Tech Data

Why Managed Security Presents a Golden Opportunity for MSPs

INTRODUCTION

Businesses ignore the need for cyber protections at their own peril. The threat landscape is vast, diverse and increasingly dangerous, with hackers constantly introducing new malware variants and identifying network vulnerabilities to exploit. A single cyberattack can deliver a serious setback to any company's plans and operations, forcing it to spend money and effort on remediation — resources that otherwise would be allocated to fulfilling strategic goals. Moreover, 60% of small-to-medium-sized companies that suffer a cyberattack are out of business within six months, according to the U.S. National Cyber Security Alliance.

While these trends explain why CEOs consider cyber threats a top risk of doing business, recognizing the problem doesn't always translate to knowing how to solve it. It has become enormously difficult for companies to address cyber threats on their own, and getting help isn't easy: there's a massive shortage of cybersecurity professionals worldwide, which makes securing talent expensive. Making matters worse, security solutions are getting more complex as vendors add features and functions to combat new threats and attack methods.

But the challenge businesses face in securing their workloads, network and data is also an opportunity for managed service providers (MSPs). MSPs with the will and means to become managed security service providers (MSSPs) not only address an acute need in the marketplace, but are positioned to create revenue streams and expand their customer base.

To seize the opportunity, MSPs must move beyond the foundational blocks of managed security to the advanced and comprehensive security offerings the modern business needs. Of course, MSPs will need help from a trusted partner to acquire the requisite skills to sell comprehensive managed security solutions. Fortunately for them, that help is available.

60% of small to-medium-sized companies that suffer a cyberattack are out of business within six months, according to the U.S. National Cyber Security Alliance.

THE STATE OF SECURITY

What makes cybersecurity so vexing is the nature of the threat landscape. It's a huge beast with tentacles everywhere, constantly reinventing itself by introducing new threats, modifying existing ones and, all the while, intensifying the potential for damage. Networks are constantly under threat, being forced to fend off a barrage of attack attempts; on average, a cyberattack occurs every *39 seconds*.
Many attacks are automated, using bots to constantly test a network's defenses. While large enterprises face big challenges in fending off the ceaseless barrage of threats, it's even more overwhelming for MSPs' clients, a demographic consisting primarily of SMBs that lack the advanced monitoring, detection, investigative and forensic tools to deal with these threats in-house. Nor do they have the needed fastresponse mitigation technology and procedures.

All of which means that this is the perfect time for **MSPs to become MSSPs.**

MSPs can fill the void by providing managed security services that relieve customers of the burden of maintaining and managing the security environment. It's no wonder that managed security now accounts for a substantial portion of the cybersecurity market; in fact, research firm IDC has identified managed security as 2019's fastestgrowing technology category, on pace to reach $21 million by year's end and growing at a 14% annual clip. That growth rate compares to 11% for security analytics, intelligence response and orchestration software, and 9.3% for network security software. (Even though IDC treats managed security services as a separate category, these other high-growth areas can be included in MSSP offerings.)

BEYOND THE BASICS

While just about every MSP delivers foundational security services such as endpoint protection, firewall and patch management, the way to stand out from the competition is by providing advanced and comprehensive services. **Here are some examples:**

ADVANCED

Data and discovery classification
Governance, risk and compliance
Identity and access management
Log management
SIEM
Mobility security and management
Endpoint encryption

COMPREHENSIVE

Threat intelligence
Sandboxing and APT (advanced persistent threats) protection
Incident response training
Predictive analytics
DNS management and mitigation
Privileged user management
Encryption key management

MANAGED SECURITY MARKET DRIVERS

Skyrocketing demand for qualified cybersecurity talent is a major driver of the managed security services market. (ISC)² Research estimates the shortfall of cybersecurity professionals totals nearly 3 million worldwide. A study by security association ISACA reveals that 32% of organizations spend up to six months filling cybersecurity positions, and 60% spend at least three months — numbers up from 26% and 55%, respectively, in 2018.

It stands to reason that if businesses can't hire cybersecurity workers, they will seek help from third parties such as MSPs. However, other market drivers are also at play. Even if the skills gap didn't exist, cybersecurity teams would be challenged by the constant evolution of the threat landscape: consider that hundreds of thousands of malware variants are introduced each day. Many of those variants consist of ransomware, which in recent years has been one of the biggest security threats to businesses of all types and sizes. In 2019, ransomware attacks will cost organizations an estimated $11.5 billion, according to Cybersecurity Ventures.

