Enterprise Strategy Group | Getting to the bigger truth.™

ESG RESEARCH REPORT

Security Megatrends and Their Impact on Endpoint Security

By Dave Gruber, Senior Analyst; and Bill Lundell, Director of Syndicated Research

December 2021

This ESG Research Report is brought to you in its entirety and without modification courtesy of

IBM Security

Contents

List of Figures

Executive Summary

Report Conclusions

ESG conducted an in-depth survey of 359 IT and cybersecurity professionals responsible for evaluating, purchasing, and managing endpoint security products, processes, and services. Survey participants represented midmarket (100 to 999 employees) and enterprise-class (1,000 employees or more) organizations in North America (United States and Canada).

Based upon the data gathered as part of this project, the report illustrates:

- IoT and personal devices are expanding the endpoint security market opportunity. As the mobile threat landscape grows, more than half of cybersecurity professionals report that their organization protects corporate-owned mobile devices with its endpoint security platform. Additionally, with no end in sight for the work-from-anywhere model, nearly half now want help securing non-corporate, employee-owned devices, whether laptops and desktops or mobile devices. IoT projects are accelerating, supporting both corporate functions like office automation and facility management as well as more traditional industrial devices that are responsible for operating manufacturing and critical infrastructure.

- DLP and endpoint management are converging with endpoint security. While prevention, EDR, and web security remain foundational to endpoint security needs, securing local data has taken on an increased level of importance. As such, more than three-quarters think data encryption will help, while more than two-thirds want specific data leakage protection capabilities. More than half think endpoint management and endpoint security capabilities align and would fit nicely together in a single solution.

- Zero trust and XDR initiatives are causing many to upgrade endpoint security. Nearly three-quarters of organizations have already committed to zero trust or are underway with their implementation. And since device-level security is a core component of a zero trust architecture, it follows that three-quarters have an active project to upgrade their endpoint security solutions to facilitate their zero trust strategies. As organizations consider XDR, nearly half think it will replace their EDR solutions either immediately or within a year.

- EDR vendors are preferred for XDR, and most think their current EDR provider can deliver XDR. Many organizations are already loyal to their EDR solution providers and therefore will consider XDR options from those same vendors before looking elsewhere. Beyond sentiment, more than half are already working with their EDR provider to evaluate their XDR offering, while another 41% have plans to do so. While the efficacy of prevention continues to be critical to the success of endpoint security programs, improving detection and response leads the pack when it comes to what is top of mind for endpoint security buyers.

- Microsoft is now a serious contender for most organizations, threatening incumbent solutions. Microsoft continues to advance endpoint security capabilities, motivating almost two-thirds of respondents to consider Microsoft's native endpoint security controls as their primary solution. Attractive bundling and pricing options are motivating many, with Microsoft Defender for Endpoint included within the E5 bundle.

- Endpoint security spending is up, and a majority plan to change out current endpoint security solutions. Three-quarters of organizations will increase spending on endpoint security in the coming 12 months. More than two-thirds either recently replaced their solution or are in the process of investigating a converged endpoint security platform to reduce complexity or costs. However, half still say that they prefer best-of-breed security solutions whenever possible.

Introduction

Research Objectives

Cybersecurity megatrends, including zero trust, XDR, a pandemic-induced increase in remote workers, and the move to public cloud, are influencing the way organizations think about endpoint security. These megatrends add new requirements for endpoint security, while necessitating new levels of integration with other core security controls. Additionally, mobile and IoT are driving massive growth in the number and diversity of devices that must be protected. To better secure their growing attack surface, IT and security teams are thinking differently about endpoint security platforms, what they must include, and how they fit into the broader security stack.

Native, operating system-level endpoint security controls and their evolving security platforms are challenging standalone endpoint security vendors. As Microsoft gains ground, buyers are facing pressure to reevaluate investments to find cost savings through platform providers, though new opportunities are emerging for supplemental solutions that close gaps left by these providers. As advanced threats push security controls to their limits, SOC teams are struggling to detect and respond. The XDR movement has promised to address this issue, providing new levels of detection and response leveraging telemetry from multiple security controls.

In order to gain insight into these trends, ESG surveyed 359 IT and cybersecurity professionals at organizations in North America (United States and Canada) responsible for evaluating, purchasing, and managing endpoint security products, processes, and services.

This study sought to answer:

- What devices and workloads are currently protected and secured by endpoint device security solutions?
- What types of IoT devices do organizations currently, or expect to, protect with endpoint security solutions?
- Would organizations like to see endpoint security and endpoint management capabilities converge and become part of an integrated endpoint security solution?
- Would organizations be willing to change out their endpoint security solutions if it could help accelerate zero trust implementations?
- What impact is XDR expected to have on EDR solutions? What are the most critical capabilities that XDR must provide before organizations would consider decommissioning their EDR solutions?
- What are organizations' current positions on how Microsoft Defender will likely fit into future endpoint security strategy and endpoint protection platform (EPP) decisions? What weaknesses, if any, are perceived with Microsoft Defender?
- Relative to other areas of cybersecurity, how do organizations expect endpoint security spending to change, if at all, over the next 12 months? Do organizations have an active project underway, or one in the planning phase, to replace its current endpoint security solution(s) with a consolidated endpoint security platform?

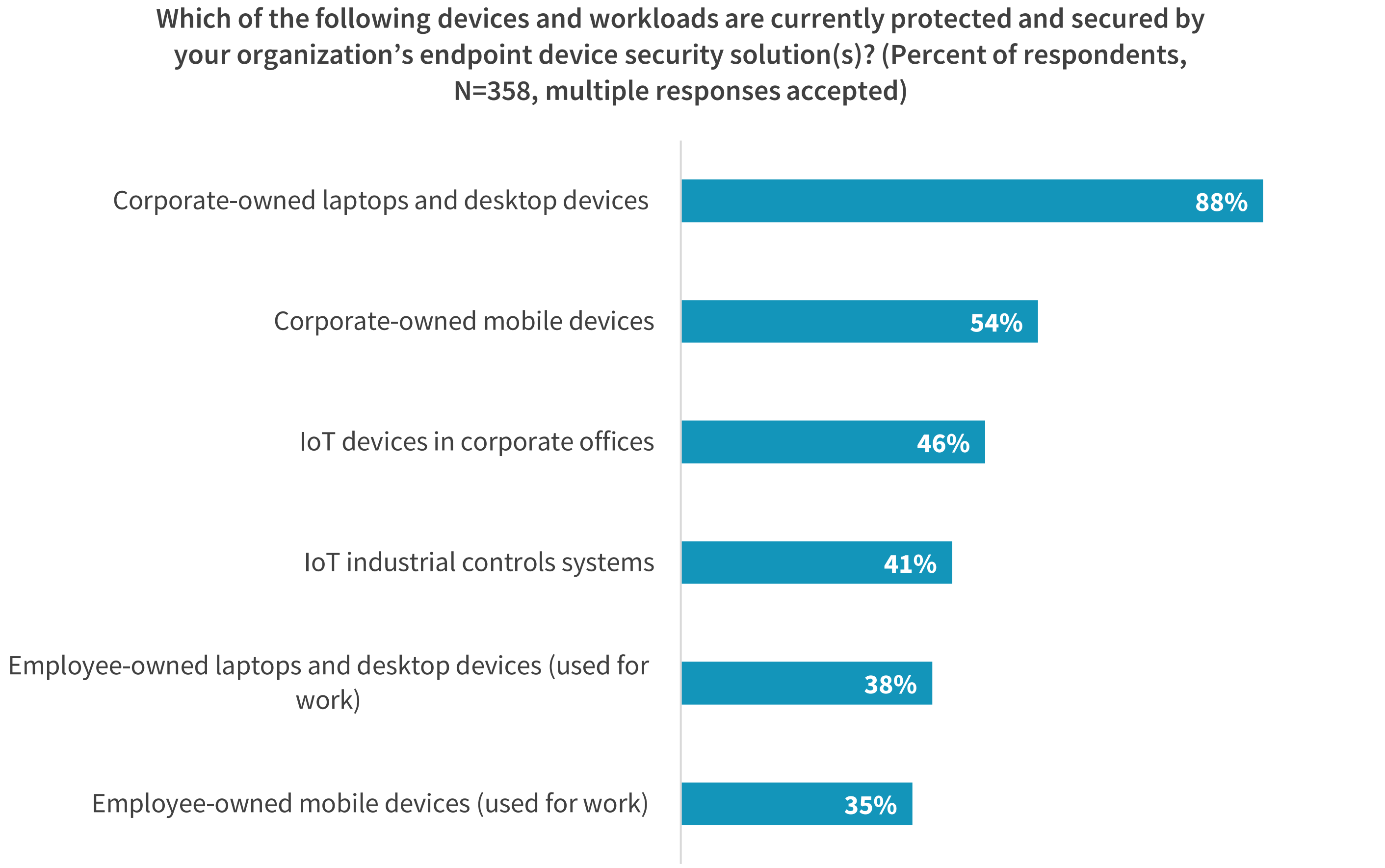
Survey participants represented a wide range of industries including manufacturing, financial services, healthcare, communications and media, retail, government, and business services. For more details, please see the Research Methodology and Respondent Demographics sections of this report.

Research Findings

IoT and Personal Devices Are Expanding the Endpoint Security Market Opportunity

As the mobile threat landscape grows, more than half (54%) of cybersecurity professionals report that their organization protects corporate-owned mobile devices with its endpoint security platform (see Figure 1). IoT projects are getting back on track, causing many to expect IoT devices to now be secured through a common endpoint security platform. Additionally, with no end in sight for the work-from-anywhere model, nearly half now want help securing non-corporate, employee-owned devices, whether laptops and desktops (38%) or mobile devices (35%).

