The Power of Managed Detection & Response

A bluedog Whitepaper

bluedog
SECURITY MONITORING

The Power of Managed Detection and Response

Executive Summary

A single cyber-attack can cost a small or medium-sized company up to $200,000[1]. This means going out of business for most of them. More importantly, as the first chapter of this whitepaper is going to show, cyber risks to small companies are by no means rare.

Media outlets tend to focus on reporting cyber-attacks on large companies, the size of Twitter and Google, because those data breaches affect more end users. But the attacks on small companies are much more numerous for a simple reason: they are easier targets.

Most SMEs (even those in IT and tech) lack the resources to *really* protect themselves from cyber-attacks. This makes them easy targets, even for less skilled cyber criminals.

This is where managed detection and response comes into play. Chapters one to three of this whitepaper are focused on what managed detection and response is, why do SMEs need it, and how to make sure you choose the right service from the right provider.

All in all, this whitepaper is designed to be a starting guide for SMEs that are cyber-security-conscious and to offer them the tools to shelter their data and their systems from attacks. Of course, all recommendations are budget-friendly.

[1] https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html, retrieved October 2020

Table of Contents

Global Security Threats for SMEs and the Challenges in Coping with Them

The COVID-19 pandemic sent employees from small and big companies alike to work from home. And it looks like remote work is here to stay[2]. This meant relying more heavily than usual on conferencing solutions and other teleworking software. 20% of companies made the switch to telework without a single thought to cyber security[3].

We all remember the attacks on the most used video conferencing app, Zoom[4]. When the login credentials were exposed on the Dark Web, the attackers didn't just gain access to Zoom accounts. They most likely also gained access to company systems.

And this is just the tip of the iceberg. Attacks on SMEs aren't novel. As early as the 80s the Morris worm nearly wiped out everything on the internet (albeit, truth be told, the internet back then was far from the internet we know today). More than three decades later, cybercrime is expected to cost us $6 trillion by 2021[5].

And yes, a lot of that money will be paid by SMEs. Remember the Zoom incident mentioned above? As soon as an attacker gains access to employee credentials, they can start attacking the company network from within.

This is what is called an insider-related cyber incident. Most of these incidents don't happen, as one might think, because of the employee's malice, but because of their negligence of lack of knowledge.

According to IBM and Ponemon Institute, small businesses (those that have less than 500 employees) spend $7.68 million per insider-related incident[6].

And it's not just about the money you can lose directly! A cyber incident comes with a lot of downtime:

---

[2] https://www.cnbc.com/2020/05/11/work-from-home-is-here-to-stay-after-coronavirus.html, retrieved October 2020
[3] https://www.alliantcybersecurity.com/the-flight-to-remote-working-cybersecurity/, retrieved October 2020
[4] https://www.cpomagazine.com/cyber-security/half-a-million-zoom-accounts-compromised-by-credential-stuffing-sold-on-dark-web/, retrieved October 2020
[5] https://www.ciosummits.com/, retrieved October 2020
[6] https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/, retrieved October 2020

Figure 4: For the most severe security breach managed in the past year, the number of hours systems were down correlated with organizational size (N=2265). Percentages are rounded.

