OCTOBER 2021

WHITE PAPER

GROWING YOUR MSP BUSINESS WITH CYBERSECURITY: TOP QUESTIONS TO ASK BEFORE STARTING

INTRODUCTION

As economies attempt to recover amidst rising threats from new COVID-19 variants, Managed Service Providers (MSPs) encounter increased pressure to deliver greater value, take on more responsibilities, and improve cybersecurity/compliance capabilities. It's a welcome mix of challenges with enormous opportunities due to a business environment shaped by the new normal.

Today, businesses are forced to manage a distributed workforce, move processes to the cloud, thwart cyberthreats, and face regulatory pressures. They're also doing this with IT teams that are not only understaffed but also have inadequate security and compliance backgrounds. Those operating in industries such as retail, healthcare, or financial services/banking, or in California, New York, and regions of the EU, are often caught in the crossfire between cyberthreats and data privacy regulations.

MSPs are well aware of this growing demand. In the latest edition of the annual MSP Day Report, "Security concerns" was identified by MSP respondents as the No. 1 key driver behind SMB adoption of managed services. It's the first time for security to earn that distinction in the report. Last year, it was second to "Increasing complexity of IT".[2]

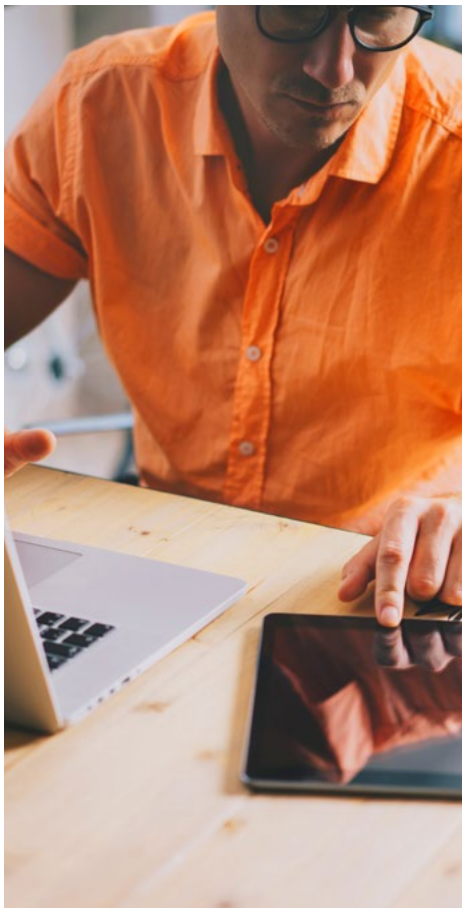
Although some MSPs offer traditional cybersecurity services such as anti-virus (AV), intrusion detection system (IDS), firewall management, and pen testing, customers are pushing for more comprehensive capabilities. The urgency to deliver is there, but MSPs have their hands full. A survey conducted by Kaseya showed that most MSPs (40% of respondents) had less than 10 employees and that some of these 10-man teams manage up to an astounding 15,000 endpoints.[3]

Taking the big leap into cybersecurity then becomes even more of a challenging undertaking for an MSP. It's going to entail a huge investment in time, effort, and financial resources—to learn and acquire new technologies, establish new partnerships, train existing staff or hire more experienced talent, and so on.

Diving in headfirst and changing direction midway aren't practical business decisions. So, before you start ramping up expansions in the cybersecurity side of your MSP business, devise a well-thought-out plan. Asking the following three questions will help point you in the right direction.

83%

With limited resources and know-how for the challenges at hand, companies are looking outside their organization for help. Already, 83% of decision-makers with in-house security teams are considering outsourcing security tasks to an MSP as early as this year.[1]



1. WHAT SHOULD I LOOK FOR IN A TECHNOLOGY?

Advanced threat actors such as organized crime groups and nation states are now increasingly launching highly sophisticated multi-vectored attacks.[4] However, that doesn't mean you should start amassing an arsenal of security solutions to counter them. Many technologies out there are point solutions that only focus on a particular set of threats or attack vectors.

For point solutions to have a fighting chance against these sophisticated attacks, they have to be integrated, automated, and orchestrated. That's going to take a lot of time, money, and engineering resources—perhaps hundreds, if not thousands, of lines of code. Remember, time is not on your side. Businesses are looking to outsource their security tasks now. By the time you're done (assuming you do get done), many of your prospective customers would have already gone to your competition.

TURNKEY

Adopting a turnkey solution means one that is easy to deploy. Many enterprise-grade security solutions, such as a Security Information and Event Management (SIEM), for instance, can take weeks or months to deploy.[5] And you don't have the luxury of time at the moment.