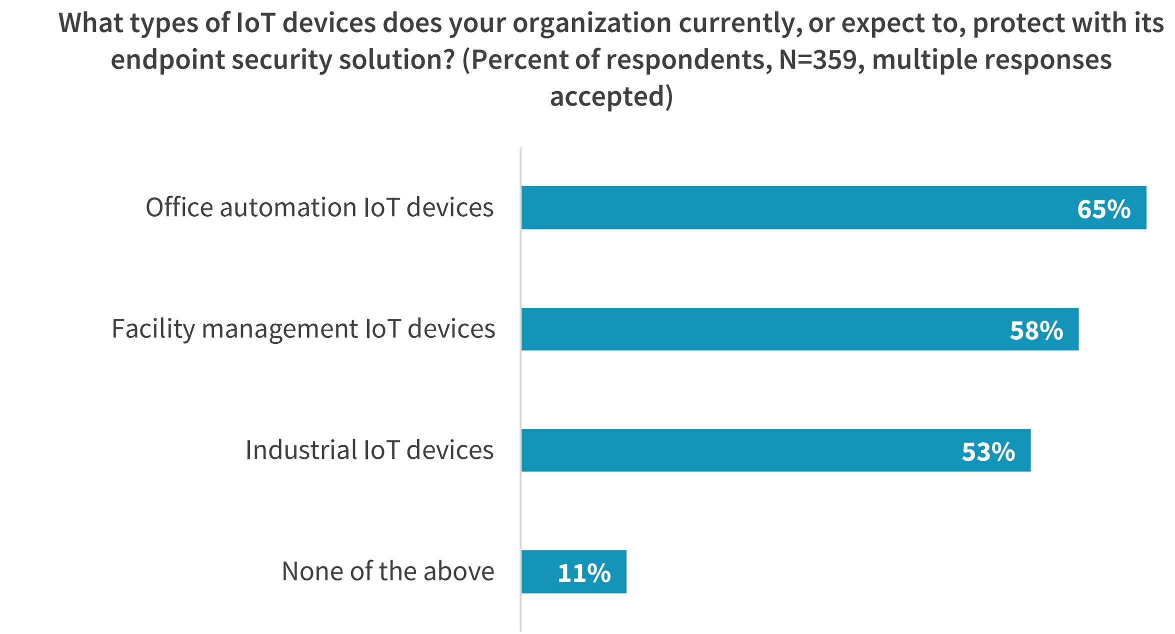
Figure 1. Device Coverage Requirements Continue to Expand



Source: Enterprise Strategy Group

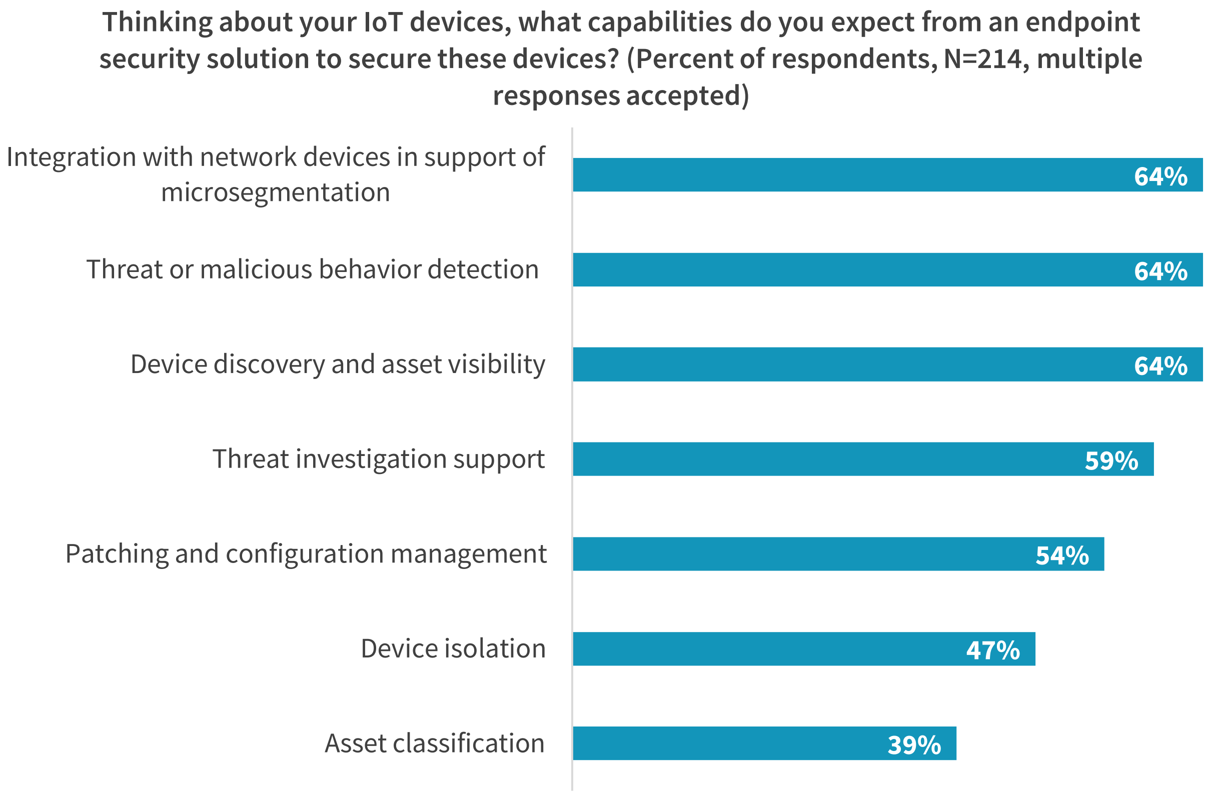
According to Figure 2, IoT projects are accelerating, supporting both corporate functions like office automation (65%) and facility management (58%) as well as more traditional industrial devices (53%) that are responsible for operating manufacturing and critical infrastructure. Buyers expect prevention, detection, and response to encompass IoT devices, matching traditional endpoint capabilities. Yet requirements vary between corporate IoT devices and industrial controls, causing many to consider different security solutions for individual use cases. Specifically, Figure 3 reveals that integration with network devices in support of microsegmentation (64%), threat or malicious behavior detection (64%), and device discovery and asset visibility (64%) are the top capabilities respondents expect from an endpoint security solution.

Figure 2. Desired IoT Device Type Support



Source: Enterprise Strategy Group

Figure 3. Desired IoT Security Capabilities



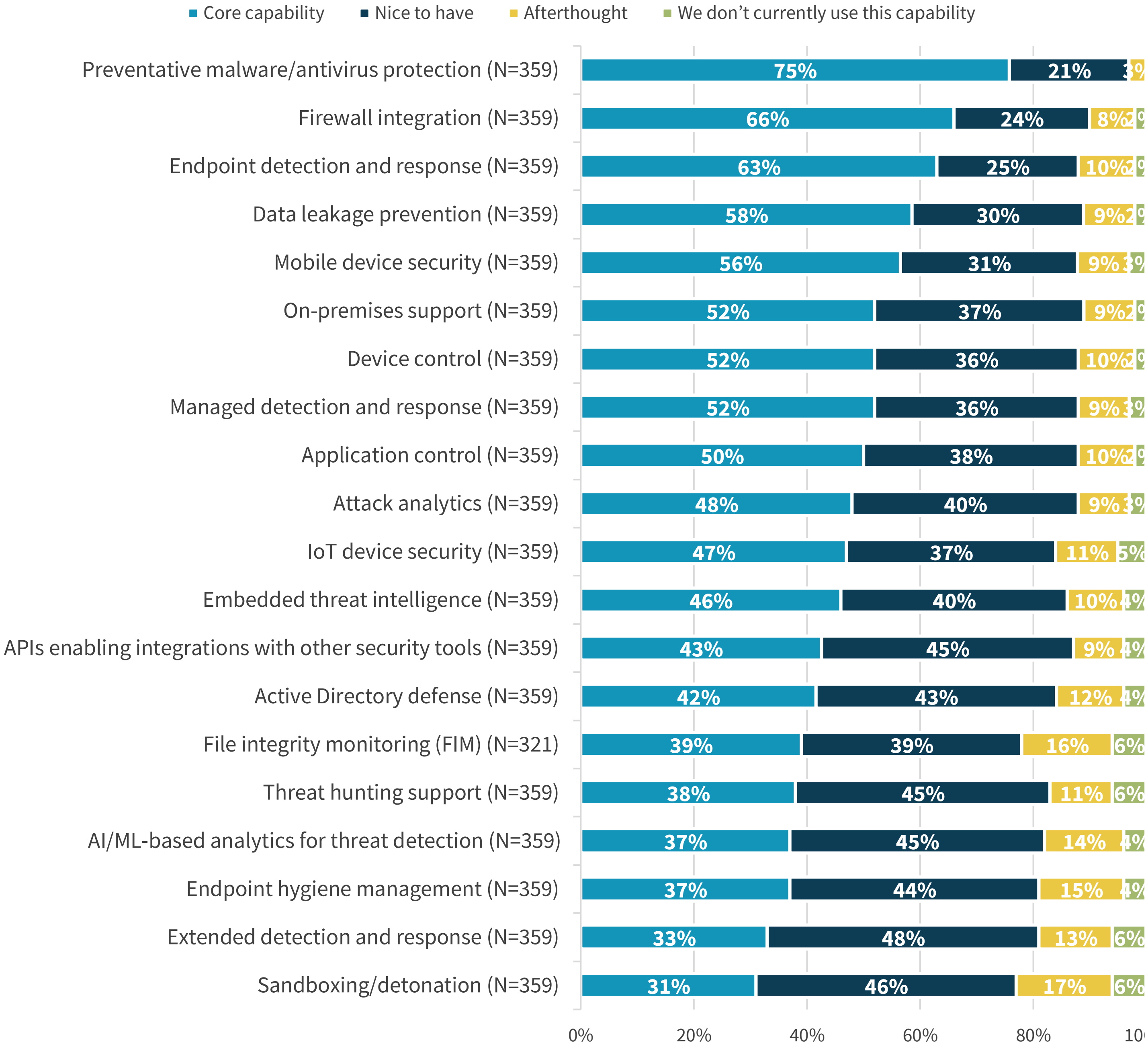
Source: Enterprise Strategy Group

DLP and Endpoint Management Are Converging with Endpoint Security

In support of zero trust and an expanding attack surface made up of a diverse collection of devices, security teams want more. While prevention, EDR, and web security remain foundational to endpoint security needs, securing local data has taken on an increased level of importance (see Figure 4). The trend toward converging more security capabilities on the endpoint continues, adding IoT and mobile device security. Cloud-delivered endpoint security is desired by many, but on-premises needs continue, with more than half still requiring on-premises solution support.

