Managed Security Services: A Seller's Guide

By George Hulme

APRIL 2017 | US$25 | S100417

Channel Partners™

Managed Security Services: A Seller's Guide

By George Hulme

APRIL 2017 | US$25 | S100417

Channel Partners™

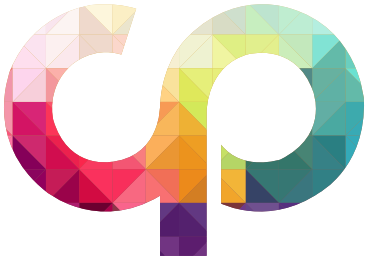
Table of Contents

Channel Partners™

About the Author

GEORGE V. HULME is an internationally recognized security and business technology writer. For more than 20 years, he has written about business, technology and IT security topics. From March 2000 through March 2005, as senior editor at InformationWeek magazine, Hulme covered the IT security and homeland security beats. His work has appeared in CSO Online, Computerworld, Network Computing, Government Computer News, Network World, San Francisco Examiner, TechWeb, VARBusiness and dozens of other technology publications.

linkedin.com/in/georgehulme
@georgevhulme



Managed Security Services: A Seller's Guide

A recent report from Symantec says 43 percent of digital attacks on organizations last year targeted businesses with fewer than 250 employees. Your customers are struggling to keep their systems safe — and finding that a comprehensive cybersecurity program is expensive, complex and often beyond their ability to architect.

Many times, they don't even know what they don't know.

No wonder many small and medium-sized enterprises (SMEs) are enlisting channel partners as tactical and strategic cybersecurity reinforcements. Allied Market Research sees the managed security service provider (MSSP) market reaching nearly $41 billion by 2020. It will get there at a rapid clip via 16.6 percent compound annual growth. The research firm also found that while all market segments, based on organizational size, will grow, sales to small and medium-sized customers will increase the most.

Top services to resell include managed firewalls, intrusion protection/detection, unified threat management, security information and event management, and endpoint security such as anti-malware and file monitoring. These and other offerings are delivered as a mix of cloud-based and on-premises managed services, with sales of fully cloud-based managed security services increasing at a steady clip. That ability to enable protection remotely is dependent on fast and dependable connectivity to customer sites, meaning sales of a service like remote monitoring could come with a side of new fiber links.

SME Security by the Numbers

51% Small businesses that do not allocate any budget towards risk mitigation for cyberattacks. (Source: Experian/CSID)

Average cost to an SMB of a data breach or cyberattack. (Source: Keeper/Ponemon) **$879,582**

60% SMB employees who reuse the same password for all accounts — even as hacked passwords account for 63% of breaches. (Source: Keeper/Ponemon)

62% Organizations that use managed security and privacy services. (Source: PwC)

Ransom demand for over 20% of ransomware attacks; nearly 60% demanded over $1,000, and 1% asked for over $150,000. (Source: Osterman) **$10,000+**

Besides helping keeping malware off the customer's premises, cloud-based security services can be extended to protect home- and branch-office and mobile employees. Before switching a customer from on-premises to cloud-delivered security, however, know what bandwidth the business will need, and make sure you have a backup connectivity plan. There are various bandwidth calculators that can help with estimates; it's better to overprovision. A single security camera backing up to cloud-based storage consumes 60 GB per month on its own, according to Comcast. One end user streaming music devours that much downstream data *per hour*.

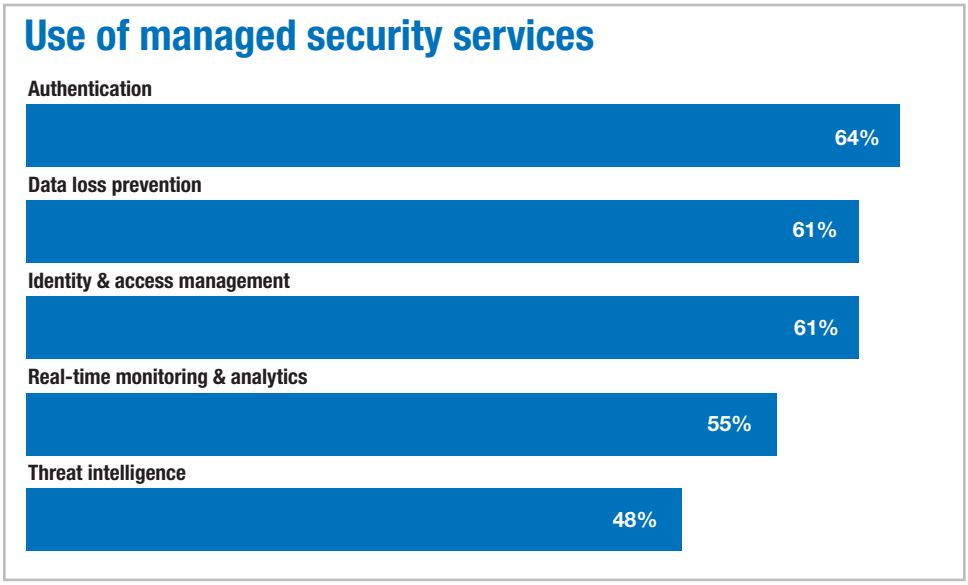
Even if customers keep some security systems on their local networks, they must enhance their monitoring of these tools, usually by engaging a remote security operations center.

