WHITEPAPER

Why Managed Endpoint Security?

LevelBlue | SentinelOne

Introduction

The speed, scale, and sophistication of modern cyberattacks continuously challenge the security defenses of businesses of all sizes. Signature-based antivirus, which often helps protect a network from a known threat in future attacks, is no longer sufficient to defend against malware, ransomware, and fileless attacks. Organizations not only need cutting-edge endpoint security technology, but also often need managed services with the skills and expertise to continuously protect, detect, and respond to threats. Utilizing a managed service can help augment a business' existing Security Operations Center (SOC) or remove the need to build one. This frees up resources and allows the business to focus on its core competencies, its customers, and the bottom line.

Market Trends

Ransomware Is on the Rise

Ransomware-as-a-Service has made ransomware more accessible to a broader audience of bad actors, in effect, reducing barriers to entry. More bad guys, with less skill, are still able to effectively deploy a crippling ransomware campaign. And the more skilled bad guys, those who have staying power and a vested interest in profitably continuing their campaigns, reinvest a portion of their "revenue" back into "R&D". They continuously evolve their tactics, techniques, and procedures on the front lines of the cyber war.

Beyond the ransom itself, there are other costs associated with ransomware. The cost of lost production must be considered as well. Your business being down due to a ransomware attack can cause your customers to lose faith in your ability to deliver for them. This can lead to increased customer turnover, and increased costs of acquiring new customers due to diminished trust.

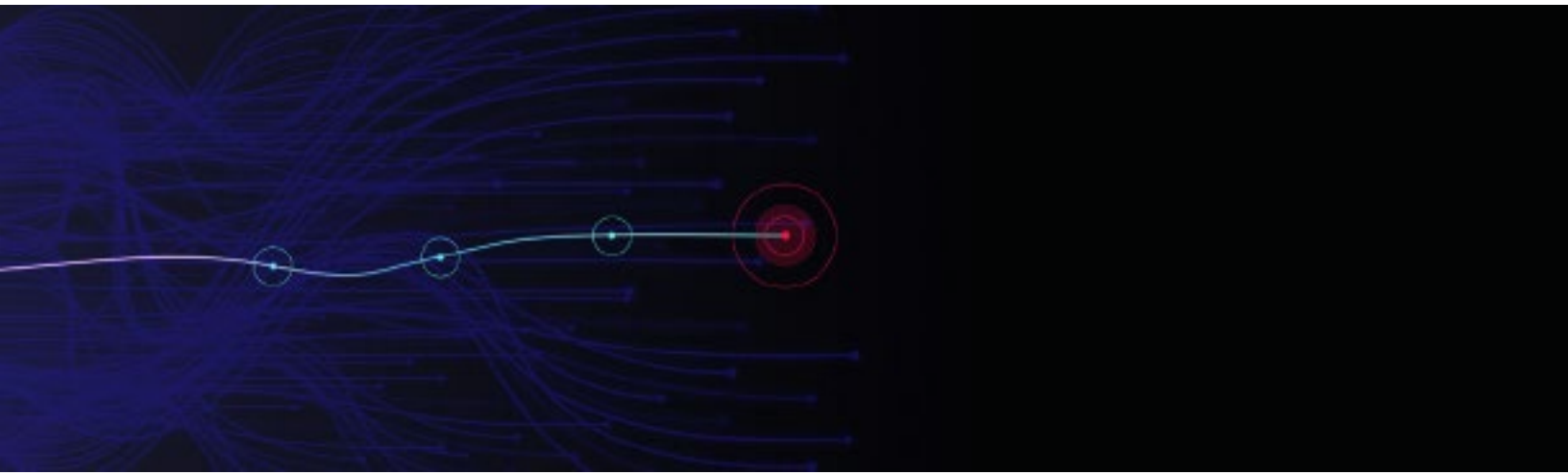
For some ransomware attacks, the attackers first scrape your data before encrypting it. In those cases, even if you pay, there is no guarantee that the thieves will not quietly sell your data to others, making your business even more vulnerable and diminishing your competitive advantage.

Sophisticated Attacks

Sophisticated attacks are more complex by nature and therefore, more difficult to defend against. This unfortunate trend is on the rise as a successful way to infiltrate a company. According to the Ponemon Institute's Third Annual Study on the State of Endpoint Security Risk, two-thirds of IT security professionals indicate their company experienced one or more endpoint attacks that compromised data.[2] Malicious actors can find so much success here because there are many ways to gain entry through them. For example, weaponized documents may be sent as email attachments in spearphishing campaigns which execute PowerShell exploits. Their fileless, malicious code takes advantage of your normal system process and spreads laterally at machine speed. And then there are fileless attacks which operate from memory. Threat actors are determined and constantly evolving, searching for any way to get into your system.

