MSSPs are here to stay—what to know when considering one

HPE GreenLake

Do security issues keep you up at night? Are you concerned that your small IT staff is stretched too thin on other projects to handle the demands of an ever-evolving cybersecurity landscape?

One option many businesses are turning to is managed security services providers (MSSPs)—service organizations that pick up the security reins. These organizations typically offer firewalls, intrusion detection, privately secured networks, and other antiviral services. MSSPs help businesses keep an eye on the threat actors and are available 24x7.

A recent report from Kaspersky found that 69% of organizations of all sizes are using, or plan on using, an MSSP to handle security operations.[1] With this surge in use, it's important for enterprises to know the full scope of what MSSPs can handle, the potential challenges managed security partnerships can pose, and the factors businesses should consider when selecting an MSSP vendor.

Outsourcing to drive innovation and scale

As mentioned, MSSPs can provide an invaluable service for businesses who need assistance handling a full-scale cybersecurity operation. However, beyond the tools and round-the-clock availability they offer, MSSPs also bring a wealth of domain expertise and experience in dealing with attacks of all kinds. This is particularly important for a business in startup mode that may not have a robust security staff filled with industry experts. MSSPs are dedicated security professionals who have the right skill sets and access to resources and tools that small-sized businesses may not have.

Equally as important is having access to these security professionals as businesses scale. When a business gets bigger and begins processing more and more data, be it internal or customer data, the attack surface a threat actor can target also grows. IT teams in rapidly growing businesses may lack the skills needed to handle necessary security operations.

As a business grows, developers can often go rogue, creating or using applications without getting approval from the business, leading to the shadow IT effect. With applications piecemealed together, there's a lack of standardization of security from one tool to the next, which creates loopholes where attackers can strike. Some MSSPs also have access to service professionals who can sit in with developers and help design applications with security squarely front of mind. Additionally, MSSPs can help developers customize applications that sit high on the technology stack to be secure from attack. The skill sets and expertise that MSSPs offer can help these businesses meet the security challenges that come along with growth.

Perhaps most importantly, outsourcing security operations also frees up IT professionals to focus on more strategic initiatives. Rather than having to worry about keeping the business safe from attack and monitoring the network all day and night, IT professionals can focus their attention on tasks such as delivering digital transformation goals or improving the experience for end users and customers.

While there certainly are plenty of good reasons to use MSSPs, outsourcing security presents some challenges.

[1] "IT security economics part 4: managing your IT security team—How IT security leaders can unlock the potential of their teams," Kaspersky blog

Managed security services challenges

MSSPs often sell their services as a commodity, which means that their packages of solutions may fit most of an enterprise's security challenges but not all of them. With this in mind, MSSPs cannot be painted as a one-size-fits-all solution to every security problem a business has. The bigger the job for an MSSP, the more complicated it becomes to create a wide-reaching security operation that keeps every single element of the enterprise safe.

In some cases, using an MSSP may create a situation where the security awareness and skills inside the organization slip or where others ignore security altogether. IT and non-IT employees who had security responsibilities in the past may find themselves unclear of their roles. Without a clear understanding of how the MSSP fits in with a business, people may not know what to do or whom to notify if a hacker strikes. Businesses need to keep employees involved in security functions and set up new roles, responsibilities, and communication protocols.

Transparency within an MSSP can also create issues. For example, what happens if the MSSP notices a vulnerability within its systems and solves it but doesn't notify the customer about it? These types of growing pains can occur if the business and the MSSP don't clearly outline how they should communicate with each other about back-end issues.

