ConnectWise®

Advanced Cybersecurity & Threat Protection

ConnectWise eBook Series

An MSP's Guide to Protecting SMB Clients

Delivering Managed Detection and Response Services

Contents

Security is a Threat …

As a managed IT service provider (MSP), security is rapidly becoming one of the biggest threats to both your customers' and your own 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 business (SMBs).

There are two growing trends that put SMBs at 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

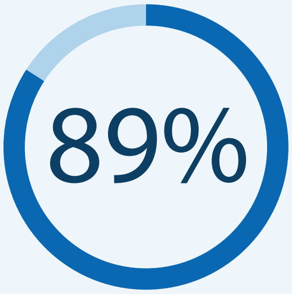
Source: Underserved and Unprepared: The State of SMB Cyber Security in 2019, a Continuum Study conducted by Vanson Bourne, 2019

… and an Opportunity

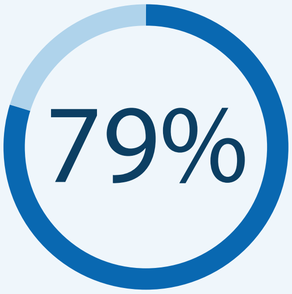
Because SMBs typically don’t have the skills, awareness, or resources to protect themselves against today’s advanced cyberthreats, they need the help of a trusted MSP more than ever. While offering security services is a clear revenue opportunity, it’s also becoming the biggest differentiator for MSPs. SMBs will favor (and migrate to) those MSPs that can truly protect them with a full spectrum of 24x7 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 an attack affects your customers? Read on for insight into what MSPs need to do right now to protect their customers and themselves.

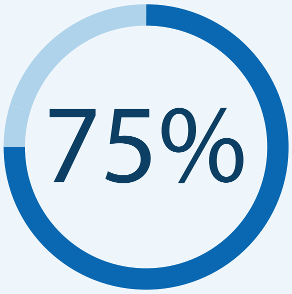
Cybersecurity is a Top Priority for SMBs



of SMBs see cybersecurity as the top priority or in the top five priorities in their organization



of SMBs 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: Underserved and Unprepared: The State of SMB Cyber Security in 2019, a Continuum Study conducted by Vanson Bourne, 2019

<< Back to Table of Contents

Clients Want Greater Protection for Their Business

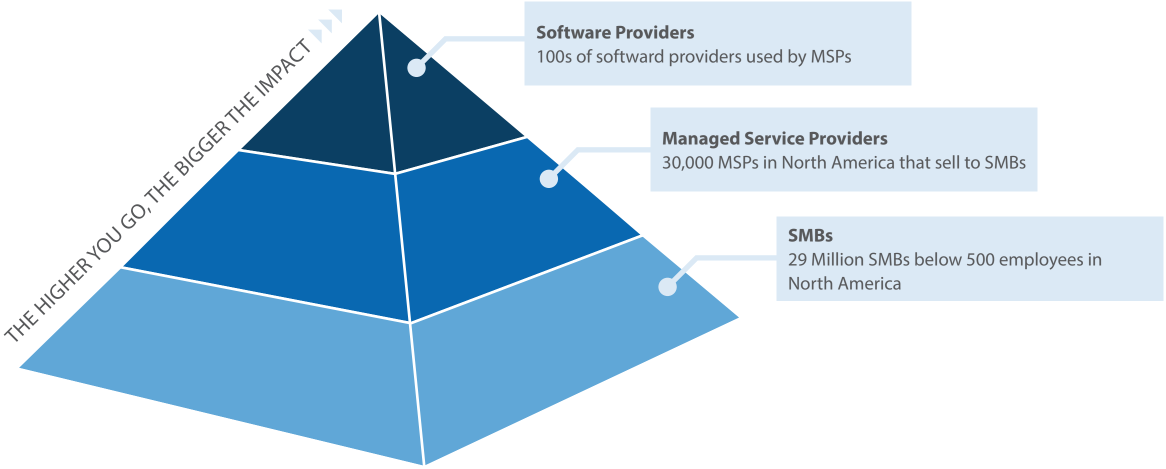
Today, 64 percent of SMBs report having suffered a successful attack, with the average cost to the business of $53,987.[1] They aren't alone: MSPs are increasingly victims of successful cyberattacks, with more than **300 attacks on MSPs** in the first half of 2019.[2] Nearly three-quarters (74 percent) of MSPs have suffered at least one cyberattack.[3]

With both SMBs and MSPs experiencing more cyberattacks, security is becoming a decisive factor in whether an SMB chooses or continues to work with an MSP. Nearly all SMBs (93 percent) would consider switching to a new MSP if that provider offered the "right" cybersecurity solution.