"Companies of all sizes need to be armed with better tools and increased cyberintelligence to ward off and alert to attacks," says John Christly, CISO at Netsurion, a channel-focused provider of managed merchant security services. "Gone are the days when a typical firewall could be set up once and run without constant monitoring, tweaking and ensuring the data coming from it is correlated with other systems. Some breaches may look like normal web traffic coming out of the firewall, while other attacks can even seem like legitimate DNS traffic, which may pass right by the typical unmanaged firewall."

Small Business, Not-So-Small Security Demands

While the SME space provides substantial channel opportunities, MSSPs recognize that their reseller partners face challenges. This market segment not only lacks the internal expertise — and often budget and other available resources — to adequately defend their systems, they often don't have the knowledge to understand what they need to be successful. Customers not only need enterprise-class security services at a price they can afford, they also need considerable education.

How can you successfully sell security to SMEs?



Source: PwC, CIO and CSO, The Global State of Information Security® Survey 2017, October 5, 2016

John Humphreys, senior vice president of alliances at managed detection and response services provider Proficio, has some ideas.

First, pick a provider that treats SME customers with the same attention to detail as their enterprise clients.

"Creating a customized runbook, no matter how small the company may be, is just one service," Humphreys says. "MSSPs should have a well-documented onboarding process to collect network information and escalation policies. Onboarding should be an efficient process, but some MSSPs may want to cut off communications before the customer is ready."

You should also ensure suppliers have incident response teams ready to go.

"In 2017, we'll see more SMBs needing automated incident-response solutions to react quickly to threats, especially if in-house staff are not available after business hours," he says. "MSSPs and resellers alike need to step up to the plate by not only identifying threats, but also orchestrating a response in real-time."

Endpoint security platform provider EnSilo's co-founder and CEO, Roy Katmor, agrees that both a cybersecurity plan and the ability to respond to incidents is crucial, but these must take business realities into account.

"The strategy should be practical, taking into consideration the business operations and requirements," says Katmor. "For example, the MSSP should be aware that unplugging a worker's laptop once a threat is found on the device could mean lost productivity and an impact on financials. While most MSSPs won't provide strategy implementation and its continuous review, there are numerous consultants who can."

When selecting an MSSP to be the cybersecurity reinforcements your SME customers need, look for:

- **A broad understanding of the threat environment.** Large MSSPs are protecting enterprises in many industries and geographic locations, even internationally. Besides enabling them to keep their services current with the threat landscape, it should translate into situational awareness. Look for newsletters, alerts, blogs and other information streams that can help inform your clients regarding the nature of current threats and attacks. For example, security blogs from the major providers are gold mines of information for newsletters. Kaspersky's ThreatPost reported on an under-the-radar Chrome fix from Microsoft recently, while McAfee alerted partners to attackers taking advantage of the Ask Partner Network toolbar.

- **Cost-effective, predictable offerings.** Building a security operations center is expensive for the largest of enterprises — it's certainly out of the realm of possibility for SMEs. However, MSSPs should be able to use their economies of scale and cost-effectively provide security services 24x7 to SMEs for a predictable ongoing operational expense. Suddenly, employee turnover, security systems management, end-user education and such are no longer solely the customer's problems. And the MSSP can meet these challenges Not that security is inexpensive — if a service sounds too good to be true, dig deeper.

- **Breach response and investigation capabilities.** What happens when an SME customer discovers a breach? Usually, panic. (It may be some comfort to point out that at least they now have that ability.) The MSSP should be able to provide incident response capabilities that are tightly coupled with security monitoring services so adverse events are quickly remedied. These services may include everything from restoring systems to previously known-good states to forensically analyzing the attack and, if necessary, working with law enforcement.

