Tech Data | *Security Solutions*

Ready to Build an Advanced Security Practice? Become an MSSP.

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. In fact, 60% of small-to-medium-sized businesses (SMBs) 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.

> **With the growing complexity of the threat environment,** it's 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.

In fact, the security skills shortage was among the top three factors that increased the average cost of a data breach in 2020.[1] 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).

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. Finding a trusted partner to acquire the requisite skills to sell comprehensive managed security solutions is a prerequisite. Fortunately, that help is available.

MSPs with the will and means to become managed security service providers (MSSPs) will not only address an acute need in the marketplace, they'll be well positioned to create revenue streams and expand their customer base.

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 and modifying existing ones, while intensifying the potential for damage. Networks are constantly under threat, being forced to fend off a barrage of attack attempts. Many of those attacks are automated, using bots to constantly test a network's defenses.

> While large enterprises face big challenges in defending against the ceaseless barrage of threats, **it's even more overwhelming for clients of MSPs,** who are often SMBs that lack the advanced monitoring, detection, investigative and forensic tools to deal with these threats in-house. Nor do they have the needed fast-response 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. **Consider this data from IDC:**[2]

Worldwide spending on security-related hardware, software, and services will be **$125.2 billion in 2020**, reaching **$174.7 billion in 2024** with a compound **annual growth rate (CAGR) of 8.1%**.	Security services will be the largest and fastest-growing segment of that market, accounting for roughly half of all spending throughout the forecast period for a **10.5% five-year CAGR**.	Finally, of the security services market, managed security services are predicted to be the fastest-growing segment with a **five-year CAGR of 13.6%**.

Companies with 500-1,000 employees will see some of the strongest security-related spending growth with five-year CAGR of 9.3%, while businesses with fewer than 500 employees will spend more than $30 billion combined on security solutions.[2]

BEYOND THE BASICS

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 these advanced and comprehensive services:**

ADVANCED SERVICES
Data and discovery classification – With the average total cost of a data breach reaching $3.86 million in 2020 ($8.64 million in the U.S.), companies must discover and classify their data as a foundational component of their data security and data privacy strategies.
Governance, risk and compliance (GRC) – While heavily regulated industries like finance, energy, or healthcare most require integrated GRC, any organization can benefit from enabling all stakeholders to share knowledge and collaborate on actions with equal access to real-time data. Helping your customer adopt processes and systems that enable risk-aware decisions and compliance tracking can help them improve their ability to detect and contain a data breach.
Identity and access management (IAM) – Define and manage user roles and access privileges—and the circumstances under which users are granted those privileges—in order to grant access to the right enterprise assets to the right users at the right time. This includes helping your customers onboard and offboard employees as needed to protect access to assets.
Unified endpoint management (UEM) – Particularly now with a remote and mobile workforce, clients require deeper visibility into suspicious activity on not only company-owned devices and things, but endpoints for which they don't have physical access. Having better visibility can accelerate investigation and response time to isolate and contain damage.
Log management – Tighten up security and protect against attacks by helping your clients choose which events to log—using 24/7 real-time system monitoring and alerts—and manage them in any way that best meets their needs.
Security information and event management (SIEM) – SIEM solutions centrally collect and analyze data from multiple systems and provides reporting and forensics about security incidents or alerts to security issues.
Endpoint encryption – Protect clients' operating systems from keylogger installs or corrupt boot files and lock files stored on endpoints to prevent unauthorized users from accessing the data.

COMPREHENSIVE SERVICES
Threat intelligence – Become a member of an Information Sharing and Analysis Organization (ISAO) to collaborate with your customers and provide training—all under the veil of mutual non-disclosure agreements—to freely share timely, analyzed, and highly relevant threat data with each other. Sharing threat intelligence can reduce the average total cost of a data breach by $202,874.[3]
Sandboxing and advanced persistent threats (APT) protection – Help customers detect malicious code by executing and observing it on end-user systems in a sandbox—a safe and isolated environment that replicates an operating environment.
Incident response training – Educate your clients by helping them develop playbooks and testing them in real-world scenarios on how to manage and respond to security incidents. According to one report, the average total cost of a data breach for companies with an incident response (IR) team that also tested an IR plan using tabletop exercises or simulations was $3.29 million, compared to $5.29 million for companies with neither an IR team nor tests of the IR plan.[3]
Predictive analytics – Help customers predict an attack before it occurs, by detecting anomalies in traffic flow and data and notifying businesses even before the attack occurs. Instead of discovering and remediating an attack after it occurs, your clients will have time to raise the alarm and ready their defenses.
DNS management and mitigation – Due to the many pages that companies create for their digital business—websites, microsites, landing pages, etc.—the DNS is typically complex, making it difficult to manage and making it susceptible to attack. Your clients can benefit from first consolidating their DNS services for simplified support, managing changes within the DNS, and implement DNS security and mitigation measures.
Privileged user management – Because privileged user accounts are high-value targets for cybercriminals, helping customers securely manage these accounts—which may be administrators, devices, applications, and others—and keeping them from accessing critical corporate resources is a top priority.
Encryption key management – With the encryption keys, a cybercriminal can return encrypted data to its original unencrypted state and then steal or otherwise exploit it. Controlling and maintaining data encryption keys with an encryption key management system is key to protecting your customer from malicious actions.