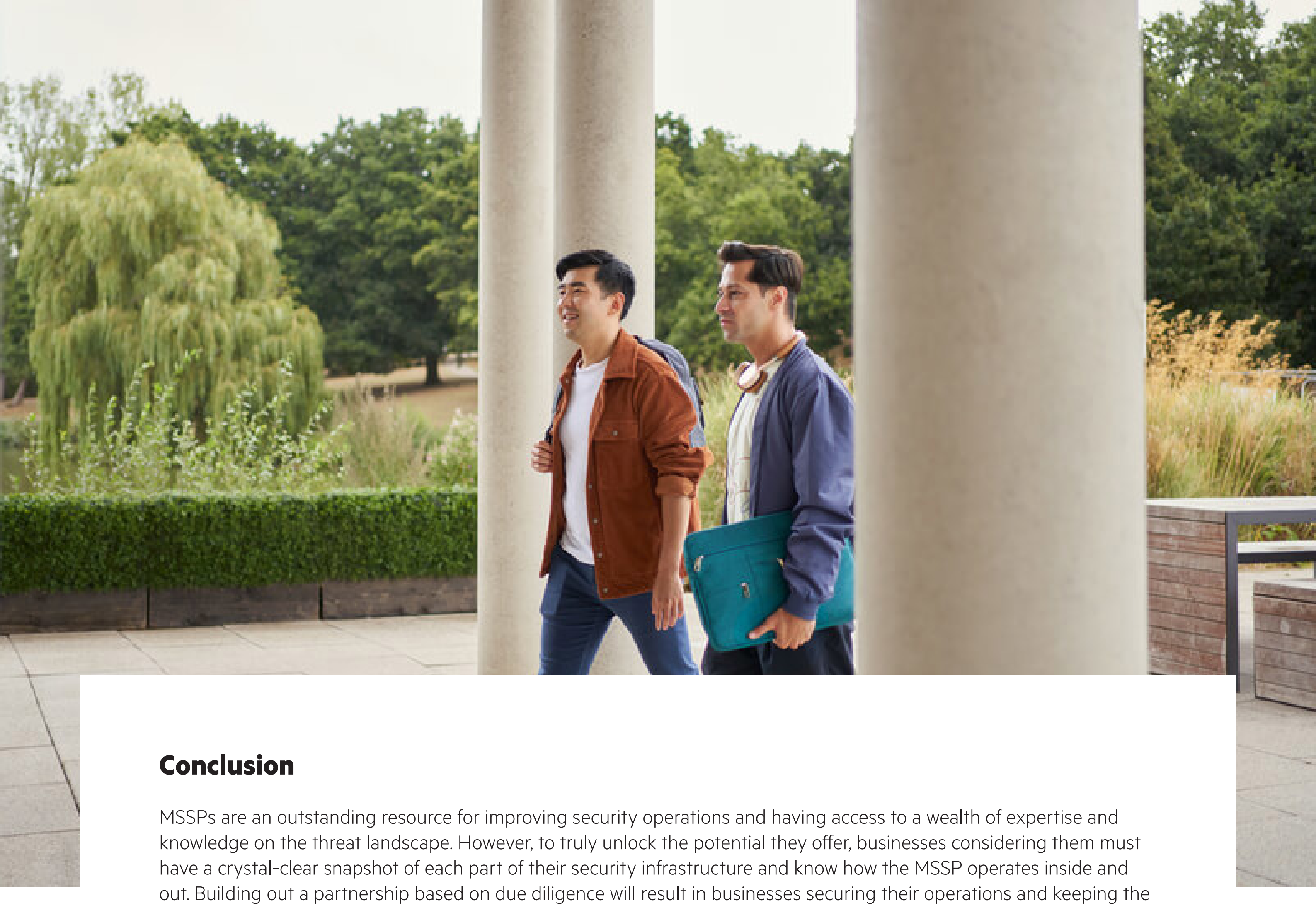
Once a business has weighed the benefits and potential challenges of using an MSSP and decided to select one, the real work begins. There are still questions to ask to ensure the partnership is set up for success.

Key MSSP considerations

Before signing on with an MSSP, businesses must have clearly defined security goals, know the full scope of their security needs, and be confident that their chosen provider has the skill sets and acumen to meet those needs. This involves having up-front conversations between IT leaders and the C-suite (along with other leadership) to create alignment between security and business goals and understand where vulnerabilities and security gaps exist.

This can be more daunting than it sounds. Many businesses outsource other operations such as cloud management, payroll, and building services. The fact that these operations are handled by outside parties doesn't mean they're secure from attack. Other third-party tools and services may fall out of the scope of what the MSSP can protect against. This sort of holistic alignment on all systems being used is a crucial step to ensuring an MSSP can fulfill their role in the larger security goals of the business.

Businesses also need to ask themselves how the MSSPs they're considering will fit into their current systems and if additional re-tooling will need to be done to them to ensure a smooth integration. In the same vein, the business needs to ask themselves if they understand how deep the scope of their partnership goes, if the MSSP is part of industry groups that set standards, and if it has demonstrated how it plans to innovate in the future. It cannot be overstated how important it is to have complete insight into each element of an MSSP engagement, as any knowledge gaps and misalignment in roles can create situations where security issues still occur.



Conclusion

MSSPs are an outstanding resource for improving security operations and having access to a wealth of expertise and knowledge on the threat landscape. However, to truly unlock the potential they offer, businesses considering them must have a crystal-clear snapshot of each part of their security infrastructure and know how the MSSP operates inside and out. Building out a partnership based on due diligence will result in businesses securing their operations and keeping the safe as they chart a course ahead.

Learn more at

hpe.com/us/en/greenlake/compliance-monitoring.html

Visit **HPE GreenLake**

Make the right purchase decision.
Contact our presales specialists.

Chat now (sales)

Call now

Get updates

Hewlett Packard
Enterprise