Thus, a turnkey solution that can start protecting your customers' IT assets within a few hours or, better yet, minutes, can help you get quick wins. It will also enable you to secure your customers without causing considerable disruption to their business operations.

ADDRESSES A BROAD SET OF SECURITY NEEDS

Your customers' IT infrastructures can vary considerably with a mishmash of endpoint, network, server, and cloud environments. Good luck deploying multiple point solutions on all that. Instead of building a battery of point solutions on every single environment, it would be much easier if you focus on finding an all-software solution that can help you address a broad set of security needs across multiple environments, out of the box.

MULTI-TENANT

MSPs can serve hundreds of clients.[6] Since you'll be serving multiple customers, the solution you need must already support multi-tenancy. A multi-tenant-ready solution should be able to give you visibility across multiple customers and their respective environments.

While seemingly informative, too many screens (a consequence of using multiple point solutions) with disjointed data sets may only lead to confusion, information overload, analysis paralysis, and alert fatigue. Ideally, your solution should have an intuitive dashboard where you can quickly view, correlate, analyze, and manage large data sets on a single pane of glass.

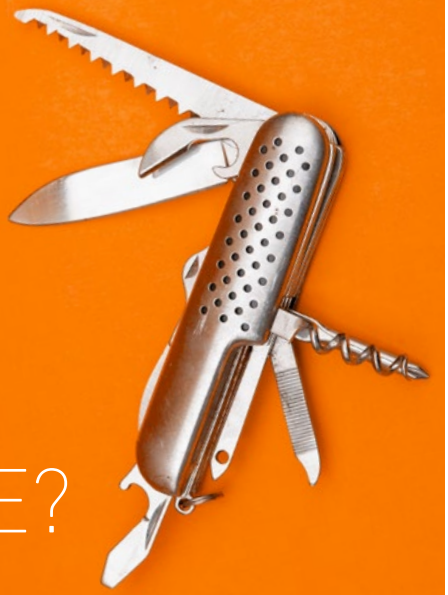
INTEGRATES WITH EXISTING SOLUTIONS

Many MSPs already have Remote Monitoring and Management (RMM) and/or Professional Services Automation (PSA) solutions for tracking and managing customers and customer IT assets. A solution that integrates with popular RMM and PSA solutions can help streamline processes and give you better control and visibility over the endpoints you need to secure.

SCALABLE

As you add more customers to your platform and as each customer grows in size, your current capacity will no longer suffice. Once you reach maximum capacity, some customers could start experiencing protection bottlenecks and downtimes. That's why, in scouting a security solution, it's important to look for enterprise-grade technology that scales. A scalable solution will enable you to continue servicing your customers even as demand grows.

2. THERE ARE MANY VENDORS & TECHNOLOGIES. HOW DO I KNOW WHICH ONES TO USE?



Traditionally, organizations that embark on a cybersecurity program end up accumulating an expansive collection of security point solutions for data privacy, network security, data loss prevention, endpoint security, identity authentication management, cloud applications security, cloud infrastructure security, and more.

According to the Cyber Resilient Organization Report 2020, almost 30% of organizations use more than 50 separate security solutions and technologies.[7] Having too many disjointed tools has an adverse effect on an organization's ability to detect and respond to a cybersecurity incident. The same report found that organizations with over 50 tools were less capable of detecting and responding to an attack than those with less than 50.

STANDARDIZED TECHNOLOGY STACK

Having too many point solutions can become a nightmare from an administrative, maintenance, and support standpoint. You'll be forced to deal with numerous vendors with different licensing, SLA, and support processes. Oftentimes, if something goes wrong and you don't know exactly where the problem lies, you'll need to go through multiple vendors and their respective tech support teams before you can get to the root cause and, ultimately, have the issue resolved.

