



# What Every SMB Must Know About Security Threat Prevention, Detection, and Response

White Paper | 2022



# Security threats are unnecessarily outpacing the SMB

In today's "smart" connected world, cybercriminals and their tools are having a field day. Anything connected to the Internet is within reach as bad actors execute phishing campaigns and malware strains that are increasingly sophisticated and diverse. This means that businesses of any size are in the crosshairs, should they not have the appropriate security protocols in place.

Indeed, the SMB (small to mid-sized business) is no stranger to security threats, but how they deal with these threats differs considerably from the activities of an enterprise organization. For example, more than half (53%) of SMBs handle all their security-related activities in-house, yet 41% say their biggest challenge is "speed of incident response."<sup>(1)</sup>



41% of SMBs say their biggest challenge is "speed of incident response."<sup>(1)</sup>

This comes as no surprise, given that internal resources and expertise are well-known shortcomings for the SMB.

Security posture visibility is another challenge that is specific to the SMB. While enterprise organizations undergo regular risk assessments, such a thing is much less common in smaller operational settings. This leads to security blind spots that hinder successful threat prevention and detection.

## What must SMBs do to keep up?

**Regardless of operational structure and any inherent limitations, every SMB must be able to:**

- Fully understand the security risks of doing business
- Make informed decisions on the risks they will address, as well as those they will accept as part of doing business
- Utilize technologies and services that are appropriate for the specific risks they want to address
- Accomplish the above in a way that is cost-effective for—and presents value to—the business as a whole



This white paper covers the important information every SMB should know about security threat prevention, detection, and response. This includes the average costs as well as how to source vendors and technologies according to your organization's specific needs.

## Being reactive is not an option


The smaller the organization, the greater the difficulty it has taking proactive security measures. Most SMBs operate in a lean staffing environment where those responsible for security-related activities such as log monitoring and vulnerability management are often tasked with additional business-sensitive directives.

Another issue is that most SMBs do not employ a security expert in-house. According to Gartner, even mid-sized enterprises have a 20:1 IT staff to cybersecurity expert ratio. The unintended consequence of non-dedicated, undertrained staff is a reactive security posture.

However, the cost of being reactive is high. In our work with SMBs locked down by ransomware, we have seen victims pay as much as \$7,000–\$10,000 per device to get their business back online. We’ve also seen a 110–person company undergo an \$800,000 ransomware recovery (incident response, forensics, legal costs, etc.). Indeed, the ransom payment is usually the least expensive part of bringing your business back from an attack.


By contrast, a proactive approach to security prevention, detection, and response significantly reduces the chances of a large capital outlay due to a breach or ransomware event. Yet, for many SMBs this is easier said than done; however, the advent of third-party, 24/7 Managed Detection and Response (MDR) services presents new viability for the SMB.

## What’s the build vs. buy on MDR?



The vast majority of SMBs are not able to maintain 24/7/365, steady-state monitoring with their internal staff. <sup>(2)</sup>

One reason is that most SMBs are staffed with IT professionals, but not necessarily those who specialize in—or are completely dedicated to—IT security.



The cost to attract, hire, and maintain qualified security personnel internally is prohibitive in and of itself; consider that the cybersecurity professional’s average salary is \$135,000. <sup>(3)</sup>

Now multiply that \$135,000 by seven, which is the number of full-time employees required to maintain 24/7/365 security threat detection and response activities.

In short, forging a trusted partnership with a service provider minimizes the costs of ongoing security while giving your business the coverage it needs. In this scenario, the time and money spent to recruit, hire, train, and compensate internal resources is instead dedicated back into your core business activities.



### Prevention:

Blocking and stopping cybersecurity attacks before they create an incident.



### Detection:

Keeping watch over the IT environment for early indicators of compromise.



### Response:

Taking the appropriate action steps when a legitimate threat is detected so it is quickly contained, and its impact is minimized.

## Advanced prevention technologies are a great first step

Every business is a cybercrime target, whether they expect it or not. There are teams targeting a large number of companies through Internet-based, dragnet-style campaigns, where success is measured by only a small percentage of hits due to high profitability per hit.

Most SMBs rely on the standard anti-virus protection that comes with their computer. While the convenience of a free, included product is cost-effective, these built-in products provide only basic levels of protection and fail to block the advanced threats that are now commonplace.

