IDC

SPOTLIGHT

Sponsored by: Kaseya

This document explores the endpoint detection and response needs of small and medium-sized businesses and examines the ability of managed service providers to address them.

Plugging the Antivirus Gap for Small and Medium-Sized Businesses: Endpoint Detection and Response for Everyone

January 2025

Written by: Mike Jude, Ph.D., Research Director, Endpoint Security

Introduction

The cybersecurity threat is increasing and becoming much more sophisticated. The introduction of AI-enabled attacks will accelerate and improve the effectiveness of attack vectors. This will pose a challenge for even the largest enterprises.

Yet the threat isn't particular — it targets not only large enterprises but also small and medium-sized businesses (SMBs). In fact, SMBs are perhaps a more attractive target for bad actors.

SMBs are generally able to devote fewer resources to cybersecurity as they often cannot afford critical cybersecurity functionality or cannot acquire cybersecurity expertise. As a result, one of the most prolific employers of professional labor and the primary source of innovative ideas is minimally unprotected.

AT A GLANCE

WHAT'S IMPORTANT

- SMBs are highly vulnerable to cybersecurity threats.
- EDR is essential but challenging for SMBs.
- MSPs play a key role in SMB cybersecurity.

KEY TAKEAWAYS

- AI-driven threats amplify risks for SMBs.
- MSPs must adapt to SMB needs.

Of course, this deficiency can be addressed. Managed service providers (MSPs) have an opportunity to provide solutions to this largely underserved market as they can expand their offerings from purely endpoint-focused solutions and deliver endpoint detection and response (EDR), which SMBs increasingly need. However, not all security solutions are optimized for the SMB space. Complex and expensive solutions are anathema to small businesses.

This document explores the EDR needs of SMBs and examines the ability of MSPs to address them. The intent is to inform decision-makers and MSPs about the dynamics shaping this market.

