



ESG RESEARCH REPORT

Technology Perspectives from Cybersecurity Professionals

By Jon Oltsik, Senior Principal Analyst and ESG Fellow

July 2022





Contents

List of Figures	3
List of Tables	3
Executive Summary	4
Report Conclusions	4
Introduction	5
Research Objectives	5
Research Findings	6
Cybersecurity Professionals Have Strong Opinions about Technology and the Industry	6
Organizations Are Changing Security Technology and Purchasing Strategies	7
Organizations Want More Products from Fewer Vendors	9
The Move to Cybersecurity Platforms Is Gaining Momentum	11
Conclusion	19
Respondent Demographics	20

List of Figures

Figure 1. Cybersecurity Professionals’ Opinions.....	6
Figure 2. Most Organizations Have Employed or Expect to Employ a Security Platform Strategy	7
Figure 3. Most Important Product Considerations	8
Figure 4. Industry Associations and Peers Most Common Sources of Cybersecurity Information	9
Figure 5. Plurality of Organizations Are Consolidating Security Vendors or Considering Doing So	10
Figure 6. Most Common Reasons for Vendor Consolidation.....	10
Figure 7. Attributes of an Enterprise-class Cybersecurity Vendor	11
Figure 8. Definitions of Cybersecurity ‘Platform’	12
Figure 9. Security Technology Platform Deployment	13
Figure 10. Most Important Attributes of CNAPP Platforms.....	14
Figure 11. Most Important Attributes of SASE Platforms	15
Figure 12. Most Important Attributes of Threat Detection and Response Platforms	16
Figure 13. Most Important Attributes of Zero Trust Platforms	17
Figure 14. Steps Taken in Pursuit of Security Platforms	18
Figure 15. Respondents by Age Group.....	20
Figure 16. Respondents by Job Title/Level	20
Figure 17. Respondents by Age of Organization.....	21
Figure 18. Respondents by Number of Employees.....	21
Figure 19. Respondents by Industry	22
Figure 20. Respondents by Region.....	22

List of Tables

Table 1. Smaller Organizations Likelier to Be Partial to Security Platforms	7
---	---

Executive Summary

Report Conclusions

In late 2021 and early 2022, ESG in partnership with the Information Systems Security Association (ISSA) conducted a survey of 280 cybersecurity professionals focused on security processes and technologies at organizations of all sizes in industries such as technology, government, financial services, and business services, among others, spanning countries in North/Central/South America, Europe, Asia, and Africa.

Based upon the research collected for this project, ESG and ISSA reached the following conclusions:

- **Security professionals want more industry cooperation and technology standards.** More than four out of five of security professionals agree that open standards are a key requirement for future security technology interoperability. Additionally, more than three-quarters of respondents would like to see more industry support for open standards. ESG and ISSA hope this research acts as a catalyst toward more industry cooperation and standards development as it's obvious that security professionals see the potential benefits and are hoping this will happen.
- **Organizations are actively consolidating security vendors and integrating technologies.** Security professionals identified numerous problems associated with managing an assortment of security products from different vendors like increased training requirements, difficulty getting a holistic picture of security, and the need for manual intervention to fill the gaps between products. As a result of these issues, nearly half of organizations are consolidating or plan on consolidating the number of vendors they do business with. Additionally, more than one-third of security professionals believe their organizations would be willing to purchase most products from a single vendor, especially those who work at smaller organizations.
- **Security professionals think of “platforms” as integrated, heterogenous architectures based on open standards.** When asked for their definition of a cybersecurity technology “platform,” two-thirds of security professionals say it is an agreed-upon, standard, tightly integrated architecture provided by multiple vendors as an open suite of heterogeneous products. This reinforces the need for standards and exhibits the historical and cultural cybersecurity professional preference for best-of-breed products.
- **Endpoint protection platforms have the highest adoption.** More than half of organizations have deployed an endpoint protection platform (EPP), typically combining next-generation antivirus (NGAV) and endpoint detection and response (EDR). Security professionals describe much lower implementation of other platforms like extended detection and response (XDR), zero trust, cloud-native application protection (CNAPP), and secure access service edge (SASE).
- **SIEM and SOAR are a foundation for platform adoption.** Organizations are preparing for broader security platform use by centralizing security data on SIEM systems and bridging different technologies with SOAR-based workflows. This data indicates that SIEM and SOAR are, and will continue to be, security operations hubs.
- **Experiences vary based on organizational size.** While the data presented in this report is based on the entire survey population, responses varied widely based on the size of participants' organizations. For example, 82% of organizations with fewer than 500 employees buy products and services from 10 or fewer security vendors, compared to 50% of organizations with 500 to 999 employees and 34% of organizations with more than 1,000 employees. Similarly, only 8% of organizations with fewer than 500 employees use more than 25 different cybersecurity technology products, compared to 16% of organizations with 500 to 999 employees and 32% of those with more than 1,000 employees. Future ESG/ISSA research publications will explore these differences further.

Introduction

Research Objectives

In order to assess the cybersecurity landscape in terms of technology consolidation and integration, including how organizations define an “enterprise-class cybersecurity vendor” and the desire for cybersecurity technology platforms, ESG and ISSA surveyed 280 ISSA members, comprising cybersecurity professionals at organizations of all sizes across a variety of industries – including information technology, financial services, government, business services, and manufacturing – and geographic locations. Specifically, seventy-nine percent of respondents came from North America, 10% from Europe, and 6% from Asia, with the remaining 5% located elsewhere. For more details, please see the *Research Methodology* and *Respondent Demographics* sections of this report.

The survey and overall research project were designed to answer the following questions:

- What outlook do organizations have when it comes to using best-of-breed cybersecurity products versus integrated security platforms?
- How do organizations define a cybersecurity “platform”?
- What kind(s) of security technologies are organizations considering consuming as “platforms”?
- What product considerations are most important to organizations when purchasing cybersecurity technologies?
- What sources of information do organizations typically use in order to research cybersecurity solutions?
- What are organizations’ perspectives on the value of procuring cybersecurity solutions from fewer enterprise-class cybersecurity companies?
- What attributes do organizations consider to be the *most important* for an enterprise-class cybersecurity vendor?
- What actions have organizations taken in pursuit of implementing tightly integrated cybersecurity technology “platforms”?

