Malwarebytes

eBOOK

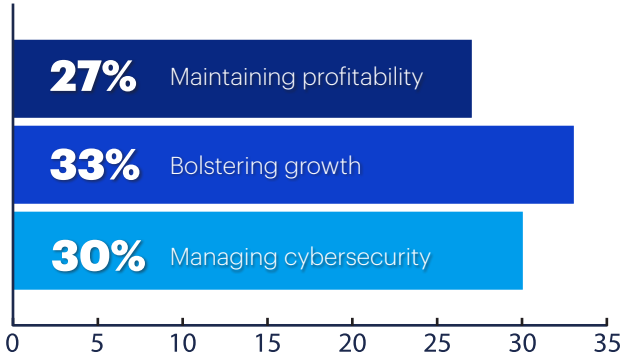
MSPs:

The 5 essentials from your endpoint security partner

Introduction

Managed Service Providers (MSPs) are an important part of the IT environment, providing the knowledge and the trusted partnerships that enable organizations of all sizes to embrace innovations made available by our era of digital transformation.

While there has never been a more exciting time to be an MSP, there are also many challenges MSPs must navigate to acquire and preserve long-lasting client relationships. Specifically, MSPs cite **maintaining profitability (27 percent)**, **bolstering growth (33 percent)**, and **managing cybersecurity (30 percent)** as some of their top business issues.[1]



1. Datto. State of the MSP Report. 2019.

When it comes to managing cybersecurity, safeguarding client endpoints is a critical piece of the MSP service offering. MSPs should have an endpoint security vendor that helps them overcome common issues that can cut into profits and lead to client churn.

Your selected endpoint security vendor should ensure that you can streamline your client deployments, simplify your ability to prioritize your response efforts, and manage your clients at scale. Ultimately, your vendor should optimize the efficiency of your time and efforts so that you can continue to grow your business and maximize revenue.

Selecting a vendor with these five, essential factors will empower your MSP business to operate efficiently and increase client loyalty.

Your vendor should:

1. **Simplify deployment** across multiple endpoints
2. Optimize time efficiency with **prioritized alerts and responses**
3. Automate **isolation and remediation** of infections
4. Make it easy to **manage your clients at scale**
5. Enable you to **demonstrate value to your clients**

1

#1: Simple deployment

Whether you're onboarding a new client or adding an endpoint for an existing one, deploying endpoint security software is an everyday occurrence for MSPs. If it doesn't go smoothly, it sets a bad, first impression for new clients, and the lengthy deployment cycles can consume your valuable service time. Therefore, it's important to prioritize partnering with an endpoint security vendor that makes new software deployments simple and fast.

Key capabilities

MSP teams have a variety of skill levels and experience, so there are a few things you should look for in your vendor to ensure deployments are a positive experience for both you and your clients.

#1: Simple deployment

Key capabilities

To support your team's preferred deployment processes, it's essential that the endpoint security software gives you multiple options for installation on your client endpoints, including active directory, SCCM, and third-party application deployment tools. And to work in your current and future clients' varied environments, look for a vendor whose product supports major operating systems, including Windows, Macintosh, and Linux. Equally important, the deployment process should minimize disruption so that your clients have an "invisible" experience. Ensure that your selected endpoint security product enables remote deployments and doesn't require a system restart following installation.

Once deployed, the solution should provide effective default group and policy configurations that protect your client endpoints while you develop and apply any additional policies that are tailored to their needs. The solution should also have a central console that immediately displays the new endpoint once it has been installed. Further, the vendor should provide a discovery tool that makes it easy to maintain an inventory of all endpoints on your client's network and the endpoint security software version that they are running.