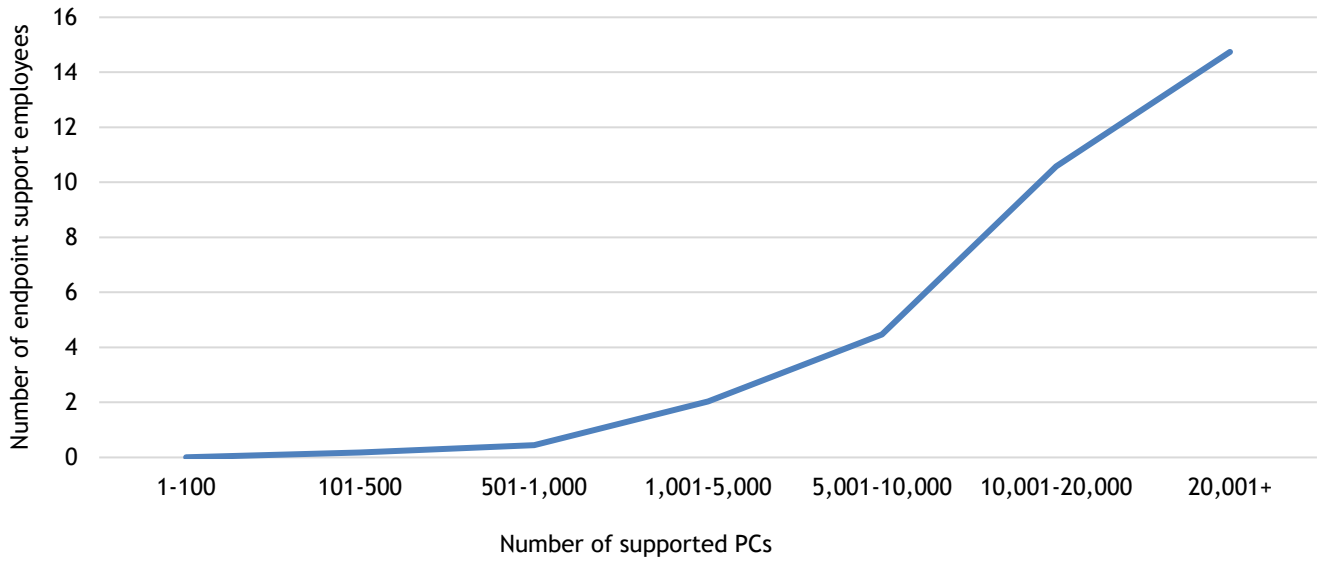
Benefits

The Virtues of EDR in Addition to Antivirus/Antimalware

Antivirus (AV) and antimalware (AM) protection traditionally defined cybersecurity for individuals and small businesses. This is not a bad thing, but it is a limited solution when considering the needs of businesses. While AV/AM seeks to prevent malware attacks by detecting and blocking them, it does not provide the capability to detect and respond to higher-level attacks that may appear legitimate in a purely malware-oriented security scheme. EDR provides this capability because it monitors the endpoint space for attacks, traces the progression of those attacks, and then provides the capability to ameliorate their impact.

EDR, in fact, acts as a force multiplier — rather than presenting security personnel with a barrage of alerts (with little context and no capability to respond), it enables a few security personnel to do the job of many. As Figure 1 demonstrates, the amount of support needed scales almost exponentially as the number of endpoints grows. Clearly, a better approach is necessary.

FIGURE 1: ***Protecting the Endpoint — Resources Don't Scale Linearly***



Source: IDC's Corporate Endpoint Protection Survey, 2024

While throwing more people at the problem may work for enterprises, SMBs do not have the luxury of adding increasing numbers of cybersecurity personnel to manage the endpoint. Large enterprises and especially SMBs need a better solution. EDR delivers this solution, but in many cases it is beyond the ability of SMBs to adopt.

Why an Enterprise EDR Solution Is Not Necessarily the Right Choice for an SMB

EDR has evolved into an essential tool for enterprises to manage their cybersecurity. There are many solutions on the market that provide detections and responses at scale. Tools are often self-managed by the business, but increasingly, they are offered to the market as a managed service. Based on recent surveys, IDC estimates that as much as 43% of the enterprise market utilizes managed EDR services to some extent.

However, such enterprise-oriented EDR solutions are not necessarily the right choice for MSPs seeking to engage with SMBs. There are several reasons for this — resources, the complexity of existing solutions, scalability, awareness, integration with existing systems, the impact of evolving threats, and limited in-house experience. Each is discussed briefly as follows:

- **Resource limitations:** Many SMBs operate with limited budgets and resources, which can restrict their ability to invest in comprehensive EDR solutions. MSPs must find ways to provide effective security without overwhelming their clients' financial capabilities.
- **Complexity of EDR solutions:** The evolving landscape of EDR solutions can be complex, making it difficult for MSPs to choose the right tools that align with the specific needs of SMBs. This complexity can lead to challenges in implementation and management.
- **Scalability issues:** As SMBs grow, their IT needs change. MSPs must ensure that the EDR solutions they implement can scale seamlessly with the business. This requires careful planning and foresight to avoid disruptions during expansion.
- **Awareness and education:** Many SMBs may not fully understand the importance of EDR or the specific threats they face. MSPs often need to invest time in educating their clients about the value of EDR solutions and the potential risks of not having them in place.
- **Integration with existing systems:** Integrating EDR solutions with existing IT infrastructure can be challenging. MSPs must ensure compatibility and smooth operations across various systems, which can require significant technical expertise.
- **Management of evolving threats:** The cybersecurity landscape is constantly changing, with new threats emerging regularly. MSPs must stay updated on these threats and continuously adapt their EDR strategies to effectively protect their SMB clients. Although many MSPs understand this, many do not, or they view the need to offer EDR solutions to their customers as complex and expensive.
- **Limited in-house expertise:** Some SMBs lack the in-house expertise necessary to manage EDR solutions effectively. MSPs need to provide not only the technology but also the necessary support and training to ensure that their clients can utilize these tools effectively.