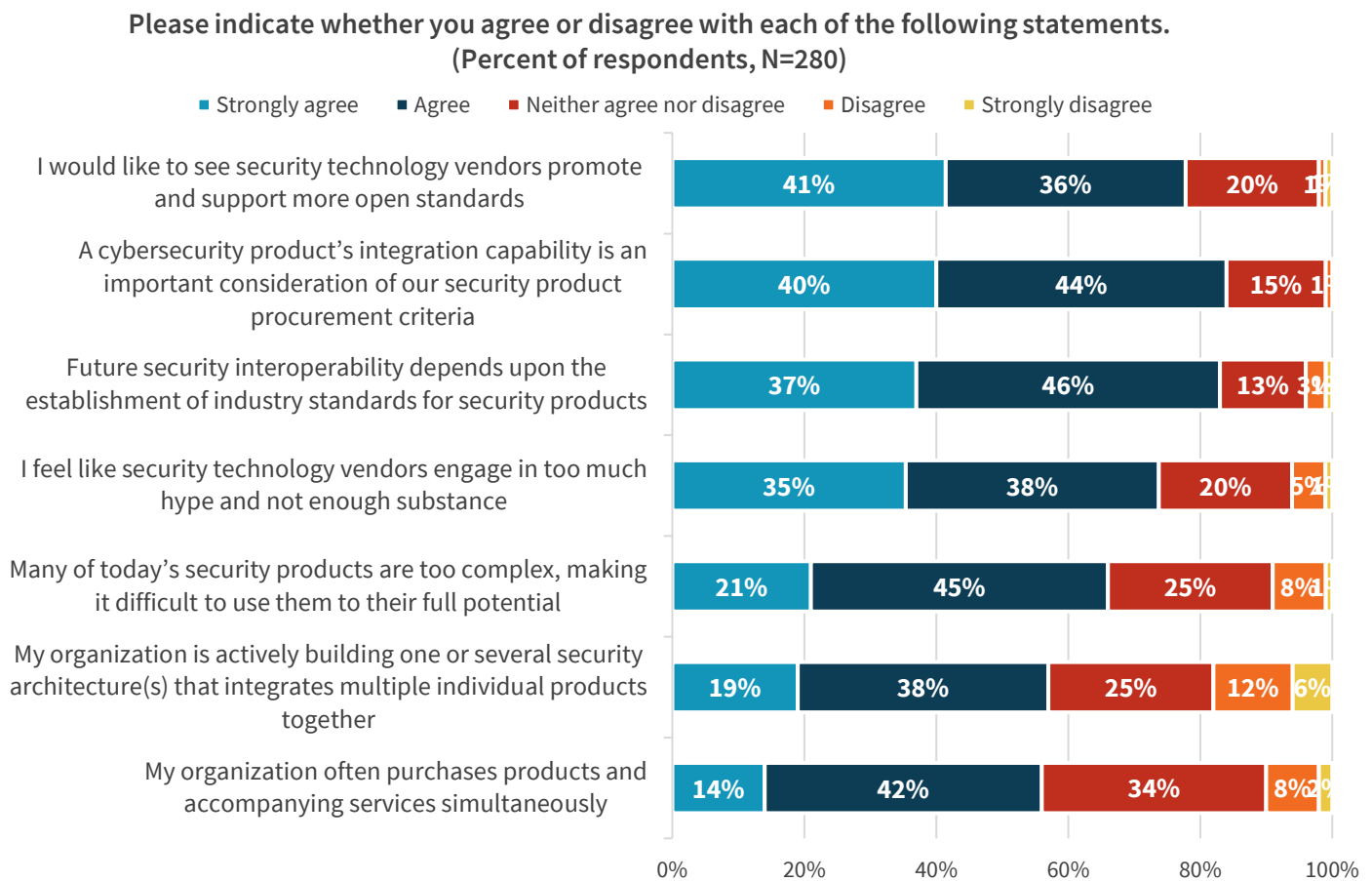
Research Findings

Cybersecurity Professionals Have Strong Opinions about Technology and the Industry

With a research focus on security technology, ESG and ISSA asked survey respondents several questions about their opinions on vendors and the industry at large. The results shown in Figure 1 reveal that:

- **77% of respondents would like to see more support for open standards.** Customers would like to see more industry and technology cooperation in the form of open standards support. ESG and ISSA agree this is important.
- **84% of respondents believe that a product’s integration capabilities are important.** The survey consistently highlighted the importance of security stack technology integration. This data point is one example of this trend.
- **83% of respondents believe that future interoperability depends upon established standards.** Security pros would like more standards cooperation, and they believe it is critical to optimize *all* security technologies in the stack.
- **73% of respondents feel that vendors engage in hype over substance.** This leads to massive confusion and only benefits cyber-adversaries. Thus, vendors offering support, education, and thought leadership will be best positioned.

Figure 1. Cybersecurity Professionals’ Opinions



Source: ESG, a division of TechTarget, Inc.

Organizations Are Changing Security Technology and Purchasing Strategies

In the past, security professionals tended to purchase best-of-breed products, believing that this strategy provided the best overall defense in depth. As the number of security controls grew, however, organizations discovered that managing numerous independent security tools came with substantial operations overhead. This led to more product integration and a preference for security product suites (or platforms) rather than individual best-of-breed tools. It appears from the research that the pendulum has swung in this direction. Thirty-eight percent of respondents say that their organization tends to purchase security technology platforms rather than best-of-breed products, while 24% say their organization continues to buy best-of-breed products (see Figure 2). As for the others, 15% of organizations buy best-of-breed products today but plan on transitioning to platforms in the future while 23% were unsure.

Figure 2. Most Organizations Have Employed or Expect to Employ a Security Platform Strategy



Source: ESG, a division of TechTarget, Inc.

The best-of-breed versus integrated product platform decision can depend on organizational size. For example, 44% of organizations with fewer than 1,000 employees were partial to security platforms, compared to 38% of organizations with 1,000 to 9,999 employees, and 30% of those with 10,000 or more employees (see Table 1). This makes sense as larger organizations likely have more security products (and vendors), making it difficult and time consuming to consolidate.

Table 1. Smaller Organizations Likelier to Be Partial to Security Platforms

	By number of employees		
	Fewer than 1,000 employees	1,000 to 9,999 employees	10,000 or more employees
My organization tends to purchase integrated security technology platforms rather than best-of-breed products	44%	38%	30%

Source: ESG, a division of TechTarget, Inc.

Cybersecurity professionals were asked to identify the most important product considerations when purchasing security products (see Figure 3). Product cost came out on top, which is a logical conclusion since all purchases are guided by budget limitations. Beyond cost however, product integration capabilities were most important (consistent with the data presented previously), followed by ease of use, third-party ratings, and customization. While organizations of all sizes were concerned about product cost, larger organizations also felt that openness and integration were important.

Figure 3. Most Important Product Considerations

Which of the following product considerations are most important to your organization when purchasing cybersecurity technologies? (Percent of respondents, N=280, three responses accepted)

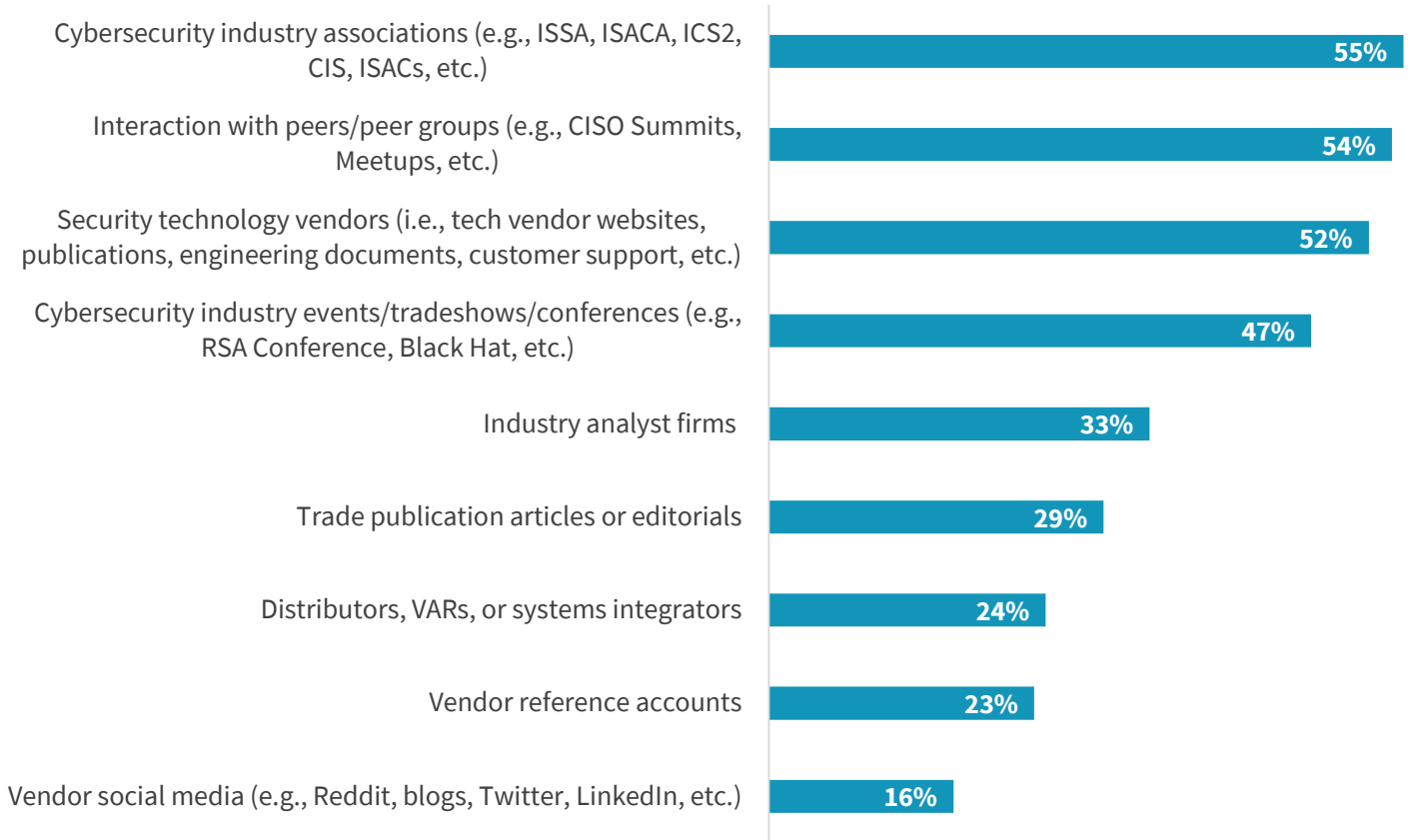


Source: ESG, a division of TechTarget, Inc.

Before purchasing security technologies, information security professionals engage in lots of upfront research. According to Figure 4, more than half (55%) of respondents seek out feedback through participation in industry associations (i.e., ISSA, ISACA, ISC2, etc.), 54% interact with peers or peer groups, 52% consult directly with technology vendors, 47% conduct research at industry events (i.e., Black Hat, RSA Conference, etc.), and 33% look for product information from industry analysts. Judging by these results, it seems clear that using multiple sources of research is a best practice.

