transition?
- ☐ What's the realistic timeline vs. the sales timeline?
- ☐ Who's responsible if migration takes longer than promised?
- ☐ What happens to your current security configurations and threat intelligence?
- ☐ Will your team need retraining, and who pays for that time?

## Section 2 - Coverage reality check

### Swapping MDR providers only works if the new one covers exactly what you need it to.

Swapping MDR providers only works if the new one covers exactly what you need it to. Some claim "full coverage"—until you realize portions of your cloud, SaaS, or network will end up being ignored. Others say you are covered, but end up slapping you with more alerts and fewer answers.

All security technologies are fallible, but some tools are better than others (as seen in third-party tests like this one). Having an MDR that works across best-of-breed technologies instead of being locked in with one vendor is important for both visibility and getting the most out of your security investments—something Expel excels at.

Here's some specific questions to ask to determine if the MDR replacement can match (or beat) your current protection.

### What gaps will you need to fill?

- ☐ Does the alternative monitor all your environments or just some?
- ☐ Are cloud workloads covered the same as on-premise systems?
- ☐ What SaaS applications can they actually monitor?
- ☐ What about Cloud Control Plane solution integrations like Wiz, Orca, PANW Prisma, etc.?
- ☐ Do they provide the same depth of network security monitoring?
- ☐ Is their threat intelligence as comprehensive as what you have now?
- ☐ What security tools will you need to add or replace?
- ☐ Does the new MDR require you to utilize their security tools?

### What's the service level difference?

- ☐ Can you reach a human analyst directly or only through tickets?
- ☐ What's their average response time for different severity incidents?
- ☐ What's the impact of a delayed response?
- ☐ Do they provide proactive recommendations or just reactive alerts?
- ☐ How transparent are they about what they're doing for you?
- ☐ Do you get dedicated analyst time or shared resources?
- ☐ What happens during maintenance windows or outages?

## Section 3 - Operational impact assessment

### Taking an alternate route may sound great on paper—until your team is buried in alerts, scrambling to learn new tools, or patching gaps with overtime.

This section helps you sanity-check how a switch might impact your day-to-day operations, your team's workload, and your ability to keep the business running going forward.

#### Practical ways to reduce phishing risk:

- ☐ How many more alerts will your team need to investigate daily?
- ☐ What's their false positive rate compared to your current solution?
- ☐ How much vendor management time will this require?
- ☐ Will your team need to supplement coverage gaps with overtime?
- ☐ What internal processes will need to change?
- ☐ How much time will integration and troubleshooting consume?

#### What about business continuity?

- ☐ What's your tolerance for reduced security effectiveness during–and after—the transition?
- ☐ Can your business handle potential service interruptions?
- ☐ How will you maintain compliance during the switch?
- ☐ What's your backup plan if the new solution doesn't work out?
- ☐ How quickly can you switch back if needed?

## Section 4 - Vendor relationship questions

### You're not just buying a service—you're signing up for a partnership, and you need one that you can trust.

Will they ghost you after the contract's signed? Or hit you with hidden fees at renewal? This section gets into the weeds of how the MDR vendor treats customers after the sales pitch ends.

#### What's the real partnership like?

- ☐ How do they handle contract renewals and price increases?
- ☐ What's their track record for service level consistency?
- ☐ How do they handle escalations and problem resolution?
- ☐ Do they provide regular business reviews and optimization recommendations?
- ☐ What happens if key personnel leave their company?
- ☐ How do they handle data portability if you need to leave?

#### What are the long-term implications?

- ☐ Are you locked into multi-year contracts with penalties?
- ☐ How flexible are they with changing requirements?
- ☐ What's their roadmap for new capabilities?
- ☐ How do they handle mergers, acquisitions, or business changes?
- ☐ What are the exit costs and data retention policies?

# Section 5 - Decision framework

## Here's where it all comes together.

If you're being asked to switch MDR providers, this section helps you separate real savings from false economy. Can your team pull this off without getting more work and being forced to use workarounds? Will the budget "win" cost you more in the long run? Let's find out.

### Verify:

- ☐ The total cost savings are real after adding all fees and requirements.
- ☐ Coverage gaps won't require expensive additional tools or services.
- ☐ Your team can handle the transition without compromising security.
- ☐ The business case accounts for productivity losses and hidden costs.
- ☐ You have a clear rollback plan if things don't work as promised.

### Questions to ask Expel:

- ☐ What optimizations or cost savings am I realizing with your MDR service?
- ☐ How does your total cost of ownership compare to alternatives?
- ☐ What new capabilities or efficiencies are coming in your roadmap?
- ☐ How can you help build the business case for continuing the partnership? (Ask about our business value analysis.)

### Red flags that suggest switching isn't worth it:

- ☐ The alternative can't clearly explain what's included in their base price
- ☐ They're evasive about implementation timelines or requirements
- ☐ They aren't willing to conduct a business value assessment
- ☐ They can't demonstrate equivalent coverage to your current solution
- ☐ The savings disappear when you add back necessary capabilities
- ☐ Your security team strongly opposes the change

## Section 6 - Building your business case

### When the pressure's on to cut costs, your best defense is the numbers.

This section helps you build a compelling argument for why switching isn't always worth the risk—and outlines smarter ways to save money without gutting your detection and response capabilities. Let the numbers do the talking.

#### Arguments for keeping Expel:

- "Switching actually costs $_____ more when you include [specific hidden costs]"
- "We'd need to spend $_____ on additional tools to fill coverage gaps"
- "Our team would lose _____ hours of productivity if we change providers"
- "The risk of reduced security during migration isn't worth _____ in savings"

#### Alternative cost-cutting options to propose:

- Optimize other security tool spending
- Renegotiate current contract terms
- Reduce redundant security services
- Consolidate other vendor relationships

#### Next steps:

- ☐ Complete this evaluation with real provider responses
- ☐ Get detailed proposals that address each question
- ☐ Request a business value analysis from your current provider
- ☐ Present total cost of ownership comparison, not just sticker price

### Bottom line:

This framework can help you ask the right questions ***before*** making budget decisions that could cost more than they save.

Don't take our word for it. Learn more about our fast onboarding and the transparent way we work—directly from our customers.

06/23/25