Devolutions

Should You Trust a Third Party with Your Cybersecurity?

THAT'S ACTUALLY A PRETTY FUNDAMENTAL QUESTION

In our last cybersecurity post on Devolutions, which explained how our MDR service works, we received a lot of great feedback. But we repeatedly got one question that surprised us: "Why would I ever trust a third party with control of my network?" Of course, our first response was that the folks who asked this question did not understand how the IT and cybersecurity services industries work. But as we thought about it some more, we thought, well, that's actually a pretty fundamental question.

Let's set aside the more surface question about how companies can trust outsiders to handle their IT and cybersecurity. The answer is no different from how you trust any vital business partner: you find reputable partners with bulletproof reputations. The more interesting question is not how but why.

The Question Behind the Question

Why should we delegate control of our digital safety net to an outside company? It comes down to three essential benefits that reputable, specialized, and experienced cybersecurity firms bring to the table:

- Level of service (can they offer it?)
- Type of technology (have they got the right one?)
- Experience and reputation (do they have it?)

Today's Lesson Is Brought to You by the Letter M

First things first: Who are these organizations pitching their services to provide outsourced cybersecurity services to you? Broadly speaking, there are three types of organizations competing to become your virtual SOC.

MSP

An MSP (Managed Service Provider) is a generalist IT company that is basically looking to take over some or all of the management of your software and hardware. These IT outsourcing services also frequently offer cybersecurity services. They are rarely specialists, but they do offer the competitive advantage of having pre-existing relationships, which helps open the door when cybersecurity needs are identified and it requires something more specialized.

MSSP

MSSP (Managed Security Services Provider) are like MSPs that are specialized in cybersecurity. MSSPs focus more on the selection and implementation of security platform management of security consoles. They then maintain and operate this software and forward alerts to your IT team to take action.

MDR

Today, with the surge in frequency and sophistication of cyberattacks, it's essential to understand the origin of alerts, identify potential impacts, and know how to close security vulnerabilities. Managed Detection and Response (MDR) services are a response to this new reality. MDR services enable a proactive approach to cybersecurity. They focus first on detection by identifying sources of risk and monitoring these vulnerabilities. The real power of the MDR is the R – where the provider analyzes the threat and provides actionable remediation measures to counter it and minimize its potential impact.

So Why Should You Trust an Outside Company?

The answer is that it's the only move that makes sense, especially if you are a small- to medium-sized business. Here are the 5 top factors driving SMBs to outsource cybersecurity:

1. Cost – Because you need protection and setting up your own in-house team is an exceedingly expensive process.
2. Speed – Hiring a team and setting up your own SOC takes time – time you don't have.
3. Experience and Expertise – Your provider, if you've chosen well, has a team of qualified security professionals who do nothing but security and have seen every trick in the book.
4. Focus – Outsourcing cybersecurity lets your IT team focus on their core tasks rather than being constantly pulled away to deal with cybersecurity issues.
5. 24/7/365 coverage – If you need to set this up in-house, it will take time and be very expensive.

Back to the Questions Behind the Question

At the top of this post, we mentioned three questions that should shape your choice of cybersecurity partner. So, let's explore each of those a little more closely.

Can They Provide the Level of Service You Need?

When you choose a service provider, be sure to ask: Does the service provider only offer cybersecurity services? More and more, opportunistic companies are adding a cybersecurity component to their IT service offering.

Unfortunately, according to many cybersecurity experts, this is a conflict of interest when it comes to serving a client. More often than not, organizations that offer IT outsourcing and computer security services can find themselves in a situation where their security personnel come into conflict with their own IT team. And it's important to understand that IT management expertise is not cybersecurity expertise. Therefore, it's essential to make sure you choose a partner whose focus is security management and whose team is 100% dedicated to cybersecurity.

What Is Appropriate Technology for Your Risk Profile?

There are a multitude of technologies you can base a managed service offering around. And, even inside a segment, the tools are very different from one another. Here are three standard tools on the market: SIEM, EDR, and IDS (or network monitoring).

SIEMs (Security Information and Event Management) are tools created to centralize security logs and events, such as failed or successful access attempts. A SIEM allows you to monitor specific elements in your network.

EDR (Endpoint Detection and Response) is a security solution designed to detect cyberattacks on individual machines. They are like next-gen antivirus programs. EDR solutions go beyond simple signature-based detection: they use memory analysis, behavioral analysis, and IOC detection. But EDR does have significant limitations. For example, they don't provide visibility on Internet of Things (IoT) devices or the Cloud. And, even in mid-sized businesses, EDR systems often cause conflict with existing antivirus software.

Based on the network communication flow analysis, IDS (Intrusion Detection Systems, also called Network Monitoring or Network Detection and Response) technologies focus on detection. Its most significant advantage: 360° visibility on machines such as printers, IP phones, IoT devices, connected telephones, security cameras, etc., can be used to detect the presence of a network. Today, it's essential to monitor all network-connected devices since they are often used as relays by hackers. IDS/NDR-type technologies also offer earlier detection, making it possible to identify intrusion signals faster.

Your provider will likely recommend one or several of these technologies, so it's important to know what they do and where their strengths lie.

Do They Have the Expertise?

Maybe the most critical factor to consider when selecting a partner is their expertise. Real-world, human experience may be the most critical component of your partner's offering. It may sound trivial, but do your homework on the team being proposed by your potential partner.

There are many areas of expertise in cybersecurity. Make sure your provider has all the qualification analysts to handle security alerts and incident response. Security analysts must have the experience and knowledge to interpret attack signals, understand hacker techniques, and provide recommendations to mitigate security risks. Make sure your security provider has the following profiles on its team: chief cybersecurity officer, cyberattack management expert, incident response expert, malicious code analyst, and malware reversers.

Takeaways

Should you trust a third party to take care of your cybersecurity? Yes, if you've done your homework and they have the skills and experience to fit your needs. The right specialist partner (like StreamScan with a 10-year track record, qualified team, and government-approved technology) will have knowledge and expertise that you can't match, and they will have the experience of responding to cybersecurity issues every single day.

When you choose your partner, keep these three things in mind. First, define the level of support you need. Second, select the technology/ies that fit best. And finally, choose an organization with the expertise to execute on your cybersecurity strategy.

Keep up with all the latest developments in cybersecurity for SMBs with the StreamScanner newsletter. Sign up here.

Need Help? StreamScan Is Here

Whether you need help conducting a security audit, developing a security plan, or implementing a Managed Detection and Response solution, StreamScan has experts with many years of experience who can help. Get in touch with us at smbsecurity@streamscan.ai or call us at 1 877-208-9040.