#1: Simple deployment

Recommendations

The list below provides recommendations to simplify your deployment efforts:

- Select an endpoint security vendor that provides capabilities to perform bulk deployment across multiple endpoints within a client site
- Pick software with versions available to support Windows, Mac, and Linux operating systems
- Choose endpoint software that, right after installation, has default security policies to protect endpoints
- Choose a vendor that has a central dashboard that provides immediate visibility into your client endpoint deployments
- Use a discovery tool to identify all the endpoints on the client network and verify that the software versions are up to date

#2: Prioritizing alerts and responses

MSPs are remarkably busy, especially as team members often serve many roles—from sales and support to project management. Choosing the wrong endpoint security product can exacerbate this issue by generating an overwhelming volume of alerts that waste team members' time by looking into non-critical threats.

Your endpoint security solution-of-choice should enable you to stay laser-focused on the major threats, so you can be efficient in responding to high priority issues as they arise. A solution that empowers you to prioritize your time and response efforts will allow you to minimize the potential impact of an infection by mitigating lateral spread, reducing dwell time, and reducing the impact of the infection.

Key capabilities

MSPs can effectively manage their client's endpoint security response needs with a solution that provides effective detection capabilities and granular threat visibility to guide your response efforts.

2

#2: Prioritizing alerts and responses

Detection capabilities

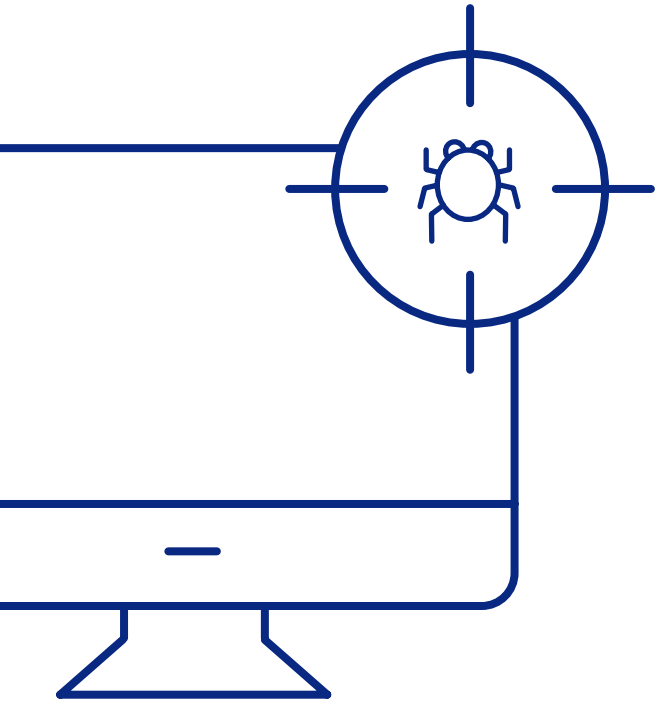
Your solution's detection engine should combine a blend of techniques. It should include traditional signature-based detections as well as advanced layers, such as application behavior and anomaly detection machine learning, to identify and respond to zero-hour threats. The solution should identify specific families of malware and categorize threats into standard levels of response actions so that your team can know what action to take, such as scanning, isolating, and remediation.

Visibility capabilities

An endpoint security solution that provides strong threat visibility will allow you to effectively coordinate your response efforts. This should come in the form of a "command center" dashboard that lets you clearly see endpoints with the highest risk threats, enabling you to quickly prioritize your time and actions.

The dashboard should let you sort and filter alerts by a group of endpoints that require immediate attention. Also, when it comes to varied MSP team skills and wondering what to do next, your solution should provide meaningful, suggestive actions on how to best respond to the threat (e.g., isolate now, remediate now).

#2: Prioritizing alerts and responses



Recommendations

MSPs should adopt the following mechanisms to optimize threat response efforts:

- Develop an incident response plan for common types of threats and infections
- Invest in an endpoint security platform with a detection engine that can identify zero-hour threats and their relative severity
- Ensure your endpoint security solution has a configurable dashboard that lets each team member highlight the priority threats (e.g., sorting tables of alerts, custom dashboard widgets, etc.)
- Create a policy for prioritizing endpoint response based on business criticality

#3: Isolating and remediating infections

3

One successful malware attack can wreak havoc on your client environments, moving laterally from the first infected endpoint to other machines. When an infection occurs, you need an endpoint security solution that lets your MSP team respond to the situation like a pro.