Figure 4. Industry Associations and Peers Most Common Sources of Cybersecurity Information

Which of the following sources of information does your organization typically use in order to research cybersecurity solutions? (Percent of respondents, N=280, multiple responses accepted)



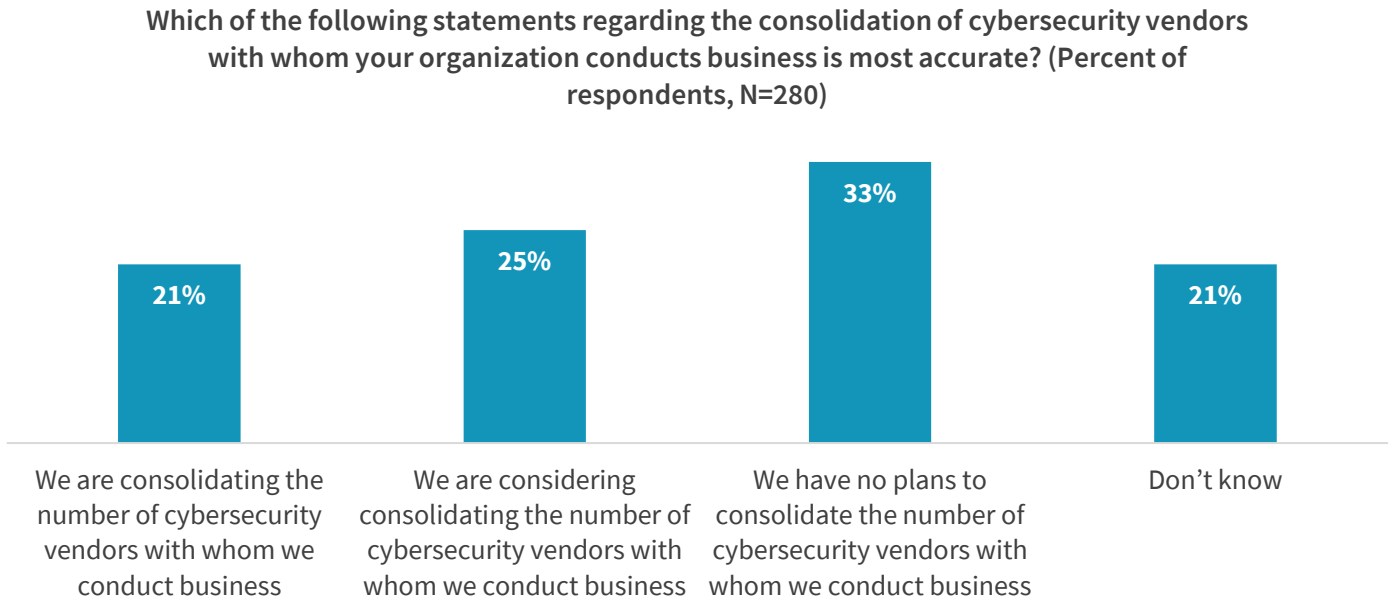
Source: ESG, a division of TechTarget, Inc.

Organizations Want More Products from Fewer Vendors

As part of their efforts around product integration and interoperability, many organizations are consolidating the number of security vendors with whom they do business. Indeed, more than one in five (21%) are consolidating the number of security vendors they do business with, and 25% are considering taking this action (see Figure 5).

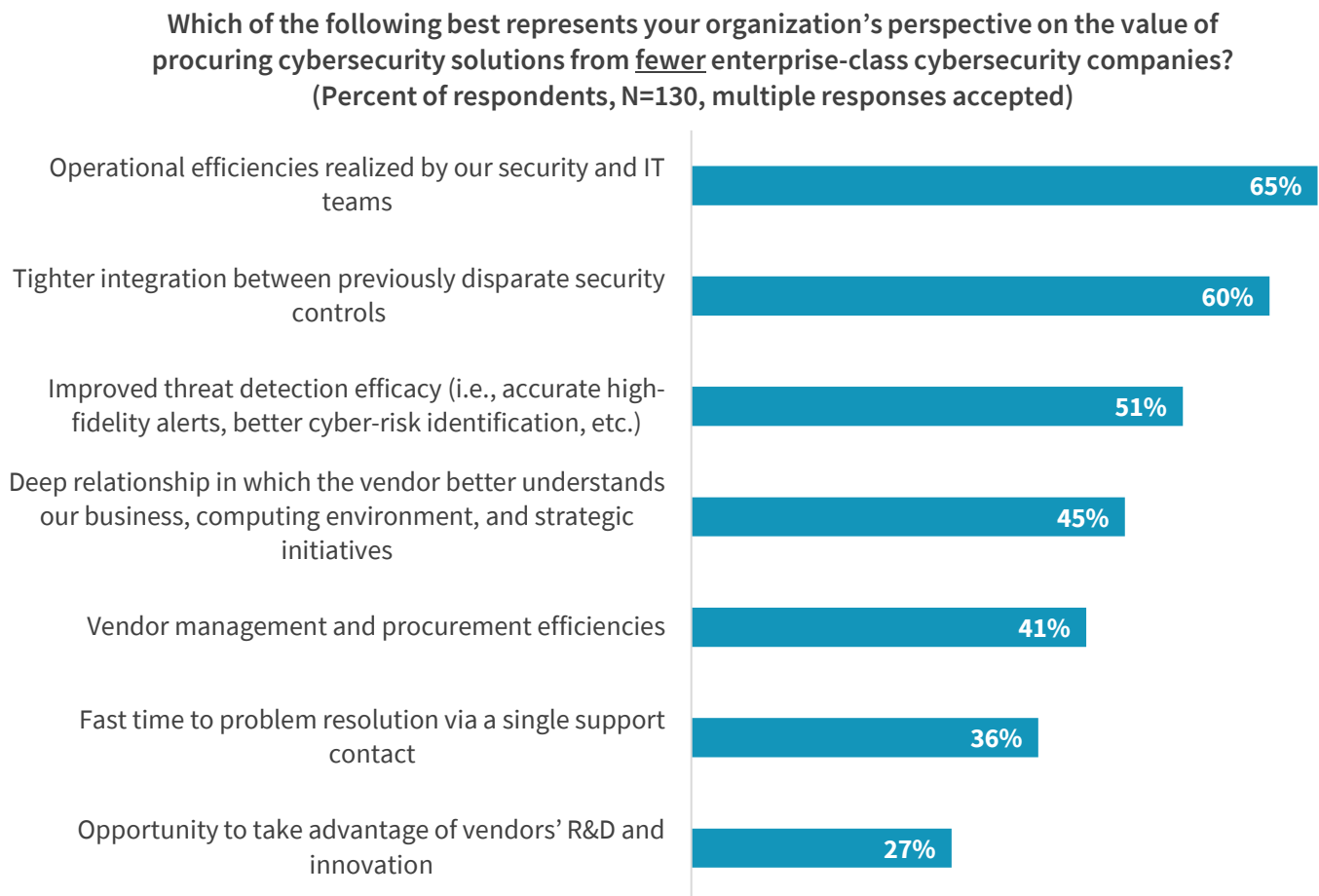
Why would organizations consolidate their security vendor count? Those doing so (or considering doing so) pointed toward several potential benefits of vendor consolidation, including improved operational efficiencies, tighter integration between security controls, improved threat detection efficacy, and building a deeper relationship with fewer vendors (see Figure 6).

Figure 5. Plurality of Organizations Are Consolidating Security Vendors or Considering Doing So



Source: ESG, a division of TechTarget, Inc.

Figure 6. Most Common Reasons for Vendor Consolidation



Source: ESG, a division of TechTarget, Inc.

While organizations may pursue different buying strategies, there is no question that the security technology market is consolidating, establishing “centers of gravity” around a few large vendors. When asked to identify the primary characteristics of these “enterprise-class” security vendors, Figure 7 reveals the most common attributes include a proven track record of execution (34%), a portfolio of products built for enterprise scale (33%), a commitment toward reducing security operations complexity (31%), and world-class threat research (30%). Regardless of current security technology procurement strategies, this foretells a future where organizations place more bets on fewer security technology vendors. As such, organizations must ramp up security evaluations of potential vendors as part of standard procurement processes.

Figure 7. Attributes of an Enterprise-class Cybersecurity Vendor



Source: ESG, a division of TechTarget, Inc.