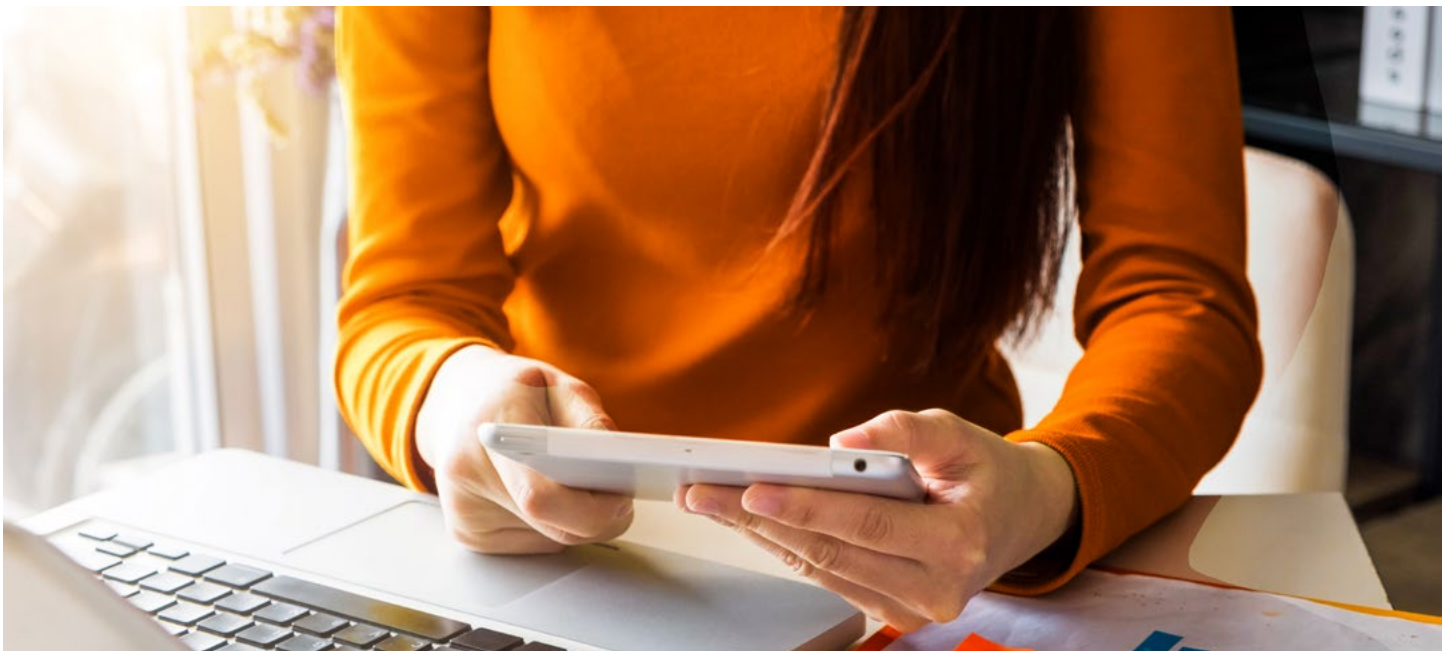
These long-drawn-out processes can be detrimental to customer satisfaction and retention. To avoid these unnecessary delays, look for opportunities where you can get a broad set of cybersecurity capabilities from a single vendor. That way, you have only one vendor to manage when you need support.

This essentially means going for a platform instead of an assortment of point solutions. This will also allow you to shorten your procurement process. Instead of vetting multiple vendors for each point solution, you can simply vet vendors for each potential platform.

EASY LICENSING MODEL

Consider working with vendors whose pricing strategy aligns with your own revenue models. Normally, MSPs bill based on usage or on a subscription basis, so look for vendors that follow the same model. This will give you and your customers maximum flexibility as you manage expenses in an OPEX-based model instead of a CAPEX-based model. With these types of billing arrangements, you'll have a healthier cash flow and won't have to worry about astronomical upfront costs.

Consequently, this would mean you'll want to look for a solution with subscription-based licensing or licensing that's based on usage or consumption. Stay away from perpetual software licenses rooted in predetermined data ingestion rates, volume licensing, or per CPU. These types of licensing will only impede your cash flow.



3. WE KNOW TECHNOLOGY. HOWEVER, CYBERSECURITY ISN'T OUR EXPERTISE. WHAT KIND OF SUPPORT SHOULD WE LOOK FOR?

Being in the MSP industry, there's no doubt you have a pretty good grasp of technology. However, cybersecurity may not be your strongest suit. Not only that, as indicated earlier, your team may already be stretched too thin. You'll need all the support you can get. The following kinds of support are essential to succeeding in the cybersecurity business.

DEPLOYMENT SUPPORT

First impressions matter. For this reason, deployments should be as trouble-free as possible. A deployment plagued with issues can ruin a customer's trust right from the start. Unless you've been deploying the same solution for years, it's probably wise to have an experienced hand on the wheel. A vendor that can offer actual assistance when you deploy their technology to your customers can minimize the risk of delays and any potential hiccups.

24/7/365 GUIDED REMEDIATION FOR CYBERATTACKS

Cyberattacks can happen anytime. Many of these attacks have a heightened degree of sophistication that may exceed your level of expertise in cybersecurity. You can't afford to be left alone at night fighting off adversaries that are beyond your skill level. The longer an attack remains active, the greater the damage it can inflict.

So, if there's a vendor out there that can be available 24/7/365, someone who can guide you in remediating a cyberattack if one ever takes place, include that vendor in your shortlist. You know your customer's environment and should own your customer relationship, but partnering with a vendor that can support you as you respond to the issue can cut down remediation time significantly.