Time-consuming remediation approaches don't deliver efficient or rapid time-to-response and can quickly eat away at your profit margins. Your ideal endpoint security partner should provide automated threat isolation and remediation capabilities that allow you to quickly and efficiently contain the attack and restore your client's endpoints to their pre-infected, trusted state.

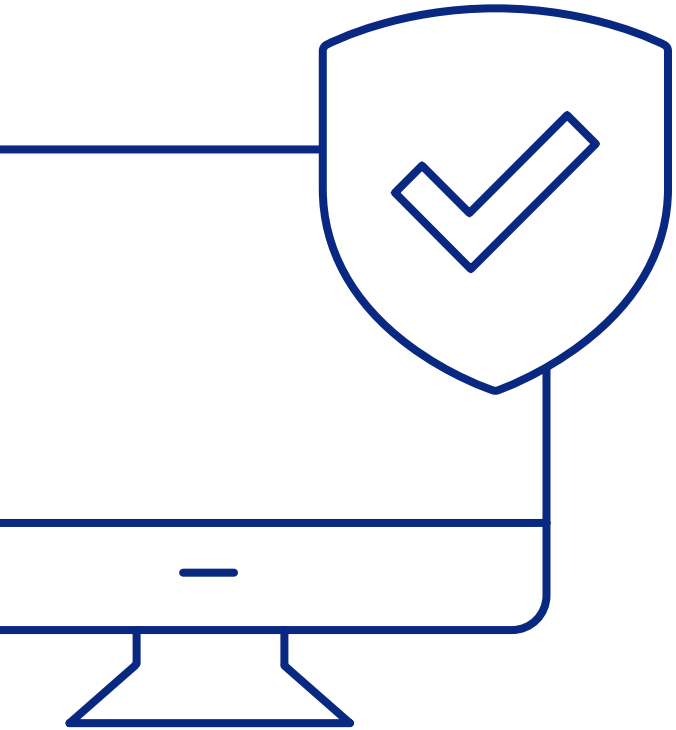
#3: Isolating and remediating infections

Key capabilities

Automation here is essential when choosing your endpoint security partner. Solutions that require lengthy and time-consuming remediation efforts will break an MSP's high-volume-low-touch revenue model and can lead to client dissatisfaction and churn. Automating your client's malware isolation and remediation processes will limit the malware from doing further damage and will significantly lower your response times.

MSPs also need a partner solution that provides automated recovery from ransomware attacks in its remediation arsenal. The endpoint security software should include just-in-time endpoint backups that allow you to wind back the clock to negate the ransomware attack's impact on your client's environment. Without this capacity, if a client gets hit by ransomware, you'll have the time-consuming project of restoring the impacted system from machine backups, which can take days. Automated ransomware rollback can handle the situation within minutes.

#3: Isolating and remediating infections



Recommendations

The list below provides tools and processes for your endpoint isolation and remediation efforts. We suggest you invest in an endpoint security partner solution that provides:

- Comprehensive isolation capabilities, including network isolation that restricts all endpoint-initiated processes from communicating, process isolation that prevents new processes from starting up on the endpoint, and device isolation that stops
- Ransomware rollback that immediately protects and restores encrypted, deleted, or modified files—returning the endpoint and valuable data to a known, good state
- Automated and thorough remediation that identifies and removes all artifacts associated with the primary threat payload

4

#4: Managing clients at scale

Without the right organizational tools, managing endpoint security for multiple client accounts can present a challenge for MSPs. This can especially be the case when it comes to managing high volumes of client endpoints. It's not simply enough for your endpoint security partner to have an effective solution—the vendor must also provide a management framework that makes it easy for you to run the business side of your endpoint security operations.

