

Are Red-Hot Security Services the Answer to Keeping your MSP Business in the Black?



Need to Grow your MSP Business?

Start with Security.

If you were to ask your customers what their biggest challenge is, they would probably tell you it's security. Fortunately, most MSPs provide some level of security to their customers, whether it's antivirus software or firewall management services. The problem is that MSPs fail to provide enough security. Relatively few MSPs currently offer critical security services such as intrusion detection/prevention systems and threat intelligence, and even fewer offer advanced security services such as log collection for security incident and event management (SIEM) systems.

That may soon change, however. The emergence of Managed Security Services Providers (MSSPs) underscores the fact that the managed service industry sees a real opportunity in making security a priority. According to IDC, managed security services are the fastest-growing portion of the IT security market, while Gartner predicts that managed and subscription-based security services will account for half of all cybersecurity revenue by 2020.¹ So how can your business tap into this rich source of security revenue? Read on to find out.

“Managed and subscription-based security services will account for half of all cybersecurity revenue by 2020.”

Got Antivirus Services? So Does Everyone Else.

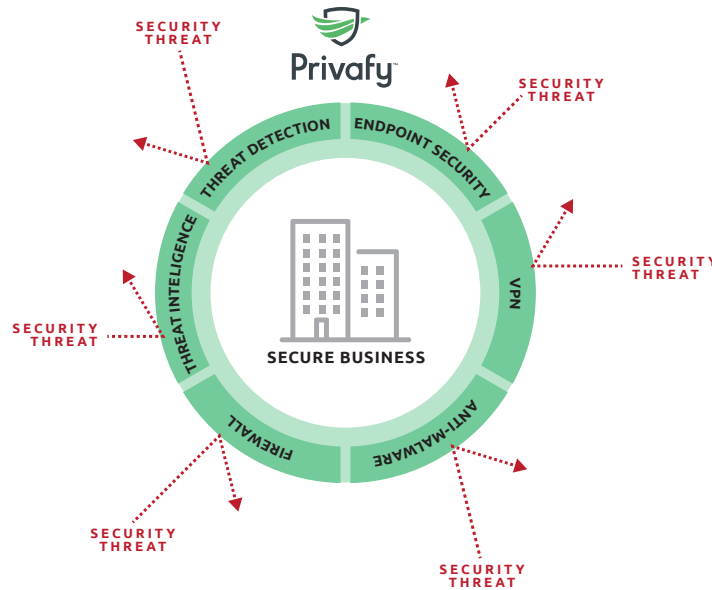
For MSPs, customer relationships are built on trust. That trust can be eroded by a single security incident, whether it's a downed server or stolen data. It's important, therefore, to ensure that you and your customers are speaking the same language when it comes to security. You might think of automatically updating antivirus definitions as a security service, and it is, but antivirus services alone won't differentiate your business—most MSPs already offer this. And antivirus detection won't stop cyber attacks that come through email phishing attacks, software vulnerabilities or many of the other methods that criminals use to compromise your customer's network.

What constitutes a complete security solution for small and medium businesses? Surprisingly, the security needs of SMBs vary little from larger enterprises. That's because cyber criminals use the same methods to attack both, and often target SMBs first with new attacks to test their effectiveness. A complete checklist of SMB security requirements would include:

- Advanced persistent threat detection and remediation, preferably enhanced with artificial intelligence and machine learning to detect new threats quickly
- Remote endpoint security, including virtual private network (VPN) technology
- Antivirus and anti-malware software with automatic updates
- Automated business software updates, fixes and patches
- Managed firewalls at every business location

¹Mike Vizan, "Spending on Managed Security Services expected to jump in 2019," SmarterMSP.com, November 15, 2018, <https://smartermsp.com/spending-managed-security-services-expected-jump-2019/>.

- Relevant, timely threat intelligence
- Compliance auditing and reporting
- Customizable security alerts and alarms with real-time 24/7 monitoring
- Security log collection and analysis.



Those features are a far cry from paying a few extra dollars per month for an antivirus license. Yet even the SMBs that are paying more for enhanced security services may not be getting the protection they need. Cisco’s 2018 SMB Cybersecurity Report revealed that SMBs only investigate 54 percent of all security alerts they receive. When the investigated alert is linked to a legitimate security threat, which happens about one-third of the time, only half of those threats (51 percent) are ever remediated.² In other words, SMBs ignore half of all security alerts, and of those they investigate and determine to be real threats, they still don’t do anything about it nearly half of the time.