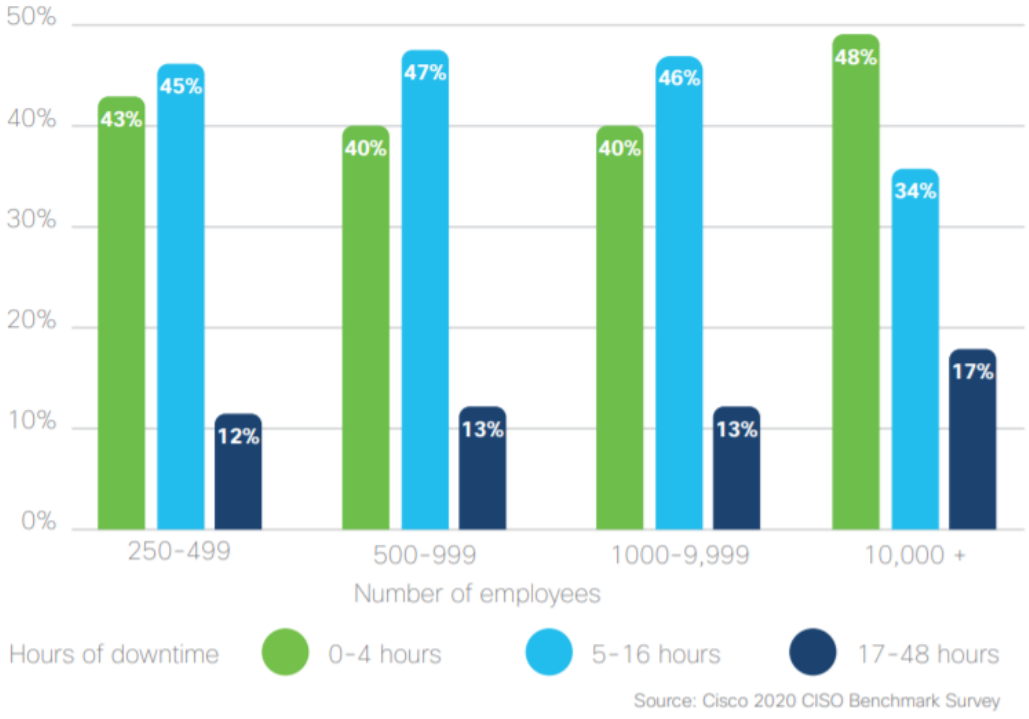


Image source[7]

The number of companies who don't have any defenses is staggering. A 2020 study[8] revealed that two in five companies in the UK and the US with less than 50 employees don't have *any* cybersecurity defense plans. That's 43% of the companies surveyed!

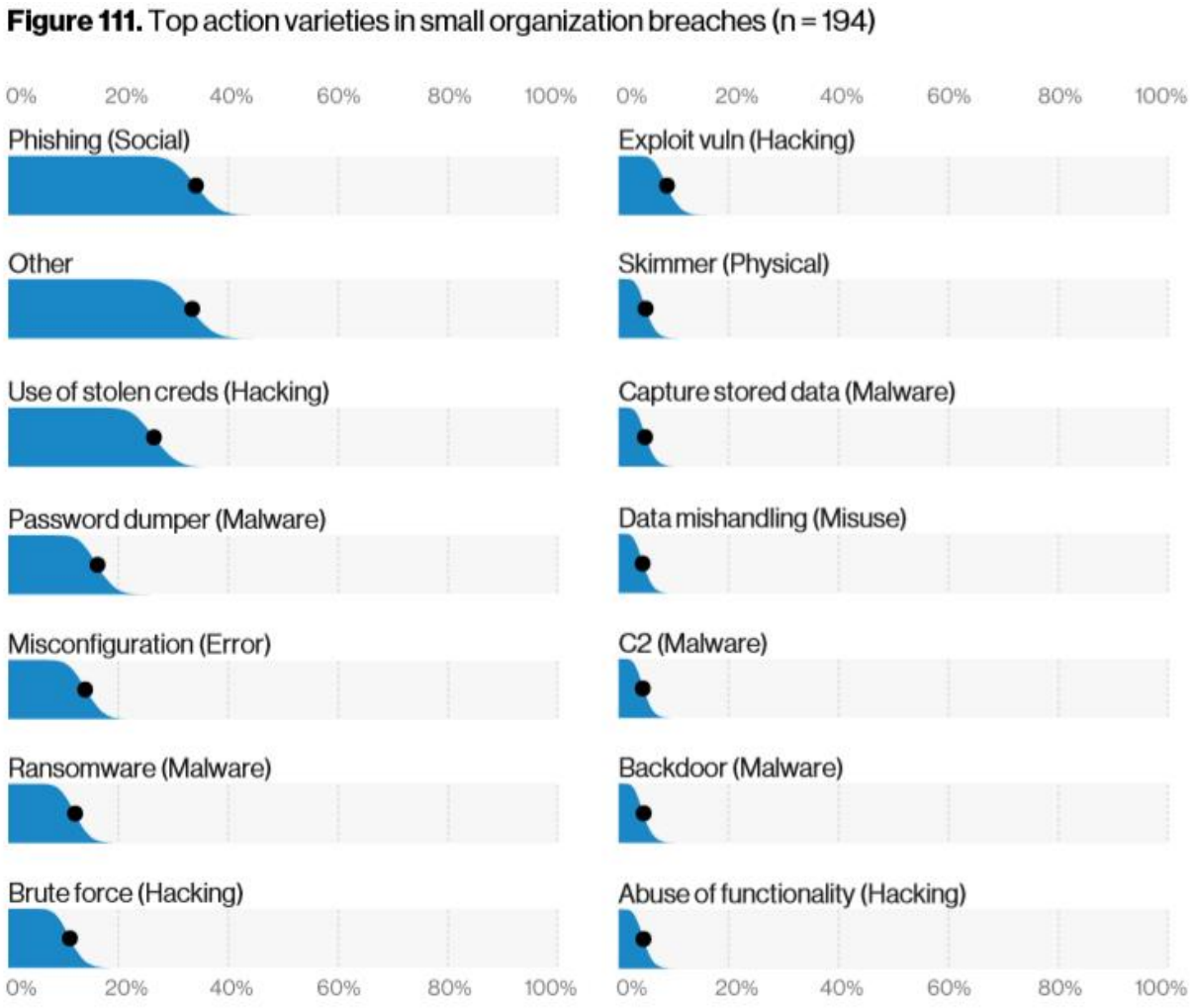
The same study showed that 23% of SMEs in the US and the UK don't use any endpoint security mechanisms. Not too big a number, right?

