

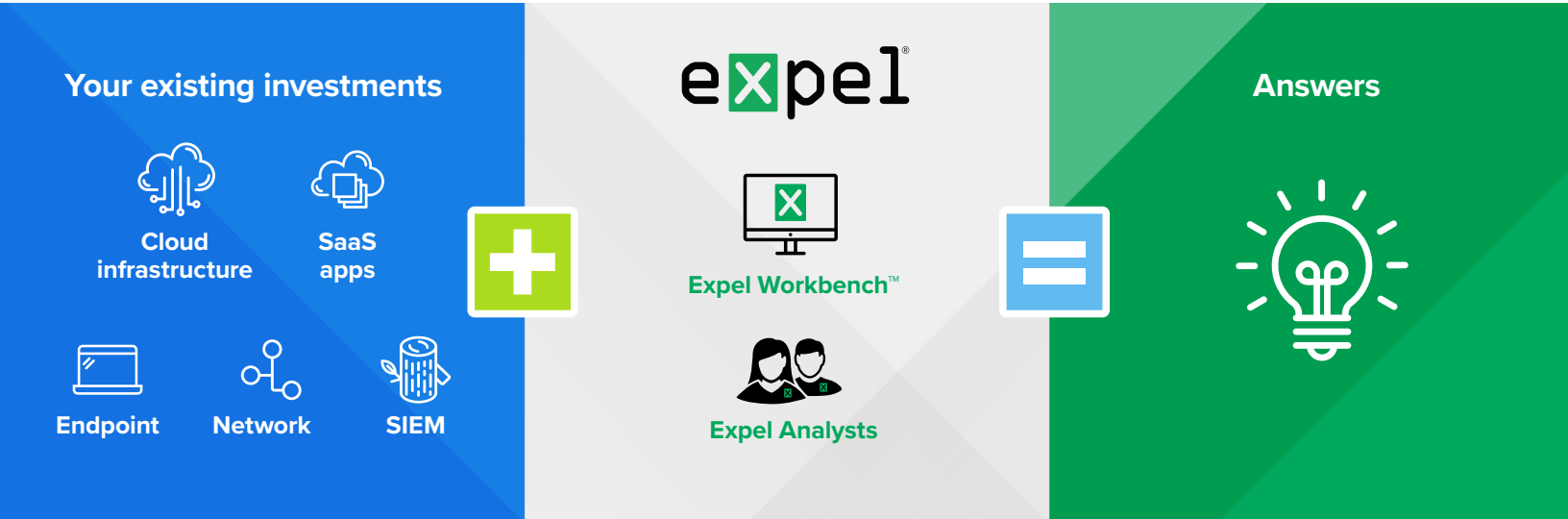


RESOURCE Communications, Inc.

# Transparent managed security

## 24x7 managed detection and response

Transparent managed security is just what it sounds like. It breaks up the proprietary black-box approach that most managed security service providers (MSSPs) and managed detection and response (MDR) providers take. You see exactly what our analysts are doing for you 24x7. Our goal isn't just to check the box and meet the SLA. We want to measurably improve your security.



## What we do

(it's more than what's in the SLA)

Expel monitors your environment 24x7 (on-prem and in the cloud) to find attackers and give you the answers you need to kick them out. We integrate with your security tech, SaaS applications and cloud infrastructure to keep your crown jewels safe. The net result? You can focus on managing risk rather than massaging alerts.

1

Use the security products you've already bought

2

Our analysts investigate alerts and monitor your environment

3

When we find a problem we tell you exactly what to do about it

4

We also tell you how to fix the root cause of recurring problems

# What you get

(hint: it's not alerts)

We use your products to detect threats, filter out false positives and quickly engage you on the threats you need to care about.

## 24x7 threat detection

Our analysts investigate threats and flag suspicious or risky activity. We'll tell you exactly what happened and when, how we detected it and what you need to do about it.

## Accelerated response

Ruxie™, our response bot accelerates our analysts' response by automatically enriching alerts and performing routine level 1 and 2 tasks.

## Actions for each incident

We recommend specific, easy-to-understand actions written in plain English so you can resolve each issue and reduce your risk.

## Hunting

Our analysts proactively hunt for malicious activity in your environment.

## Managed phishing

We'll investigate each reported email, tell you when they're real phishes and close the loop with your employees.



## Performance metrics

Dashboards measure your improvement over time, show where you're improving and let you hold us accountable.

## Resilience recommendations

You get recommendations — based on your environment and past trends — so you can fix the root cause of recurring events or prevent them from happening in the first place.

Top priority recommendation

RESILIENCE	DISRUPT ATTACKERS
<p>Block Macros from the Internet</p> <p>Block macros from running in Office files downloaded from the Internet. This can be configured to work in two different modes:</p> <ul style="list-style-type: none"><li>• Open downloaded documents in 'Protected View'</li><li>• Open downloaded documents and block all macros</li></ul>	<p>2 incidents could have been prevented</p> <p><b>EFFORT: MEDIUM</b> Group policy operation</p> <p><b>IMPACT: HIGH</b> 98% of Office-targeted threats use macros</p>

# How transparency changes our relationship

(for starters... you'll see what you're paying for)

Transparency means you share the same interface with our analysts so there's never any doubt about what we're doing on your behalf. It's a pretty radical idea in the security industry. But we couldn't imagine running a business any other way.