Figure 4. Endpoint Security Feature Priorities

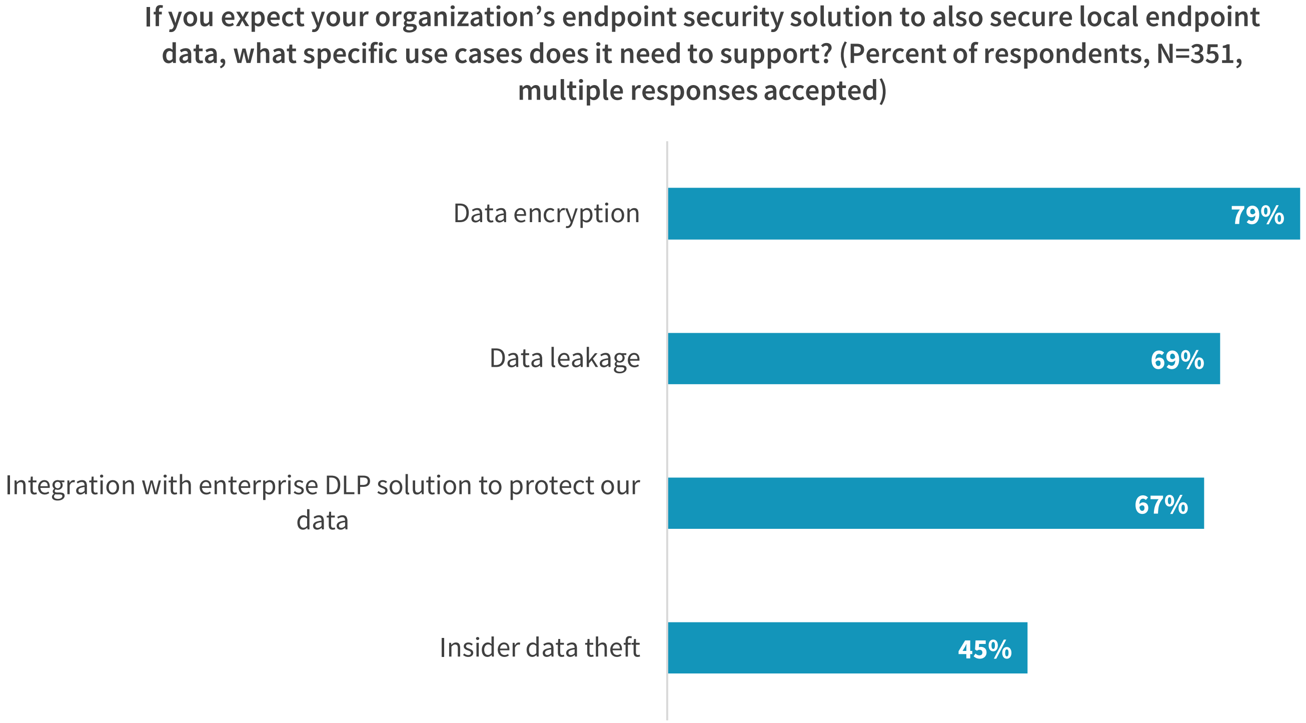
How would you describe the level of importance for each of the following capabilities in terms of the endpoint security solution(s) used by your organization? (Percent of respondents)



Source: Enterprise Strategy Group

In a world of work-from-anywhere, from-any-device policies and habits, sensitive data is increasingly consumed and stored on multiple devices, including personal devices. The growing ransomware threat has further increased data protection efforts, causing many to prioritize data security as a key capability in endpoint security. According to Figure 5, more than three-quarters (79%) think data encryption will help, while more than two-thirds (69%) want specific data leakage protection capabilities. Those who depend on enterprise data loss protection solutions want endpoint security to integrate well.

Figure 5. Data Security Is Increasingly Important

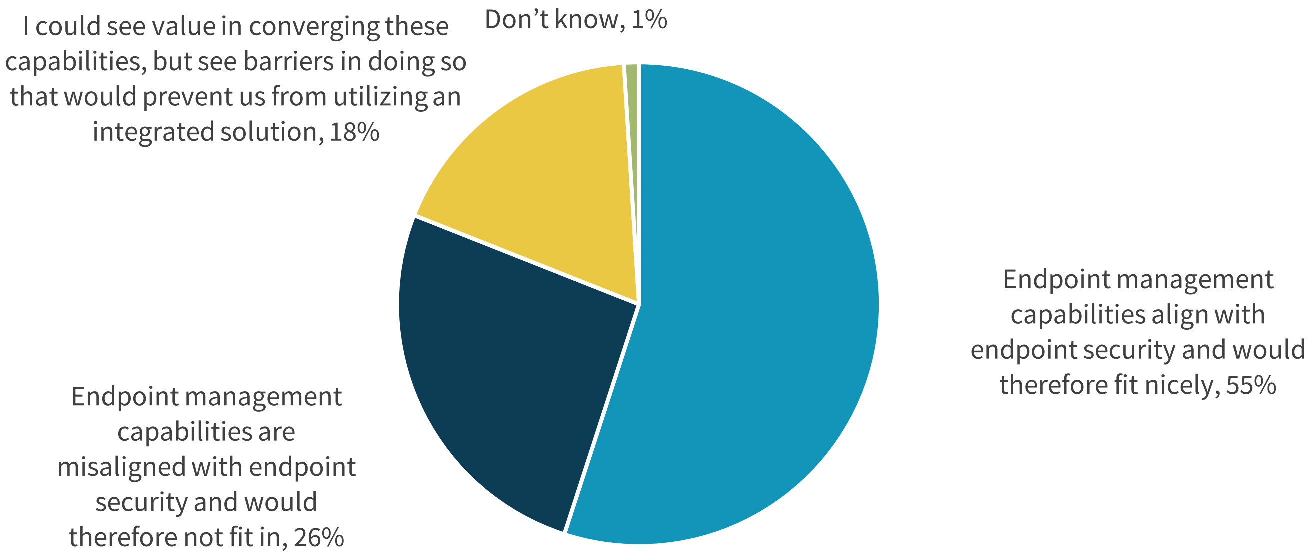


Source: Enterprise Strategy Group

While endpoint management and endpoint security solutions have long been purchased and managed by different organizations, more than half (55%) think these capabilities align and would therefore fit nicely together in a single solution (see Figure 6). Getting vulnerability assessment and alerting together with software configuration verification is integral to endpoint security, causing more than 70% to favor including these capabilities within their endpoint security platform (see Figure 7).

Figure 6. More Than Half Believe in Converged Endpoint Management and Security

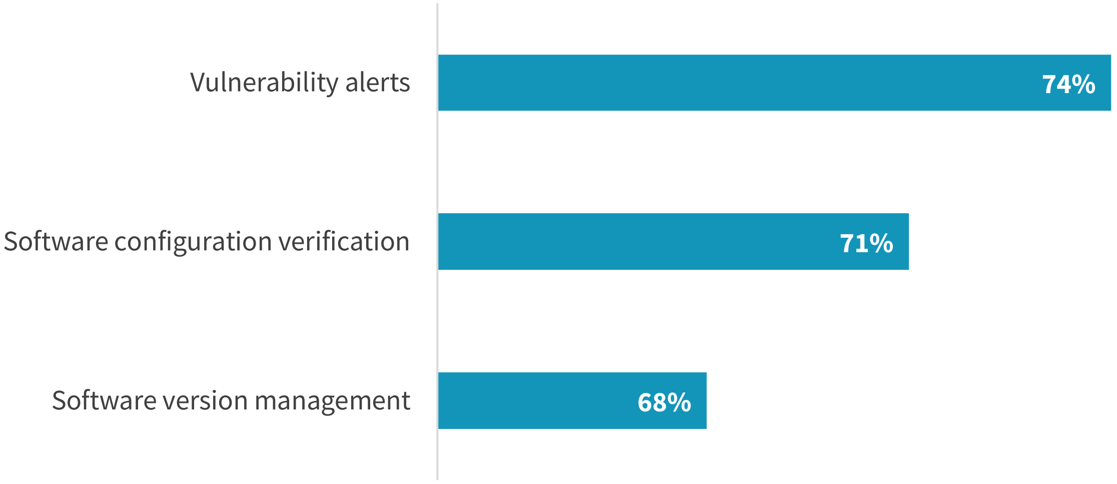
Thinking about endpoint security solutions and endpoint management solutions, would you like to see these capabilities converge and become part of your organization's endpoint security solution? (Percent of respondents, N=192)



Source: Enterprise Strategy Group

Figure 7. Desired Endpoint Hygiene Use Cases

If you expect your organization's endpoint security solution to provide endpoint hygiene capabilities, what specific use cases does it need to support? (Percent of respondents, N=344, multiple responses accepted)

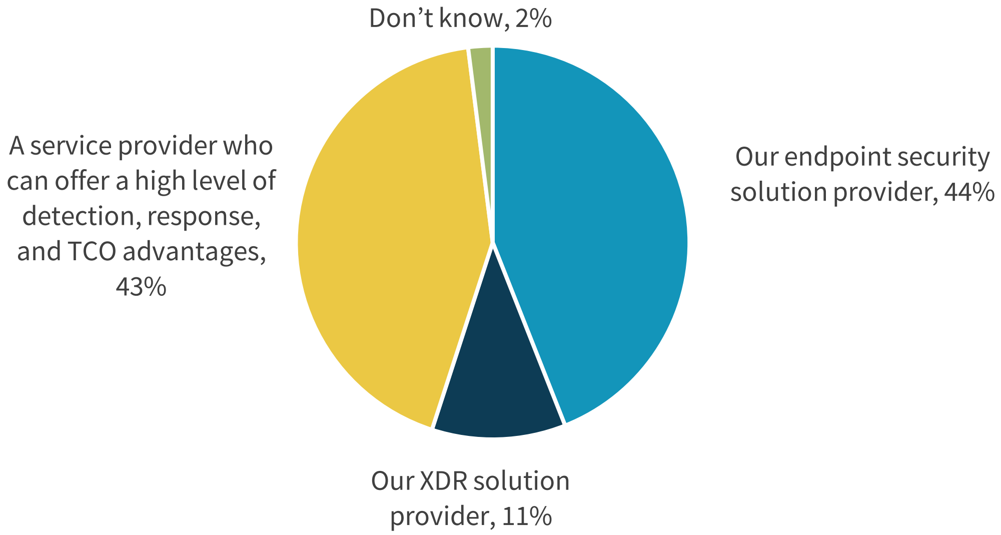


Source: Enterprise Strategy Group

Managed detection and response (MDR) services have become a mainstream element of modern security programs. Many endpoint security platform providers offer companion MDR service offerings, causing 44% of respondents to report that they prefer to acquire MDR from their endpoint security vendor (see Figure 8). As XDR emerges, there is a growing desire to acquire MDR services from their XDR solution provider. The remainder are focused on business outcomes, with 43% reporting that they will choose the MDR provider who can offer a high level of detection, response, and total cost of ownership advantages. According to Figure 9, expectations are high for MDR SLAs, with more than three-quarters (78%) demanding same-day response capabilities.

