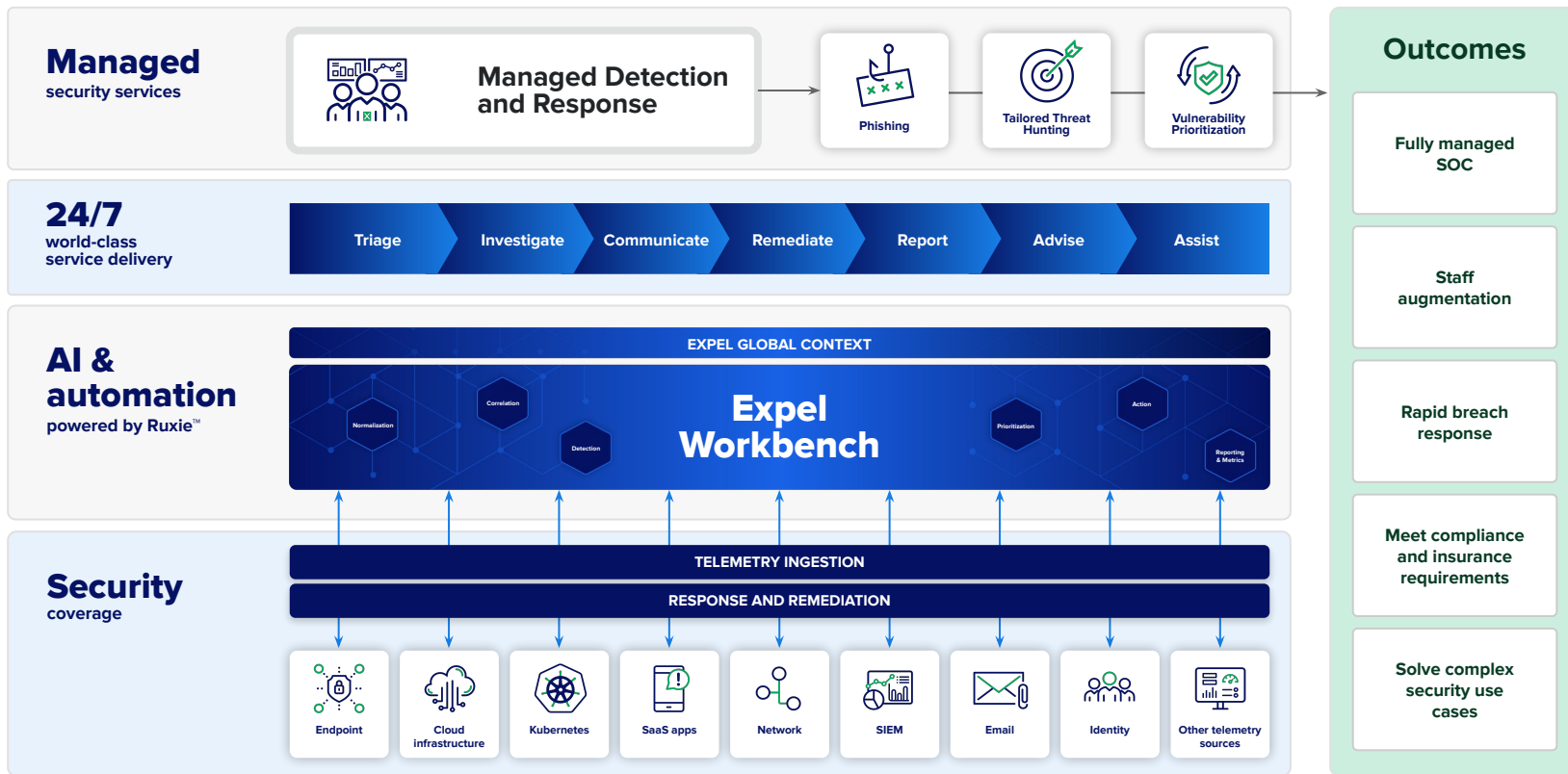




Expel Business Value Assessments

Business cases from Expel prospects/customers

How Expel helps deliver on security outcomes



Business Value of Expel MDR

Goal	Strategies & Tactics	Metrics	Solution Capabilities	Positive Business Outcomes
Reduce Costs	<ul style="list-style-type: none"> • Avoid headcount growth • Improve security posture to save on cyber insurance premiums • Optimize how SIEM is utilized, saving money in the process 	<ul style="list-style-type: none"> • SOC Headcount • Cyber premiums • Log ingestion Costs 	<ul style="list-style-type: none"> • Expel is an extension of your team, offering exceptional service delivery via your engagement manager, SOC, solution engineers, technical support engineers, and more • Get 24x7x365 monitoring off all attack surfaces with rapid threat detection, response, and remediation • Expel covers all attack surfaces without requiring you to expand your SIEM spend 	<ul style="list-style-type: none"> • Cost Avoidance of Hiring a SOC • Reduction in Cyber Insurance Premiums • Optimize SIEM Usage and Spend
Improve Efficiency	<ul style="list-style-type: none"> • Free up team's time spent on false positives and avoid analyst burnout • Access an advanced L1/L2/L3 SOC that works with your technology • Measure and improve your security program with data 	<ul style="list-style-type: none"> • Time spent on alerts / per alert • Time spent on phishing / per phish • Time to onboard acquired company 	<ul style="list-style-type: none"> • Expel triages, investigates, and delivers high-quality forensic response with clear remediation guidance • See our work as we investigate to provide answers to what the threat is, where it came from, where it is now, and what is its extent • Get metrics and reporting to gain insight into your security operations 	<ul style="list-style-type: none"> • Time Savings on Alert Management • Time Savings on Phishing • Time Savings on Detection Engineering • Speed Up M&A Integration Securely
Mitigate Risk	<ul style="list-style-type: none"> • Respond to all potential threats with speed and precision • Monitor all attack surfaces: Cloud, Identity, Endpoints, Network, and SaaS Apps • Harden your environment against threats on an ongoing basis 	<ul style="list-style-type: none"> • MTTD • MTTR • MITRE ATT&CK coverage 	<ul style="list-style-type: none"> • Expel's automated remediations will take action on your behalf when and where you need them to • Root cause analysis and resilience recommendations help you continuously improve your security posture • Have confidence that you can grow securely with Expel's 125+ integrations 	<ul style="list-style-type: none"> • Cost Avoidance of Incident Response • Rapid Detection and Response Across Attack Surfaces • Continuous Security Posture Improvement