67% Of companies with endpoint attack that compromised data

1 Third Annual Study on the State of Endpoint Security Risk, Ponemon Institute



Part of the issue is that businesses still rely on signature-based antivirus (AV) as their primary form of endpoint security. AV effectiveness is highly limited, as it only protects against previously known threats; fileless attacks and PowerShell exploits easily evade this line of defense.

A Rise In Blind Spots

For many endpoint security tools, detection of and response to a threat rely only on external factors. These include recent threat intelligence or human intervention while investigating and responding to a threat. Then there are other solutions that employ some cloud-based AI but require a constant connection to the internet in order to perform that analysis. This leaves the endpoint only partially protected when a network connection is unavailable.

Device proliferation and increase in Internet of Things (IoT) devices also bring potential gaps in visibility. Employees may access corporate data from new, unmanaged devices, creating new vulnerabilities to the corporate network. Furthermore, IoT devices add unique challenges as there are no common standards for the technology and often no way to apply a protection agent onto the IoT device. Malicious actors can take advantage of these unmonitored devices to infiltrate the corporate network.

In addition, malicious actors are taking advantage of the siloed endpoint security tools, each performing disparate elements of security on the endpoint. This mix of single purpose agents per endpoint add to the complexity and cost of managing endpoints.

Diffuse Security Perimeters

The dramatic increase in employees working remotely has caused additional challenges as workers are away from traditional on-premises security controls. Now, this dynamic workspace must be considered in effective endpoint management. This includes accounting for users logging on and off the corporate network and internet throughout the day.

Endpoint security is no longer just about protecting laptops, desktops, and servers, it is also vital to protecting your assets in the cloud. Businesses are moving more data and applications to the cloud. With this comes new needs to secure this cloud environment—including managing the endpoints that reside within it. Open source container management technologies such as Kubernetes are greatly expanding the use of cloud services and enabling even greater innovation and digital transformation.

Security Talent Crunch

The demand for qualified cybersecurity talent is causing companies to compete for the best hires. As a result, employers can expect wages to continue to increase above market rate. And, as the most talented security hires are recruited for more promising opportunities, job hopping is expected to be a more common occurrence. This churn is not only costly, but it puts pressure on employers to create an environment that will help them to retain the talent necessary to keep their business cyber secure.

Alternative: In-House SOC

For some companies, keeping their endpoint management in-house seems to be the best solution. But endpoint security means much more than antivirus software. The methods for cyberattacks continue to rapidly evolve, as does the technology required to protect against it. An effective self-managed endpoint security strategy optimizes people, processes, and technology working together. This can pose a few challenges:

People. As discussed, the current market for qualified security talent can make hiring, training, and retaining in-house security talent challenging and costly. In addition, the team must stay up-to-date with both cyber threats and solutions with access to the tools to address the threats.

Process. There are many stages to creating a process that will effectively monitor, manage, and respond to security threats of your endpoints. When there is a breach, immediate action is required to minimize damage. Some organizations choose to develop an in-house incident response (IR) team for this. These are highly-trained security experts who think quickly under pressure to address cyber threats.

Technology. Security professionals need the right tools to protect your business. Building an effective security stack can be overwhelming, even for enterprises, much more so for small- or medium-sized businesses. Too often, there is overlap in tool functionality, creating waste and data noise instead of actionable insight. This inevitably leads to a SOC which is stretched thin, overworked, and overstressed. This in turn leads to staff attrition, and the cycle of talent acquisition and training repeats, without addressing the root cause of the noise problem. Trouble is, ripping and replacing solutions from the IT security stack is not that simple. Purchase decisions have far-reaching consequences.

Our Recommendation: Managed Endpoint Security

The decision to outsource managed endpoint security is much like the decision to use public cloud services. Public cloud providers create economies of scale, attract skilled talent, and are exceptional at their tradecraft, which liberates their customers to focus on running their business, instead of running a data center. The same logic holds true for managed security service providers.

Advantages

Around the clock management. No matter your business hours, your business data always needs protection. Managed security service providers (MSSPs) can provide uninterrupted security monitoring and management, spreading the cost of 24/7 coverage across a broad customer base. By offloading the burden of building their own SOC, customers have more ready access to the tools and expertise needed to continuously protect their endpoints.

Expertise. For top security experts to want to stay with a business, they need the latest tools at their disposal and an environment where they can make a difference. A quality MSSP combines tools that empower security talent to make informed, responsive decisions to protect the business. This may serve to attract and retain the best hires, which in turn provides benefits to the clients.

Cutting-edge tech. Leading MSSPs are innovators using future-forward technology to deliver the best solutions in its security stack. Automation and AI does not replace the need for skilled operators. Instead, it enables skilled tacticians to do their job more effectively against capable and well-equipped cyber adversaries, enabling them to more effectively monitor and respond to threats more quickly.

