CONNECTWISE™

CONNECTWISE EBOOK SERIES

# An MSP's Guide to Protecting SMB Clients

## DELIVERING MANAGED DETECTION AND RESPONSE SERVICES

# CONTENTS

# CHAPTER 1: SECURITY IS A THREAT...

As a managed IT solution provider (MSP), cybersecurity is rapidly becoming one of the biggest threats to your customers and your continued business success. While massive data breaches at brand name companies continue to make the headlines, the real story is the quieter, widespread epidemic of successful cyberattacks against small- and medium-sized businesses (SMBs).

## Two growing trends put SMBs at a greater risk than ever:

1. Threats are more frequent and sophisticated, while the attack surface has expanded through cloud and mobile.
2. As enterprises work harder to implement the people, processes, and technology to protect their businesses, cybercriminals are turning their attention to a perceived softer target: SMBs.

### Keeping Your Clients Up at Night

80% of SMBs are worried that they will be the target of a cyberattack in the next six months.

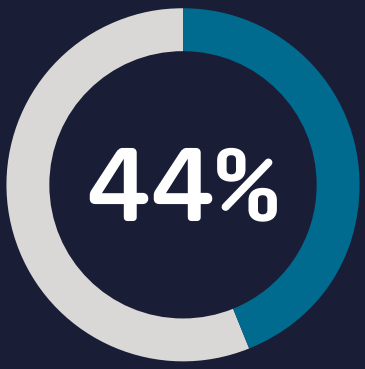
Source: **Cybersecurity in an Era of Competing Priorities: The State of SMB Cybersecurity in 2021 a Connectwise Study conducted by Vanson Bourne**

## …and an Opportunity

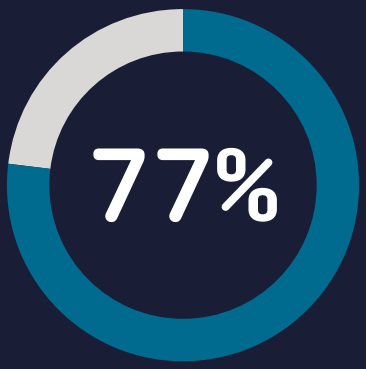
Because SMBs typically don't have the skills, awareness, or resources to protect themselves against today's advanced cyberthreats, they need the help of a trusted MSP more than ever. While offering cybersecurity services is a clear revenue opportunity, it's also becoming the biggest differentiator for MSPs. SMBs will favor (and migrate to) those MSPs that can truly protect them with a full spectrum of 24×7 threat detection and response services.

Is your business prepared to deliver the security solutions that your clients need and demand? Have you assessed your company's risk of a cyberattack? What would happen if your customers were attached? Read on for insight into what MSPs need to do right now to protect their customers and themselves.

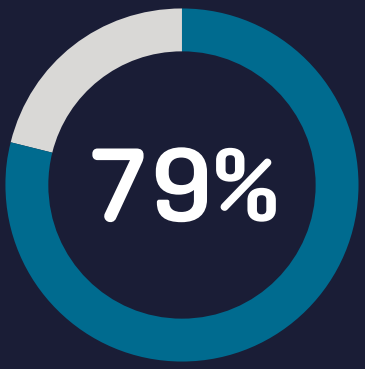
### Cybersecurity Is a Top Priority for SMBs




**see cybersecurity as one of the top three priorities in their organization**




**are planning to invest more in cybersecurity in the next 12 months**




**agree that there should be more emphasis on security in their organization**

Source: **Cybersecurity in an Era of Competing Priorities: The State of SMB Cybersecurity in 2021**

# CHAPTER 2: CLIENTS WANT GREATER PROTECTION FOR THEIR BUSINESS

In the past 12 months, 32% of SMBs have suffered a cybersecurity attack, with an average cost of $104,296. On the flip side, only 5% of MSPs reported that they experienced a significant security incident in the last 12 months.[1]