Figure 8. Preferred Source for MDR Services

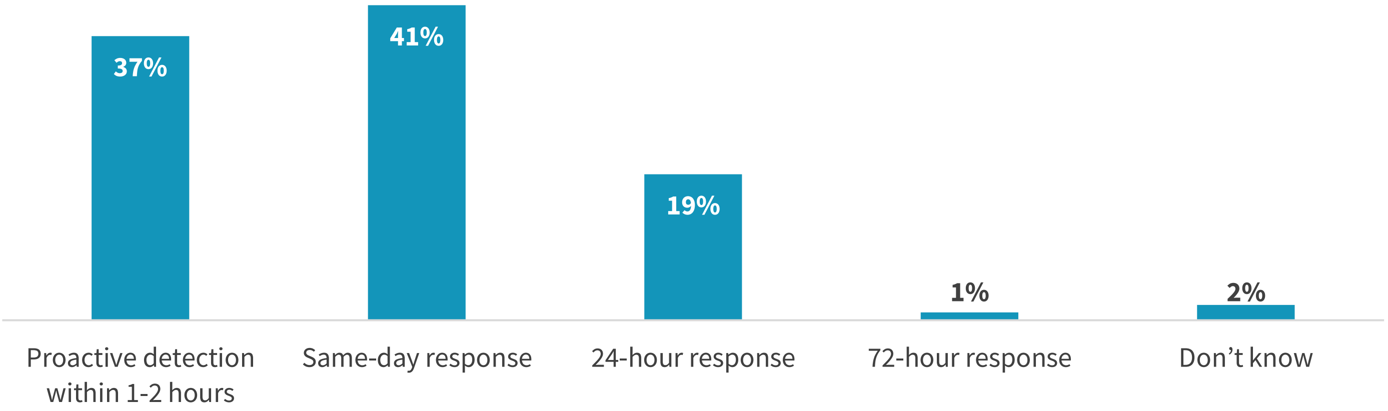
From whom does your organization prefer to acquire managed detection and response (MDR) services? (Percent of respondents, N=349)



Source: Enterprise Strategy Group

Figure 9. MDR SLA Expectations Are High

What kind of SLAs does your organization expect from its MDR service providers? (Percent of respondents, N=349)



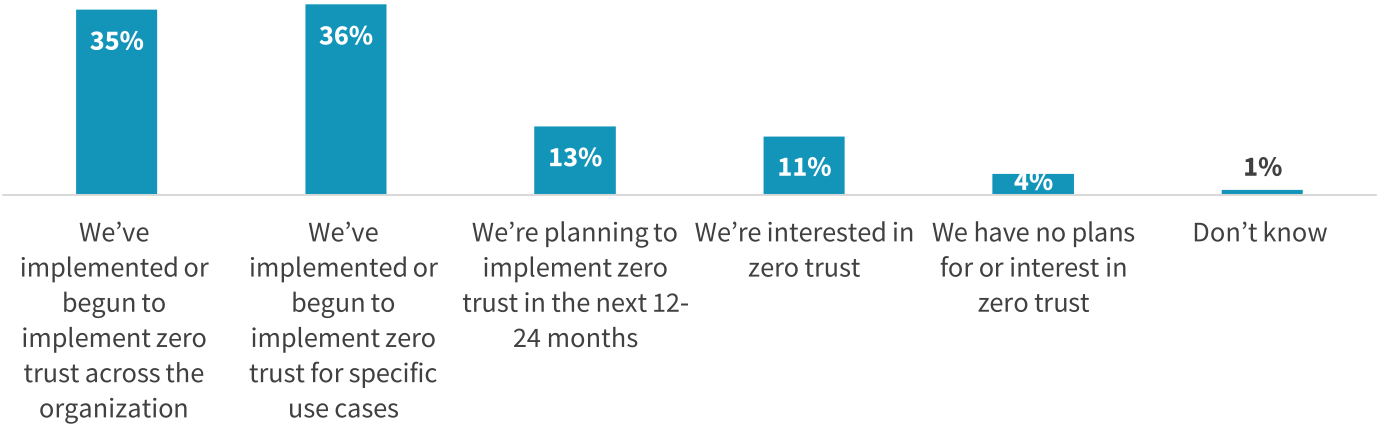
Source: Enterprise Strategy Group

Zero Trust and XDR Initiatives Are Causing Many to Upgrade Endpoint Security

Zero trust architecture has been one of the most widely written about, prioritized initiatives since the beginning of the pandemic. According to Figure 10, more than two-thirds (71%) of organizations have already committed and are underway with their implementation of zero trust, with another 24% considering or planning an initiative. Given device-level security is a core component of a zero trust architecture, it follows that three-quarters report that they have an active project underway to upgrade their endpoint security solutions in order to facilitate their zero trust strategies (see Figure 11). Zero trust also includes a data security component, supporting the desire for additional data security capabilities to be included within modern endpoint security solutions.

Figure 10. State of Zero Trust Strategies

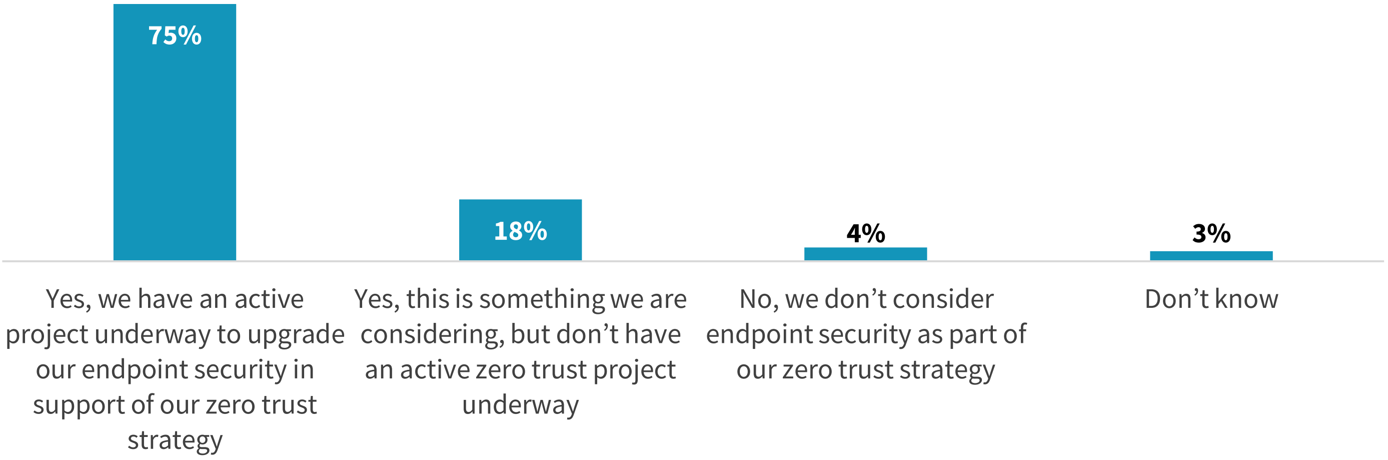
Which of the following statements best reflects your organization's adoption of a "zero trust" strategy? (Percent of respondents, N=359)



Source: Enterprise Strategy Group

Figure 11. Willingness to Swap Out Endpoint Security in Support of Zero Trust Strategies

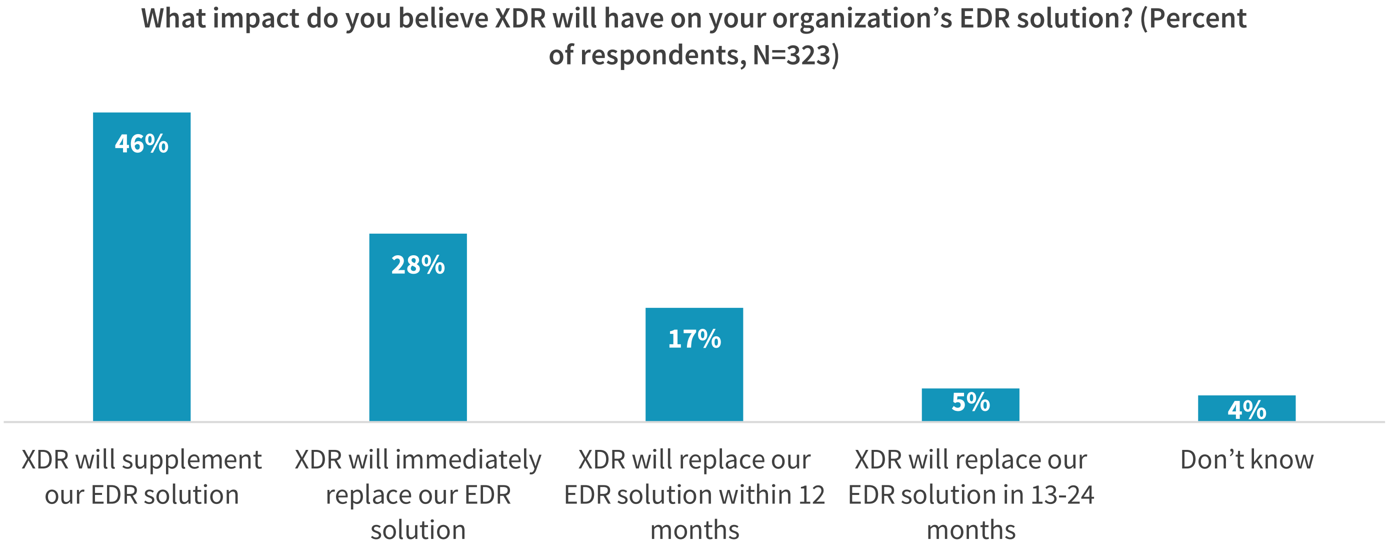
Would your organization be willing to change out its endpoint security solution if it could help accelerate its zero trust implementation? (Percent of respondents, N=342)