SOC ENGINEERS AND ANALYSTS

Threat detection and response is tricky business. False positives or false negatives can drain resources, lead to alert fatigue, put you off course, and cause all sorts of problems. You need help from highly trained and experienced professionals to get this job right. Your best option would be a cybersecurity vendor that has a dedicated security operations center (SOC). A SOC is manned by security engineers and analysts with the most advanced tools and processes in place to skillfully detect, contain, and remediate threats.

THREAT RESEARCH TEAM

Cyberattacks don't grow overnight. Threat actors still have to lay the groundwork before they can launch a full-blown attack: find vulnerabilities to exploit, develop exploit kits, acquire stolen credentials, deploy malware, and perform several other activities. If you can anticipate the attack, you can blunt or even completely eliminate its impact.

A threat research team can do that for you. By understanding current threat actor tactics, techniques, and procedures (TTPs) and applying threat intelligence, these teams can take preemptive measures to counter emerging threats.

CERTIFIED COMPLIANCE SPECIALISTS

Depending on the industry or region they are doing business in, a number of customers may be subject to HIPAA, PCI DSS, GDPR, and/or other data privacy/protection frameworks. It would bolster your credibility if you could be certified for the security framework in question.

The problem is, obtaining certifications entails a significant amount of time (6 months to a year) and resources. And then once they're obtained, maintaining those certifications can require even more resources. For smaller MSPs, this route may not be feasible. Partnering with a vendor with the required certifications as well as the GRC teams to respond to any questions would be a more practical option.

SUPPORT FOR GROWING YOUR BUSINESS

Having a partnership that gives you all the technical support you need to deploy and streamline your cybersecurity services is crucial. At the end of the day, however, you'll still need to market and sell those services in order to grow your business. Hence, it's equally important to partner with a vendor who can lend topnotch marketing and sales support.

MARKETING SUPPORT

You understand your customers more than anyone else. At the same time, your security solution vendor has a solid pulse of the cybersecurity market. An understanding of the target audience and your solution's distinguishing factors, combined with a compelling story, are key ingredients for an effective messaging strategy.[9]

If you and your vendor merge your respective expertise and knowledge, you should be able to infuse more compelling and relatable messaging in your marketing collateral for your target audience. A vendor who can provide joint collateral and easy-to-use templates can be a big boost in launching timely, highly targeted, and effective marketing campaigns.

SALES SUPPORT

A survey made by ***MSP Success Magazine*** showed that 72% of MSPs surveyed did less than two sales appointments per month and closed less than one deal per month. These low numbers of prospecting and selling activities can be attributed to the fact that most MSPs focus their hirings on tech people and neglect salespeople.[10] If budgetary constraints prevent you from growing your sales force, you might as well find support in this area elsewhere. Some vendor partner programs are designed to help MSPs in that regard.

Ideally, your vendor's partner program should include sufficient tools and support that can help you acquire new customers and drive up revenue. Look for a vendor that can offer impactful sales support services such as joint selling, lead sharing, and joint business planning. If you can find one that will also help you devise a go-to-market strategy, that would be a big plus.

CONCLUSION

Businesses are increasingly turning to MSPs for help in managing their distributed workforce, moving processes to the cloud, and improving cybersecurity/compliance capabilities. These needs are being greatly amplified in the new normal, providing MSPs with tremendous opportunities for business growth while delivering even greater value to customers.

To capitalize on these opportunities, you need to be strategic in choosing a solution and vendor to work with. A turnkey solution that enables you to scale and improve efficiency can give you a superior advantage in protecting your customers' IT assets and rapidly growing your MSP business.

ABOUT ARMOR

Armor is a global cloud security company. We make cybersecurity and compliance simple, achievable, and manageable for managed service providers (MSPs) and their customers across endpoint, network, server, and cloud environments. Armor provides unparalleled insight into threats and helps our partners respond quickly and effectively. MSPs who use Armor benefit from an enterprise-grade security platform, cybersecurity expertise, and resources to help quickly scale their cybersecurity practice. Armor has partnered with leading MSPs to secure more than 1,500 customers in over 40 countries.

SOURCES

1. "Syntax IT Data Trends Benchmark Report," 2021
2. "The Evolving Landscape Of The MSP Business Report 2021," 2021
3. "2020 MSP Benchmark Survey Results Report," 2020
4. "How Hackers Might Be Winning With Multi-Vector Mega Attacks," 2021
5. "Security Information and Event Management (SIEM)," 2020
6. "Datto's Global State of the MSP Report," 2021
7. "Cyber Resilient Organization Report 2020," 2020
8. "Why And How MSPs Adopt Cybersecurity Industry Standards," 2021
9. "How To Build An Effective Messaging Strategy," 2020
10. "Industry Survey: How Many Appointments And New Clients Does The Average MSP Secure Every Month?," 2019

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167