Privafy™
WORK ASSURED

Why More MSPs Are Adding Security to Their Services Portfolio (and How You Can Too)

A PRIVAFY WHITEPAPER

Why More MSPs Are Adding Security to Their Services Portfolio (and How You Can Too)

Is your future as an MSP *really* secure?

Give the people what they want. It's a good business mantra, whether you're the world's largest online retailer with millions of customers or a mid-sized managed services provider (MSP) with hundreds of customers. And the reality is that, right now, most small and medium businesses (SMBs) want security services from their MSP.

It's easy to see why. Cyber threats are on the rise, both in terms of the number of attacks that SMBs are exposed to and the potential damage those attacks can do. Security, meanwhile, has become increasingly complex and costly to manage as SMBs struggle to meet ever-changing requirements for data privacy and compliance. Adding to the problem is a global shortage of skilled security professionals who can command a premium for their services, and thus are often priced out of the range of most SMBs.

What seems like the perfect storm for a cyber attack is also the perfect opportunity for MSPs to expand their portfolio of services into the security space. Most MSPs offer some basic level of security (e.g., managed anti-malware subscriptions), but there is a key distinction between an MSP that offers basic security functions and a managed security services provider (MSSP). An MSSP essentially functions as a Security Operations Center (SOC) for hire, providing higher-level security services such as real-time threat blocking, threat detection and mitigation, threat hunting, auditing and compliance reporting. More than simply offering the right mix of products and technology, MSSPs also need to offer the right combination of people and processes to protect their customers against a growing spectrum of cyber threats.

Of course, the transformation from MSP to MSSP is considerably more complex than adding an extra letter. MSPs face the same challenges as any other business when it comes to security: complex solutions to manage, a shortage of security talent, increasingly sophisticated attacks and so on. But the risks of not addressing security are considerably higher for MSPs, because their future literally depends upon it. SMBs are more likely to choose a managed services partner that offers robust security services, and more likely to leave an MSP that doesn't offer those services in favor of one that does. In other words, MSPs that fail to get into the security business may find themselves out of business.

Why should you worry about security?
Because your customers are worried about it.

While cyber attacks that target large brands and global businesses are more likely to make the news, that doesn't mean that small businesses are less likely to be targeted by cyber criminals. In fact, according to a recent Ponemon Institute report, two out of three SMBs will experience a cyber attack over the next 12 months.[1] Not surprisingly, many SMBs say they are worried about being targeted with a cyber attack, with lost data, lost customers and lost reputation at the top of their worries. This might be less troubling if SMBs felt they were prepared to successfully address a cyber attack within their ranks, but they're not. The majority of SMBs believe they have insufficient IT security resources to defend themselves against a cyber attack.[2]

> **"Two out of three SMBs will experience a cyber attack over the next 12 months."**

For SMBs, the stakes are higher than you might think. According to Cisco's 2018 SMB Cybersecurity Report, just one data breach can cost an SMB as much as $2.5 million.[3] The larger the business, generally, the larger the loss. Recognizing these risks, SMBs are investing more in security each year, yet much work remains to be done. Poor security "hygiene" continues to be an Achilles' heel for many businesses, from employee passwords that never change to software programs that are never patched. And many small businesses are less likely to cross their T's and dot their I's when it comes to data security compliance, and more likely to cross their fingers and hope they don't get audited.

If SMBs lack confidence in their own abilities to protect themselves, they appear surprisingly overconfident in the security services provided by their MSPs. Research suggests that most SMBs believe using an MSP improves their security posture, even when the MSP isn't specifically contracted for security services. This can put MSPs in a perilous position, as seventy-four percent of SMBs said they would take legal action against their MSP in the event of a successful cyber attack.[4] This statistic underscores the importance of having a serious cyber security talk with your customers and aligning the security services you provide with your customers' needs and expectations.

[1] "2019 SMB Cyberthreat Study: Most SMBs Severely Underestimate Their Cybersecurity Vulnerabilities," DARKReading.com, Accessed November 5, 2019, https://www.darkreading.com/2019-smb-cyberthreat-study-most-smbs-severely-underestimate-their-cybersecurity-vulnerabilities/d/d-id/1335359.