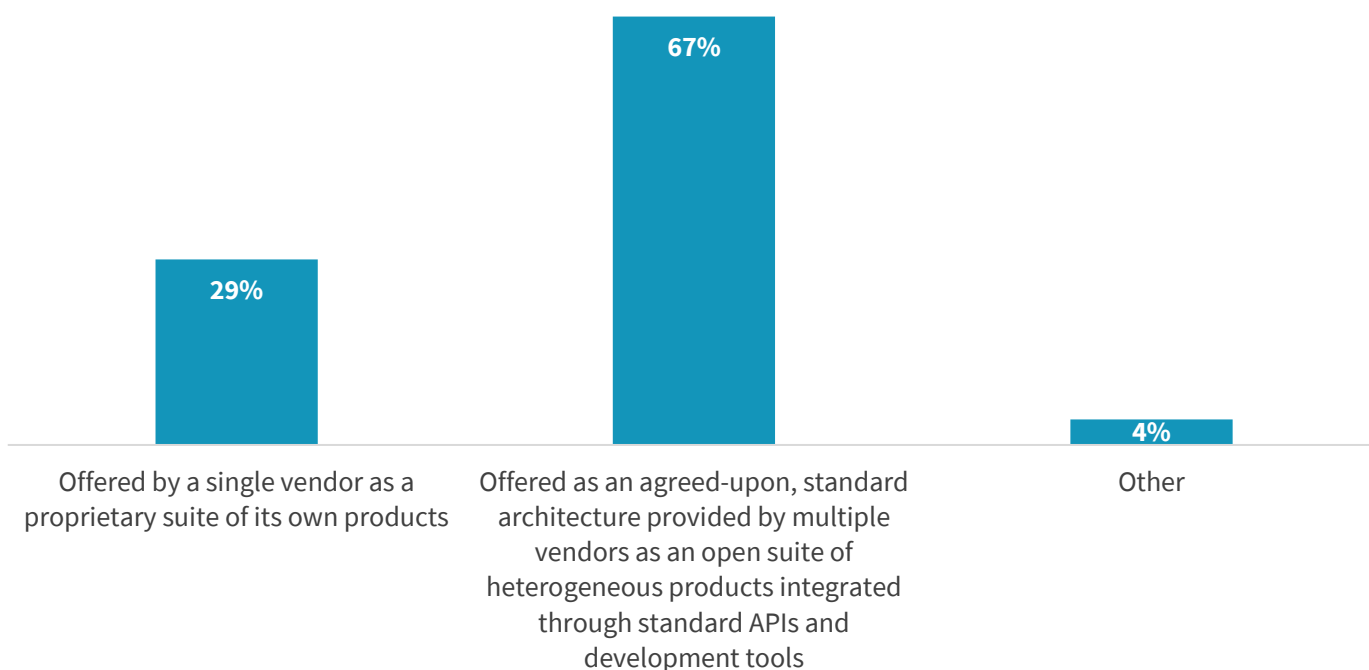
The Move to Cybersecurity Platforms Is Gaining Momentum

As organizations consolidate vendors and integrate security technologies, they may be attracted to the growing number of security technology “platform” offerings. Just what is a security technology “platform”? Two-thirds (67%) of the security

professionals surveyed believe that a security technology platform can be defined as an agreed-upon, standard architecture provided by multiple vendors as an open suite of heterogeneous products integrated through standard APIs and development tools, while 29% define a security technology platform as something that would be offered by a single vendor as a proprietary suite of its own products (see Figure 8). Security vendors should take note: This data can be seen as yet another cry for help. Security professionals are asking for more industry cooperation and standards to ease their technology integration burden.

Figure 8. Definitions of Cybersecurity ‘Platform’

In your opinion, which of the following most closely aligns with your organization’s definition of a cybersecurity “platform”? (Percent of respondents, N=280)

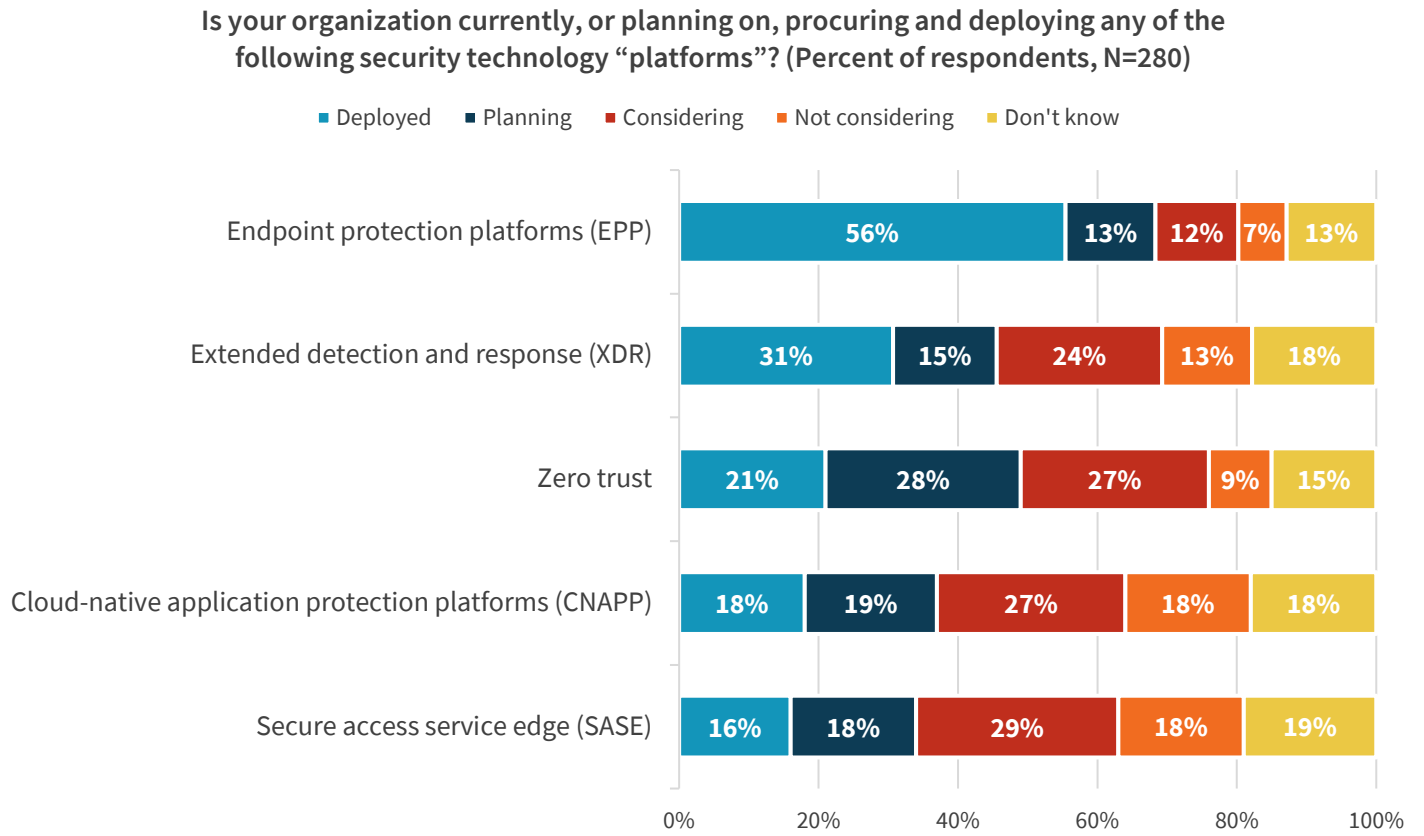


Source: ESG, a division of TechTarget, Inc.

As it turns out, organizations are actively deploying or considering deploying several types of security technology platforms. Endpoint protection platforms (EPPs) have already been deployed in over half of respondent organizations. This is not surprising as endpoint security suites have been available for several years. Other platforms are in various states of maturity and proliferation: 31% of organizations have deployed some type of extended detection and response (EDR) platform, 21% have deployed a zero trust platform, 18% have deployed a cloud-native application protection platform, and 16% have deployed a secure access service edge platform (see Figure 9).

While this data indicates security platform momentum, it may be a bit misleading. Most of these platforms are early in their development and surrounded by unprecedented vendor and market hyperbole, leading to user confusion. Lacking industry agreement, one person’s definition of XDR, zero trust, CNAPP, or SASE may be different from anyone else’s. While security platforms are growing in popularity, it may take a few years to gauge progress of the individual types.

