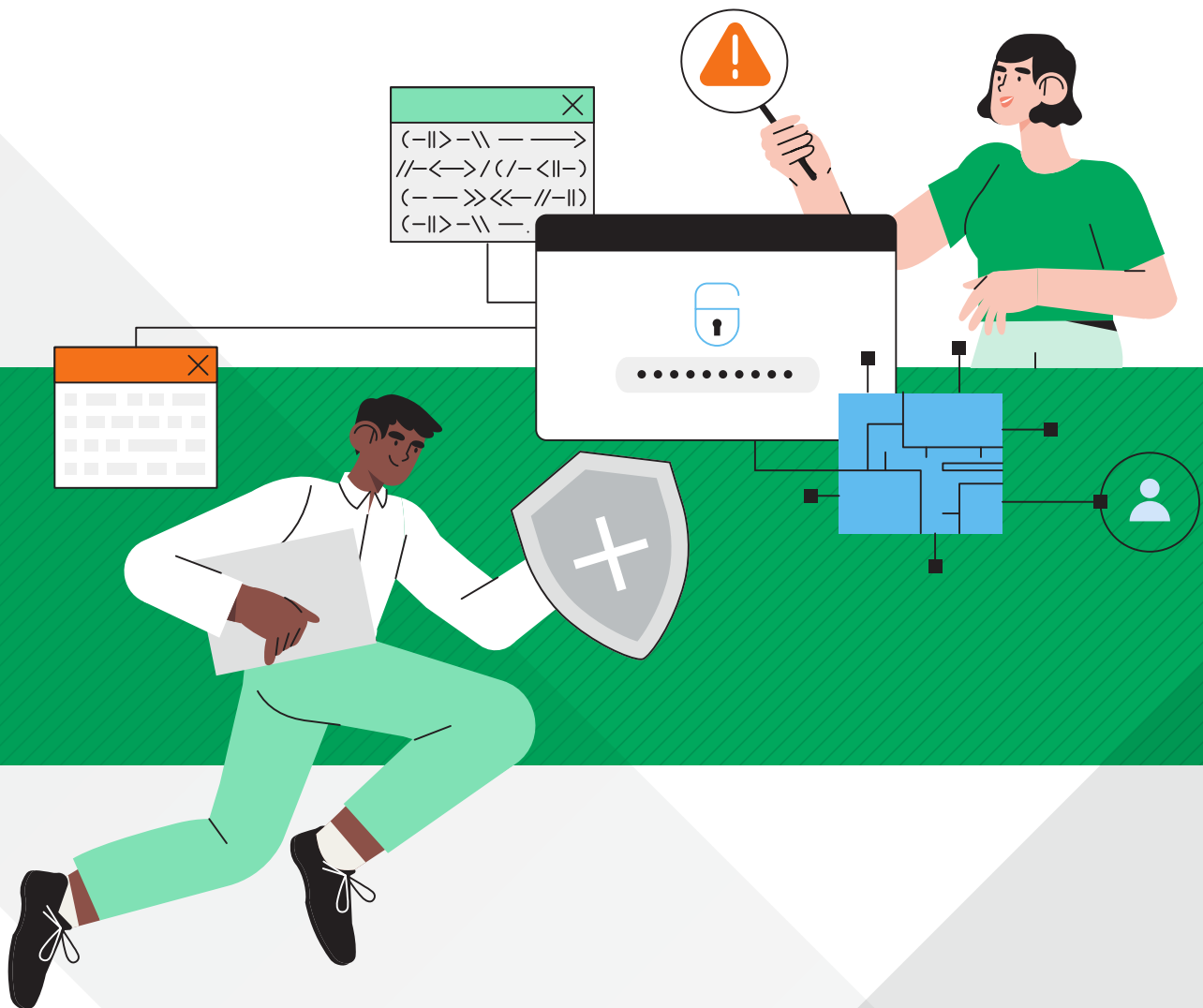




# What is MDR?

**And why is it critical to your security strategy?**



## Contents

What's happening in cybersecurity now ... and what it means for your security strategy. ....	3
The rise of MDR .....	4
MDR IRL (you know ... in real life) .....	5
Clearing the air on acronyms. ....	6
Why MDR is critical to your security posture. ....	7
Will this break the bank? .....	8
What should you look for in an MDR provider? .....	8
Coming up with an MDR vendor short list .....	10
Expel can make your life easier – and your staff happier .....	11
About Expel. ....	12

# What's happening in cybersecurity now ... and what it means for your security strategy.

Choosing how to secure your business-critical apps and data has always been a super-important issue. A strategic issue. And a fluid one, too. That's right: Cybersecurity is all that. But now — with even more dynamics in the game — the way you take on cybersecurity is increasingly important, strategic, and fluid. A good managed detection and response (MDR) partner can help you address several critical security challenges.