[2] "SMBs lack resources to defend against cyberattacks, plus pay more in the aftermath," Malwarebytes.com, October 31, 2019, https://blog.malwarebytes.com/business-2/2019/10/smbs-lack-resources-to-defend-against-cyberattacks-plus-pay-more-in-the-aftermath/.

[3] Small and Mighty: How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats, Cisco, 2018, Accessed November 5, 2019, https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf.

[4] Adrian Gendre, "How MSPs Can Overcome Optimism Bias to Sell Cybersecurity Solutions," ChannelFutures, September 17, 2019, https://www.channelfutures.com/best-practices/how-msps-can-overcome-optimism-bias-to-sell-cybersecurity-solutions.

Can you afford to start a security practice?
(Answer: You can't afford NOT to start one.)

From a business perspective, investing in security services is a clear win for managed service providers: it generates revenue, increases customer loyalty, reduces customer attrition and provides differentiation in a crowded market. But the barriers to entry can be daunting for many MSPs. A security operations center (SOC) is costly to staff, complex to manage and raises a host of new questions, such as:

What kind of firewalls, intrusion detection/prevention systems and other hardware & software do we need?

Who is going to train our security team?

How do we package our security services and at what price points do we sell them?

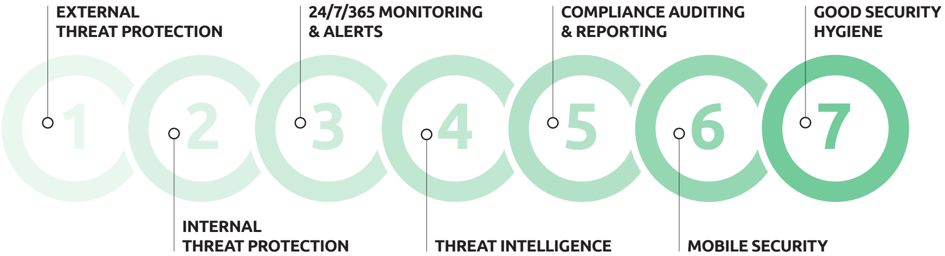
Can we support 24/7/365 security monitoring and response on our own, or do we need to bring in partners to fill the gaps?

The reality is that, while every MSP wants to grow their business, many are concerned that adding security services will be expensive and potentially disruptive to their core business. This is not an unreasonable fear. The vast majority of MSPs are themselves small and medium businesses, and face the same challenges that have prevented their SMB customers from creating their own security teams in the first place: cost, complexity, compliance. Cost is often the most significant barrier for MSPs, both in terms of the capital (i.e., equipment) and operational (i.e., people) investment required to bolster their security services prior to generating their first dollar of revenue.

An attractive alternative to building a security service from the ground up is to partner with existing Security as a Service (SECaaS) providers. By choosing this route, MSPs can bypass costly up-front investments and still deliver a proven security solution to customers as part of their broader services portfolio. A SECaaS solution already contains all the elements of a security solution—hardware, software, tier 1/2/3 security analysts—and allows MSPs to quickly generate recurring monthly revenue from security services.

What capabilities do I need as an MSSP? – The Seven Elements of Security

Security services can give MSPs a competitive advantage—provided that those services are competitive with what the rest of the industry is offering. A competitive security service in the current market is not only comprehensive but also cost efficient. SMBs can expect to pay anywhere from several hundred to several thousand dollars per month for a complete security service, depending on the number of users, network complexity, compliance/reporting requirements and other factors. But what exactly constitutes a complete security solution? You can think of it in terms of these seven key elements of security.


EXTERNAL THREAT PROTECTION
24/7/365 MONITORING & ALERTS
COMPLIANCE AUDITING & REPORTING
GOOD SECURITY HYGIENE
1
2
3
4
5
6
7
INTERNAL THREAT PROTECTION
THREAT INTELLIGENCE
MOBILE SECURITY

External Threat Protection

1 This is what most business owners think of when they think of security: blocking cyber criminals from infiltrating the network through brute-force attacks (e.g., flooding the network with password-guessing attempts) or more subtle means such as email phishing to gain login credentials. Blocking external threats is an important element of security, but one that almost every business will fail at sooner or later because of the sheer impossibility of stopping everything. In a world where each malware variant has an average life expectancy of less than one minute, businesses cannot depend on anti-virus software alone to catch the bad guys. Instead, external threat protection is really about internal data protection: stopping anything from getting out rather than stopping everything from getting in. This can be achieved through real-time threat blocking in combination with analytics, anomaly detection, identity and access management (IAM) tools and, increasingly, artificial intelligence (AI) tools.