Today, employees and companies are being attacked by advanced threats and previously unknown variants of malware much more frequently than they are by the known, recycled malware. This business reality requires prevention technologies that go beyond the basics to effectively block system and application exploits, potentially unwanted apps, ransomware, and malicious code from infiltrating endpoints.

## Ransomware Hits Home

A mid-sized retail store chain with 18 locations was hit with ransomware overnight, and every single store was down at opening time the next morning. The entirety of the store's systems and data was encrypted by the ransomware, forcing the company to operate manually.

It took a week from the identification of the ransomware for them to get the decryption program, then days more to execute the program, then weeks to fully recover.

What couldn't they do in the week-plus they were down? They couldn't electronically process payments (had to revert to cash), order supplies (risked running out of product), or consolidate store expenses/revenues back into central accounting.

## Independent features of today's advanced prevention technologies include:

- Anti-virus and anti-malware protection
- Advanced Machine Learning (AML) exploit prevention
- Ransomware detection and prevention
- Advanced threat indicators of attack identification
- In-depth threat details and root cause analysis
- Remediation and malware removal support

These features are meant to secure endpoints from inbound attacks, and for the most part they do. However, prevention alone does not provide visibility into your entire IT environment, because not everything is a trackable endpoint in the world of BYOD (bring your own device).

## Detection and response pick up where prevention technologies leave off

While the prevention capabilities of advanced endpoint protection technologies serve as a critical barrier against security threats, no single solution is 100% impenetrable. And with less than two hours between the time of exfiltration/encryption and the time of infection, a solid mechanism for detection and response is business-critical.

To be effective, detection and response activities must be conducted on a 24/7/365 basis. Furthermore, the people conducting these activities must be completely knowledgeable in their role as well as the technologies deployed. Finally, they must be dedicated to the task of threat detection and response.

As previously discussed, most SMBs don't have the financial or operational wherewithal to support an internal staff of professionals for detection and response.



Therefore, the cost-effective and best-practice solution is to outsource these functions, consuming them as a managed security service.

Robust MDR services include advanced endpoint protection (known as EDR, or Endpoint Detection and Response), as well as log event collection and correlation, and proactive threat hunting. In this scenario, professional security analysts working within a security operations center (SOC) are trained to spot and appropriately investigate and remediate any anomalies. This round-the-clock, dedicated coverage provides the necessary resources, expertise, and responsiveness for a strong security posture.

## What is XDR?

One of the newest acronyms to enter the managed security services marketplace is XDR, or Extended Detection and Response. According to the security industry's definition, XDR incorporates all things MDR and adds extended visibility into networks, systems, and cloud logfiles, activities, or metadata. There are several organizations that already offer these capabilities as part of their standard MDR service. So, buyer beware, you must look "under the hood" of any offering to determine what it really entails.

**Regardless of whether a service provider offers XDR, MDR, or EDR, the more important discussion surrounds your business' needs, and this requires answers to the following questions:**

- How many employees do you have?
- What type of business (retail, healthcare, financial, etc.) are you operating?
- Do you have a professionally installed and configured firewall?
- What kind of endpoint protection are you currently using?
- What cloud services do you use?
- What compliance requirements is your business subject to?

A meaningful partnership for efficient and effective protection is based on an understanding of your operating environment, the types of protections you currently have in place, and the security risks you are looking to mitigate.

## How to Avoid Cyberthreats

Late on a Friday, a new customer began installation of the PDI Extended Detection and Response (XDR) service to their end user systems. This customer is an SMB that relies on personal computers to keep their business running.

A few hours after the customer's implementation was complete—at 12:05 a.m. Saturday to be exact—XDR blocked an attempted execution of malware that was present on one of their remote office computers. A variant of Trickbot malware, it checked for POS systems, gathered information about the network, and scraped the system for usernames and passwords, web history, email data, and more.

Upon identifying the malware threat, our SOC analysts immediately began investigating and cleaning up the malicious files and settings, blocking the infections and stopping further malicious activity from that user profile. All this activity, from initial threat identification to complete containment of the malware, took place in under an hour.