Table of contents

This document contains an estimation of the typical ROI an organization would receive when working with Expel MDR. These assessments are based on real-life metrics gleaned from the organization in question, as well as public industry data.

Page 05 [Example 1](#) - Large healthcare company

Page 13 [Example 2](#) - Mid-size Software company



Expel Business Value Assessment

Large Healthcare Company

Company Profile

- **Type of company:** Non-profit, integrated healthcare system
- **Size:** Considered one of the largest systems in the country
 - 30,000 employees
 - 12 hospitals
 - Serving 1+ million members
- **Location:** United States
- **Use Case:** MSSP/MDR replacement due to dissatisfaction with provider

Executive Summary

Business Challenges

Missed incidents

Current provider missed incidents entirely on several occasions, or notified several hours AFTER in-house team contained the threat.

High volume of false positives

MDR provider flooding in-house team with benign alerts, leading to constant re-work and wasted investigation time.

No transparency from current provider

MDR provider operates like a service desk: no visibility into work, delivers 8+ hour turnaround times to questions/tickets, and provides little/no forensic support for alerts.

Expel Value Proposition

Cost Savings & Efficiencies

Working with Expel benefits Company financially and operationally:

- **\$4.3M** in cost avoidance savings over 3 years
- **\$1.2M** in team productivity benefits unlocked, or the equivalent of 3 FTEs
- **94%** reduction in MTTR, which ultimately reduces risk

Rapid Time to Value

Get 24x7 coverage for both your current and future environment in days, not weeks

Unrivaled Transparency & Customization

See everything our SOC is doing in real-time, and tailor our MDR service to your needs

Global risk survey highlights cyber threats as top risk organizations face today and through 2026¹

Healthcare industry not immune to threat of cyber attacks

HCA Healthcare, 2023	Threat actors exfiltrated PII for over 11 million patents following a third-party storage breach. Multiple class-action lawsuits followed alleging HCA did not properly safeguard information.
Regal Medical Group, 2023	Southern California-based medical group struck with a ransomware attack that exfiltrated PII for 3.3 million patients.
Community Health Systems, 2023	Second time in less than 10 years that Community Health attacked, where a ransomware group exfiltrated PII for over 1 million patients.