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 3.1 million worldwide with a gap of 359,000 in the U.S. alone.[4]

A study by security association ISACA reveals that 62% say that their organization's cybersecurity team is understaffed, while 57% say they have unfilled positions on their team.[5] 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 which consist of ransomware. **The cumulative costs of damage resulting from ransomware attacks nearly doubled last year—from an estimated $11.5 billion in 2019 to $20 billion in 2020.**[6] If there's an opportunity for malware to sneak anywhere into the network, attackers will find it—and cybersecurity teams will need to anticipate and fight it off.

The growing complexity of security implementations is another driver of managed security services demand. Created by the number of enabling technologies and the lack of in-house expertise, security system complexity amplified the average total cost of a data breach by an average of $291,870. 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.

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.

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. Compliance failures in 2020 accounted for an average increase in the cost of a data breach by $255,626.[7]

Finally, **2020 brought a wholly unexpected market driver for managed security services**. A global pandemic forced many employees to work from home, increasing demands on IT for videoconferencing, cloud applications, and network resources.

Of those IT leaders who said their organizations required remote work in response to COVID-19, more than three-quarters reported that remote work scenarios would not only increase the time to identify and contain a data breach, 70% said it would also increase the cost of a potential data breach.[7]

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 businesses, 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: Cybersecurity Ventures expects global cybercrime costs to grow by 15% per year over the next five years, reaching $10.5 trillion USD by 2025. Put differently, cybercrime—which is predicted to inflict damages totaling $6 trillion globally in 2021—would be the world's third-largest economy, after the U.S. and China, if it were a country.[8]

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"

As the threat landscape continues to evolve, opportunities for sales growth do as well. Is your security practice prepared?

A managed security services provider can help their clients simplify security and risk with continuous monitoring and integrated solutions and services. And it's to their benefit to do so. One report suggests that managed security services were responsible for reducing the average total cost of a data breach by $78,054 in 2020.[9]

But 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 and develop an MSSP practice. Tech Data's holistic approach to cybersecurity—with industry experts, an extensive vendor portfolio and security-related reseller enablement services—helps enhance your security practice with a full complement of solutions, services, and programs.

SECURITY SOLUTIONS & SERVICES	Tech Data provides the most complete, vendor-agnostic solutions to your customers with trusted technology through our comprehensive vendor portfolio, to help solve security challenges and comprehensive security services that allow customers to achieve their security goals—including Assessment Services, Compliance Services, Implementation Services and Incident Response Services. In addition, the Solutions Product Inventory (SPI) Tool can help MSPs position new security solutions and build solutions on the fly as they have deeper conversations with customers.
SECURITY EXPERTISE	Cybersecurity professionals are hard to find and even harder to keep. Tech Data's team of solutions-focused experts can help with reseller enablement, including the strategies and tactics needed to successfully develop a security business plan, flexible financial solutions and technology-as-a-service (TaaS) to bundle hardware, software, and services into a single subscription. In addition, Tech Data offers highly skilled technical resources to support your security team, along with best-in-class security solutions for your customers that address the complete threat cycle.
PROGRAMS	Tech Data provides instant access to experts, along with demand generation and lead nurturing programs, to help drive revenue and quickly grow a security business. MSPs can also learn more about the cybersecurity market and the threat landscape through a comprehensive training curriculum that culminates in a security profile assessment. In addition, 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. Finally, Tech Data offers the first-ever distributor-hosted Cyber Range. The Cyber Range simulates real-world situations that can help you and your customers protect against, detect and respond to cybersecurity threats, as well as allow users to test and apply many of the latest security technologies.

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 >

[1] "Cost of a Data Breach Report 2020," IBM, Ponemon Institute.
[2] "Ongoing Demand Will Drive Solid Growth for Security products and Services, According to New IDC Spending Guide," IDC, Aug. 13, 2020.
[3] "Cost of a Data Breach 2020," Ponemon Institute, 2020.
[4] "Cybersecurity Professionals Stand Up to a Pandemic," (ISC)^2 Research Cybersecurity Workforce Study, 2020.
[5] "ISACA's Cybersecurity Study Reveals Struggles with Hiring and Retention Persist, More Diversity Progress Needed," ISACA Press Release, Feb. 24, 2020.
[6] "2020 Was a Bad Year for Ransomware. 2021 Will Be Worse.," Barron's, 01/08/2021.
[7] "Cost of a Data Breach 2020," Ponemon Institute, 2020.
[8] "2021 Report: Cyberwarfare in the C-Suite," Cybersecurity Ventures, 2021.
[9] "Cost of a Data Breach 2020," Ponemon Institute, 2020.