Figure 9. Security Technology Platform Deployment



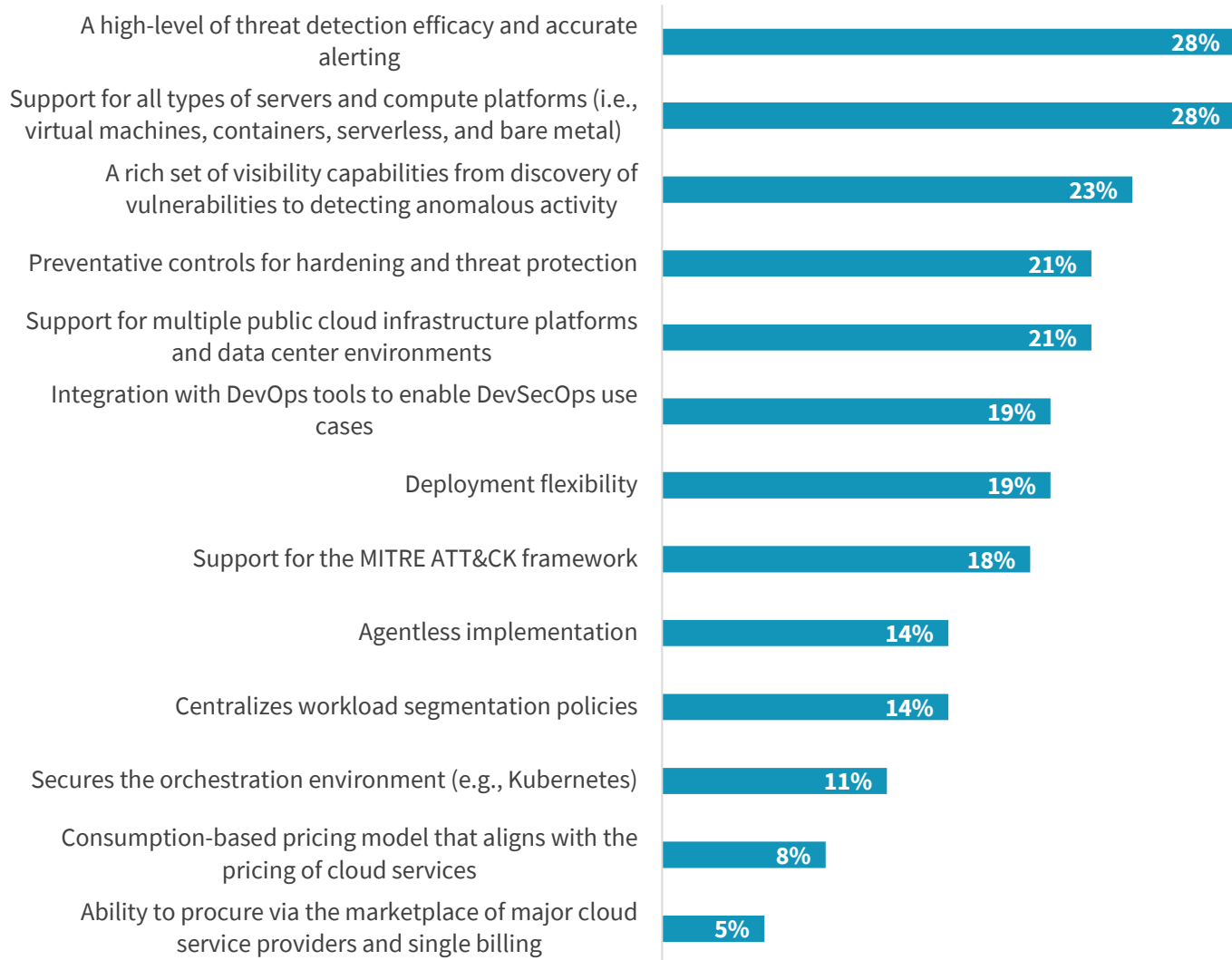
Source: ESG, a division of TechTarget, Inc.

Aside from deployment strategies, security professionals were also asked to identify the most important attributes of CNAPP, SASE, XDR, and zero trust platforms.

Security professionals believe the most important attributes of a CNAPP platform is a high-level of threat detection efficacy and accurate alerting, support for all types of servers and compute platforms, rich visibility capabilities, and preventive controls (see Figure 10).

Figure 10. Most Important Attributes of CNAPP Platforms

Which of the following would you consider to be the **most important** attributes of a cloud-native application protection (CNAPP) cybersecurity “platform”? (Percent of respondents, N=280, three responses accepted)

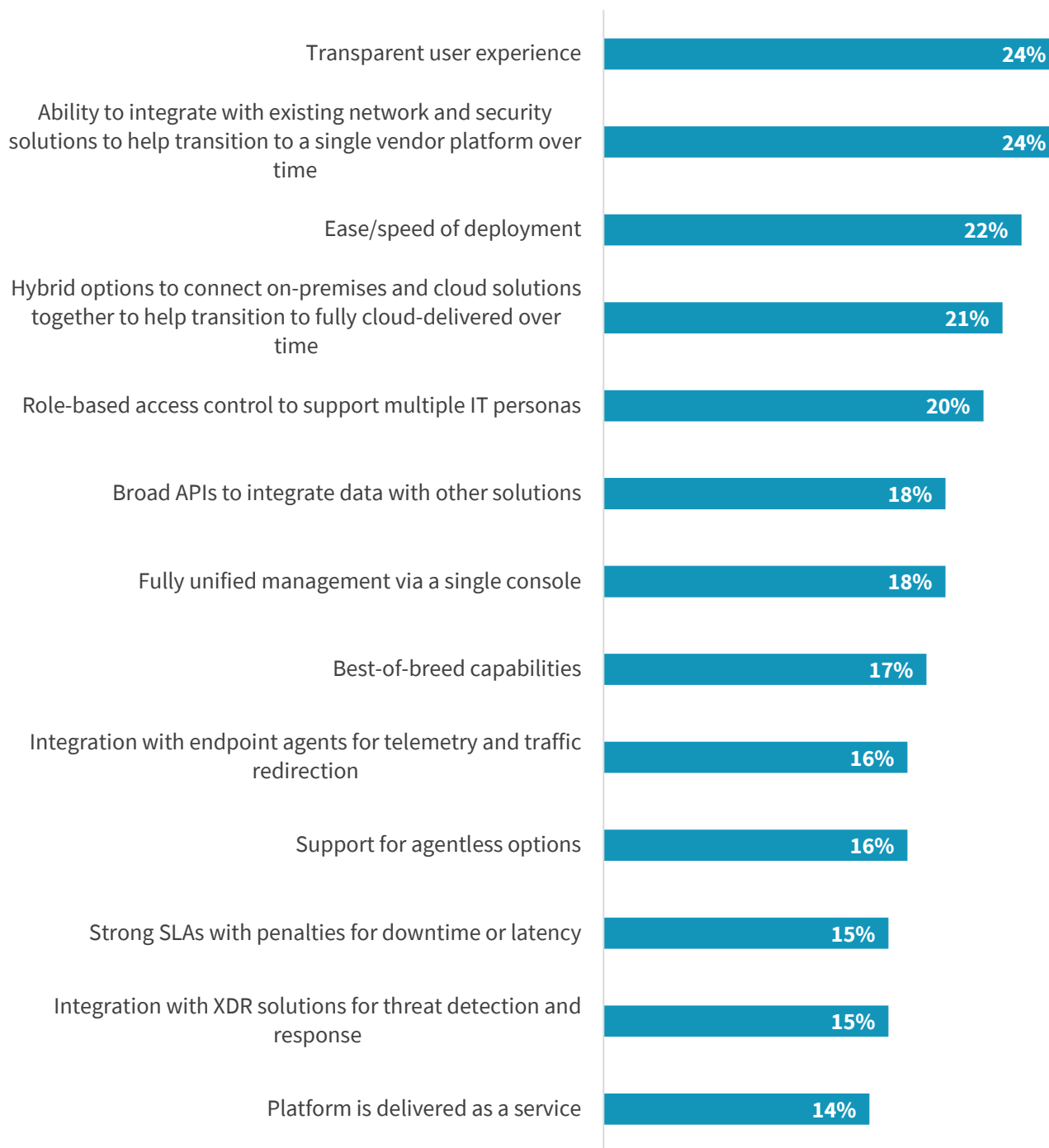


Source: ESG, a division of TechTarget, Inc.

For SASE, survey respondents believe the most important attributes include a transparent user experience, the ability to integrate with existing networking/security solutions, ease/speed of deployment, and hybrid options for on-premises and cloud coverage (see Figure 11).