**Talent shortage.** If you're reading this, you probably know about the cybersecurity talent shortage — nay, crisis. Almost everyone's struggling to [find and keep security staff](#). In July 2022, the [Philadelphia Inquirer](#) reported that about 1 million (1,000,000!) people work in cybersecurity in the United States. But nearly 600,000 positions are sitting empty — and more than 90% of those are in the private sector. That means security teams everywhere will have problems filling vacancies. That creak you may be hearing? Organizations opening their toolbox to add managed detection and response.

**Alert fatigue.** You know how it feels. You're bombarded with alerts and you just can't focus, let alone get to the strategic work of cybersecurity that proactively protects your organization. Worse yet, you're getting numb to their frequency. With alerts ranging from supercritical to insignificant, the tsunami of false positives can cause even seasoned security pros to miss real threats. Organizations need to stay alert and actively work to sidestep security alert fatigue and all the damage it can do.

**SOC time and expense.** Imagine spending more than 12 months and \$2 million to build your own security operations center (SOC) from scratch, and then having to find (and keep!) the analysts on staff 24x7 to monitor and evaluate alerts. It sounds expensive and time consuming — because it is! We get into the nitty-gritty of SOC costs in this [blog](#). But let's be real, most internal security professionals would rather focus their days creating strategies to protect the organization's assets, rather than chasing endless alerts.

**Lack of focus.** Many threat monitoring, detection, and response initiatives nosedive because the nets they cast are just too broad. The myth on the streets is that a vast collection of data and generic security monitoring is all organizations need. Don't buy it. Instead, refine your strategy to focus on key risks and outcomes — it will impact your business objectives and performance more directly.

## Incidents are everywhere

Our own report — [Great eXpeltations: Cybersecurity trends and predictions 2022](#) — lets the world know that business email compromise (BEC) and ransomware attacks are rampaging through organizations:

**50% of all incidents are being identified as BEC, and ransomware attacks cruised to record-high levels in 2021.**

## The rise of MDR

To keep up with cyberattackers, managed security providers are constantly looking for and putting in place more-powerful prevention, detection, and rapid response processes and tech. They're also pushing to improve service so they can function as part of the extended security team. This led to the rise in popularity of managed detection and response (MDR). These third-gen managed security services (MSS) evaluate security through a strategic, business, and industry lens. They provide direction and context to help businesses proactively prepare to take down cyberattacks.

### Is MDR just a phase?

No. All signs point to MDR staying and growing in importance. Gartner® estimates that by 2025, the MDR market will reach \$2.15 billion in revenue, up from \$1.03 billion in 2021, for a compound annual growth rate (CAGR) of 20.2%. [Gartner](#) also predicts that 2025 will see 50% of organizations using MDR services for threat monitoring, detection, and response, and to bolster threat containment and mitigation capabilities.<sup>1</sup>

**\$2.15B**

—  
**MDR market size  
by 2025**

**20.2%**

—  
**CAGR  
of MDR**

**50%**

—  
**of organizations  
using MDR by 2025**





<sup>1</sup> Gartner, [Market Guide for Managed Detection and Response Services](#), October 25, 2021. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

# MDR IRL (you know ... in real life)

Organizations know what's up. They see that yesterday's cybersecurity approaches are no match for the slick cybercriminals stalking the halls today. Resource-strained security pros need help. MDR services can be quick on the draw in the form of remotely managed modern SOC capabilities — including the tools, tech, and procedures clients need to beef up their existing skills. MDR service providers typically supply highly trained cybersecurity staff who they support with advanced tech and automation capabilities in a 24x7x365 SOC that the organization's security team can access through a portal. These security wizards layer on the nuanced analysis you need to recognize subtle attacks or disregard false positives from automated technology. Pow!! Faster detection, investigation, and response to threats. Always on. And cost-effective.

## MDR key components checklist

### A complete MDR offering:

-  **Serves up automated security functions.**
-  **Complements automation with a super-skilled, dedicated security team.**
-  **Provides 24x7 monitoring, analysis, and rapid response to known and unknown attacks.**
-  **Offers bonus services like regular security reviews, threat bulletins, auto-remediation with containment, process improvement, and proactive threat-hunting recommendations.**

## Clearing the air on acronyms

A ton of acronyms are floating around the cybersecurity space. Let's check out a few of the relevant ones and see how they stand up against MDR.

