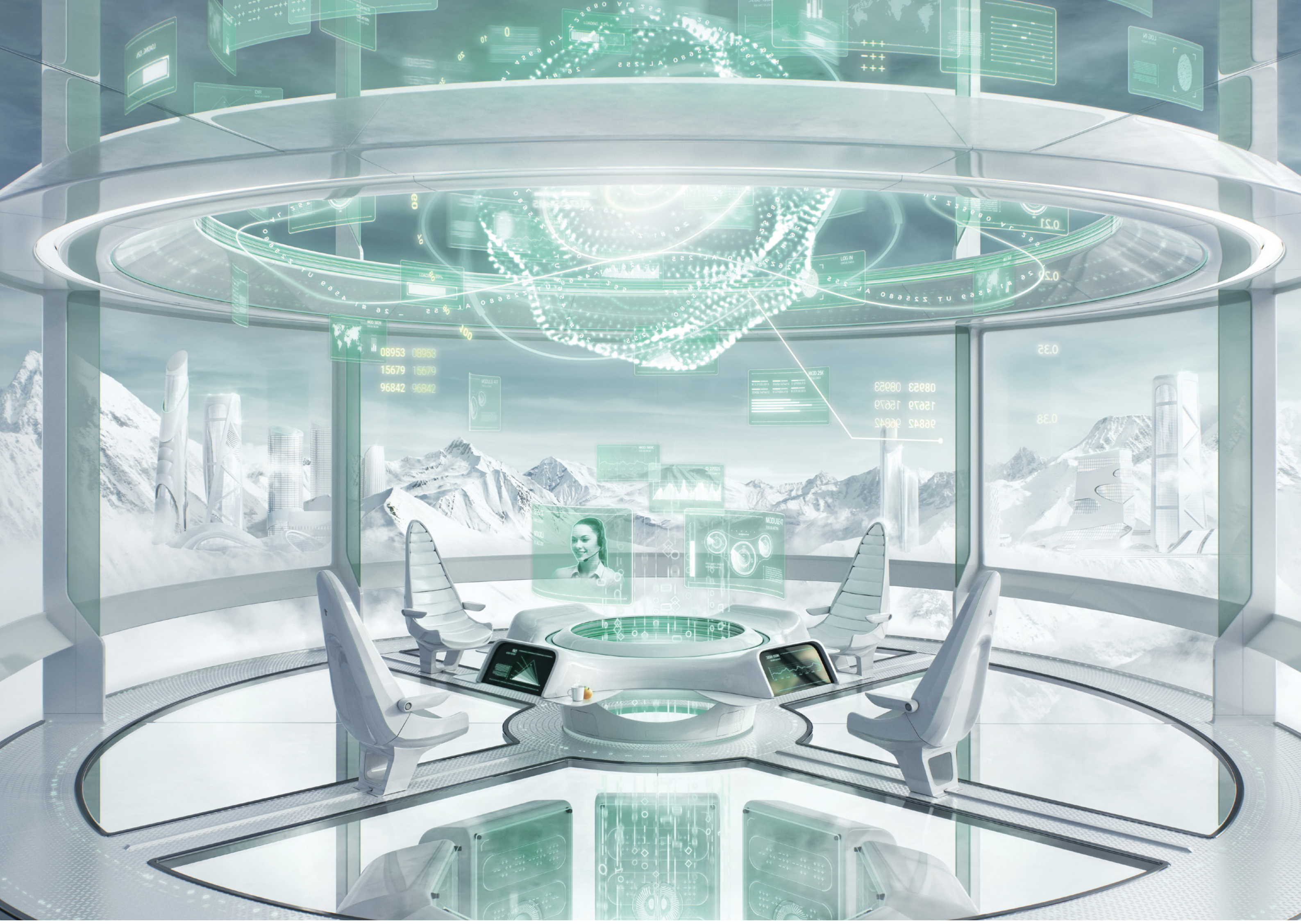

Challenge and opportunity in the MSP sector

kaspersky

Challenge and opportunity in the MSP sector

The evolving role of the MSP

Traditionally a Managed Service Provider (MSP) is defined as an IT service company remotely managing customers' IT infrastructure and/or end-user systems on a proactive basis supported by a service level agreement. In brief, the mission of an MSP was to keep their clients up and running, take care of hardware issues and make sure everything operated smoothly.

