



Nov 7, 2017 | Justin Bajko

Ready. Set. Go. Welcome to Expel.

Wow, it's launch day. We've been so heads-down over the past year and change, building tech and working with customers, it seems crazy to think we're here. I'm really excited to tell you about what we've been up to.

tl;dr: Today, we're announcing the first completely [transparent managed security service](#).

We're eliminating the black box within which managed security service providers (MSSPs) operate. You can see and use the same interface our analysts use to deliver our service. There's no "internal analyst console." There's no curtain to look (or hide) behind. With Expel, if you're ever wondering what we're doing for you or want to see how we're making decisions, you can easily look for yourself and see it all. We make it obvious what we're doing for you day in and day out. Practically, that means you can:

- **Watch investigations unfold in real time.** When Expel analysts decide something is suspicious and requires further investigation, you know immediately. And you're able to watch that investigation as it progresses. You can see evidence as we collect it as well as our analysts' findings for each piece of evidence. As it happens.
- **Take action even as the remediation plan develops.** You don't have to wait for us to finish writing up our findings for each incident before you can start taking action. Because you can see everything we're doing, as we create remediation and resilience recommendations for incidents you can begin responding while we're finishing our work.
- **Collaborate with our analysts.** Because you have the same access to our portal as our analysts, you can work hand-in-hand with us. You can take ownership of triaging an alert, you can create your own investigations, and you can add to any investigation we're already working on. You can even add your own commentary and remediation or resilience actions to an incident. Or...
- **Sit back and relax.** Because you can see with your own eyes that we're doing the right things for you and we've got your back, you can also relax knowing we'll tell you when there's something you need to worry about.

You might wonder why transparency is so important to us. Well... we believe too many companies are trapped in failed relationships with their MSSP and have had their expectations beaten down too low. It should always be obvious what value you're getting from your managed service. And you certainly shouldn't have to demand



weekly meetings and custom PowerPoint presentations thrown together by your engagement manager so you can understand what they've done for you.

Transparency ends an unhealthy and vicious cycle. If you're an MSSP customer, tell me if you've seen this before:

Problem: Customer can't see and understand what their MSSP is doing for them. Their only metric to measure the value from their MSSP is the number of alerts they've received. They complain to their MSSP. To amp up the "value" they're getting, they demand their MSSP "find more bad stuff!"

Boom!: The MSSP responds by increasing both the number and severity of alerts so they can "show more value." But...this only results in more work for the customer.

You don't deserve that. We spend our time helping you focus on the things that matter the most, and those things won't just be headline-grabbing attackers and malware. We'll also identify gaps, blind spots, misconfigurations and policy violations for you.

Okay, you get it. Transparency is important. There are also a number of other things we're doing that you'll be hearing a lot more about over the next few months. Here are a few:

- **We use the security products you've already bought.** We don't show up with a proprietary set of technology and then ignore all of the investment you've already made. We make your current investments work harder.
- **You get specific recommendations that are relevant to you.** We'll use what we know about your environment to tailor recommendations to help you respond to incidents.
- **We make recommendations to help you become more resilient.** We want to help you get better over time, and we'll use what we know about your environment as well as other customers to recommend strategic changes you can make to reduce your risk.

And we do this 24/7/365 in a way that won't ruin your budget. In fact, the cost for a 1,000-person company is typically less than the cost of a single full-time experienced security analyst. We've got three different service levels that start at \$14,000 per month for 1,000 protected endpoints. If you'd like to learn more about our pricing, the good news is that we put it on our website. [Take a look!](#)

If you're interested in learning more about Expel, [take a tour](#) of our service to learn more about how these concepts are actually implemented. You may also want to bookmark our [EXE blog](#), or tweetagramchat us (I'd get in trouble if I didn't take this a bit more seriously and tell you that you can find us on [LinkedIn](#) and [Twitter](#)) if that's your thing. And of course, [we're hiring!](#)

I'm really excited to be talking about what we're up to, and telling you more about it over the coming months. And also I'm stuck on how I want to end this thing, so I'll just stop typing now. kthxbye.

About Expel

Expel provides transparent managed security. It's the antidote for companies trapped in failed relationships with their managed security service provider (MSSP) and those looking to avoid the frustration of working with one in the first place. To learn more, check us out at www.expel.io.