Taken together, these reasons can overwhelm MSPs and their SMB customers. Yet EDR is a logical next step on the cybersecurity continuum for any sized business. In addition, cyberthreats are evolving quickly, making taking this step more critical than ever.

Trends

Several evolving trends will drive the SMB market to adopt more comprehensive EDR solutions. Chief among them are the increasing threat of AI and the trend of SMBs to seek cybersecurity solutions from their MSPs.

AI Will Amplify the Threat

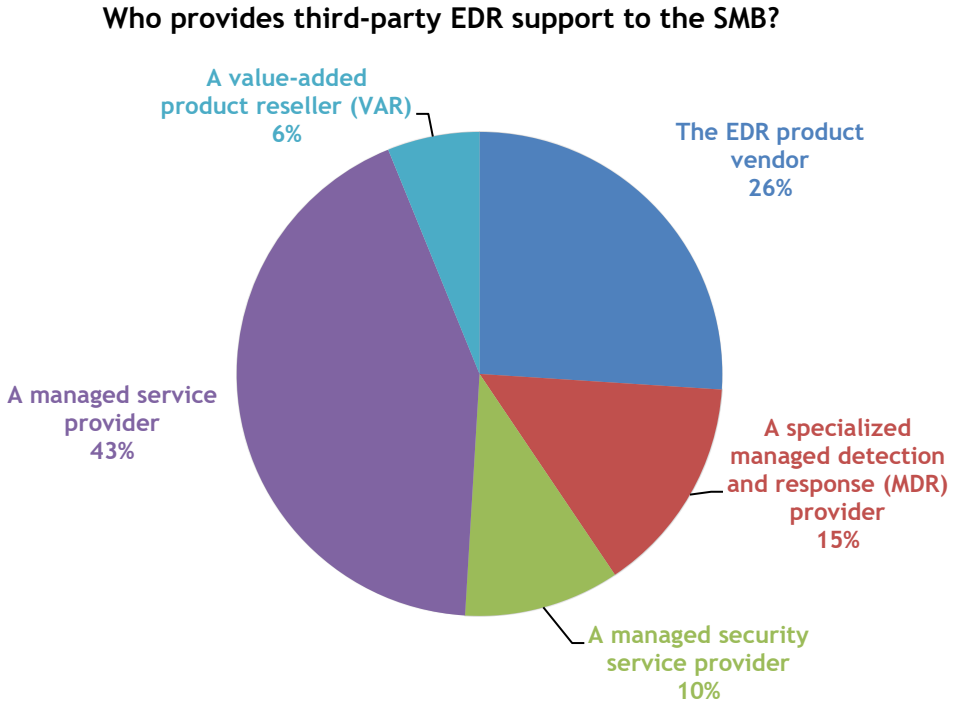
Cybersecurity professionals tend to think in terms of the advantages of using AI technologies to improve detection, presentation, and analysis; however, the more immediate impact is the use of AI to improve threat vectors. For example,

AI as an aid to phishing attacks enables phishing at scale with believable and often successful inducements to compromise cybersecurity safeguards. This can overwhelm EPP, even for large organizations. However, for smaller companies, AI can prove to be a devastating advantage in the hands of bad actors.

SMBs Will Increasingly Look to Their Suppliers for Cybersecurity Support

Of course, SMBs understand their cybersecurity preparedness, but their ability to internally manage security is often constrained. This has led many smaller companies to turn to third parties for cybersecurity support. As Figure 2 illustrates, SMBs often utilize value-added resellers, EDR product vendors, managed detection and response (MDR) providers, and managed security service providers for cybersecurity support. However, by far the most utilized source of third-party support is a MSP. Forty-three percent of respondents to a recent IDC survey reported that they use a MSP to support their cybersecurity efforts.