Right! But the BullGuard study goes on to say that 32% of those that *do* use endpoint security mechanisms rely solely on free, consumer-grade solutions. That means that more than 50% of the surveyed company practically don't have elementary cyber security measures in place.

[7] https://www.cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html, retrieved October 2020

[8] https://www.prweb.com/releases/new_study_reveals_one_in_three_smbs_use_free_consumer_cybersecurity_and_one_in_five_use_no_endpoint_security_at_all/prweb16921507.htm, retrieved October 2020

A 2019[9] Verizon report showed that 28% of the breaches that year involved a SME. And they are exposed to all types of risks.



Back to the BullGuard study cited above, 60% of SMBs say that they don't feel like they could be the target of a cyber-attack. This even though nearly one-in-five companies in that study *already were* victims of a cyber-crime.

Why do SMB owners seem to bury their head in the sand when it comes to cyber security? The answer is two-pronged:

- Lack of knowledge: most of them are not IT specialists so it takes time for them to understand the risks they are vulnerable to. More often than not, this happens when it's too late: after they have fallen victim to their first costly attack.

[9] https://enterprise.verizon.com/resources/reports/dbir/, retrieved October 2020

- Lack of budget: there is an on-going shortage of cyber security specialists. Most of them are hired by large companies, with large budgets, that can afford impressive salaries. More importantly, a single expert is not enough for a company – the threats are diverse and ever-changing, so a full team is needed to stay on top of every risk[10].

Does this mean that it's a moot point to even try and stay on top of cyber security challenges as a SME? Not at all!

The cyber security market has evolved to mitigate these risks, so there are affordable solutions and services that you can implement. Read on to find out more about one of them.

What Is Managed Detection and Response?

Briefly put, Managed Detection and Response (MDR) is an outsourced service that offers companies threat hunting capabilities and threat response as soon as they are discovered. MDR is not just a

[10] Check out our whitepaper on skills shortage in the cyber security industry to better understand this problem:

technology stack; it also involves human intervention. Managed detection and response providers offer their customers access to their pool of engineers, researchers, and security experts who are tasked with monitoring network security, analyzing all incidents, and quickly responding to any threat.

In a world where cyber security threats are on the rise, but the budget to deal with them is not, companies that offer managed detection and response services support businesses that are lacking the skills or, the time, or the disposable money to deal with security.