## Watch investigations as they unfold

You see exactly how our analysts are approaching each investigation including their rationale, methods and what they've discovered to date.



## Take action even as the plan develops

Don't wait until the investigation is over. You can take action as soon as we identify a critical remediation step.



## See exactly how you're improving

Detailed dashboards measure how well we're doing and quantify the improvement so you can draw a straight line from what you pay us to the value you get.



## See and fix recurring problems

Prioritize actions and investments using data from your own environment. Fix the root cause of recurring events or prevent them from happening in the first place.

# Getting started

(lightning ⚡ fast onboarding)

Our goal is to let you install and configure Expel without ever having to call us. Customers can typically get up and running within an hour. If it takes longer, we want to hear about it.



**Download and install Expel Assembler™ VM or connect via API**



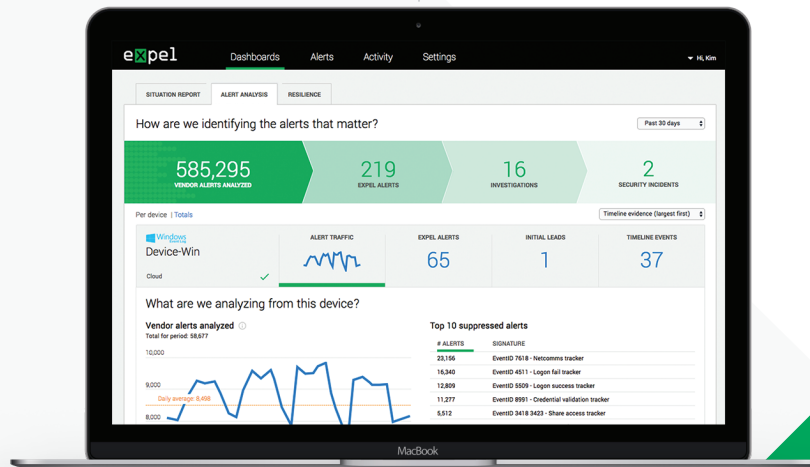
**Connect your tools to Expel Workbench™**



**Expel analysts monitor your environment**



**You get answers and recommendations**



## Our integration partners

We're constantly adding to our integration list. If you have other tools that do similar things let's talk. Chances are we can work with them.

### Cloud infra

- AWS
- Azure
- GCP

### SaaS apps

- O365
- G Suite
- Duo
- GitHub

### Endpoint

- CrowdStrike
- Microsoft
- Palo Alto
- SentinelOne

### Network

- Cisco
- Darktrace
- Palo Alto
- Zscaler

### SIEM

- Azure
- Sumo Logic
- Splunk
- Exabeam

To view all the tech we plug into visit [expel.io/tech](https://expel.io/tech)

## Benefits

(not just words... there's a dashboard to track them)

Companies come to us because they want to increase their security quickly or get their own security operations team out of the weeds so they can focus on more valuable and satisfying work. Here's how we help.



### Reduce cost and risk

Fewer incidents means less disruption for your employees and customers



### Increase security fast

Transform your security operations team with less investment and overhead



### Detect and respond faster

Find and resolve threats sooner, measure your progress over time



### Make your team happier

Eliminate tedious tasks you hate so you can focus on the work you love

# What we replace

(in case you're wondering)

Expel replaces what customers spend on managed security service providers. In our view, MSSPs have reached the ceiling of the value they can provide. They've beaten their customers into submission and taught them to expect less by taking a transactional one-size-fits-all approach, managing to their SLA and prioritizing the quantity of alerts over quality of service. When it comes time to renew, their customers are left wondering what value they got.

## Comparison of Expel's capabilities vs. MSSP

Capability	expel	MSSP
Onboarding time	Within hours	A few months (if you're lucky)
Monitoring technology	Your existing security tools	MSSP vendor's proprietary tech stack
What you get	Answers that tell you what to do	Alerts you need to investigate
How you measure value	Security operations dashboard	# of alerts on salesperson's PPT graph
Customer portal	Rich, real-time and collaborative	Limited after-the-fact data
Transparency	You see exactly what our analysts see	N/A
Resilience recommendations	Actions to improve long-term security	N/A
Remediation guidance	Detailed findings reports	N/A
Proactive threat hunting	Yes	N/A
Pricing	Three simple options	A confusing menu nobody understands

Working  
with Expel

 better.com

“By working with Expel as opposed to trying to hire, train and ramp a brand new team of experienced SOC analysts, we saved nearly 80 percent.”

– CISO, Better.com

Expel's a managed detection and response (MDR) provider whose mission is to make great security as accessible as the internet. The company's SOC-as-a-service capability offers 24x7 security monitoring and response for cloud, hybrid and on-premises environments.