Source: Enterprise Strategy Group

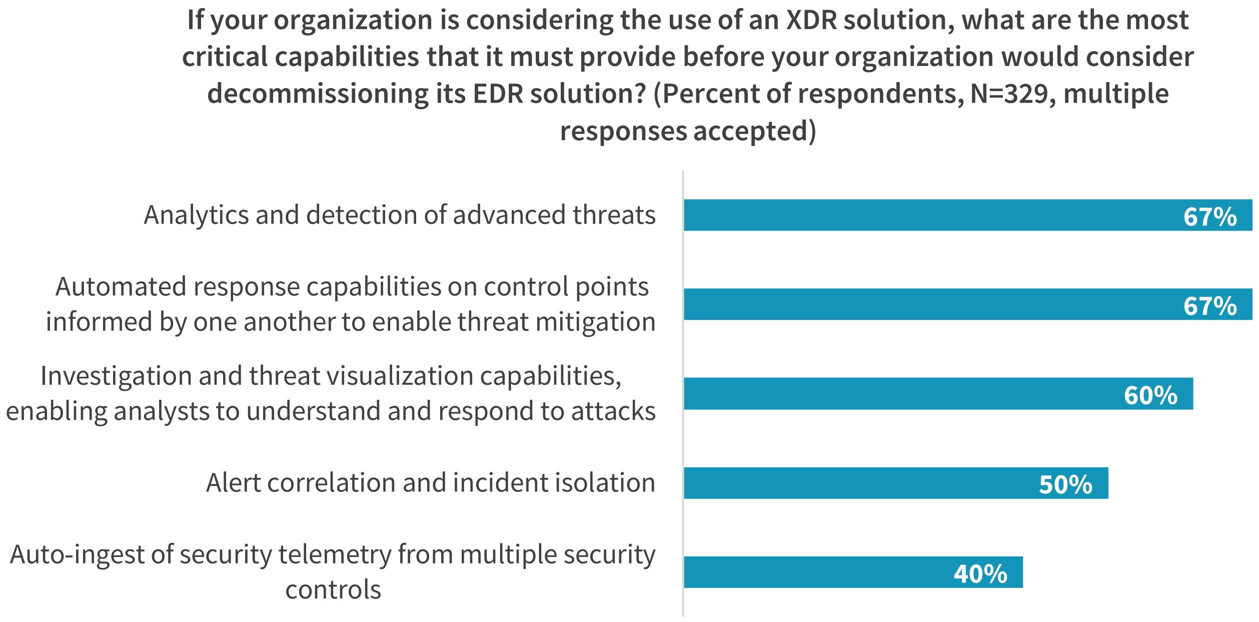
The emergence of extended detection and response (XDR) solutions is causing many to consider the implementation of new XDR solutions to help detect and respond to advance threats. According to Figure 12, as organizations consider XDR, 45% think XDR will either immediately or within 12 months replace their EDR solutions, while almost half (46%) plan to begin by supplementing their existing EDR solutions before considering replacing them. XDR is making some big promises, but it's still the early days and there is some proving to do before most will commit to long-term use of XDR, wanting to first determine whether XDR solutions can really detect and automate the response to more advanced threats (see Figure 13). If XDR can deliver, it seems likely that EDR solutions will become a thing of the past.

Figure 12. Expected Impact of XDR on EDR



Source: Enterprise Strategy Group

Figure 13. Most Critical XDR Capabilities



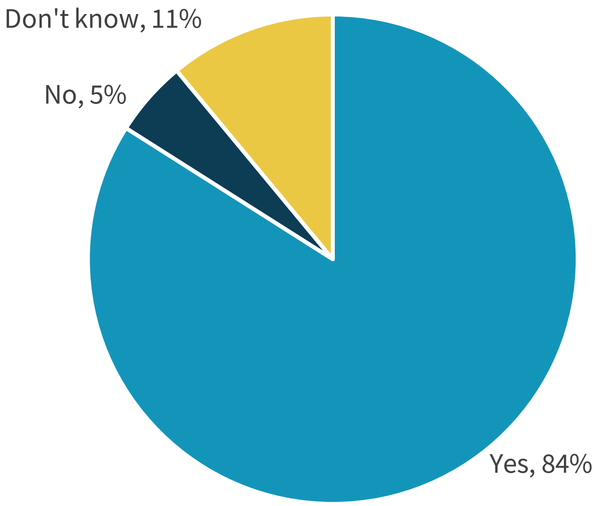
Source: Enterprise Strategy Group

EDR Vendors Are Preferred for XDR, and Most Think Their Current EDR Provider Can Deliver XDR

With XDR solutions being offered by so many security solution providers, security teams have a variety of options when it comes to acquiring XDR. Many have already become loyal to their EDR solution providers and therefore will consider XDR options from those same vendors before looking elsewhere, with 84% indicating that they believe their current EDR vendor is capable of providing a highly effective XDR solution (see Figure 14). Beyond sentiment, Figure 15 shows that more than half (56%) are already working with their EDR provider to evaluate their XDR offering, while another 41% have plans to do so. The XDR upgrade seems to favor existing endpoint security vendors, at least for those who are also responsible for purchasing core endpoint security solutions.

Figure 14. Most Believe EDR Providers Are Capable of Delivering XDR

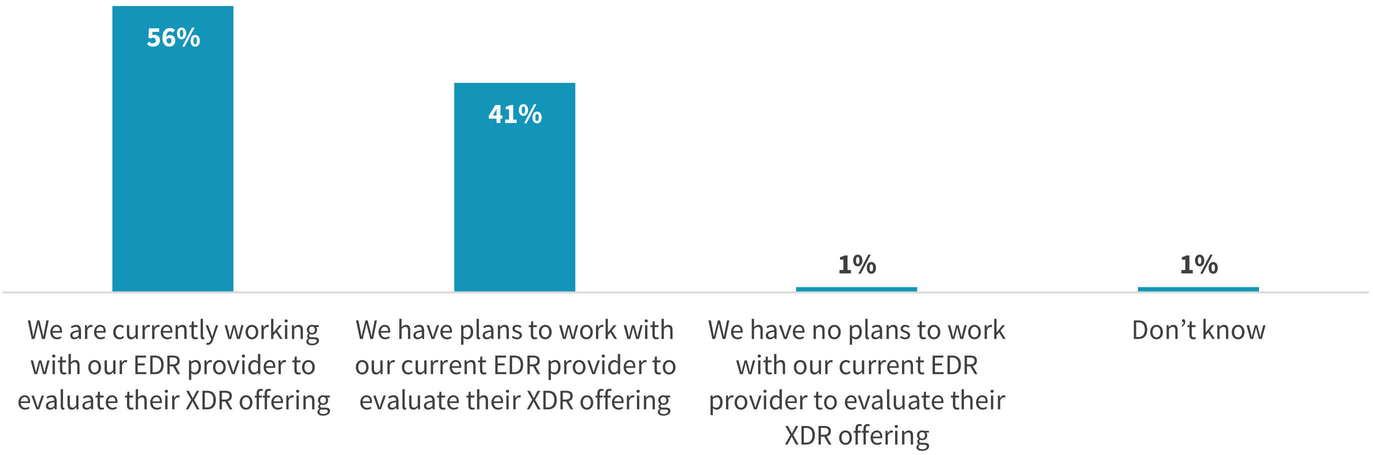
Do you believe that your organization's current EDR provider is capable of delivering a highly effective XDR solution? (Percent of respondents, N=352)



Source: Enterprise Strategy Group

Figure 15. EDR Providers Are Positioned to Win the XDR Opportunity

Which of the following best describes your organization's plans with regard to procuring an XDR solution from its EDR provider? (Percent of respondents, N=295)