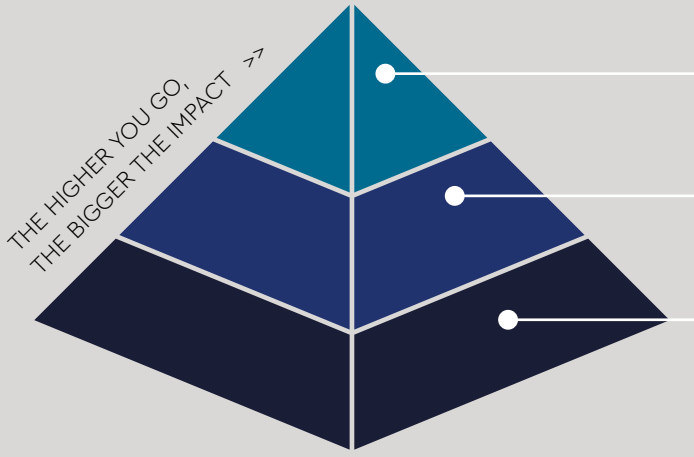
With SMBs and MSPs experiencing more cyberattacks, security is becoming a decisive factor in whether an SMB chooses or continues to work with an MSP. Sixty-one percent of SMBs agree that their organization lacks in-house skills to deal with security issues properly.

In the event of an attack, 82% of SMBs who use an MSP would hold the MSP at least partly accountable for it. Perhaps even more worryingly, 68% of organizations would take legal action against their IT solution provider.[2]

Certainly, a successful cyberattack on an MSP could have far-reaching repercussions on customer retention and acquisition. In fact, 92% of SMBs would consider moving to a new MSP if offered the right cybersecurity solution.[3]

MSPs need a unified strategy that addresses both their own security risks and weaknesses and those of their clients. The success of that strategy will depend on choosing a cybersecurity approach that delivers greater visibility and faster conclusions for better client outcomes.

## The MSP Cybersecurity Risk Pyramid




**Software Providers**
100s of software providers used by MSPs

**Managed Service Providers**
130,000 MSPs globally that sell to SMBs

**SMBs**
213 Million SMBs below 500 employees globally

Source: **Cybersecurity in an Era of Competing Priorities: The State of SMB cybersecurity in 2021**

# CHAPTER 3: OVERCOME SECURITY CHALLENGES FOR YOUR BUSINESS AND YOUR CLIENTS

Many MSPs offer a foundational layer of cybersecurity tools such as antivirus and firewall software; you may be struggling with how best to address today's evolving security demands—for both your clients and your own business. While disparate tools may cover one threat vector well enough, others might get missed. For example, endpoint security software might catch a threat on an endpoint. Still, it can't detect rogue activity on the network, login attempts to the domain from eastern Europe, or domain lookups from the same geolocation for an outbound connection.

In addition to having multiple, siloed cybersecurity tools across multiple clients, which hinders protection and detection across the entire attack surface, MSPs face other common challenges:

- Lack of in-house cybersecurity expertise and staffing
- Lack of scalable cybersecurity offerings
- The budget, time, and resources to build and manage a 24/7 security operations center (SOC)
- Difficulty successfully selling cybersecurity offerings, which limits investment budget for growth and staffing

Perhaps the biggest challenge for MSPs is time to market. SMBs need protection today and they'll choose the MSP that can deliver it now. Even for those with adequate resources and expertise, there's often not enough time for MSPs to build a comprehensive security capability from the ground up.

Instead, MSPs need to look to a partner with turnkey managed cybersecurity services that will help them differentiate their services, retain clients, and grow their revenue—today.

### Who's Responsible?

Of those who use an MSP, 82% would hold their MSP accountable at some level.

68% of SMBs would take legal action against their MSP in case of a successful attack.

Source: **Cybersecurity in an Era of Competing Priorities: The State of SMB Cybersecurity in 2021**

# CHAPTER 4: WHY MDR IS THE RIGHT CHOICE

Many MSPs take advantage of the rapid threat detection that endpoint detection and response (EDR) technology provides, but they don't always have the people, skills, and technology to appropriately remediate the threats.

This is why managed detection and response (MDR) is one of the fastest-growing segments of the security market. MDRs use the power of EDR technology to find and respond to active threats, plus they include 24/7 monitoring services with cybersecurity experts, or a SOC, that investigate, contain, and eliminate threats.

More than half of respondents (51%) in a survey reported that their organization is already using MDR services, while 42% have either plans or interest in the services.[4]

This means MSPs can get comprehensive coverage across endpoints, servers, network devices, DNS, and more. MDR provides complete visibility and enables proactive cybersecurity as well as threat intelligence and analytics that can help to drive automation across a client's environment.