Figure 11. Most Important Attributes of SASE Platforms

Which of the following would you consider to be the most important attributes of a cybersecurity “platform” for SASE? (Percent of respondents, N=280, three responses accepted)

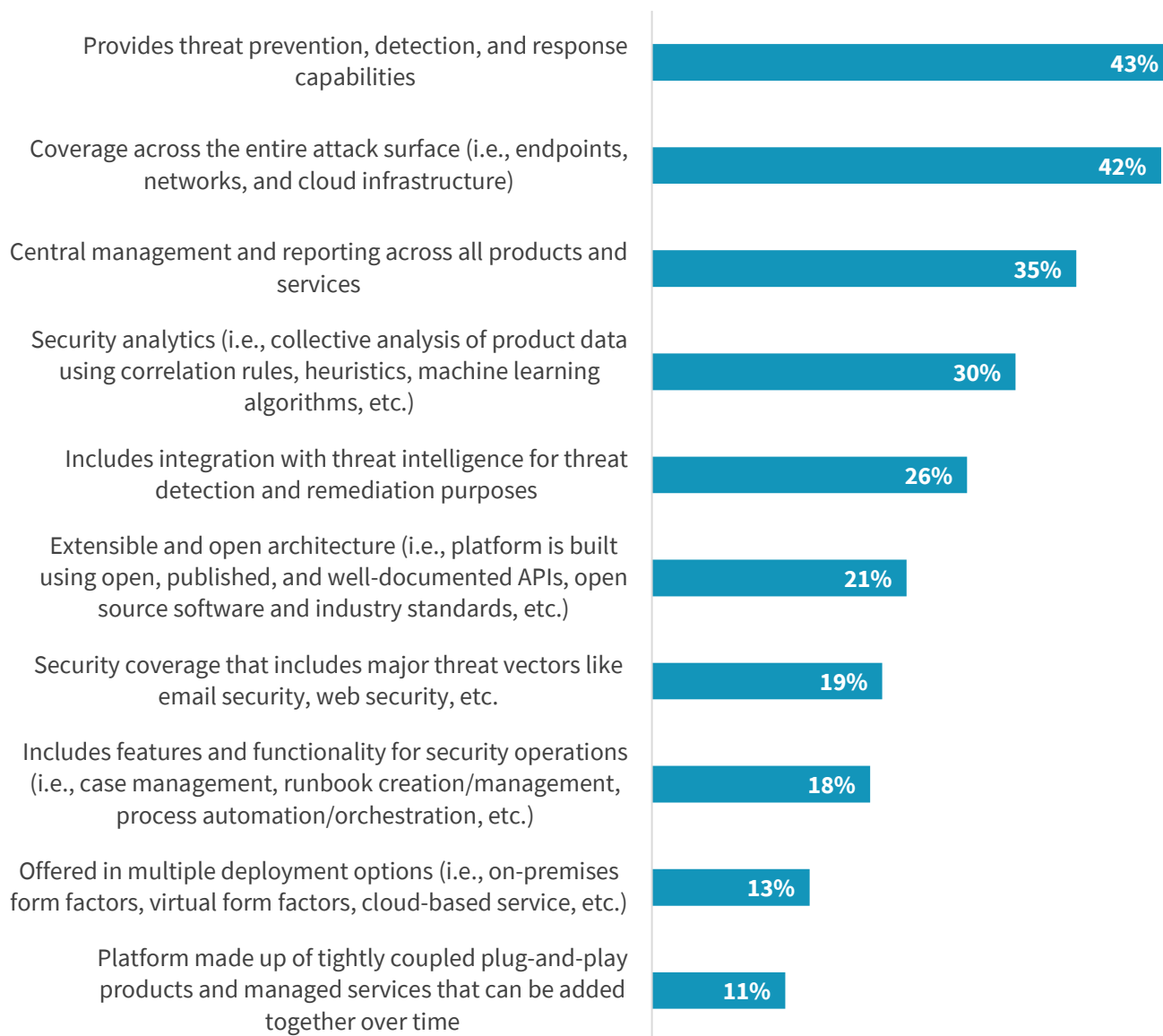


Source: ESG, a division of TechTarget, Inc.

Regarding XDR (or any type of threat detection and response platform), cybersecurity professionals want a platform that provides threat prevention, detection, and response capabilities, covers the entire attack surface, offers central management and reporting, and delivers security analytics (see Figure 12).

Figure 12. Most Important Attributes of Threat Detection and Response Platforms

Which of the following would you consider the **most important** attributes of a cybersecurity “platform” for threat detection and response? (Percent of respondents, N=280, three responses accepted)



Source: ESG, a division of TechTarget, Inc.

Finally, the most important attributes of zero trust platforms include coverage for cloud and on-premises environments, integration with identity providers, risk assessment capabilities, and anomaly detection (see Figure 13).

Figure 13. Most Important Attributes of Zero Trust Platforms

Which of the following would you consider to be the **most important** attributes of a cybersecurity “platform” for zero trust? (Percent of respondents, N=280, three responses accepted)



Source: ESG, a division of TechTarget, Inc.

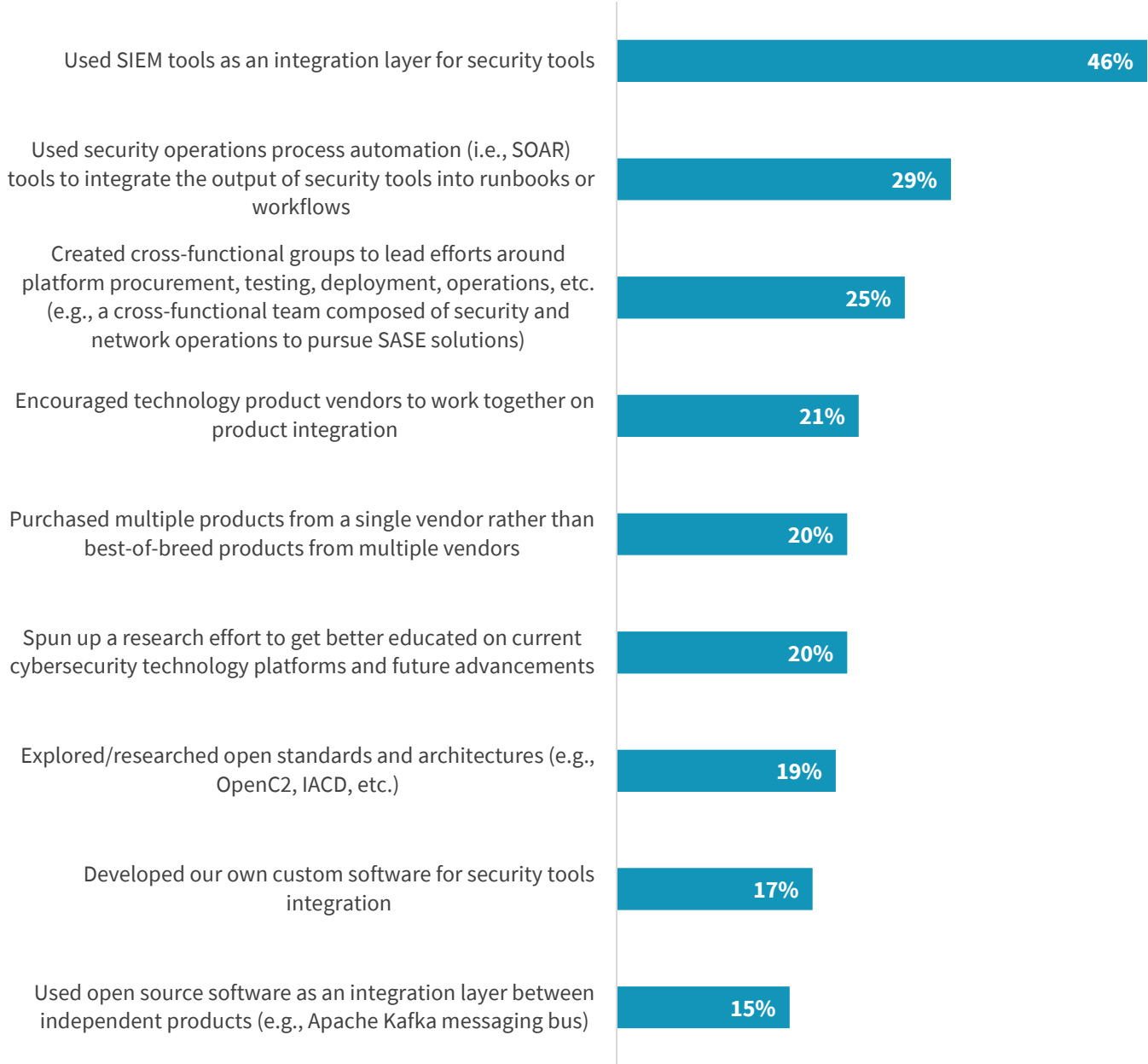
The data indicates that many organizations have deployed some security technology platforms but are planning to deploy or considering deploying others. What are they doing to prepare for this eventuality? The data in Figure 14 reveals:

- **Nearly half (46%) use security information and event management (SIEM) as an integration hub.** In other words, platform data is aggregated with other data sources into a common security data repository (i.e., the SIEM). Security operations teams can then integrate innovative technology platforms into their standard operating procedures. This data indicates that SIEM is and will remain an important security operations hub.
- **29% use SOAR tools to integrate platforms into workflows.** In this case, SOAR is used to unify platforms through automated processes and workflow orchestration across different tools. This speaks to the need for automation and orchestration to improve security efficacy and operational efficiency.