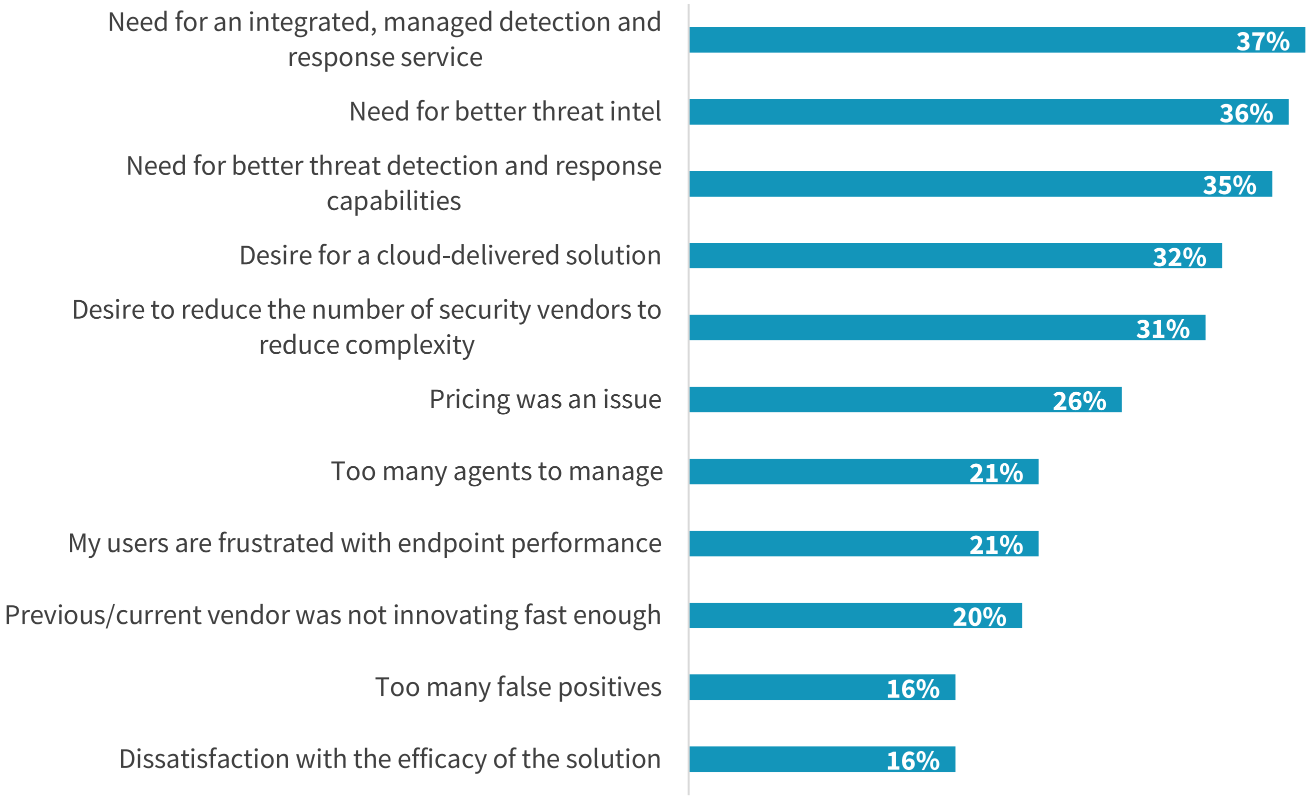


Source: Enterprise Strategy Group

What’s really driving organizations to upgrade endpoint security solutions? While the efficacy of prevention continues to be critical to the success of endpoint security programs, improving detection and response (37%) leads the pack when it comes to what is top of mind for endpoint security buyers (see Figure 16). And it’s not just about the technology. Buyers want their technology supported by a high level of managed detection and response services together with up-to-the-minute insights through threat intelligence, both embedded in prevention, detection, and response, and from their MDR provider.

Figure 16. MDR/XDR and Better Threat Intel Drive Change

If your organization recently switched, has an active project to switch, or is planning to switch endpoint security solution vendors, what drove/is driving this change? (Percent of respondents, N=300, multiple responses accepted)



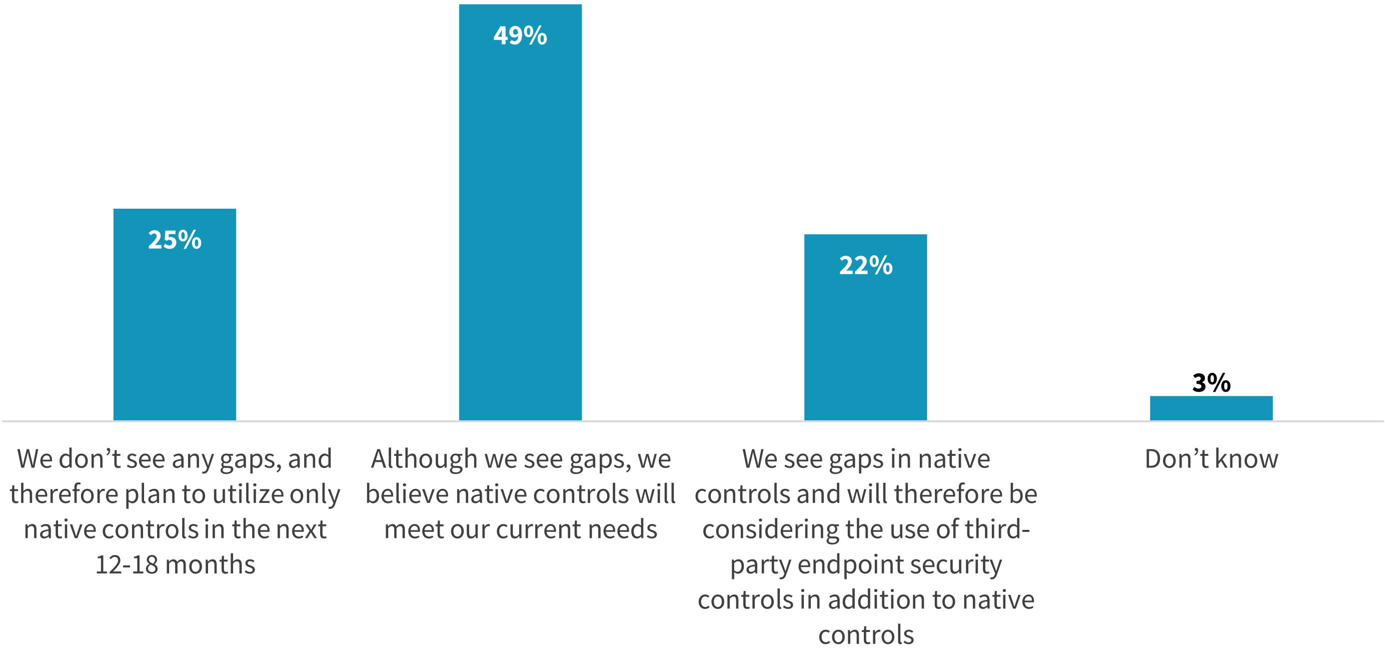
Source: Enterprise Strategy Group

Microsoft Is Now a Serious Contender for Most Organizations, Threatening Incumbent Solutions

According to Figure 17, while more than two-thirds (71%) believe there are gaps in native endpoint OS security controls, nearly half (49%) think that they can live with the gaps. Those who do not will consider adding third-party endpoint security controls to close the gaps.

Figure 17. Few Are Worried About Remaining Gaps in Native Endpoint Security Controls

If your organization is considering the use of native endpoint security controls offered by OS providers, do you believe that there would be endpoint security gaps that would require the use of additional endpoint security products? (Percent of respondents, N=359)



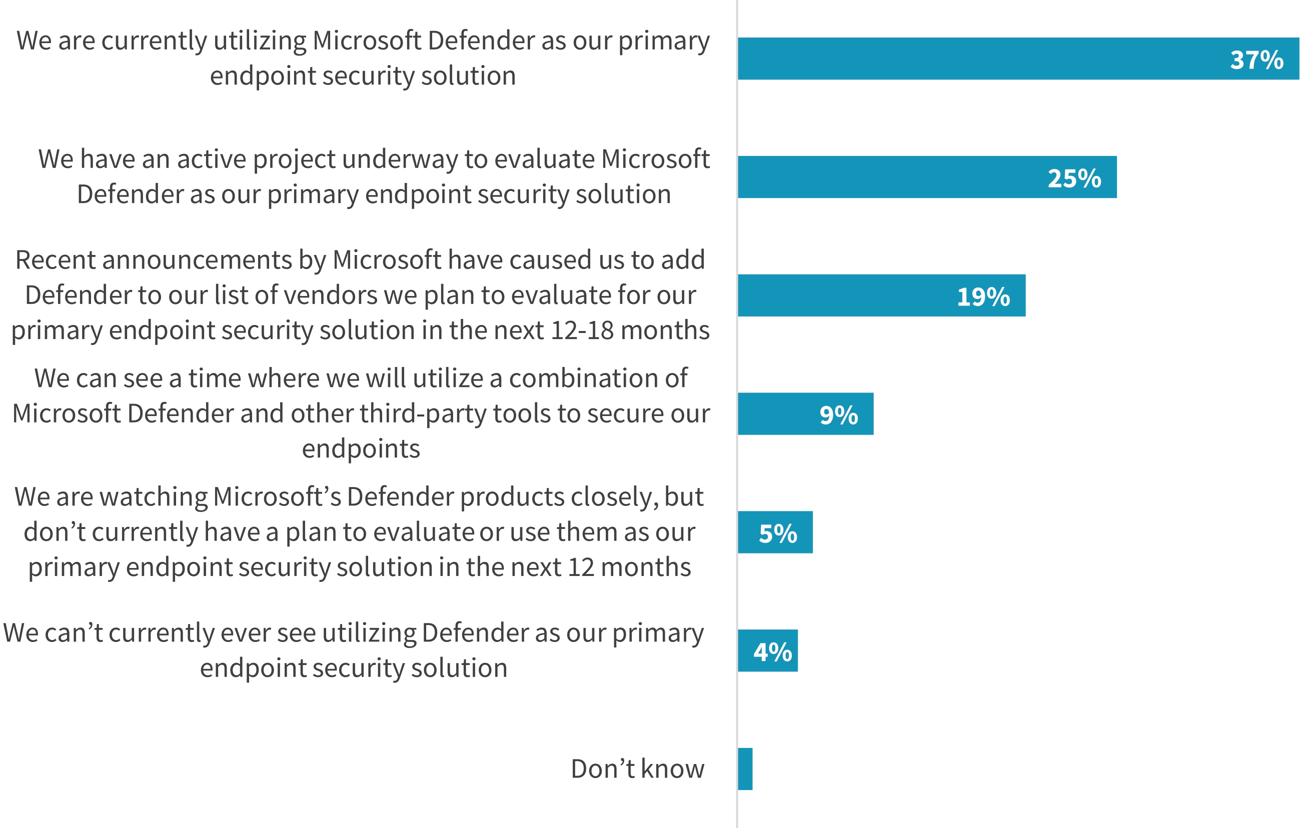
Source: Enterprise Strategy Group

Microsoft continues to advance endpoint security capabilities, motivating almost two-thirds (62%) of respondents to consider Microsoft's native endpoint security controls as their primary solution (see Figure 18). This is a significant uptick from ESG research just two years ago, when 56% said they thought Microsoft could be a contender sometime in the future.[1] Attractive bundling and pricing options are motivating many, with Microsoft Defender for Endpoint included within the E5 bundle. As organizations consider this option, most will need to assess the breadth and depth of the offering to ensure that capabilities are sufficient to replace incumbent solutions. Exploring where organizations see gaps in Defender, more than one-third (35%) perceive detection and response to be a weak link, together with cloud workload protection support (see Figure 19). This provides an opportunity for other endpoint security platforms that provide leading endpoint detection and response capabilities to step in to fill the gaps.