Internal Threat Protection

2 A Cisco study found that seventy-five percent of security breaches are due to insider threats.[5] That's an alarming statistic that illustrates the importance of internal threat protection. While nearly half of those breaches are attributable to human error (i.e., accidentally releasing data), businesses must monitor the activities of employees, partners and other "trusted" entities that have access to their networks and their data. Internal threat protection starts with strong security policies: manage data access privileges based on roles/responsibilities, be diligent about how sensitive data is stored in the cloud and on personal devices, require partners to maintain their own security policies (including the latest patches on their software systems), etc. If these actions can be automated (e.g., automatically update data access privileges when an employee's role or status changes), businesses will have a better chance of eliminating insider threats.

[5] Shane Schick, "Insider Threats Account for Nearly 75 Percent of Security Breach Incidents," SecurityIntelligence, August 28, 2017, Accessed November 5, 2019, https://securityintelligence.com/news/insider-threats-account-for-nearly-75-percent-of-security-breach-incidents/.

3

24/7/365 Monitoring and Alerts

Information overload is a real problem for security analysts. Networks can generate millions of security logs per week, and even aggressive filtering tools are likely to inundate security analysts with hundreds of false positives: incidents that appear to be dangerous but, on examination, are harmless. There are several ways that businesses approach this problem: they may limit their view of network traffic (although this can result in missed threats), use automation and AI to better rank and prioritize threats (the current best practice), or handle each threat on a case-by-case basis (which can be very time-consuming and slow down a security team's overall response to urgent threats).

It's not uncommon for smaller businesses to outsource their security expertise to a third party, either in the form of a part-time consultant or a managed service provider. MSPs that perform this role still face the same challenges of information overload, but with an added benefit: real-time monitoring services provide MSPs with a unique opportunity to demonstrate their value to customers on a frequent and consistent basis. A daily or weekly summary of stopped threats and security measures taken, for example, keeps customers in the security loop and shows them exactly what they're getting for their monthly service fee.

4

Threat Intelligence

Network security monitoring can tell you what's happening in your network, but such a provincial view of security can leave your business unprepared for the next threat. For this reason, many businesses use threat intelligence feeds to find out what kind of cyber threats are affecting their region and industry. This intelligence helps security analysts and threat hunters prepare and prioritize their security activities. Curated by security experts, threat intelligence feeds provide a current snapshot of what's happening in your industry, whether it's a new malware variant being targeted to healthcare companies or a new information on malicious domains that can be added to a business' blacklist policy.

"In some cases, businesses have less than 72 hours to report on data breaches once they have been detected."

5

Compliance Auditing and Reporting

Compliance has become a lightning rod for security in recent years, as requirements become more stringent and potential fines continue to rise in the wake of well-publicized security breaches. In the last year alone, regional compliance requirements for companies that do business in California (CCPA) and the European Union (GDPR) have been added to the list of HIPAA, PCI DSS and other industry-based compliance initiatives. In some cases, businesses have less than 72 hours to report on data breaches once they have been detected, which can result in parallel fire drills as companies scramble to mitigate the threat and demonstrate procedural compliance. As a result, SMBs in particular are looking for their security providers to offer assistance with this process through automated auditing and reporting tools that are built around specific compliance requirements.

6

Mobile Security

As the traditional nine-to-five desk job has morphed into a more flexible, mobile model, mobility security plays an increasingly important role in the life of a business. There are a variety of mobility security factors in play: mobile endpoint security (e.g., smartphones, tablets), wi-fi network security (including private communications on public wi-fi networks), virtual private network (VPN) tunneling, mobile/cloud app security and more. SMBs in particular can find it challenging to deliver consistent levels of security across a mixed variety of devices, mobile apps and locations, presenting MSPs with an opportunity to fulfill that role as a security services partner.