That has changed!

Cybersecurity: a bright new future… for some

During the last few years the huge demands of data-driven digital infrastructure mean cybersecurity has truly taken center stage for MSP clients. Organizations of all sizes have clearly indicated to the market they are ready and willing to pay more to protect their business.[1] Businesses are choosing to outsource cybersecurity because protection is increasingly complex and there's a chronic shortage of skilled cybersecurity professionals, so they can't hire security expertise in-house.

SMBs, the target of a staggering 43% of all cyberattacks,[2] are no exception. 62% of SMB respondents to a recent survey by market research firm Vanson Bourne confirmed they didn't have any in-house capability to address cybersecurity issues, while 52% said they felt "helpless to defend themselves" from newer cyberattacks.[3]

As a consequence, the MSP market is driven by a predicted 200% growth in cybersecurity services. Global annual sales will double during the next half decade. Gartner estimates "services (subscription and managed) will represent at least 50 percent of security software delivery by 2020,"[4] making managed security services one of the fastest growing segments in IT markets.

MSPs around the globe are transitioning into cybersecurity service brokers (in some cases into full-fledged MSSPs – Managed Security Service Providers) – expanding their value proposition and generating additional margin addressing existing and new clients' security needs.

In many ways this should be an inevitable transition. For an MSP taking care of a client's IT infrastructure maintenance and network management storage, offering managed security services for networks and infrastructure is the logical next step. Fast-to-adapt MSPs understand they will forge longer-term relationships by addressing the critical needs of their existing clients, as well as attracting new business through security solutions and bringing them on board for standard services as well.

So what are the pain points?

The 80/20 rule applies to MSPs. Already 80% of managed endpoints are overseen by 20% of MSPs. Consolidation is restricting the growth of many MSPs or forcing them out of business. Larger MSPs are transitioning to become full-fledged MSSPs, and the complexity of the MSSP business model is an important element of MSP global consolidation.

Pure market forces are driving this consolidation trend through a relentless process of mergers and acquisitions.[5]

- The traditional MSP market growth is slowing just as the MSP cybersecurity market 'explodes'.
- The MSP cybersecurity market winners will be the ones who get to market first.
- Full-fledged MSSPs rely on size and 'muscle' to counter the cyber skills shortage and attract talent.
- Even the largest players are increasingly compelled to pool technology and expertise with direct competitors due to the ever more complex threat landscape.

[1] https://www.businesswire.com/news/home/20190326005174/en/SMBs-Leave-MSPs-Cybersecurity-Vanson-Bourne-Report

[2] https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

[3] https://www.businesswire.com/news/home/20190326005174/en/SMBs-Leave-MSPs-Cybersecurity-Vanson-Bourne-Report

[4] https://www.securityweek.com/global-security-spend-set-grow-1338-billion-2022-idc

[5] https://www.channele2e.com/news/european-msp-mergers-and-acquisitions/

As a result, smaller MSP operators risk being left behind. 93% of respondents, in a recent survey by market research firm Vanson Bourne,[6] indicated they would consider moving to a new MSP if that MSP offered the "right" security solution. But many MSPs (especially smaller-scale MSPs offering services to SMBs) are not currently set up to do anything beyond the basics of cybersecurity (if that). The future viability of their business depends on adapting.

How do MSPs transition to providing effective security services for their clients?

The fundamental questions MSPs must address are:

- Will our existing clients stay with us if we don't offer cybersecurity services?
- Will we attract new clients without offering security services?
- Will our clients wait as we transition or will they move their business to more security prepared competitors?
- How do we make all the necessary changes to become a provider of the cybersecurity services our clients are looking for?

Below are the four directions existing MSPs can take faced with the challenge of redefining themselves as a provider of cybersecurity services.