1: Aon Global Risk Management Survey, 2023, <https://www.aon.com/en/insights/reports/global-risk-management-survey>
2: FBI IC3 report, 2023, <https://www.ic3.gov/>
3: IBM Cost of a Data Breach Report 2023, <https://www.ibm.com/reports/data-breach>

IMPACT

249

Ransomware attacks in US Healthcare in 2023²

53%

Increase in healthcare data breach costs since 2020³

USD \$10+

Million in total data breach costs for Healthcare industry³

Current MDR is producing unsatisfactory security outcomes and leaving Company open to risk

Why make a change?

Current MDR provider costs \$650K per year with little to show for it:

- 8+ hours to triage alerts, with little to no forensics to support Company's response capability.
- Missing critical incidents which introduces outsized risk to the business.
- Draining team productivity instead of creating space to work on strategic initiatives.



Current provider missed a critical incident

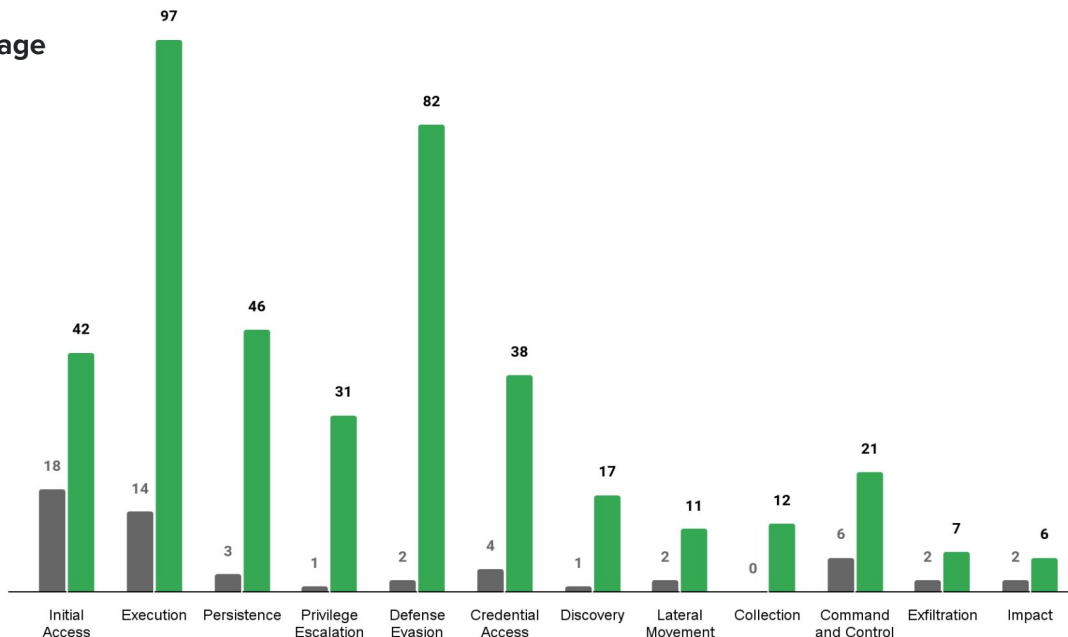
- Several employee accounts involved in credential harvesting incident, including one with Director-level access in surgical services.
- Left undetected this attack could have led to:
 - Ransomware / downtime which would directly impact patient outcomes
 - Patient / employee data theft
 - HIPAA violations / HIPAA audits
 - Cyber insurance claims & premium increases
 - Negative impacts to reputation

Assessment Results

Uplevel MITRE ATT&CK coverage across tech stack in days

MITRE Coverage by Tactic¹

■ Without Expel
■ With Expel



Rapid Time to Value

 **7 days**

Time to value reported by
42% of Expel customers²

 **30 days**

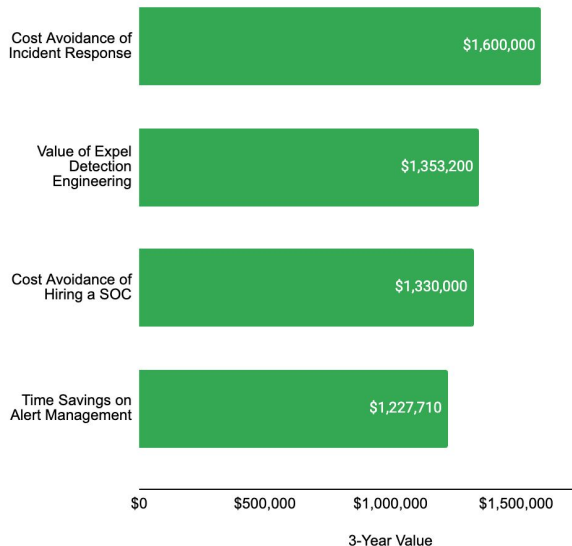
Time to value reported by
71% of Expel customers²