FIGURE 2: ***SMBs Depend on Third-Party Support***



Source: IDC's Video Surveillance Survey, February 2023

However, this dependency on MSPs is not a panacea. MSPs that support many businesses often default to providing EDR solutions that are easy to maintain and cost effective to offer but that only address the most basic of customers' cybersecurity needs. Enterprise-grade cybersecurity is often not available at all or not at a reasonable price for SMBs. The responsibility lies with MSPs that wish to do business within the SMB market to deliver reasonably priced EDR and easy-to-use solutions to their SMB customers.

MSPs must tailor EDR solutions that enable SMBs to achieve enterprise levels of cybersecurity. These solutions must be easy to implement and maintain. For those SMBs that are resource constrained, EDR should also be available as a managed service.

Considering Kaseya

One vendor that has designed a product set to help MSPs profitably address the SMB market is Kaseya. Kaseya is focused on MSPs that need to deliver cybersecurity solutions to the SMB market. This outlook balances the needs of SMBs to manage an enterprise-level cybersecurity threat with the needs of MSPs to deliver services cost effectively. To this end, Kaseya offers a comprehensive suite of cybersecurity solutions. Among these are security solutions, unified continuity solutions, networking solutions, and business management tools. In detail:

- **Security solutions:** These include EDR, AV/AM, and MDR. Individually, these products provide robust protection, but as a portfolio they provide a comprehensive solution set that covers the most prevalent security threats.
- **Unified continuity and file backup:** These include file backup and sync solutions. These are essential for protecting critical data and ensuring quick recovery in cases of data loss.
- **Networking solutions:** These offerings are designed to ensure secure and reliable connectivity.
- **Business management tools:** These tools assist MSPs in managing their operations effectively.

Kaseya has purposefully built a portfolio that a MSP can use to build SMB-oriented services. These services are well-integrated and promote an ease of use that is attractive to MSPs and SMBs.

Challenges

Kaseya's approach is not without its challenges. Chief among these is the fact that it is competing in a crowded field with many similar offerings. Although there are benefits associated with Kaseya, they can be lost in the background noise of many competing value propositions.

Kaseya must demonstrate a value proposition that resonates with its MSP customers and articulates an approach to EDR that is compatible with end-user customers. This is possible but requires demonstrating that the solution set is materially different and superior to competing brands and alternatives.

Conclusion

As cybersecurity threats grow increasingly sophisticated, particularly with the rise of AI-enabled attacks, SMBs face significant challenges in protecting their IT assets due to limited resources, expertise, and budgets. MSPs have emerged as essential partners in bridging this gap, offering scalable, tailored solutions such as EDR to address the needs of SMBs. However, the complexity, cost, and scalability of enterprise-grade EDR solutions often make them ill-suited for SMBs, requiring MSPs to innovate and provide affordable, easy-to-implement managed services. SMBs' growing reliance on MSPs for cybersecurity solutions highlights a critical opportunity for providers such as Kaseya. By offering cost-effective, streamlined, and scalable EDR solutions, MSPs can significantly enhance SMB cybersecurity preparedness, especially as AI-driven threats continue to evolve.

About the Analyst

Michael Jude, Ph.D., *Research Director, Endpoint Security*

Mike Jude is the research director for endpoint protection and EDR within IDC's Cybersecurity Products Group. Dr. Jude's core research coverage includes consumer digital life protection (CDLP) as well as modern endpoint protection for the enterprise. Jude also covers the rise of EDR solutions and their evolution into the XDR space. He has been with IDC for five years, following roles in many other analyst firms as well as industry.

MESSAGE FROM THE SPONSOR

Datto, a Kaseya company, delivers robust, scalable, and reliable Backup and Disaster Recovery (BCDR) solutions alongside Remote Monitoring and Management (RMM), PSA, SaaS Backup, Networking, and advanced cybersecurity solutions. Datto Endpoint Detection and Response (EDR) is independently verified and proven as a leader against malware and advanced threats. Miercom, a global leader in cybersecurity testing, found that Datto EDR detects and stops 99.62% of all malware when combined with Datto AV. Request a Demo of Datto EDR here: https://www.datto.com/request/datto-edr/.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com