Managed detection and response services provide both the dedicated personnel and the dedicated technology to improve security operations for companies of all sizes. The MDR approach comes on three levels:

- Threat identification
- Investigations
- Threat response

This service is designed to complement traditional managed security options that usually focus on broader security alerts, as well as on management and triage. You will find countless definitions of MDR online, depending on what type of service each company offers. The MDR packages you can buy also come with different features and options.

However, there are a few common traits between these packages. They typically offer:

Resource Augmentation

This is the key offer for companies who lack the cyber security personnel they need to deal with threats. MDR service providers add their own teams' skill sets to help their clients' staff identify and manage threats better.

Forensic investigations, threat hunting, and incident response are the areas where SMEs most commonly need help. Of course, this can vary from company to company.

Security Maturity

Most SMEs have rudimentary security systems in place, if any (see the previous chapter). MDR comes with a mature approach to cyber security.

This usually includes being proactive in threat management, being available 24/7, and constantly updating the security solutions stack as need arises.

Curated Technology Stack

For SMEs that lack both the personnel and the expertise to deal with cyber security, identifying the ideal technology stack is a major bottleneck. This is where MDR experts step in.

Ideally, your MDR provider should not only offer security experts and operational best practices, but also advise on the security stack you need. This advice should always feature in the company's specific needs, as well as the available budget.

Reduced Time to Detection and Response

MTTD and MTTR are two components every MDR provider should offer. Managed detection and response is only effective if it's *fast* – much faster than what you can achieve on your own.

Response times should always be part of the SLA and so should the commitment to continuous improvement.

Why Do You Need Managed Detection and Response?

The number of unfilled cyber security positions is expected to reach 3.5 million by 2021[11]. This makes it incredibly hard for SMEs to afford and to find cyber security experts. While this is the first and most significant reason why MDR services are useful, there are a lot of other ones.

Deploying Complex EDR Solutions Is Challenging

For companies without large cyber security teams in place, it's challenging to deploy the complex EDR (Endpoint Detection and Response) solutions they need. Even when such tools exist, it's hard to find the skills and the time to leverage them to the fullest in-house.

This is why some companies end up paying a lot for EDR solutions but they never use them to the fullest. MDR integrates these tools in the service provided and makes them a part of the detection, analysis, and threat response roles.

Large Volumes of Security Alerts Have to Be Managed

The sheer volume of alerts IT teams typically receive is impressive. Even companies with a dedicated IT team in place find it hard to manage them.

A lot of these threats can't be identified as malicious on the spot – for instance, the vulnerability scanning tool doesn't mark them as such. Or it does, but erroneously. This is why almost every alert has to be individually and manually checked by a human expert.

Even more, security teams have to correlate these threats. Correlating them can pinpoint to a larger and more significant threat that cannot be revealed by automated tools alone. Small security teams can be easily overwhelmed by the amount of data they have to go though.

MDR addresses this problem by not only detecting a threat, but also analyzing all the factors and indicators associated with it. A proper MDR service will also provide recommendations (even some that concern the organizational structure) based on the security events it identifies.

[11] h https://cybersecurityventures.com/jobs/, retrieved October 2020

This is, perhaps, one of the most significant values MDR brings to the table. Automated tools may have the ability to block a threat and neutralize it in the short run. But the human factor is key in contextualizing and analyzing all threats so that they can be neutralized in the long run, as well.

Solve the Cyber Security Skills Gap

We talked about this at length. The skills gap in the industry is significant.

But MDR does more than supplement your IT team with a few extra hands. It can also help address more complex issues that a regular IT team can be overwhelmed by. Even more, MDR service providers offer their customers access to tools they couldn't otherwise access.

Typically, all this is done at a cost much lower than hiring a whole security team. Which brings us to the next point:

MDR Saves You Money

As shown before, the skills and human resources shortage in the cyber security industry comes with an added problem: real experts aren't just hard to find, they are also very expensive.

MDR services are designed to kill both birds with one stone: not only will you not have to concern yourself with finding the right experts, but you won't have to break the bank paying them, either.

An MDR provider has done both for you. They can afford to pay huge salaries because they manage multiple clients at a time. Similarly, the cost of the tools they use or create is shared between these clients.