Tech Stack Covered:

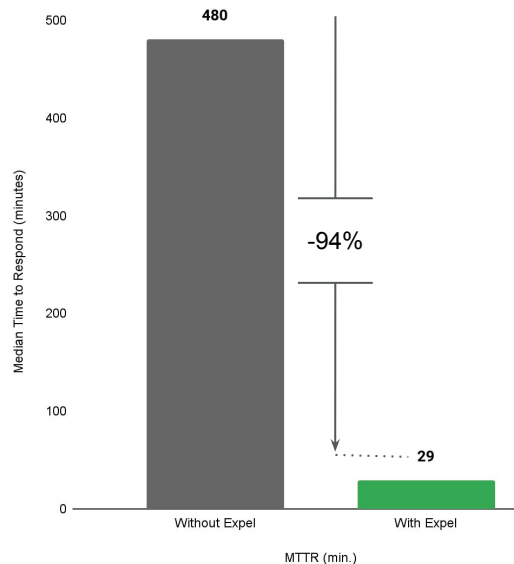


Unlock tangible operational and economic benefits

3-Year Economic Benefits



Median Time to Respond (MTTR)



BUSINESS VALUE

\$5.51M

3-year total financial benefit of partnering with Expel

7 Months

Payback period to get a return on investment

94% reduction

in MTTR, leading to shorter incident dwell times and risk reduction



Expel Business Value Assessment

Mid-size Software Company

Company Profile

- **Type of company:**
Gaming/Entertainment Software
- **Size:** Mid-size
 - 2,500 employees
- **Location:** United States, EMEA, Asia
- **Use Case:** Looking to bring on an MDR for the first time

Executive Summary

Business Challenges

High volume of alerts

Security team is flooded with alerts and they don't have the resources or bandwidth to respond to all alerts.

Insufficient resources to handle growth

They've grown so much it's hard to keep up, their tech footprint continually expands with company growth. There aren't enough team members to handle the workload and they're getting burnt out.

Expel Value Proposition

Cost Savings & Efficiencies

Working with Expel benefits Company financially and operationally:

- **\$1.3M** in cost avoidance savings over 3 years

Rapid Time to Value

- Get 24x7 coverage for both your current and future environment in days, not weeks
- Benefit from comprehensive coverage across attack surfaces and multi-cloud environments

Reduction in alert noise

See everything our SOC is doing in real-time, and tailor our MDR service to your needs

Speed of Response Matters

16
days

**average
dwell time¹**

84
minutes

**average eCrime
breakout time²**
*(initial access to
lateral movement)*

43
minutes

**median
ransomware
encryption time³**
(per 53 GB of files)

20
minutes

Expel's MTTR
*(from alert to
remediation)*

1: Mandiant M-Trends Report, 2023: <https://www.mandiant.com/resources/reports/get-your-copy-m-trends-2023-today>

2: CrowdStrike Global Threat Report, 2023: <https://www.crowdstrike.com/global-threat-report/>

3: Splunk Research, 2022: https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

Assessment Results

Project Economics

Total Benefits
\$1.35M

3-Year Simple ROI
51%

Internal Rate of Return (IRR)
49%

Payback Period
Month 9

Net Present Value
\$360.9K

Cost of Capital
12%

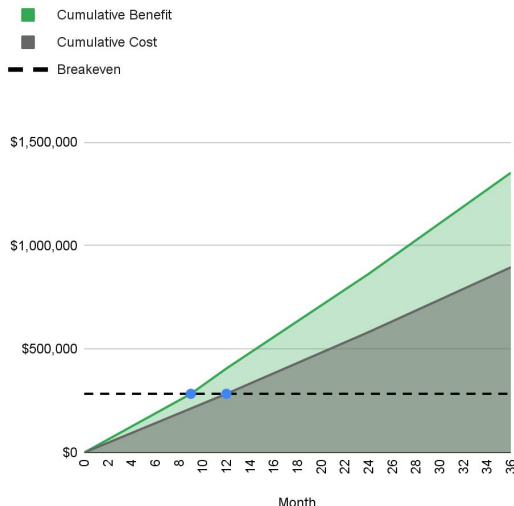
BENEFITS	YEAR 1	YEAR 2	YEAR 3	TOTAL
Cost Savings on SIEM	\$110,000	\$127,700	\$146,639	\$384,339
Cost Avoidance of Hiring	\$78,750	\$105,000	\$110,250	\$294,000
Cost Avoidance of Incident Response	\$80,000	\$80,000	\$80,000	\$240,000
Potential Cyber Insurance Savings	\$70,000	\$73,500	\$77,175	\$220,675
Productivity Improvement	\$67,600	\$70,980	\$74,529	\$213,109
TOTAL BENEFITS	\$406,350	\$457,180	\$488,593	\$1,352,123