Your partner should make it simple for you to issue licenses for conducting pre-sales software demonstrations, adding endpoints to existing client environments, and onboarding new client endpoints. You'll also need visibility into your available licenses to ensure that you always have the desired amount on hand. To support this, your vendor should provide current data that allows you to keep an accurate count of your consumed versus available licenses. Further, it's important to confirm that your vendor has a simple process for upgrading or downgrading software products (i.e., moving to other products within the vendor's portfolio) to suit your clients' changing needs.

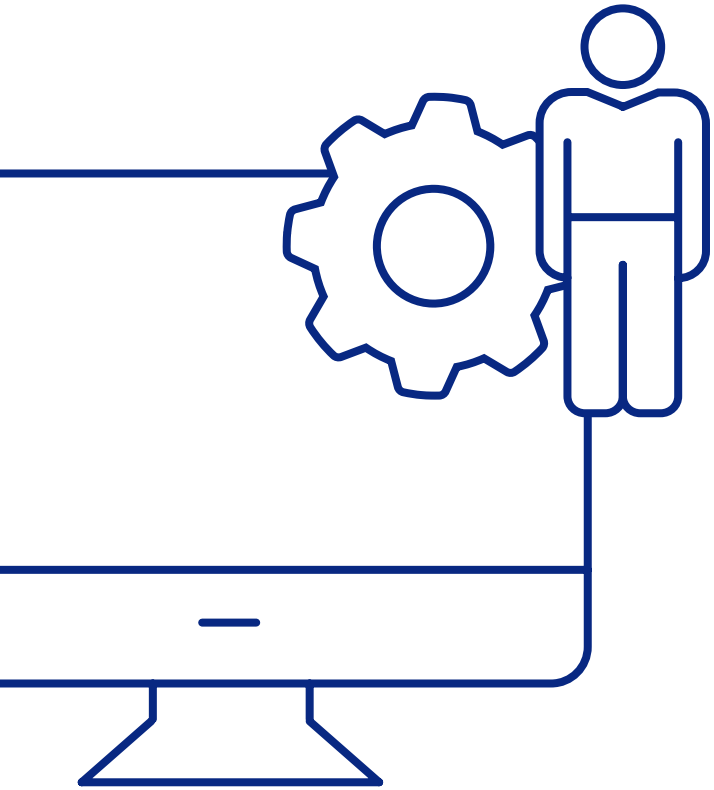
#4: Managing clients at scale

Key capabilities

You should carefully review an endpoint security vendor's ability to support your MSP business and your clients at scale. Look for a vendor that provides multi-tenant management of your client sites, including users and endpoints, through a central console. Rather than relying on a cumbersome process of accessing separate dashboards for each client, this approach will empower you to efficiently manage your clients from a single place.

The console should provide current status and reporting on your client sites, as well as provide user permissions that allow your clients to see their endpoint data. Your vendor should also have a flexible licensing model that lets you manage and quickly provision all your clients from a single shared license pool.

#4: Managing clients at scale



Recommendations

MSPs should choose an endpoint partner with the following capabilities to manage clients at scale:

- Select an endpoint security platform that provides multi-tenant management of clients through a single user interface
- Ensure endpoint security licenses are immediately available for your demonstrations, evaluations, and new client provisioning
- Select an endpoint security platform that provides intuitive, point-and-click control for upgrading or downgrading software versions, license pools, and role-based access of client users

#5: Demonstrating value to your clients

Conveying the value of your MSP business is essential to drive growth and profitability. If clients are not fully aware of the value that your endpoint security service provides, it can be difficult to navigate conversations about renewing the service or upgrading to premium software offerings. When it comes to demonstrating value to your clients, the saying “show, don’t tell” holds true. Metrics from your endpoint security partner will make this possible.

The value of your endpoint security services can be shown with data on the number of threats your MSP detected and remediated over time for clients. Context makes this data more meaningful and relevant, so your endpoint security vendor’s reports should provide clear descriptions that allow your clients to fully grasp the severity and volume of the threats that were prevented from impacting their staff productivity and business operations, which, in turn, will help them understand the value of your service.