Deep integrations. Combining technology and tools together through API integration in a well-orchestrated security stack is a complex, time-consuming process. Partnering with an MSSP helps to address these issues. To keep up with technology changes and maintain security protocols, ongoing maintenance and upgrades are needed as well. An MSSP can offer the resources and capabilities to allow for a variety of integrations and bring more comprehensive solutions to the customer.

Knowing your network. Knowing which devices are connecting to your network is fundamental to successfully securing endpoints. In addition to employees who connect, you may also have 3rd parties connecting as well, increasing your risk of a breach. An MSSP can help you maintain real-time inventory, monitoring, and the security status of assets on your network. Automation and AI serve the customer well, issuing alerts when new devices join the network, highlighting agent deployment gaps, and monitoring device communication patterns for anything out of the ordinary.

White glove onboarding. Integrating new products and services into your operations might come with a learning curve. Proper onboarding is a critical step in getting started correctly and gaining your return on investment. An MSSP can assist with this onboarding process to help businesses implement and adopt the new technology faster.

How Does It Work?

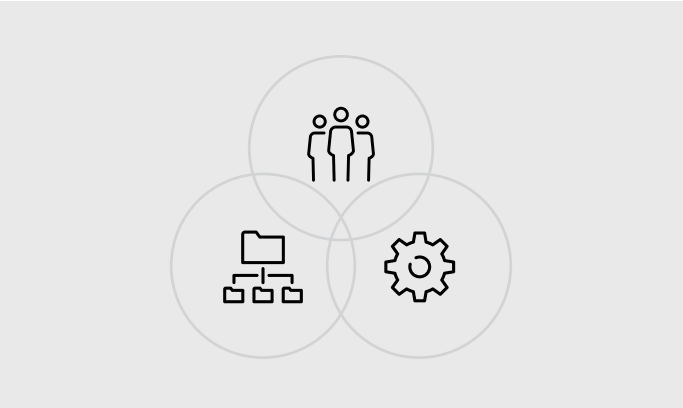
Implementing a managed endpoint security solution can be a complex process. Careful consideration should go into identifying and partnering with the right managed security service provider for your business. They should align with your business objectives and security architecture frameworks you have in place or are planning to implement. And, just as it is important to consider people, process, and technology for in-house, the same considerations should be addressed with a managed service:

Technology. First, the managed service should be built on the foundation of industry-leading endpoint security software technology. Utilizing top-of-the-line technology helps create more efficiencies within the SOC team, enabling them to be more effective. Software that incorporates AI and machine learning, and that can take independent action on endpoints are necessary to quickly neutralize threats. Your solution should provide the SOC team the tools to oversee and manage the entire attack chain, including to monitor, prevent, detect, and respond as needed.

Solutions that offer these abilities and can deliver orchestrated and automated response actions on the endpoint through deep platform and intelligence integration should be favored. They can better enable the SOC management team to detect more vulnerabilities, assess threats, and act faster, all with greater confidence and accuracy. A managed security service provider can also pull in strong intelligence tools such as the LevelBlue Labs Open Threat Exchange® (OTX). OTX is a threat data platform that allows you to collaborate with a worldwide community of threat researchers, helping you to stay ahead of the latest emerging threats, helping to deliver added context and threat detections. This can be especially helpful against today's sophisticated attacks.

Process. In addition to top-tier technology integration, a managed endpoint security provider should work closely with you during onboarding. Onboarding is a crucial time where businesses can configure the solution to best align with the business objectives. It is through proper policy configuration and system-tuning processes that the SOC team can create the right response rules given different attack scenarios. For example, you may have standard processes that would trigger a false positive; these could be filtered, suppressed, or excluded from your policy. You can create orchestration rules for situations where the response action would always be the same. A formal incident response plan will provide the framework for the SOC team to manage the threats your business faces in an efficient manner.

People. Finally, and most importantly, the individuals within the SOC team should be transparent and highly available, working closely with your personnel on communicating incidents and collaborating to achieve your security and compliance goals. These regular touchpoints should be clearly defined and documented as a part of the service. These analysts also bring visibility of the global threat landscape, bringing vital situational awareness to threat hunting and response.



Closing

Cybersecurity is a team sport. Working in silos, trying to manage endpoint security all in-house, or worse—not managing it—are no longer viable options. Businesses should look to a qualified solution provider to help evaluate the tools available and the level of management they want to perform in-house vs. outsourcing to experts. And it does not have to be an all-or-nothing decision. Many businesses perform some management in-house but augment their security staff with managed solutions to reduce the burden of managing endpoint security and help reduce the risk of compromise. Staff can then be re-deployed towards other important cybersecurity functions which helps overcome the cyber-skills shortage.

Protecting your business from cyber threats can seem overwhelming. However, a qualified MSSP can help you better understand the opportunities to better protect your business, fit for your unique needs today and in the future.

LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.