- **A plan to move beyond "checkbox security."** Helping to meet regulatory mandates such as HIPAA, PCI-DSS, Sarbanes-Oxley, data breach disclosure laws, various financial services regulations and other compliance cases requires deep insights: into an organization's systems, relevant laws and best-practices to make sure the organization remains compliant. But security is about more than checking boxes and satisfying auditors. It's about reducing risk. MSSPs have the knowledge and ability to show SME customers how to cost-effectively build on investments in compliance.

Good Communication Is Smart Cybersecurity Business

One of the biggest challenges MSSPs face is customer churn, often stemming from dissatisfaction over not getting the services they expected or as they understood them to be.

Of course, churn is also a big problem for the reseller who suggested the provider.

Long-term satisfaction often comes down to the MSSP's ability to properly set expectations, says Nick Selby, CEO of Secure Ideas Response Team.

"The customer often hears what the marketer says, and what the marketer says is often much different than the service that is actually provided," says Shelby. "When a marketer says that a customer is receiving world-class, specialized security analysis, and tells the customer that their network will be monitored 24/7, 365, by specialized security analysts, the customer imagines some kid in a hoodie trained at Fort Meade carefully watching packets going by."

While that is a comforting thought, it's also highly unlikely.

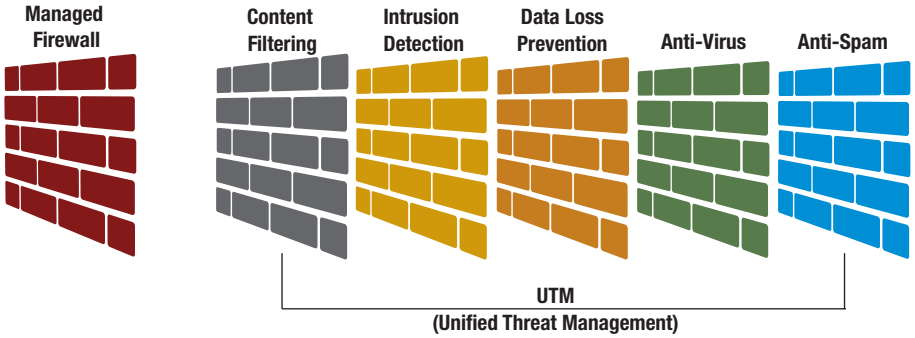
"In fact, a bunch of automated processes are running, which will trigger automated alerts," he says. "These alerts are reviewed as they come up. It isn't the network traffic that's being monitored, it is those automated alerts that are being monitored. And a lot of those alerts are being monitored in an automated fashion as well."

That's a simple example of an honest communication disconnect. Messaging issues also arise when it comes to what segments of the network and customer systems are being monitored, what is being protected, or what types of incidents will trigger a notification to the customer.

"Too often, customers are left with different understandings of what they actually bought," Shelby says.

Good First Step: UTM

A managed unified threat management (UTM) appliance is a useful starting point for customers with only rudimentary security as it bundles essentials like anti-spam (to block ransomware attempts) and intrusion detection behind a managed firewall.



Source: Comcast

Technology advisers need to not only advise customers on the services they need, but also ensure on an ongoing basis that they're getting what they pay for.

"One could make the argument that, if you're not buying many of these services, you may not know how to do that," he says. "It is incumbent upon MSSPs to go the extra mile for their customers. Especially at the lower price ranges where it can be presumed that the customers may be less capable of doing these things for themselves."

Therefore, transparency into the services being provided from the MSSP via the partner to the SME is essential. The customer needs to know precisely what services are being provided and where both the MSSP's and their own responsibilities begin and end. This will in turn build trust, especially when something happens and the supplier must respond to an attack or breach. It's that trust, along with successful execution of services, that builds long-term loyalty.

"I think that it's the responsibility of somebody selling security services to look out for number one, and in this case, number one is the customer," Shelby says.

Related Reports

Fiber Gives SMBs a Fast Business Boost

Many SMBs are unaware of the benefits fiber-optic internet offers, from blazing fast connection speeds to priority customer service. Or, they may think costs are too high. In this Report, three use cases examine just how fiber can improve an SMB's productivity and efficiency — without damaging the all-important bottom line.

Banking IT Innovation: Building on Bandwidth

Banking accounts for the largest portion of all financial services IT spending — and the sector's appetite for adopting new technologies shows no signs of slowing. As banks strive to improve customer experiences with digital initiatives while also driving down costs, bandwidth is critical. This Report presents case studies on four banking institutions using fiber to unlock opportunities to stay competitive.