From the MSP perspective, 83 percent report that providing an inadequate solution that resulted in a client breach could lead to the client taking legal action against the MSP.[5] Certainly, a successful cyberattack on an MSP could have far-reaching repercussions on customer retention and acquisition. SMBs that plan to change MSPs are more likely to have seen inadequate cybersecurity protections from their MSP (32 percent) compared to those who plan to stay with their current provider (25 percent).[6]

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

The MSP Cybersecurity Risk Pyramid


THE HIGHER YOU GO, THE BIGGER THE IMPACT
Software Providers
100s of softward providers used by MSPs
Managed Service Providers
30,000 MSPs in North America that sell to SMBs
SMBs
29 Million SMBs below 500 employees in North America

[1] "Underserved and Unprepared: The State of SMB Cyber Security in 2019," Vanson Bourne, 2019
[2] Internal ConnectWise research
[3] "Under Attack: The State of MSP Cybersecurity in 2019," Vanson Bourne, 2019
[4] "Underserved and Unprepared: The State of SMB Cyber Security in 2019," Vanson Bourne, 2019 NO #4 notation
[5] "Under Attack: The State of MSP Cybersecurity in 2019," Vanson Bourne, 2019
[6] Underserved and Unprepared: The State of SMB Cyber Security in 2019

Overcome Security Challenges for Your Business and Your Clients

Many MSPs already 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, but it can't detect rogue activity taking place 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 security tools across multiple clients, which hinders protection and detection across the entire attack surface, MSPs face other common challenges around security:

- Lack of in-house security expertise and staffing
- Lack of scalable security offerings
- The budget, time, and resources to build and manage a 24x7 security operations center (SOC)
- Difficulty successfully selling security 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 that use an MSP, 69% claim they would hold their MSP accountable at some level in the event of an attack, with 35% saying they would hold their MSP solely accountable.

74% of SMBs would take legal action against their MSP in case of a successful attack.

Source: Underserved and Unprepared: The State of SMB Cyber Security in 2019, a Continuum Study conducted by Vanson Bourne, 2019

Why MDR is the Right Choice

To protect their clients and t0eir own businesses from attack, MSPs need effective, rapid threat detection and response. The problem is that many MSPs don't have the people, skills, and technology to achieve it on their own.

This is why managed detection and response (MDR) is one of the fastest-growing segments of the security market. More than half of respondents (51 percent) in a survey reported that their organization is already using MDR services while 42 percent have either plans or interest in the services.[7]

Compared to siloed point solutions, MDR delivers 24/7 threat monitoring, detection and response capabilities with comprehensive coverage across endpoints, servers, network devices, DNS, and more. When MDR is done correctly, it provides complete visibility and enables proactive security as well as threat intelligence and analytics that can help to drive automation across a client's environment.

Because MDR unifies security 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 □ Alert fatigue at high volume	✓ Alerts correlated across tools ✓ 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 ✓ Ability to create SMB-based intelligence
Visibility	□ Siloed visibility from individual tool sets □ Summary and value reports must be cobbled together	✓ Integrated views enable proactive stance on cybersecurity for clients ✓ Integrated solution provides 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

[7] "Is Managed Detection and Response (MDR) the New Managed Security Service?" Christina Richmond, ESG, May 2019

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 cyberthreats 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 security stack, look for a trusted partner with a robust MDR platform that offers:

- A unified experience across all security services and tools
- Fully integrated view of threats and risk across entire environment
- Visibility and automation
- A 24x7 security operations center
- Certification training for sales and engineers to grow and support the business

Deliver the Protection Your Clients Demand

ConnectWise Fortify™, now with managed detection and response capabilities, provides the first unified security stack enabling MSPs to protect themselves and their clients from the evolving threat landscape. With an always-on, proactive security system that automatically correlates threats, processes alerts, and orchestrates required remediation, only ConnectWise offers both the tools and expertise needed to keep pace with the ever-evolving threat landscape and deliver the peace of mind your customers crave.

ConnectWise is the first MSP software provider to offer a true MDR solution for MSPs and their end clients with a solution that includes:

- A unified experience across all security tools, resulting in events/alerts that are automatically correlated
- Proactive, outcome-oriented security with faster time to resolution, enabling MSPs to be the hero
- Protection that starts at home with Fortify for the MSP which includes everything MSPs require to protect themselves and mitigates the risk of becoming a pawn in the weaponization of their tools by attackers
- Extensible platform that easily provides room for growth of services and onboarding new clients

ConnectWise Leads the Industry

1.3 Million
Endpoints Monitored

6,000
MSP Partners

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 platform that helps you address today’s evolving threat landscape, proactively respond to security incidents, and mitigate risks for your customers as well as for your own business.

Take the Next Step

Learn more about what MDR can do for your business at www.ConnectWise.com

Request a demo of the new MDR capabilities of ConnectWise Fortify to see how we protect your clients and your business from cyber threats.

Speak with a sales associate at 800.671.6898