MDR has been validated time and again in both efficiency and necessity. However, this has led to a crowded marketplace, with thousands of offers and various types of services and features. How can you choose between all of them?

Let's find out!

How to Choose a Managed Detection and Response Provider?

We have established that managed detection and response services can keep your company safe. But how can you choose from the hundreds of providers out there?

The 2019 edition of Gartner's Market Guide for Managed Detection and Response Services[12] divides providers into four different groups, based on technology stacks:

1. The provider has the full stack
2. Managed point solutions from the provider: Endpoint Detection and Response (EDR) and Network Detection and Response (NDR)
3. BYO (Bring Your Own) – the provider doesn't come with their own stack but they will help manage and leverage yours
4. The provider only offers one type of technology, typically with its own MDR in place: IaaS (Infrastructure as a Service), SaaS (Software/Security as a Service), OT (Operational Technology), IoT (Internet of Things) or IIoT (Industrial Internet of Things)

While this is a good classification and a good starting point, it sheds very little light on how to choose the provider you need within these four groups.

So, let's say you know which of these approaches works best for you. Let's move on to finding the perfect provider. Here are some criteria to look for:

A Combined Approach

Your MDR provider should not rely on a single data input source. They should look at security detection tools, third-party data sources, threat intel feeds, the IT asset database, and more, depending on the complexity of your network.

When you shortlist candidates, make sure to take this into account. How thorough are they with their approach?

[12] https://www.gartner.com/en/documents/3947444/market-guide-for-managed-detection-and-response-services, retrieved October 2020

Take into Account Your Specific Needs

Some MDR providers specialize in very small companies. Others work with large corporations only. And, of course, there are those who specialize on a single industry whose threats they are most familiar with: legal, medicine, IT, and so on.

Before you make the hire, do your own homework. Qualify and quantify your company's needs and send them to the shortlisted providers. Can they tackle them all?

Don't Forget about the Human Factor

The right MDR approach combines technology stacks with human input (see the *What is MDR?* chapter). Take a close look at their organizational structure. Do they have enough experts to ensure your safety? Are those experts well-versed in your specific needs?

Last, but not least, think about your own human factor. Does the company offer on-going training for your own staff or at least a threat prevention crash-course? Remember that most threats can be tied to insiders, so this is quite important.

Focus on Ongoing Improvement

Cyber threats are very diverse. What's more, this diversity grows every day. The fact that you are safe today doesn't guarantee you will be safe tomorrow.

Add your company's evolution to this – adding new devices, hiring new staff members, adding new tech solutions and software to your stack – and you'll see why quantifying threats isn't something that can be done only once.

It's an ongoing process. Just like strengthening your defenses should be. Is your provider focused on this?

Transparency Is Key

Your CIO/CISO should always be kept in the loop. The MDR provider should offer unprecedented transparency when it comes to your security.

Will your CIO/CISO have access to all dashboards and data visualization tools? How will the communication between your IT team and the MDR team happen? With what frequency?

While MDR has "managed" in the name, you shouldn't simply pay the invoice and forget about it. Make sure someone in your team has access to all the data and all the statistics. This way, you can help mitigate threats and, when you change MDR providers, you won't have to start from scratch.

If you're looking for a managed detection and response service, you have come to the right place. Bluedog Security Management checks all the boxes above and more. Head on to our contact page and let's talk about how our MDR service[13] (with an MDR Compliance feature!) can help you.

[13] https://bluedog-security.com/managed-detection-and-response/, retrieved October 2020

About BlueDog Security Monitoring

Our goal is to provide businesses with a level of network protection typically only afforded by large corporations. We aim to bring high-quality technology, support, and service to the small to medium business, helping protect their business from cyber threats.

Our company is growing quickly, through our simple and affordable end-to-end network monitoring solution. Recently voted one of the Top 10 cybersecurity start-ups of 2019 by Enterprise Security Magazine. Whether you are a small business, or an MSP or IT services reseller or distributor, get in touch and have a chat with us.

20-22 Wenlock Road, London, N1 7GU

info@bluedogsec.com

+44 20 8819 6254