[1] Source: ESG Survey Results, *Trends in Endpoint Security*, March 2020.

Figure 18. Current Position on Microsoft Defender's Place in Future Endpoint Security Strategies

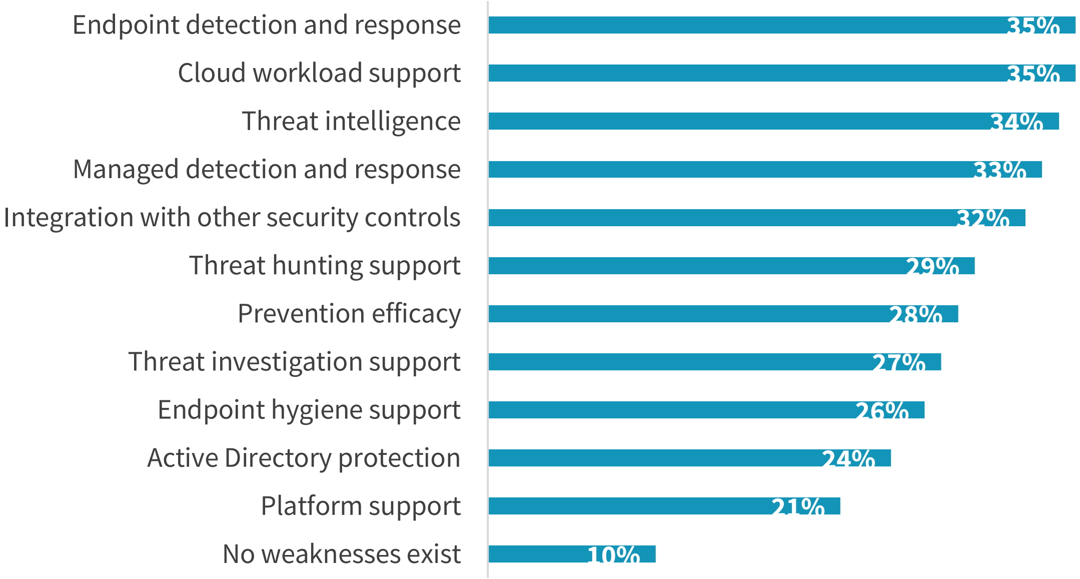
Which of the following statements best reflects your organization's current position on how Microsoft Defender will likely fit into its future endpoint security strategy and endpoint protection platform (EPP) decisions? (Percent of respondents, N=359)



Source: Enterprise Strategy Group

Figure 19. Perceived Microsoft Defender Weaknesses

What weaknesses, if any, do you perceive still exist in Microsoft Defender? (Percent of respondents, N=359, multiple responses accepted)



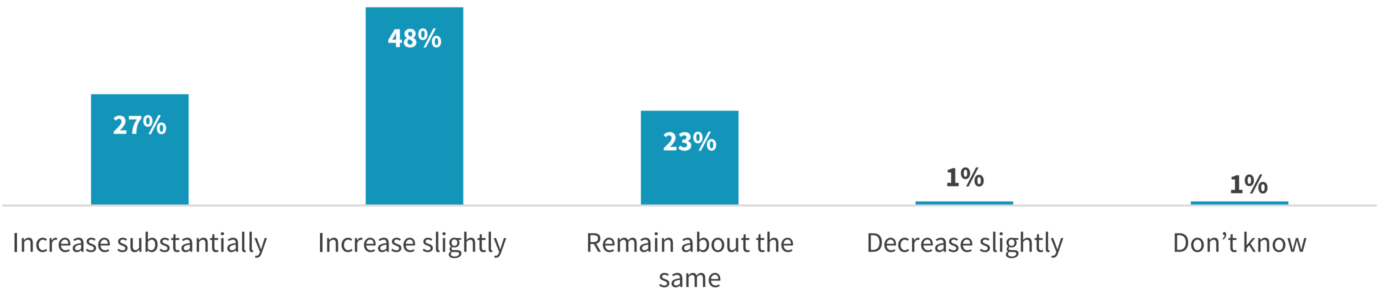
Source: Enterprise Strategy Group

Endpoint Security Spending Is Up, and a Majority Plan to Change Out Current Endpoint Security Solutions

According to Figure 20 , three-quarters of organizations will increase spending on endpoint security in the coming 12 months. More than two- thirds (71%) either recently replaced their solution or are in the process of investigating a converged endpoint security platform to reduce complexity or costs (see Figure 21). However, half still say that they prefer best-of-breed security solutions whenever possible.

Figure 20. Expected Change in Endpoint Security Spending

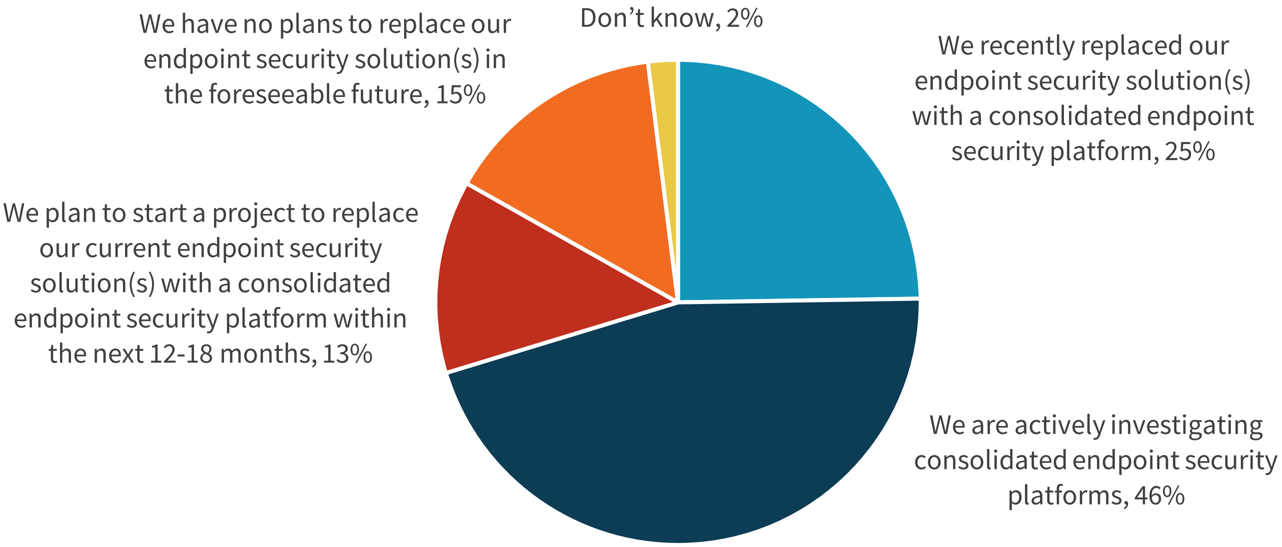
Relative to other areas of cybersecurity, how do you expect your organization's endpoint security spending to change, if at all, over the next 12 months? (Percent of respondents, N=359)



Source: Enterprise Strategy Group

Figure 21. Most Organizations Open to the Idea of a Consolidated Endpoint Security Platform

Does your organization have an active project underway or is it in the planning phase to replace its current endpoint security solution(s) with a consolidated endpoint security platform? (Percent of respondents, N=359)



Source: Enterprise Strategy Group

Conclusion

Endpoint security solutions continue to be in play, with most security teams wanting more in terms of coverage and capabilities. Zero trust and advanced detection and response requirements are key drivers. Meanwhile, as Microsoft continues to advance native endpoint security capabilities and offer attractive purchase options, many will be evaluating whether Defender can get the job done.

As the diversity of devices and workloads continues to expand, security teams are expecting greater coverage from endpoint security solutions, extending prevention and EDR support to corporate IoT devices, mobile devices, and cloud workloads. Many expect additional capabilities, looking for vulnerability assessment and DLP support to be added. Cloud-delivered deployment is desired by many, but on-premises use cases will continue for the foreseeable future.

As detection and response continue to be a top priority for many, the XDR movement is causing most to reconsider EDR investments in favor of broader XDR solutions. Most plan to give their EDR provider a first shot at delivering. Combined with upgrading detection and response software, most want managed detection and response (MDR) services from their provider.

ESG believes that the endpoint security market is entering a significant transition period, as endpoint security providers redefine the scope of their offerings, within a world of zero trust and XDR. With the continuing growth and diversity of device and workload types, expect endpoint security providers to invest heavily in cloud security capabilities, together with further investment in analytics and advanced detection beyond the endpoint.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM Security X-Force research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development, and delivery organizations, monitors 150 billion+ security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBMSecurityIntelligenceblog.

IBM Security

Learn about IBM Security ReaQta, an automated,
AI-powered approach to endpoint security.

LEARN MORE

Research Methodology

To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between June 17, 2021 and June 25, 2021. To qualify for this survey, respondents were required to be IT or cybersecurity professionals personally responsible for evaluating, purchasing, and managing endpoint security products, processes, and services. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 359 IT and cybersecurity professionals.