The growing complexity of security implementation is another driver of managed security services demand. Effective, comprehensive cybersecurity requires a layered approach that addresses all points where an attack can occur, from the perimeter to the endpoint to the applications to the data itself.

> If there's an opportunity for malware to sneak anywhere into the network, **attackers will find it —** and cybersecurity teams need to anticipate, **and fight it off.**

Many attacks occur as a result of a bad decision by a user. Phishing attacks have become increasingly sophisticated, disguising emails as if they were coming from a sender known to the recipient to get them to click on an infected URL or attachment. Preventing users from making bad decisions requires education — another area where MSSPs can play an essential role by developing awareness and education programs they can implement, and even manage, for clients.

Any business that handles private data is subject to regulations on how to process, store and transmit the data.

MSSPs additionally have a part to play in helping clients achieve regulatory compliance. Any business that handles private data is subject to regulations on how to process, store and transmit the data. Industries such as healthcare, finance and retail have particularly stringent regulations and standards that if violated can result in punitive actions such as monetary fines and lawsuits. Smaller businesses often don't have the knowledge or skills to implement compliance programs, but that doesn't exempt them from these requirements.

BENEFITS OF ADDING MANAGED SECURITY

This urgency to deliver effective security across the business landscape — especially among small and midsize businesses — translates to substantial benefits for providers that increase their managed security offerings.

For starters, addressing this dire need for clients opens new revenue streams, creating major profit potential. Most MSPs cover only the basics of security, such as endpoint protection and patch management, so those that invest in advanced, comprehensive security solutions have an opportunity to stand out against the competition and attract new business at healthy margins.

Beyond that, there are intangibles that come into play. Although no security strategy is 100% foolproof, MSPs can help manage risk and prevent a threat that could seriously cripple a business, or even spell its demise. Putting a dollar value on that prowess isn't easy, but it is a tremendous value-add.

Some clients, especially smaller business, may not grasp the seriousness of cyber risks, which means MSPs must put some effort into making a strong business case for developing a robust cybersecurity strategy. To help make the case, MSPs should inform clients of the continuous stream of attacks aimed at organizations of all sizes day after day: in 2018 alone, cyberattacks cost organizations

Once MSPs start delivering managed services, they can report regularly to clients on the number of attacks their services prevent. When clients see attack statistics, they gain a better grasp of the value MSPs provide. This strengthens the IT trusted advisor role, which in turn translates to customer stickiness for the long term.

HOW TO ADD A SECOND "S" TO "MSP"

An MSSP is not made overnight. A provider needs to offer services such as penetration testing, advanced malware detection, threat intelligence and sandboxing, along with acquiring the requisite skills and capabilities to deliver the services.

An MSSP is not made overnight. A provider needs to offer services such as penetration testing, advanced malware detection, threat intelligence and sandboxing, along with acquiring the requisite skills and capabilities to deliver the services.

Help is available for those MSPs willing to invest in security. Tech Data Security Solutions offers a full complement of solutions, services, consulting and education to help MSPs develop an MSSP practice. Tech Data's security experts bring a wealth of solutions experience, skills and knowledge to work with MSPs to identify vendoragno Tech Data's security experts also help MSPs with strategy development, marketing and sales execution, so they can prepare a security growth plan through solution sales.

MSPs can learn more about the cybersecurity market and the threat landscape through a comprehensive training curriculum that culminates in a security profile assessment. Tech Data's Practice Builder program helps providers develop expertise in areas such as identity and access management, threat management, application and data security, and vulnerability assessment and management. Once MSPs acquire the requisite security knowledge, they can get assistance from Tech Data experts to build offerings designed to meet their customers' needs.

CONCLUSION

Cyberattacks will remain a top risk for businesses for the foreseeable future as the threat landscape continues to evolve and intensify. Businesses need effective cybersecurity solutions and services, but they have limited budgets, and cybersecurity skills are in short supply. With all this in mind, businesses need help, and increasingly they turn to their MSPs to implement and manage their security solutions.

For MSPs, this creates a substantial opportunity to deliver the managed security services their clients desperately need. But to seize the opportunity, MSPs have to invest in developing skills and capabilities to build an MSSP practice. With help from Tech Data Security Solutions, MSPs can position themselves to address their clients' acute security needs — while forging a healthy growth path forward.

Are you ready to learn more about transforming your business to become an MSSP?

Please contact us at securityservices@techdata.com or visit

CLICK HERE