COSTS	YEAR 1	YEAR 2	YEAR 3	TOTAL
Expel MDR - Annual Subscription	\$XX	\$XX	\$XX	\$XX
Implementation Fee	\$0	\$0	\$0	\$0
Training / Certification Fee	\$0	\$0	\$0	\$0
Support Fee	\$0	\$0	\$0	\$0
Account Management Fee	\$0	\$0	\$0	\$0
TOTAL COSTS	\$284,000	\$298,200	\$313,110	\$895,310

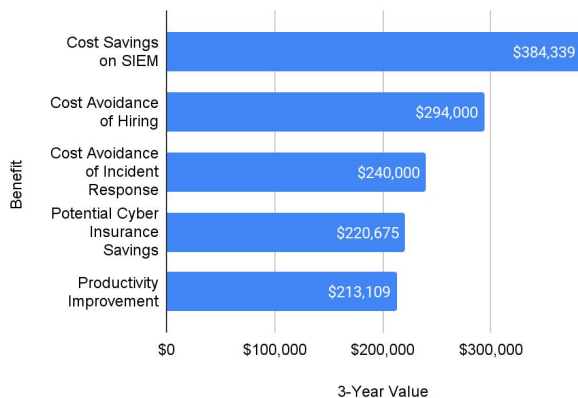
NET BENEFIT	\$122,350	\$158,980	\$175,483	\$456,813
--------------------	------------------	------------------	------------------	------------------

Unlock tangible operational and economic benefits

3-Year Economic Benefits



3-Year Benefit Value



BUSINESS VALUE

\$1.35M

3-year total financial benefit of partnering with Expel

9 Months

Payback period to get a return on investment

Benefit Calculation: Cost Savings on SIEM

Assumptions	
SIEM ACV	\$100,000
Annual Uplift	7%
Cost Reduction with Expel	100%
Pro Serv Annual Costs	\$10,000

Benefit Calculation	
Year 1 Cost	SIEM ACV + Pro Serv costs
Year 2 Cost	Year 1 SIEM ACV * (1 + Annual Uplift) + Pro Serv costs
Year 3 Cost	Fully Loaded Cost of FTEs (FTEs * Fully Loaded Cost) * (1 + Year 3 Salary Increase)

Basis for Assumptions	
SIEM ACV is an estimate based on Microsoft Sentinel's publicly available pricing . We assume Company would require 100GB of ingest per day, which would be ~\$125K. With discounts, expecting ~\$100K	Pro Serv Annual Costs is an estimate of how much customer may spend on various professional services engagements to care for a SIEM
Annual Uplift is an estimate of based on standard SaaS pricing arrangements	Cost Reduction with Expel is based on conversation with Company team about potential option to remove need for SIEM entirely if they have Expel

Benefit Calculation: Cost Avoidance of Hiring

Assumptions	
Number of FTEs Needed	3
Time to Hire (Months)	3
Fully Loaded Cost (Salary, Payroll, Benefits, etc.)	\$35,000
Cost of Recruitment (time/effort across company to hire, recruitment fees, etc.)	5%
Year 3 Salary Increase (raise, promotion, etc)	5%

Benefit Calculation	
Current State Cost	Recruitment Cost (FTEs * Fully Loaded Cost * Cost of Recruitment) + Prorated Fully Loaded Cost ((FTEs * Fully Loaded Annual Cost) * (12 - Time to Hire)/12)
Year 2 Cost	Year 2 Cost = Fully Loaded Cost of FTEs (FTEs * Fully Loaded Cost)
Year 3 Cost	Fully Loaded Cost of FTEs (FTEs * Fully Loaded Cost) * (1 + Year 3 Salary Increase)