As you might imagine, mobility security is not a one-size-fits-all solution. For example, SMBs may have very different security requirements if they use remote agents for their call center, particularly when those agents handle sensitive personal or financial data. Despite the fact that VPN technologies have been around for years, all VPN solutions are likewise not created equal, with some methods offering much higher levels of security than others. SECaaS is naturally suited to mobility security, but MSPs still need to make sure that the solution is suited to the individual customer.

7

Good Security Hygiene

Perhaps the greatest security threat to SMBs isn't cyber crime but the criminal neglect of good security practices, from choosing secure passwords—the most common passwords are still, you guessed it, "guest" and "1234"—to keeping current with the latest software patches and fixes. These practices, collectively known as good security hygiene, prove that an ounce of prevention is indeed worth a pound of protection. Most data breaches occur not so much because a cyber criminal succeeded at unlocking a secret password, but because an employee in the organization failed to lock their own front door by sharing unencrypted communications over a non-secure network or mistakenly downloading malware from a phishing email.

How can security services protect businesses from themselves? By automating good security practices. For example, a security service might manage network access with a mandatory password change every three to six months, automatically encrypt all employee communications or automate security patches across all the applications that a business uses. In every case, MSPs should look to combine good hygiene with simplicity, since the more complex a security procedure is, the more likely that employees will look to circumvent it or use non-secure methods to support it (e.g., by posting passwords on sticky notes around their monitor).

Privafy: Security, Simplified

As an MSP, you can build a best-of-breed security solution and staff a security operations center to monitor it, but it will take a considerable investment in time and money—costs that will be passed on to your customers in the form of monthly service fees. The question then becomes, can you deliver a security solution that you can confidently get behind at a competitive rate? If the answer is "no," then you need to partner with someone who can.

Security-as-a-service (SECaaS) providers represent an attractive alternative to do-it-yourself SOCs. SECaaS providers can deliver a complete, proven security solution as a cloud-based service that addresses the security gaps between an MSP and MSSP: 24/7 monitoring, external and internal threat protection, AI-driven analytics, automated threat response and more. In selecting a SECaaS partner, MSPs should be prepared to ask some hard questions, such as:

How much will I need to invest initially to get started?

Is this a white-label service that I can brand as part of my own services portfolio?

What kind of monthly revenue margins can I expect?

How long will it take to install the solution at a customer site?

Do you offer different service tiers for different customer types (e.g., micro-businesses, medium enterprises, multi-site businesses)**?**

There is one simple choice that MSPs can make: partner with Privafy. Privafy's unique security-as-a-service protects your customers and your customer revenue with a highly scalable security platform developed by experienced engineers and managed by an experienced team of security analysts. Privafy offers unprecedented simplicity: within minutes, customers can install our data collection device (NetEdge) into their network and begin receiving real-time protection and alerts through our easy-to-use, web-based dashboard.

Privafy delivers a complete security solution as part of your services portfolio, including dashboards that feature your logo. Whichever service levels customers choose, they receive complete security protection including:

- Total network traffic analysis driven by AI technology and advanced machine learning to block, stop and mitigate external and internal threats;
- Fully automated security tasks, from software patches to password update reminders;
- Unique key encryption/exchange technology that delivers a highly secure VPN experience;
- Real-time security dashboards that can be viewed from a desktop, laptop, tablet or other mobile device;
- 24/7/365 SOC services including tier one (threat blocking) through tier three (threat hunting) level support.

To learn more about Privafy services and how you can become a Privafy partner today, visit us at **privafy.com**.

Privafy™

WORK ASSURED

About Privafy

For business leaders in charge of sensitive information, Privafy's security-as-a-service application has reimagined how to protect data-in-motion. The company's cloud-native technology integrates all the functionality of traditional point solutions to provide comprehensive protection as data traverses between locations, clouds, mobile devices, and IoT. Deployed in minutes, Privafy works seamlessly with existing infrastructure to protect organizations of all sizes against today's most damaging data-centric attacks, all while disrupting the cost associated with complex, archaic network solutions.
Learn more at **www.privafy.com**