1. MSPs can stick to their existing model offering limited security services.

Such is the fast-evolving nature of cybersecurity defences and the demand for increased security, this is likely a short-term solution. MSPs have been including very limited security services for decades, but navigating a sophisticated threat landscape with a managed firewall, spam filtering and basic antivirus is not likely to satisfy the future security demands of their clients.

2. MSPs can develop managed security services one step at a time.

Providing comprehensive cybersecurity solutions for clients is a huge step for most small-to-medium MSPs. However, past experience selling limited antivirus and firewall solutions enables MSPs to build on their traditional, self-delivered services by partnering with a specialist cybersecurity vendor, such as Kaspersky. MSPs can gradually define and deliver in-house security technology, in partnership with their chosen vendor.
The advantage of this layered, one step at a time approach is that the MSP utilizes the flexibility of their chosen cybersecurity vendor to plug the gaps that they are unable to fill. This enables them to avoid simply outsourcing cybersecurity and becoming a 'broker of security services'.

This hybrid model is proving to be a way forward for increasing numbers of MSPs. The key lies in finding a specialist cybersecurity vendor offering easy-entry, easily integrated endpoint protection. (Kaspersky Endpoint Security Cloud is an example.) Partnering with a reliable, flexible vendor allows MSPs to integrate vendor technology all the way up to the most advanced security services. This enables MSPs the opportunity to tailor **managed security solutions** to fit clients' requirements in an evolving cyber threat environment.

Starting out, it's advisable for MSPs to conduct an audit to clarify:

- What cybersecurity their clients think they need and can afford, and what services do they realistically require? Global cybersecurity vendors possess vast knowledge about SMB and enterprise security requirements and can help an MSP determine the exact services for their clients.
- How easily can specialist cybersecurity technologies be slotted onto the MSP's existing security services?
- Will the cybersecurity vendor share access to their experts/training to foster relevant skillsets within the MSP?

[6] https://www.businesswire.com/news/home/20190326005174/en/SMBs-Leave-MSPs-Cybersecurity-Vanson-Bourne-Report

3. Team up with a specialist cybersecurity provider by outsourcing 100% of the cybersecurity services demanded by their clients and becoming a ‘broker of security services’.

Fitting into a global service brokerage trend in IT, outsourcing is a valid and realistic path for expanding MSPs. But to outsource cybersecurity completely, an MSP needs to choose their security service vendor wisely. The vendor must demonstrate the knowledge, organizational ability, technology, tools, resources, and an impeccable track record handling MSPs’ security needs in the specific geographical area and for the typical profile of clients. MSPs need to identify cybersecurity providers offering whole solutions not just a package of tools, and look for specializations fitting specific client needs, not one-size-fits-all solutions. The end objective is for the managed security solution provider to function like an extension of the MSP’s team.

The advantage of this approach is the MSP can focus entirely on their core services with the added value of delivering cutting edge security solutions for their clients.

4. Make the internal changes necessary to become a full-fledged Managed Security Service Provider (MSSP), defined by Gartner as “an organisation that provides outsourced monitoring and management of security devices and systems.”[7]

But to do that, MSPs must cover all aspects of providing security – new skillsets, tools and certifications – whilst ensuring existing business functionality. The ‘new’ MSSP not only has to guarantee protection for their clients from ransomware, data loss and fraud, but also inform their clients about the latest evolving malware and cybercriminal activity, and provide up-to-date advice and services to meet rapidly-changing government regulations.

Most smaller-sized MSPs simply do not have the financial, organizational and knowhow resources to do all that. The competition is powerful, expanding fast through acquisitions, and well-funded. What’s more, cybersecurity operations within organizations are not only expanding but also fragmenting. In a recent study 46% of security professionals confirmed they now used products from 11 or more vendors.[8] Moreover, the volume of threats and attacks is increasing, which means organizations must implement a complete strategy including all aspects of prevention, not simply defense.

A further challenge is sourcing security experts. A recent report from CyberEdge suggested eight out of ten organizations are restricted by the global shortfall of skilled IT security personnel.[9] Legal liability and how to protect from punitive damages in case of a significant breach is another risk. Finally, is the company’s own cybersecurity in order? Any organization claiming to be an MSSP must be able to demonstrate to the world their in-house security is impeccably managed and everything they advise a customer to do security-wise, they’re already doing.