- 25% created cross-functional teams for platform research, testing, deployment, and operations. By integrating various point tools, platform acceptance depends upon cooperation across various security and IT groups. These organizations are proactively addressing organizational challenges for platform proliferation.

Figure 14. Steps Taken in Pursuit of Security Platforms

Which of the following actions has your organization taken in pursuit of implementing tightly integrated, cybersecurity technology “platforms”? (Percent of respondents, N=280, multiple responses accepted)



Source: ESG, a division of TechTarget, Inc.

Conclusion

Based on the research presented in this report, organizations are consolidating security vendors, integrating technologies, and openly considering security platforms in lieu of best-of-breed point tools. Furthermore, 36% of organizations might be willing to buy most security technologies from a single vendor.

These changes are driven by several factors including security technology complexity, limited efficacy, and the global cybersecurity skills shortage (note: For more on the ramifications of the skills shortage, see the ESG/ISSA Research Report, [The Life and Times of Cybersecurity Professionals](#)).

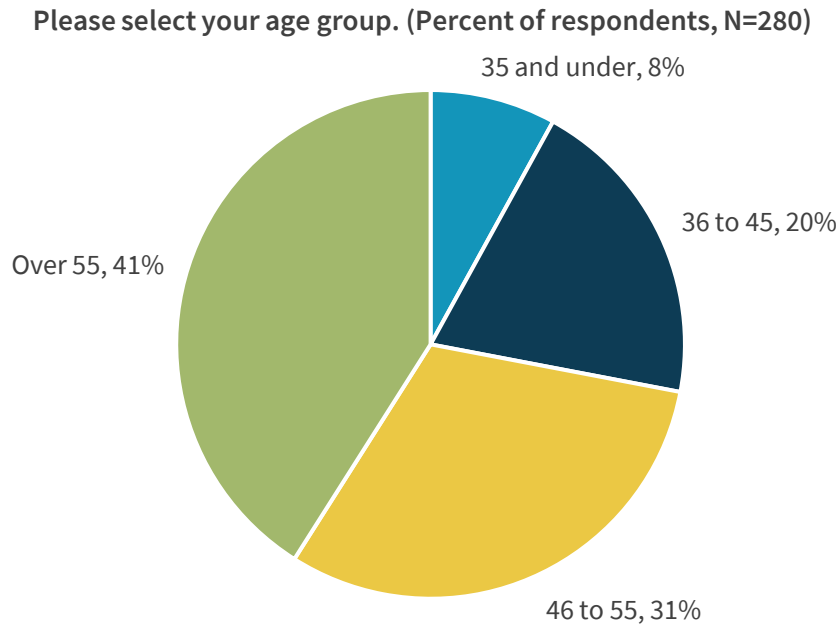
To prepare for and execute on these changes, security professionals should:

- **Push vendors toward industry standards.** While there are a few established security standards from MITRE, Oasis, and the Open Cybersecurity Alliance (OCA), most vendors pay little more than lip service to many of these efforts. This lukewarm behavior would change quickly, however, if large companies pushed their security vendors toward more cooperation and industry standards adoption. ESG/ISSA suggest that large organizations do so on an industry basis, possibly in cooperation with industry ISACs. Standard data formats, APIs, transport protocols, and messaging would go a long way toward easing the integration burden, which security professionals desire.
- **Hire or establish a cybersecurity architect role.** Defining needs, assessing the current technology stack, and adopting an end-to-end security architecture will require extensive skills and experience across a range of security tools. Large organizations should train or hire someone with expertise spanning endpoint, network, and cloud security, while smaller firms may want to work with professional services firms with these capabilities.
- **Establish best practices for vendor qualification.** As organizations buy more security technology from fewer vendors, they should develop a more comprehensive process for all security technology procurement. This should include a list of vendor security process requirements (i.e., a secure development lifecycle, third-party risk management, security training for developers, cyber-supply chain security best practices, etc.) along with processes for continuous vendor security auditing. Vendors that cannot meet these new requirements should be eschewed unless they can prove that they are addressing and overcoming any shortcomings.
- **Develop a three-year strategy for security technology integration.** A security technology architecture may take years to establish as security teams replace point tools, consolidate vendors, and integrate technologies. This process should start with a solid three-year plan that details the current security stack/architecture, defines gaps, and specifies project phases for addressing weaknesses. It's also important to create metrics to measure benefits as independent tools begin to interoperate (i.e., MTTD, MTTC, MTTR, etc.). Finally, CISOs should communicate the three-year plan in business terms to executives and corporate boards. This will help them measure security efficacy/efficiency improvements and project ROI.

Respondent Demographics

The data presented in this report is based on a survey of 280 qualified respondents. Figure 15 through Figure 20 detail the demographics of the respondent base at an individual and organizational level.

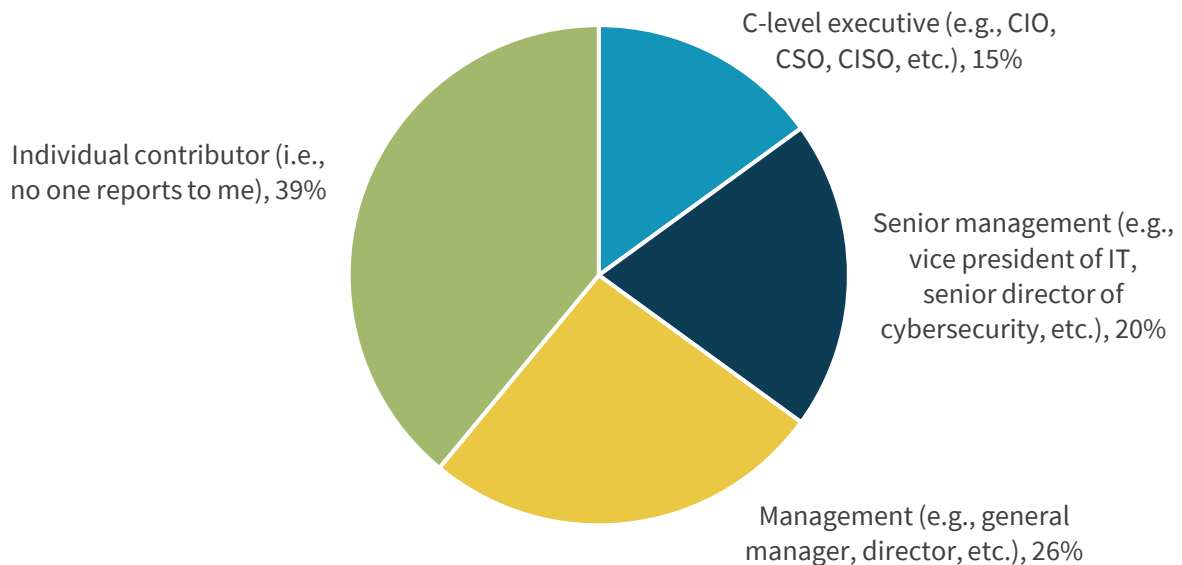
Figure 15. Respondents by Age Group



Source: ESG, a division of TechTarget, Inc.

Figure 16. Respondents by Job Title/Level

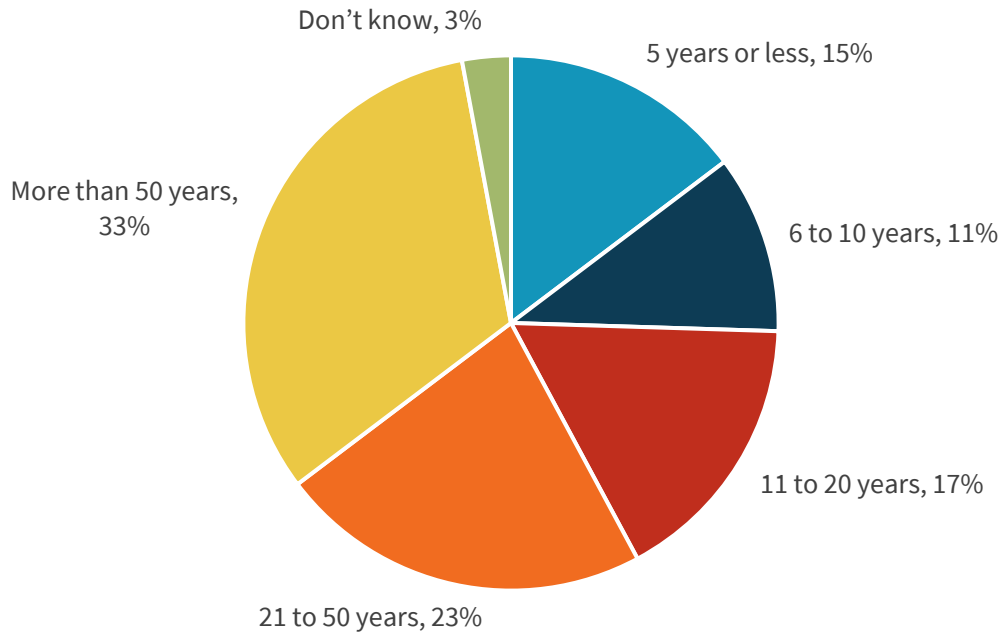
Which of the following best describes your current job title/level? (Percent of respondents, N=280)



Source: ESG, a division of TechTarget, Inc.