## There is a big difference between detection and response

Detection and response are core components of every security program. But while these two activities must coexist in the business environment, an examination of the service levels provided through these words often reveals they are operating independently.

First, technologies and processes must be in place to detect active security threats. Then, additional technologies and processes must be in place to effectively respond to those threats, up to and including remediation.

The above is important to keep in mind when sourcing vendors and technologies. Most SMBs do not have the internal fortitude to fully support detection and response as an end-to-end process. The solution is to partner with the solution provider whose processes and technologies best fit the organization's business operations.

## Which factors indicate strong alignment?

**The following factors are key indicators of whether a potential MDR/XDR partner is a best fit for your business' threat prevention, detection, and response needs:**

- Asks questions to fully understand the business' existing resources, as well as its known and unknown security risks and gaps
- Provides technologies and services that bridge security gaps to ensure complete coverage
- Monitors system and event logs according to the latest threat intelligence, 24/7/365
- Puts forth the effort to foster a partner relationship that charts a path to increasing security maturity
- Accomplishes the above through simplified technology interfaces and communications

The ideal scenario for the SMB is a relationship that affords little to no internal technology and human resource overhead on their part. Not only is this highly cost-effective, but fully outsourced MDR/XDR also shields the SMB from the inefficiencies of multi-tasked internal resources.

## A strong security posture is possible, even for the SMB

While it's impossible for any company to account for all of its security vulnerabilities, it is possible to create a strong security posture to protect the organization from cybercrime. And, because this possibility isn't tied to large financial spends or a robust in-house staff, a strong security posture is certainly possible for the SMB.

MDR/XDR service providers are available to take the burden of threat prevention, detection, and response off the shoulders of the SMB and place it in the hands of dedicated, well-qualified professionals. The key is to find a partner relationship that adds immediate value as well as an ongoing ROI for the way you do business.



## Simple ROI Model of Internal vs. Outsourced XDR

Based on 24/7/365 Coverage, 100-Person Company

### Internal XDR:

Advanced Endpoint Protection (Annual License)	\$20,000
Log Management/SIEM (Annual License)	\$12,000
Staffing (7 Members, Mix of Jr and Sr)	\$945,000
Threat Intelligence (Annual Subscription Fees)	\$100,000
Training (\$5,000 x 7 Staff)*	\$35,000
<b>Total Annual Cost</b>	<b>\$1,112,000</b>

\* First-year cost, with an adjusting cost thereafter based upon employee turnover.

\*\*Services and pricing estimated according to PDI XDR service.

### Outsourced XDR:

Managed Detection and Response (Annual License)**	\$50,000
Advanced Endpoint Protection	Included
Log Management/SIEM	Included
Fully Trained Staff	Included
Incident Response	Included
Threat Intelligence	Included
Proactive Threat Hunting	Included
SaaS Threat Monitoring (Cloud IaaS and PaaS)	Included
Log Data Retention (365 Days)	Included
<b>Total Annual Cost</b>	<b>\$50,000</b>

## PDI Security Solutions

PDI Security Solutions are purpose-built to unify control with a robust security platform, network security appliance, and managed security services. We help multi-site operators, convenience store retailers, and small to medium-sized businesses connect, secure, monitor, and scale highly distributed environments while protecting their critical data and assets.

PDI Managed Security gives you peace of mind that your business is protected, agile, and compliant across all locations and applications. We're here to support your network and security needs and protect your IT environment from threats and vulnerabilities.

<sup>(1)</sup> ControlScan, "2019 Managed Detection and Response Research Report," September 2019.

<sup>(2)</sup> ControlScan, "2019 Managed Detection and Response Research Report," September 2019.

<sup>(3)</sup> Gartner, "How CIOs in Midsize Enterprises Can Best Fill Staffing and Skills Gaps in Security," May 2019.



## About PDI

Professional Datasolutions, Inc. (PDI) software helps businesses and brands increase sales, operate more efficiently and securely, and improve critical decision-making. Since 1983, PDI has proudly served the convenience retail and petroleum wholesale industries. Over 1,500 companies, representing more than 200,000 locations worldwide, count on PDI's solutions and expertise to deliver convenience and energy to the world.

For more information about PDI, visit us at [www.pditechnologies.com](http://www.pditechnologies.com).