In conclusion however, once MSPs have chosen their direction and put in place best-fit cybersecurity services, these MSPs stand to gain significant competitive advantage tapping into a fast-growth market and delivering considerable added value for their clients.

Security Operations Center (SOC)

Cybersecurity going forward is not just about technology, it’s about the people behind the technology. The future is likely to see a fluid interchange between in-house staff and specialist security providers. Establishing a Security Operations Center (SOC), outsourced to a security provider, is a potential way forward to supply clients of all sizes with the risk assessment, analysis and knowledge needed to reinforce security across all client operations. A future trend will likely be MSPs boosting their cybersecurity credentials by partnering with a specialist cybersecurity provider who has the capacity to provide an effective SOC for their clients.

[7] https://www.gartner.com/technology/it-glossary/mssp.jsp

[8] https://s1.securityweek.com/stepping-increasing-demand-managed-security-services

[9] https://cyber-edge.com/wp-content/uploads/2018/03/CyberEdge-2018-CDR.pdf

Conclusions

“Security is going to be a completely disruptive force for MSPs in the industry.”[10]

“If you’re going to successfully take on security in 2019, you’re going to need a plan.”[11]

Fast-evolving advanced threats, increasing volumes of malicious cyber-activity and changing regulatory requirements all mean MSPs face headwinds when transitioning to offer comprehensive and effective security solutions for their clients. But for MSPs that choose an approach suited to their business model, enabling them to meet their clients’security needs effectively, the business rewards are great.

Kaspersky solutions

Kaspersky research has shown that more than 50% of MSPs believe that cybersecurity for IT operations is the main trend to affect the MSP market over the “next three to five years”.

Kaspersky is a global specialist security provider and since the launch of our MSP Program in 2017, more than 2,000 providers have joined our ecosystem worldwide. Kaspersky solutions empower MSPs with most-tested, most-awarded security that adapts to any environment or security need, and is fully compatible with remote monitoring and management (RMM) systems and professional services automation (PSA) platforms.

Kaspersky’s flexible offering includes products and technologies for endpoint protection, mail server protection and virtualization. Protection for endpoints, including managed security, remote monitoring and mobile device management, remain the main area of profit for service providers - with both Kaspersky’s flagship products, Kaspersky Endpoint Security for Business and Kaspersky Endpoint Security Cloud, holding the leading positions among partners participating in the Kaspersky MSP program.

Managed service providers registered in the program can choose between cloud and on-premises endpoint protection – with options ranging from flexible, quick to roll out and easy to run products, to scalable, fully integrated, tiered endpoint security platforms – all depending on the customer needs.

Kaspersky’s self-service License Management Portal (LMP) for MSPs works in synergy with the Kaspersky United Partner Portal to make MSPs’ sales operations faster, smoother and more transparent. With the LMP, MSPs can try both cloud and on-premises solutions, evaluate their features and build services for their customers. The portal also integrates with cloud product management consoles via single sign-on - making the whole user lifecycle smooth and hassle free – and provides actionable recommendations on upsell opportunities, license usage for cloud products and more.

Toine van Bilsen, the owner of QNS in the Netherlands (on receiving a 1000th Partner Award from Kaspersky) noted: “Customers can rely on us to provide a perfect insight into the status of all of their endpoints with the help of Kaspersky Security Center. In addition, we can access professional support in our local language in case we encounter any problems. We are very satisfied with our working relationship with Kaspersky.”

For more information on how we can assist MSPs with their clients’ cybersecurity needs, please visit **https://www.kaspersky.com/partners/managed-service-provider**

[10] https://www.continuum.net/blog/which-major-forces-will-disrupt-the-msp-market-in-2019

[11] https://www.continuum.net/blog/which-major-forces-will-disrupt-the-msp-market-in-2019

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Cybersecurity for SMB: kaspersky.com/business
Cybersecurity for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Known more at kaspersky.com/transparency

Proven.
Transparent.
Independent.