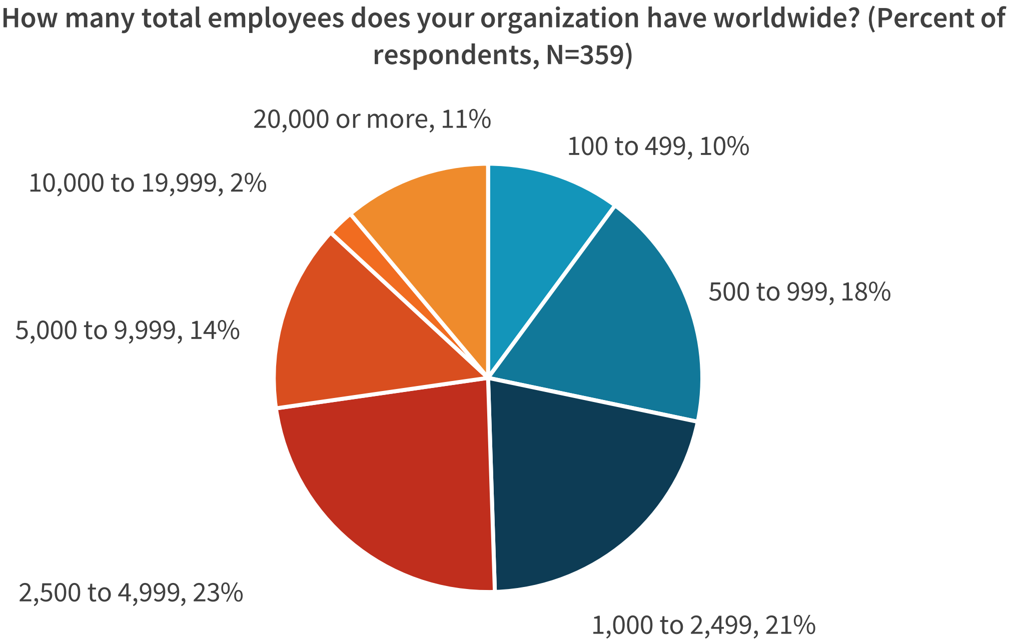
Please see the *Respondent Demographics* section of this report for more information on these respondents.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

Respondent Demographics

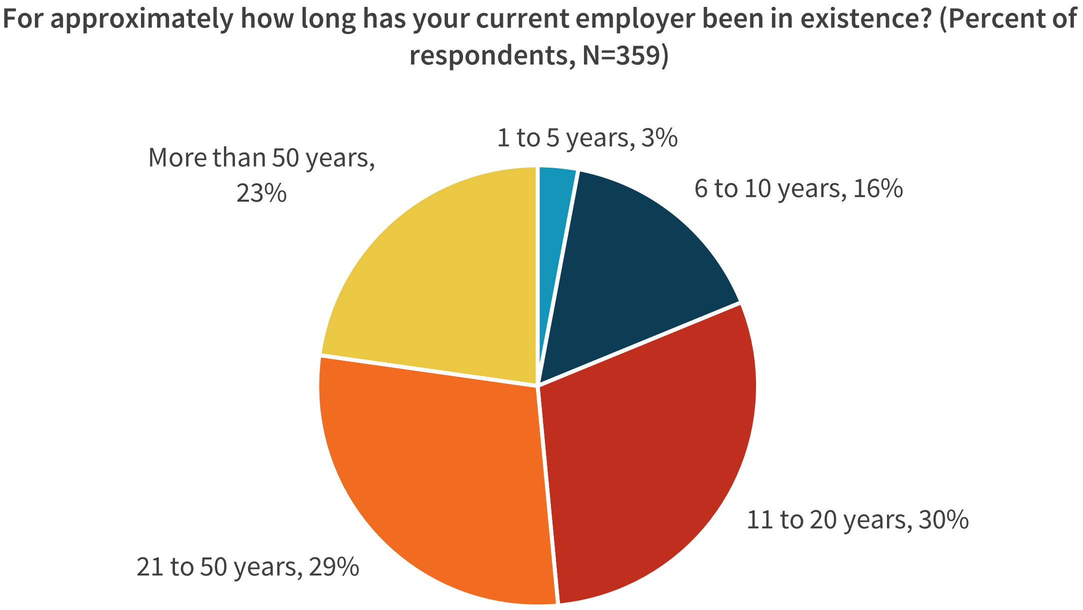
The data presented in this report is based on a survey of 359 qualified respondents. Figure 22 through Figure 25 detail the demographics of the respondent base at an organizational level.

Figure 22. Respondents by Number of Employees



Source: Enterprise Strategy Group

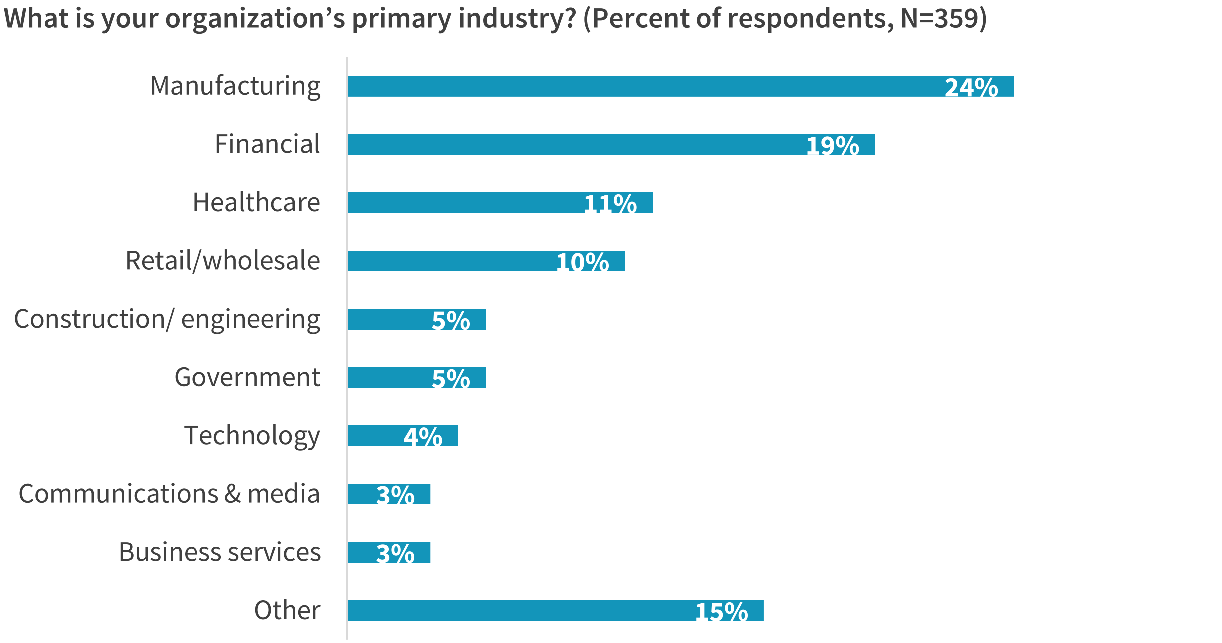
Figure 23. Respondents by Age of Company



Source: Enterprise Strategy Group

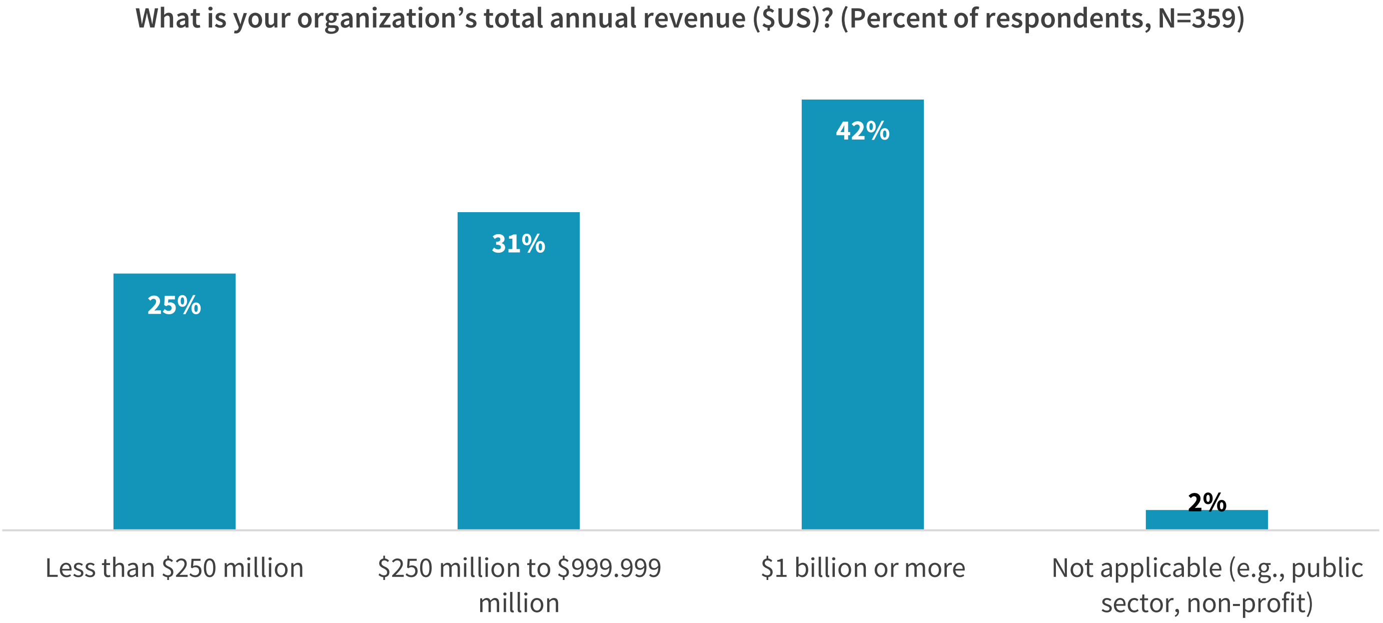
Respondents were asked to identify their organization's primary industry. In total, ESG received completed, qualified responses from individuals in 22 distinct vertical industries, plus an "Other" category. Respondents were then grouped into the broader categories shown in Figure 24.

Figure 24. Respondents by Industry



Source: Enterprise Strategy Group

Figure 25. Respondents by Annual Revenue



Source: Enterprise Strategy Group

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com ✉ contact@esg-global.com ☎ 508.482.0188