Because MDR unifies cybersecurity tools and centralizes visibility and contextual information into a single repository, it drives faster and better outcomes than multiple, siloed tools. It gives partners the information they need to act and respond to security events impacting their clients and their own infrastructure. These differences and others set MDR apart from traditional managed security services (see comparison chart).

| Use Case | Traditional Managed Security Services | Managed Detection and Response |
|---|---|---|
| **Alerting** | SOC alerts based on singular tool<br>Alert fatigue at high volume | Alerts correlated across tools<br>No alert sent if pattern not detected, dramatically reducing alert fatigue and noise |
| **Threat Intelligence** | No integrated threat intelligence | Threat intelligence feeds included in automated analysis<br>Ability to create SMB-based intelligence |
| **Visibility** | Siloed visibility from individual toolsets<br>Summary and value reports must be cobbled together | Integrated views enable a proactive stance on cybersecurity for clients<br>Integrated solution provides a single lens into risks |
| **Reporting/ Compliance** | Independent reports based on individual tools | Comprehensive client value reporting |
| **Data Sources** | Limited to support provided by individual tools | Pluggable framework enables rapid additions |
| **Remediation/Response** | Limited to what is available in individual tools or through manual efforts | Integrated source enables automated actions |

Source: **https://www.esg-global.com/blog/is-mdr-the-new-mss**

# CHAPTER 5: EVERYONE WINS WITH MDR—EXCEPT FOR CYBERCRIMINALS

| SMB Benefits of MDR | MSP Benefits of MDR |
|---|---|
| **Data Protection:** Protection for critical and sensitive data such as financial, customer, and employee information, as well as applications and intellectual property | **Actionable Visibility:** Proactive, outcome-oriented security that delivers on end-client expectations and MSPs be the hero |
| **Faster Response:** Faster incident response to cyber threats that mitigates damage to the business | **Efficient, Unified Security Stack:** Opportunity to grow the business with new clients while reducing client churn |
| **Lower Risk:** Reduced risk of financial and reputational loss, non-compliance penalties (e.g., for healthcare and financial industries), mitigation costs, and more | **Turnkey and Fully Managed Protection:** Increased revenue and share of wallet as well as new revenue streams |
| **Peace of Mind:** Increased confidence in their provider delivering the level and type of security the business needs | **Enhanced Security:** Improved security and reduced risk within their own business |

## To get the benefits of a unified cybersecurity stack, look for a trusted partner with a robust MDR platform that offers:

- A unified experience across all cybersecurity services and tools
- Fully integrated view of threats and risk across entire environment
- Visibility and automation
- A 24/7 security operations center
- Certification training for sales and engineers to grow and support the business

# CHAPTER 6: DELIVER THE PROTECTION YOUR CLIENTS DEMAND

**ConnectWise Fortify™** includes enterprise-grade EDR tools geared toward MSPs. This includes MDR capabilities that enable MSPs to protect themselves and their clients from the evolving threat landscape.

The always-on, proactive cybersecurity system automatically correlates threats and processes alerts, then our our world-class, MSP-focused SOC orchestrates any required remediation. The combination of tools and expertise keeps pace with the ever-evolving threat landscape and delivers the peace of mind your customers crave.

## MDR with ConnectWise Fortify includes:

- Proactive, outcome-oriented cybersecurity with faster time to resolution, enabling MSPs to be the hero
- Protection that provides everything MSPs need to mitigate risk for their clients and business
- Room for growth of service and onboarding clients with an extensible platform

## ConnectWise Leads the Industry

**52 million**
Events processed per minute

**97%**
Are Managed by CW SOC

**85,000**
SMB Customers

**50+**
Industry Awards

# CONCLUSION

## Be Ready for What's Next

SMBs are looking for help to protect their businesses against the increasing volume and cost of cyberattacks. You can be the hero with a robust MDR tool that helps you address today's evolving threat landscape, proactively respond to cybersecurity incidents, and mitigate risks for your customers and your own business.

### Take the Next Step

Learn more about what MDR can do for your business at **connectwise.com.**

Request a **demo of the MDR capabilities in ConnectWise Fortify** to see how we protect your clients and your business from cyberthreats,