5

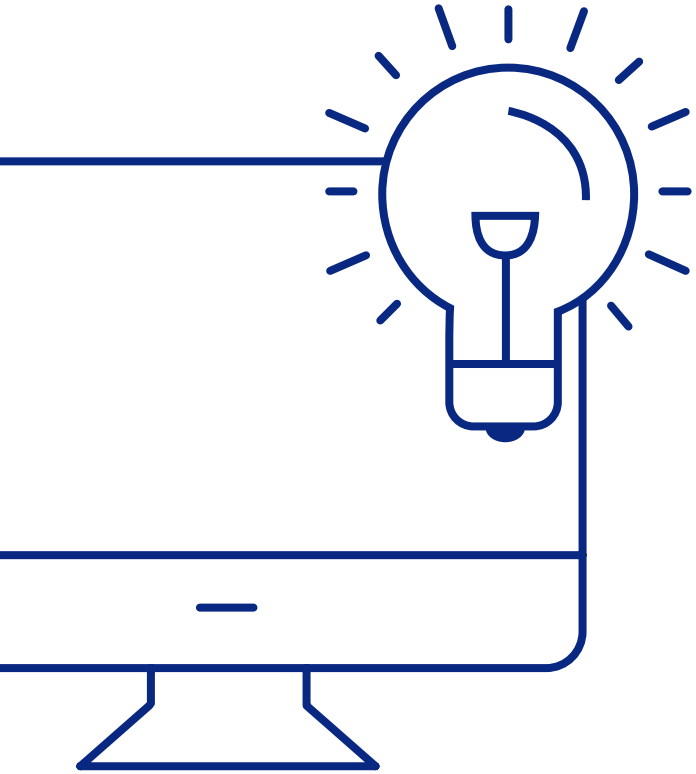
#5: Demonstrating value to your clients

Key capabilities

Your endpoint security vendor should provide a wide range of reporting capabilities that show your customers the value of your endpoint security service. Your vendor should have time-based, summary reports that detail the number of detections and remediations, along with top malware families and endpoints that are most at risk. Your clients should also have access to this data, as desired, so your vendor should provide a self-service option that allows your clients to generate reports on their own sites and endpoints.

Sending your clients regular reports, such as quarterly endpoint security health updates, should not be a time-consuming process. Your ideal vendor should streamline this for you by providing branded reports that are automatically generated and emailed to your clients on your behalf.

#5: Demonstrating value to your clients



Recommendations

MSPs should adopt the following mechanisms to demonstrate value:

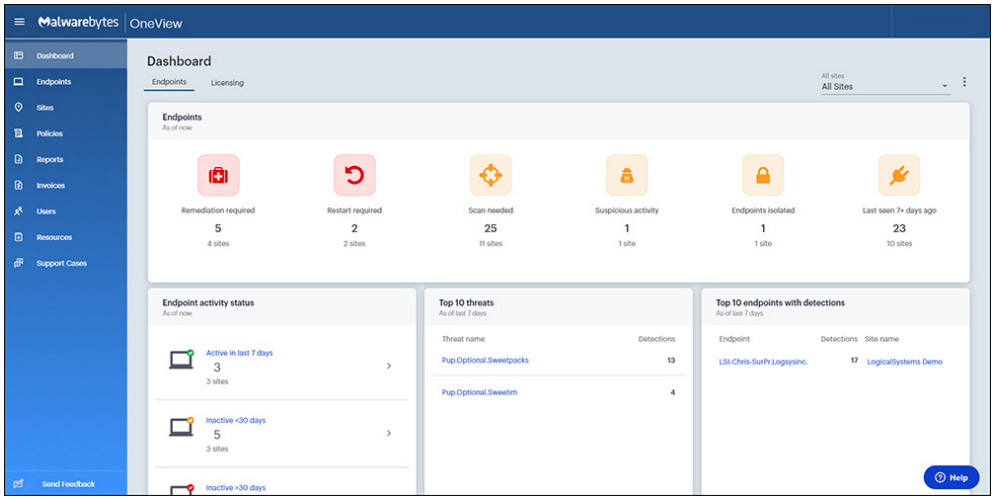
- Select an endpoint security vendor that provides reports summarizing your MSP security activities, per client, and over time
- Train your MSP team on your best practices for delivering reports to your clients, including any narrative they should include to convey the value of specific data
- Develop materials, such as case studies, that can educate your clients on the potential impact of the high-severity infections that your endpoint security service caught and remediated
- Include an action plan on how your MSP can enhance the client's security practices to protect them from the rising volume of new malware threats