---

### SIEM

You can make a SIEM do just about anything if you put your back into it (and consultants ... and cash) — but it's important to clarify (and reclarify) what you need your SIEM to do. You could totally pass on a SIEM, especially if other existing tools or partnerships can take care of your use cases. For example, if you have no regulatory requirements and limited log sources (maybe a few SaaS apps) you may not need to pour funds into a SIEM if a third party (like Expel) can deal with your use cases directly. But no matter whether you choose to use SIEM or not, MDR should be able to work effectively.

---

### MSSP

A lot of organizations placed their faith and resources in managed security service providers (MSSPs) that couldn't effectively connect with other third-party security services. Their efforts only had limited success. And organizations were stuck with tired security platforms that failed to weed out repetitive, noncritical security threat alerts which led to ... yeah, that's right ... our old friend: alert fatigue.

---

### MDR

There are many flavors of MDR. At Expel, we think it's important to plug into the cloud infrastructure services and security tech you already own, so you can make the most of what you've got. Think of it as BYO-tech MDR. We'll tell you 24x7 when there's something you need to worry about, why, and what you need to do to make sure your secrets stay secret.

# Why MDR is critical to your security posture

An MDR solution can help address the four primary cybersecurity challenges you are likely facing today: talent shortage, alert fatigue, SOC cost, and lack of focus. Done right, an MDR service vendor:

- Takes on responsibility, actively learns your business, and treats all of its unique parts uniquely — so you can relax knowing your people and assets are secure and protected.
- Closes existing security gaps using proprietary detection tools — so you can confidently say “we’re good.”
- Applies metrics that actually mean something — to help you make the most of your existing security investments and focus on the future.
- Uses automation to speed up response-and-resolution times to <3 minutes — without cutting back on quality.

A good MDR vendor does way more than find and stop threats. At Expel, we arm you with visibility, metrics, and recommendations to keep strengthening your security while protecting current investments. We'll benchmark you against similar companies and give you guidance for improvement. And our easy-to-read dashboards will lay out exactly what we're doing for you. With Expel, you can be more secure than you could on your own.

## Faster and more secure with Expel



# 96%

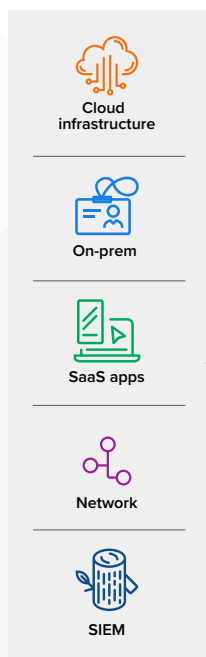
Less time on threat response<sup>2</sup>



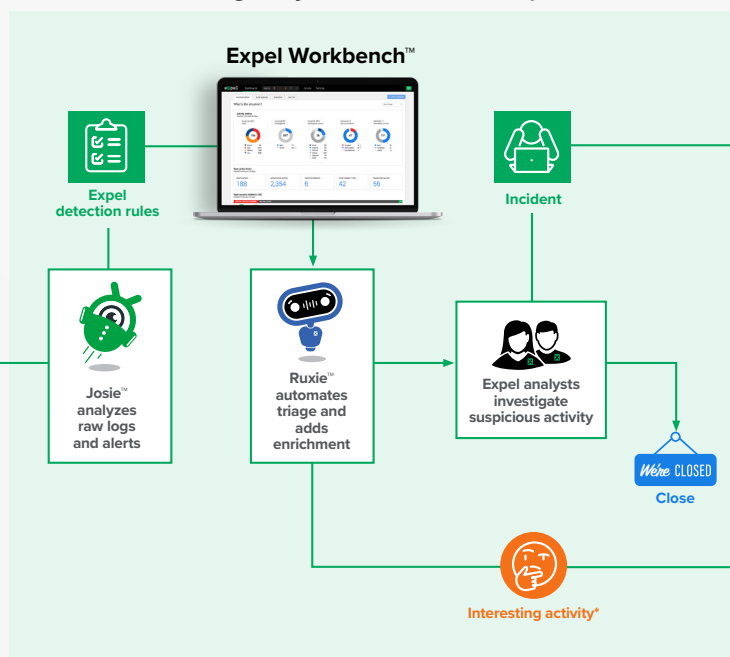
# 95%

Reduced risk of security breach<sup>3</sup>

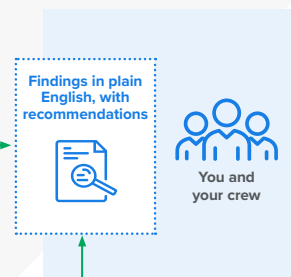
**You connect your tech via API**



**Our bots and analysts investigate your alerts and respond**



**You get fixes and next steps\***



2, 3 Forrester, The Total Economic Impact of Expel, March 2022.

