ANALYST CONNECTION

Sponsored by: Datto

Small and medium-sized businesses face the same cybersecurity threats that large enterprises do, but with significantly fewer resources. Endpoint detection and response solutions help SMBs meet the threat while reducing cybersecurity overheads.

Endpoint Detection and Response: A Necessary Tool to Augment Endpoint Protection

October 2024

Questions posed by: Datto

Answers by: Mike Jude, PhD, Research Director, Endpoint Security

Q. What are the key factors driving the adoption of endpoint detection and response (EDR) solutions among organizations today?

A. Endpoint protection is becoming more problematic as threats from bad actors increase over time. Organizations are finding that cybersecurity is growing more complex at the same time that they are being pushed to digitize their operations. As a result, endpoint detection and response solutions are being adopted to address the gaps in cybersecurity that these dynamics introduce.

IDC research indicates that the number of technical personnel needed to secure the endpoint rises in a nonlinear way as the number of vulnerable devices increases. While such complexity may be addressable by large organizations, small and medium-sized businesses (SMBs) may not have the resources to keep up with the increased need to manage the endpoint. EDR can help SMBs keep up with this complex threat environment. EDR is essentially made up of three functions:

- **Assess:** Determine whether an attack is happening
- **Monitor:** Provide real-time detection of advanced threats and provide root cause analysis to aid in a response
- **Respond:** Isolate compromises and launch dynamic or scripted responses

EDR also helps organizations cope with the gaps that can be introduced by digital transformation. Both large and small businesses employ digital technologies to improve business efficiency. However, such digitization often exposes an organization to the increased potential for cyberattacks as new systems are brought online. EDR solutions can plug these gaps, providing breathing space for the security operations center (SOC) as new systems are introduced and tested.

In addition, cybercriminals are now more sophisticated, utilizing cutting-edge technologies to design and launch new attacks. As their techniques and procedures for penetration evolve, organizations of any size, but especially SMBs, are challenged to keep up.

The bottom line is that as bad actors focus on the endpoint, SMBs are increasingly their target. Attackers know that SMBs may have weaker defenses, yet their data is just as valuable as that of larger businesses. This drives the need for advanced detection and response capabilities, especially at the endpoint. EDR solutions can provide this coverage.

Q. Antivirus (AV) has been the traditional go-to security solution for many years. Where does an EDR fit into that picture? Is it needed in addition to antivirus?

A. While antivirus solutions have been very successful in reducing the volume of known threats constantly bombarding businesses of all sizes, AV has been less successful in detecting and responding to new and novel threats. EDR helps address this by adding a much-needed layer of defense, complementing AV, so that endpoints are better defended against multistage attacks.

EDR detects and responds to more complex multistage attacks that are likely to evade AV solutions. These advanced persistent threats (APTs) are increasingly the approach preferred by cybercriminals. Without EDR to identify the attack and trace the kill path to its origin, an attack that initially seems contained can persist in the organization's computing ecosystem, where it can continue to compromise valuable data.

EDR uses behavioral analytics to catch threats that can evade traditional signature-based antivirus. With the advent of AI-enabled cyberattacks, the ability to monitor threats that can evade antivirus but violate expected user behaviors is a critical defense against compromise.

It bears noting that SMBs are faced with the same threats with which large enterprises must deal, yet they may not have the same expertise or resources. EDR is essential for small businesses for reasons including proactive threat detection, comprehensive security coverage, incident response capabilities, visibility and insights, cost-effective security, and adaptability to evolving threats.

Q. What are the main differences between solutions designed for large enterprises versus those tailored to meet the needs of small and midsize businesses?

A. From a business perspective, SMBs and larger enterprises are similar and worry about similar things, such as revenue, costs, and operations. Despite having these general objectives, an SMB often has fewer resources with which to achieve them. This drives SMBs to seek cybersolutions that emphasize simplicity, cost, and ease of adoption.

In the case of simplicity, the more complex the cybersecurity solution, the more resources that need to be devoted to implementing and maintaining it. Large enterprise solutions often come with complex configurations and resource-heavy features that may overwhelm SMBs. A complex solution may require more training to utilize, delaying its benefits until the organization comes up to speed.

Cost, of course, is a universal concern. However, there can be more to cost than the sticker price of a particular EDR solution. It can also include intangible impacts such as the need for additional trained technical staff. SMB-focused solutions are typically more cost-effective without sacrificing critical functionality.

SMBs also need solutions that are easy to deploy and manage, offering protection without large IT overheads. This is in keeping with the idea of simplicity and cost-effectiveness. A complex solution that requires professional services from the vendor to implement may be more than an SMB can accommodate. "Out of the box" solutions are desirable.

Q. Alert overload is a common consequence of most EDR offerings. By default, these tools require advanced security training and years of experience to identify indicators of compromise. How can administrators and analysts reduce EDR noise and the resulting volume of alerts?

A. A common issue among SOC support staff is the unrelenting volume of alerts. As noted, a senior security professional requires years of training and extensive on-the-job experience. With the constrained labor pool for cybersecurity professionals, acquiring this kind of talent can be beyond an SMB's means.

Especially for SMBs, an EDR solution can take the place of some of this expertise and training. It can do this by utilizing the MITRE ATT&CK model to identify and understand the alert. It can also utilize a "canned" experience to focus on the most important alerts. Finally, adding a managed defense and response service to the EDR solution can leverage industrywide expertise to identify emerging alerts.

Q. What criteria should small and midsize organizations consider when evaluating an EDR solution?

A. When it comes to EDR solutions, one of the most critical considerations is the vendor. Does the vendor offer comprehensive threat detection capabilities, ease of implementation and integration, scalability, support, and training? What about cost-effectiveness, reputation and reliability, customization and flexibility, and compliance and reporting features?

Beyond the laundry list of considerations — all of which apply to large enterprises as well — does the vendor have experience in the SMB space? Does the solution have the scalability to grow with the SMB, or does an organizational change require a rip-and-replace upgrade? The solution should scale with the business without requiring constant upgrades or additional complexity.

Finally, does the vendor have comprehensive support and service? IDC surveys constantly reinforce the notion that a vendor that provides excellent support, even if the solution has problems, is valued over those that don't. A vendor that listens and is available will provide assurances that the EDR solution will be there when needed.

About the Analyst

Mike Jude, PhD, *Research Director, Endpoint Security*

Mike Jude is a research director for IDC's Endpoint Security practice within the Security and Trust group. Dr. Jude's core research coverage includes solutions that defend personal computing devices, physical servers, and mobile devices against a widening array of cyberattacks.

MESSAGE FROM THE SPONSOR

Sponsored by Datto, a Kaseya Company

Tailored for today's MSP and SMB, Datto EDR provides effective endpoint detection and response in an affordable, easy to use, manage and deploy package. Unlike other EDR products that are built for large-scale enterprise SOC teams, Datto EDR eliminates common EDR issues, such as high-cost, management complexity and alert fatigue. Each alert comes with a quick, easy-to-execute set of response guidelines to support your team in isolating infected hosts, terminating processes, and collecting additional evidence. Learn more at https://www.datto.com/.

IDC Custom Solutions

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

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.