Making MSPs successful

At Malwarebytes, our MSP partners are a top priority. We've taken direct input from our partners and given thoughtful care to creating a solution and program that is tailor-made for our MSP partners' success. When you select Malwarebytes as your endpoint security vendor-of-choice, you not only get a best-in-class endpoint security solution, you get all of the essential client management and partner resources to accelerate growth, remain cutting edge, and deliver on your clients' expectations.

Centralized client management

Malwarebytes OneView provides centralized management of your client's endpoint security, licensing subscriptions, and endpoint reporting.



With Malwarebytes OneView, you get client management and monitoring that is a breeze.

The multi-tenant console enables you to streamline operations with centralized management of client endpoints, license subscriptions, reporting, and global policies.

With an intuitive display of client sites and licenses, OneView allows you to easily track and manage client license subscriptions across sites and provide a higher level of service and attention.

Best-in-class endpoint security solutions

Our cloud-based endpoint security portfolio provides a broad range of solutions that can support your clients—large or small—all from a single user interface:

Malwarebytes Incident Response

Threat detection and remediation tool that scans networked endpoints for advanced threats and thoroughly removes them

Ideal for your clients with fewer endpoints and a low volume of cyberattacks.

Malwarebytes Endpoint Protection

Advanced endpoint threat prevention solution that uses multiple detection techniques for full attack chain protection

Great for your clients who experience frequent attacks and malware infections.

Malwarebytes Endpoint Detection and Response

Modern endpoint detection and response that makes it easy to quickly investigate, isolate, remediate, and recover from threats

Perfect for your clients who are risk adverse and are high-value targets of ransomware and other cyber threats.

Experience the advantages

The Malwarebytes cloud-based architecture and flexible deployment options make it simple for you to onboard new clients, even across sites and multiple endpoints. And, your clients will receive integrated, proactive security with automated threat detection and protection—across web, memory, application, and files—that applies adaptive detection techniques, including behavioral monitoring and cloud-based machine learning.

In the event of a successful attack, our solution's active threat response capabilities optimize your MSP cost efficiency with effective threat response at a fraction of the cost of endpoint reimaging. Malwarebytes provides automated, granular attack isolation to prevent the attack from spreading, and, our "one-and-done" remediation maps the correct path to permanently remove all traces of the malware. With Malwarebytes, your MSP team can manage response efforts with the greatest of ease and efficiency.

Our tailored partner program

The Malwarebytes Managed Service Provider (MSP) Premier Partner Program (MP3) provides a powerful framework for you to meet the security needs of your clients. We know it's important that your preferred endpoint security vendor maximizes your efficiency and increases your bottom line. To achieve these goals, our MSP Premier Partner Program (MP3) focuses on providing our partners:

Ease of doing business

We provide you with simple, responsive selling tools that are accessible in your portal, including a resource center for on-demand collateral and creative co-marketing that helps you generate more leads.

Accelerated profits and growth opportunities

Our dedicated sales, marketing, and technical resources enable your sales team to deliver the products and services your clients need—priced and licensed how they want.

Grow your business with flexible licensing

Our flexible "pay as you grow" and "pay as you go" licensing model or Malwarebytes USM solutions, whether managed by you or your client, offer more opportunities for you to position your brand as the trusted security advisor that clients need.

Learn more

For more information about
the Malwarebytes MSP Program:
malwarebytes.com/msp