## Will this break the bank?

Of course you want to know the bottom line. We commissioned our friends at Forrester Consulting to conduct a total economic impact (TEI) study and figure out the potential ROI for a composite organization, comprised of interview results with four decision makers with experience using Expel. Drumroll please ...

The study found an ROI of 610% and net present value (NPV) of (clears throat) \$9.9 million.

No one can deny it: Those are big, bold, and — dare we say ... of course we do! — impressive results. How'd they come up with numbers that big? The study calculated benefits such as reducing the time spent responding to security threats by 96% (from 530 minutes down to 23 minutes), based on the cost of a three-year subscription. Expel also decreases the likelihood of a security breach by 95%. Check out the numbers in the [full study](#).

### Key TEI findings



**610% ROI**



**\$9.9M NPV**

## What should you look for in an MDR provider?

Picking the right MDR should be super engaging and exciting. Faster detection, shorter response times, and detailed compliance-ready documentation? Cybersecurity nirvana!

To get the most value from your MDR provider, you have to first take stock of your own assets. What apps, data, and mission-critical business processes do you need to protect? Then figure out the levels of protection and monitoring you need for each. Now you can start evaluating MDR offerings based on how well they match up with your specific needs.



What should you look for in an MDR provider?		Expel	Other MDRs
Detection	Monitors endpoint, network, SIEM, SaaS apps, and/or cloud	●	●
	Applies business context to prioritize alerts	●	●
	Correlates alerts across multiple technology categories (network, endpoint, and cloud)	●	●
	Provides threat hunting across cloud, endpoint, and SaaS environments	●	●
	Uses transparent detection logic that's fully visible to the customer	●	●
	Provides learning from global customer environment to respond to threats faster	●	●
Response	Automates common security workflows	●	●
	Recommends strategic improvements to detection, prevention, and response activities based on historic attacks	●	●
	Uses analysts to execute alert triage	●	●
	Uses automation to execute alert triage	●	●
	Provides comprehensive remediation guidance	●	●
	Automatically performs remediation capabilities across multiple attack surfaces	●	●
	Provides phishing triage for user-reported attacks	●	●
Metrics	Measures how quickly analysts review alerts	●	●
	Provides alert and investigative detail by security tech	●	●
	Measures how well your security technologies contribute to detection and investigation	●	●
	Provides benchmark against similar companies	●	●
Outcomes	Performs alert to fix in 21 minutes average	●	○
Personalization	Configures rules based on your environment (i.e., suspicious login locations)	●	●
	Uses customer environment context for more accurate detection and response	●	●
	Enables auto-remediation for configurable hosts or user accounts	●	●
	Provides direct access to analysts via collaboration tools such as Slack and Teams	●	●
Experience	Easy onboarding, set up in hours	●	●
	Provides full real-time visibility into what our analysts are doing, while they're doing it	●	○
Integrations	Out-of-the-box API-based integrations for best-of-breed security technology	●	●
	Pricing that encourages and accommodates customers to integrate ALL tech	●	●

## Coming up with an MDR vendor short list

Some organizations use analyst rankings or peer communities to come up with a short list of MDR vendors.

### Speaking of analysts

[Here's](#) our latest ranking in The Forrester Wave™: Managed Detection and Response, Q1 2021 report. (Spoiler alert: We're a leader!). In fact, listen to the love we get from Forrester: "Expel proves elite practitioners, strong platforms, and collaboration can coexist." (Yeah, that's the sound of us blushing.)

### cNPS = 80

Our customers love us too, based on our customer net promoter score (cNPS) of 80 – which is kind of miraculous in the cybersecurity space.

### Questions to ask

Once you've got your short list, we've got a list of [12 questions](#) to ask prospective MDR providers.

**Our customers  
love us too**

**Customer NPS**

**80**

# Expel can make your life easier – and your staff happier

## Five top reasons customers choose Expel.

1

We need to secure AWS, Azure, and/or GCP ... fast!



2

We want a SOC, but there's no way we're building it from scratch.



3

We have a SOC, and we want to outsource part or all of it.



4

We are not happy with our MDR/MSSP and want to switch.



5

Our senior staff is buried in level-1 work and we want them to be happy again and focused on the really interesting proactive security initiatives.



If any of these reasons speak to you, we can help.

### Learn more

To stay on top of security trends and get tips and tricks that can help keep your organization secure, subscribe to the [Expel blog](#). Of course, if you want to find out more about how we can help we can do that too. [Let's talk](#).



## About Expel

Expel helps companies of all shapes and sizes minimize business risk. Our technology and people work together to make sense of security signals — with your business in mind — to detect, understand, and fix issues fast. Expel offers managed detection and response (MDR), remediation, phishing, and threat hunting. For more information, visit our [website](#), check out our [blog](#), or follow us on [LinkedIn](#) or [Twitter](#).