Can’t Ante Up for Something Bigger Than Anti-Virus? Now You Can.

Many MSPs find themselves between a rock and a hard place when it comes to building a security practice. They need security experts to manage and respond to alerts, but finding those experts can be a challenge in itself. With security expertise in high demand and short supply, industry analysts warn that 3.5 million cybersecurity positions will be left unfilled by 2021.³ MSPs also need compliance experts to support customers in the face of new and changing regulations. And they need hardware and software experts to integrate firewalls with SIEM systems and intrusion detection/prevention systems solutions to close their security gaps.

²Small 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>.

³Steve Morgan, “Cybersecurity Talent Crunch to Create 3.5 Million Unfilled Jobs Globally by 2021,” Cybercrime Magazine, October 24, 2019, <https://cybersecurityventures.com/jobs/>.

As you would expect, building out a security practice isn't cheap. The largest MSPs can afford to invest in a security solution and wait for the revenue to arrive, but most MSPs don't have the time or the money to invest in new technology or security team salaries, effectively shutting them out of the security services market. That is, until now. Privafy has created a cloud-based security-as-a-service (SECaaS) platform that MSPs can resell to their customers as part of their own service portfolio.

The Privafy security solution delivers complete, end-to-end security as a service, including real-time threat detection and remediation, remote endpoint security and global threat intelligence. With Privafy, your business can compete for security services revenue with a competitive solution that delivers:

- Real-time threat detection and prevention that blocks zero-day viruses, denial-of-service attacks, email phishing attempts and other malware
- An easy-to-use security dashboard that shows threats blocked, security alerts and more;
- Automated firewall provisioning and management tools
- Remote endpoint security including advanced, proprietary VPN protection
- Advanced artificial intelligence and machine learning techniques to detect and block threats that other solutions miss
- Global threat intelligence culled from Privafy's growing network of customers.

Expand Your Total Addressable Market in Minutes

How long would it take your business to piece together a complete security solution, compile a playbook of security best practices and hire a team of security experts to monitor it 24/7? Weeks? Months? How about minutes. With Privafy, your customers can connect into our cloud-based security platform in minutes. No complex integration is required; if you can plug a pair of network cables into a LAN port, you can begin using the Privafy solution to protect your customers in moments.

The market opportunity for managed security services is already here. Many SMBs currently report feeling "helpless" to defend themselves against new cyber attacks. Two out of three SMBs say they would be unprofitable in less than three months after losing critical business data through a breach or ransomware⁴ and SMBs plainly acknowledge that they're understaffed when it comes to security. The question isn't whether your customers are ready for managed security services, but whether you are. With Privafy, the answer is a resounding Yes.

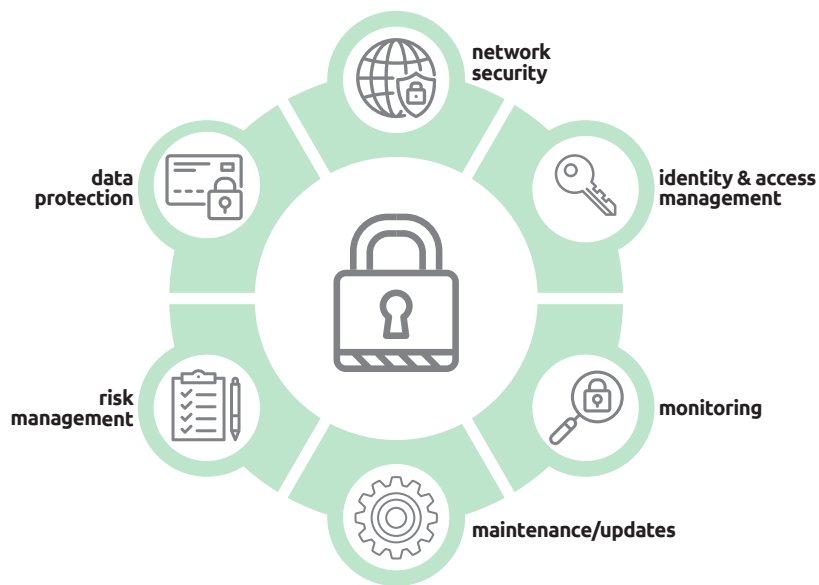
⁴2017 State of Security Among Small Businesses in North America, Better Business Bureau, Accessed November 5, 2019, https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf.