Basis for Assumptions	
Number of FTEs Needed is based on feedback from Company team on hiring plan without an MDR	Cost of Recruitment is a conservative assumption on the time and potential fees of hiring a team would be
Time to Hire is based on talent market assumption and Expel's experience building SOC teams	Year 3 Salary Increase is a conservative assumption on the potential cost of living, merit, and/or promotion costs that come with retaining talent
Fully Loaded Cost is a conservative assumption of what a SOC analyst would cost in Barcelona, Source: Glassdoor	Cost Reduction with Expel is based on feedback from Company team that they can avoid staffing a 24X7 SOC with the purchase of Expel MDR

Benefit Calculation: Increased Productivity

Assumptions	
Hours Spent on Alerts (Weekly)	15
Hourly Rate of Personnel	\$100
Weeks in a Year	52
Time Spent on Alerts With Expel	87%

Benefit Calculation	
Year 1 Cost	Hours Spent on Alerts Weekly * Weeks in a Year * Hourly Rate of Personnel
Future State Cost	Hours Spent on Alerts Weekly * (1 - Time Reduction with Expel)) * Weeks in a Year * Hourly Rate of Personnel
Annual Benefit	Current State Cost - Future State Cost

Basis for Assumptions		
Hours Spent On Alerts (Weekly) is based on Expel's experience working with customers who managed detection & response in house	Hourly Rate of Personnel is an assumption based on the title and seniority of the Company team handling alerts today	Time Reduction with Expel (%) is a conservative assumption on the time savings Expel gives its customers, Example 1, Example 2

Benefit Calculation: Potential Insurance Savings

Assumptions

Premium Reduction	\$70,000
-------------------	----------

Basis for Assumptions

Premium Reduction is a conservative assumption on the insurance savings Expel gives its customers, [Meet Group Case Study](#). One anonymous customer saved over \$250K per year.

Benefit Calculation: Cost Avoidance of IR

Assumptions	
Billable Hours	600
Hourly Rate	\$400
Total Retainer	\$240,000

Benefit Calculation	
Avoidance of IR	$(\text{Billable Hours} * \text{Hourly Rate}) / 3$ <p>This calculation assumes that an IR retainer would be amortized over 3 years</p>

Basis for Assumptions	
Billable Hours	is based on the average time to contain a breach as found in IBM's latest Cost of a Data Breach report . The average MTTC is 73 days. At 8 hours of work per day, that comes out to 584 hours.
Hourly Rate	is an assumption based on market rates for Incident Response. Example, Comodo IR: https://www.comodo.com/incident-response/

Other MDRs unlikely to yield similar benefits

Analyst Validation

Forrester Wave™: Managed Detection And Response, Q2 2023

THE FORRESTER WAVE™

Managed Detection And Response

Q2 2023



VENDOR	Expel	Other
CURRENT OFFERING	4.6	2.36
Time To Value	5	3
Threat Hunting	5	3
Threat Intelligence	3	3
Case Management	5	3
Analyst Experience (AX)	5	1
Analytics	5	3
Extended Detection and Response (XDR)	5	3
Managed Detection	5	3
Managed Investigations	3	3
Managed Response	5	1
Dashboards & Reporting	3	3
Metrics	5	3
Scripting Engine	5	1
Product Security	5	1
Platform Capabilities	5	1
Product vision	5	3
Market approach	5	3
Adoption	5	5
Planned enhancements	5	3

Customer Validation



Expel

★★★★★ 58 reviews



Expel User Ratings

9.5

Ease of Use
Managed Detection
and Response (MDR)
Average: 9.0

9.7

Quality of Support
Managed Detection
and Response (MDR)
Average: 8.9

8.9

Ease of Setup
Managed Detection
and Response (MDR)
Average: 8.9

Gartner
Peer Insights™

Expel Ratings Overview

4.8 ★★★★★ 60 Ratings (All Time)

Customer Experience

Evaluation & Contracting 4.8

Planning & Transition 4.8

Delivery & Execution 4.8

Service Capabilities 4.8

Why Expel?



Fast time to value

84% of customers agree onboarding is seamless



World-class detection and threat intelligence

88% agree that Expel has a breadth and depth to their detections



Unrivaled transparency and customization

94% agree Expel enriches alerts with meaningful and high ROI context



Industry-leading protection across all metrics

85% of customers agree that Expel offers industry-leading protection, across every metric



Proactive risk, resilience and posture improvements

95% of agree that Expel has improved their security posture

Next Steps

Find out how your organization could benefit from Expel MDR — request an assessment today.

Get your assessment →

Thank you.