While it's clear that small and medium businesses need managed security services, what's in it for you, the managed service provider? Let's start with attracting new customers. Managed security services could be the carrot needed to attract customers to a managed service plan. And then there's customer loyalty to consider. With other MSPs competing for your customers, managed security services strengthen the bond between you and your customers. So, if you're looking to hold on to your customers and add a few new clients, adding comprehensive security services to your portfolio could be the best move you make this year.

Boost Your Monthly Recurring Revenue Without Adding More Staff

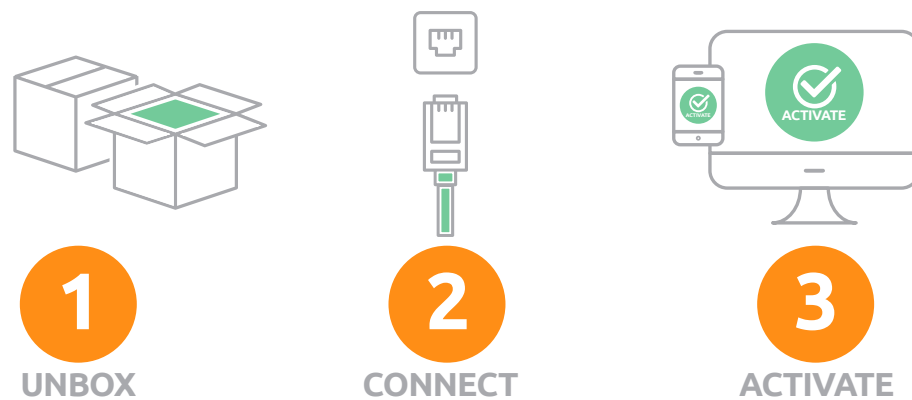
Privafy's security-as-a-service is designed to complement the services you already provide today, such as networking, email/communications, backup & disaster recovery, help desk support and cloud & business application management. Delivered as a custom-branded service, the Privafy solution fits in seamlessly with your existing service portfolio. Equally important, Privafy fits in with the security investments your customers may have already made, such as antivirus software licenses and network firewalls, to fill in the gaps in their security solution.

Why is seamless integration important? Because customers, particularly SMB customers, are likely to resist a "rip-and-place" strategy for security. They have a comfort level with the tools they use today, and are looking to beef up their security posture rather than put their existing security products out to pasture. With Privafy, your customers can build on the security investments they've made to block more attacks, provide stronger security and ensure compliance against even the most stringent regulations such as HIPAA and GDPR.



Because security is an ongoing requirement, Privafy's service provides ongoing monthly revenue for your business—without any upfront investment in capex or opex. Yet unlike other managed services, Privafy's security service delivers tangible value to your customers through daily alerts and weekly/monthly reports that detail the number of threats that you've detected, blocked and remediated. Anecdotally, MSPs have reported that security services have led to "lightbulb moments" in their relationships with customers because they can literally see what they're paying for each month.

Growth can be a double-edged sword for MSPs: on one hand, growth is good because it means more revenue, but it also means that MSPs have to invest in the infrastructure and people to support that growth, which can lead to exposed risk down the road. Privafy removes the risk from growth by providing a solution that scales in the cloud. As you sell more security licenses, Privafy simply provisions more capacity for your customers in the cloud. As new offices/locations are added to the service, Privafy can ship its NetEdge appliance directly to your office or to the customer site for connection to the Privafy servers. Within minutes of being connected, the NetEdge box should be completely autoconfigured and ready for operation, allowing you to start billing for security services the same day the box arrives.



The Bottom Line: How Much Growth Can I Really Expect?

There are a lot of factors that go into your pricing plan, but let's say for the sake of illustration that your MSP is charging customers \$2,500 per month for server and software maintenance, storage, backup and other common IT services. Now, how much more would they pay for an end-to-end security solution that gave them complete peace of mind against data theft, ransomware, DoS attacks and other malware? 15 percent more? 25 percent more? Even if they paid a premium of only 10 percent for comprehensive security services, that would still add revenue of \$100,000 per year for every \$1 million of billable revenue.

Security services from Privafy can be your secret weapon to retaining customers and attracting new customers in the coming years. It's also a great way to get the contract renewal conversation started, because your customers understand that every day they wait to address security is another day that cyber criminals have to exploit their security weaknesses. We've removed the barriers to managed security: investing in people and products to deliver a competitive service. But the next step is up to you.

To learn more about Privafy's security service for MSPs, including detailed information on pricing tiers and plans, or for a free on-site demonstration, visit us at privafy.com.



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