Figure 17. Respondents by Age of Organization

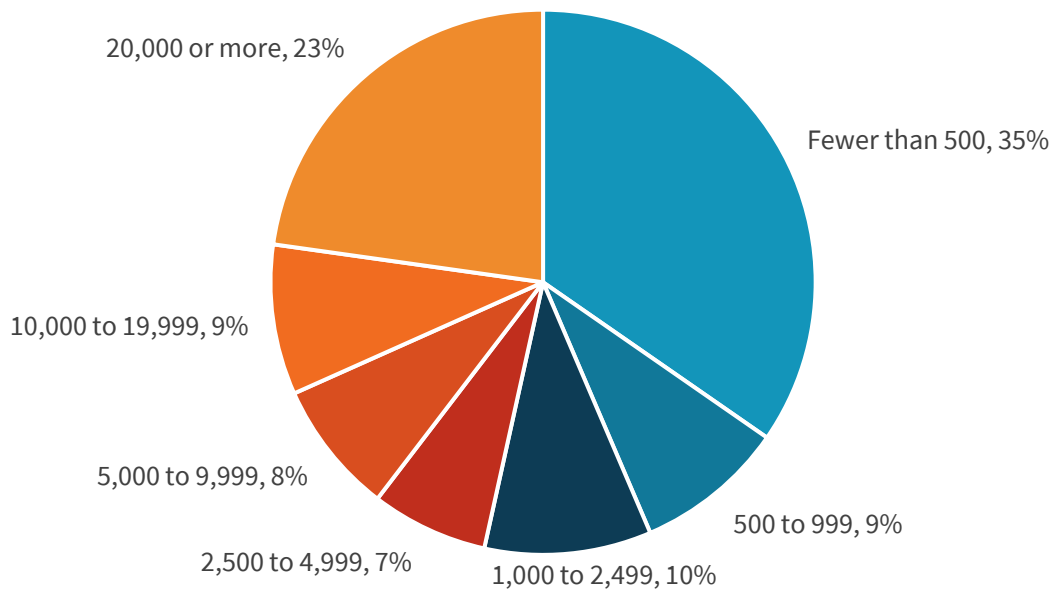
For approximately how long has your current employer been in existence? (Percent of respondents, N=280)



Source: ESG, a division of TechTarget, Inc.

Figure 18. Respondents by Number of Employees

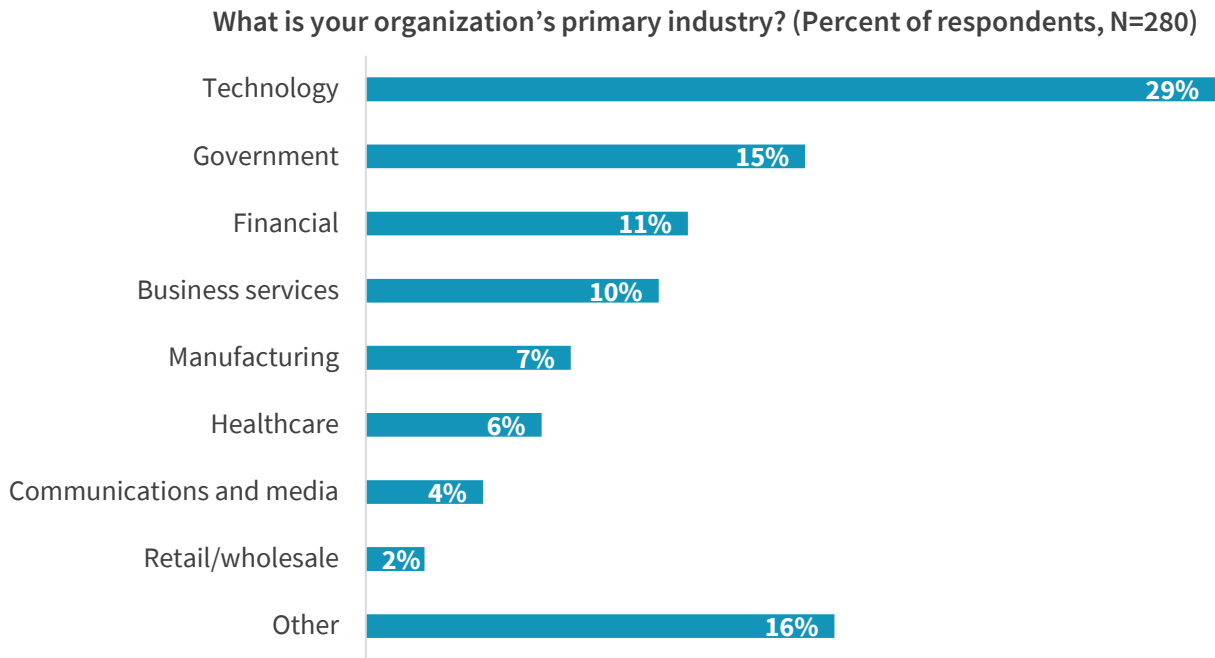
How many total employees does your organization have worldwide? (Percent of respondents, N=280)



Source: ESG, a division of TechTarget, Inc.

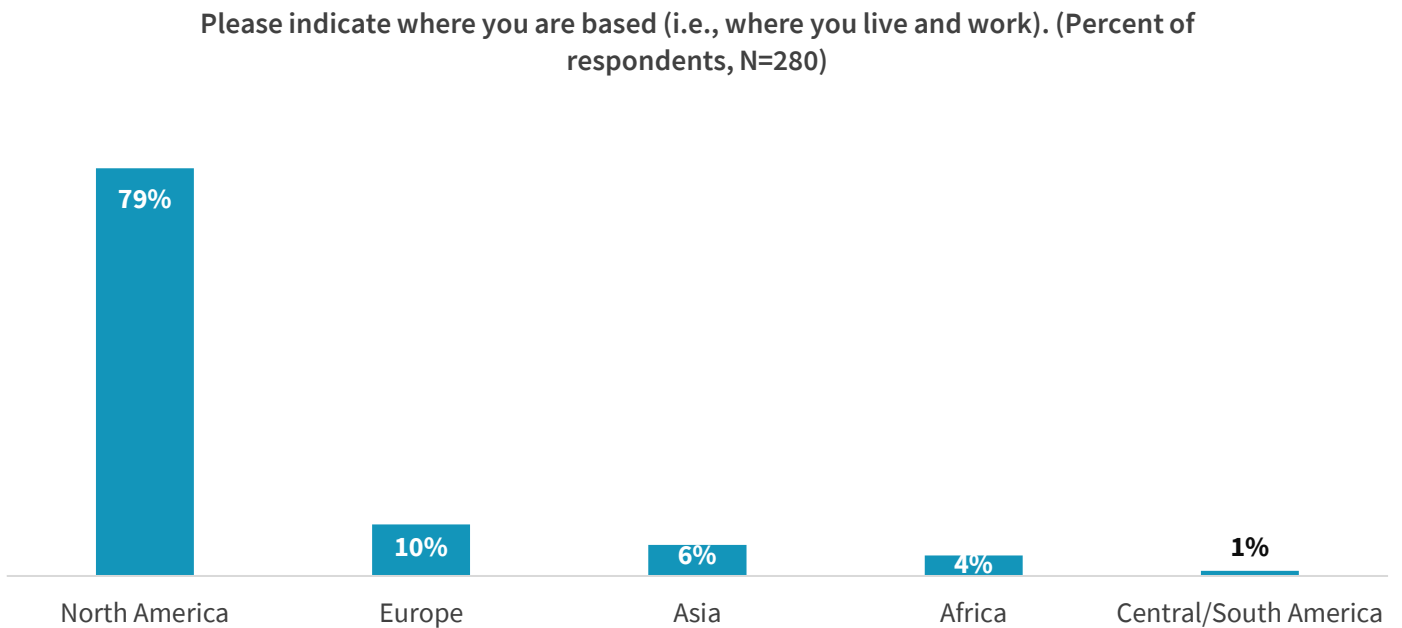
Respondents were asked to identify their organization’s primary industry. In total, ESG received completed, qualified responses from individuals in 22 distinct vertical industries, plus an “Other” category. Respondents were then grouped into the broader categories shown in Figure 15.

Figure 19. Respondents by Industry



Source: ESG, a division of TechTarget, Inc.

Figure 20. Respondents by Region



Source: ESG, a division of TechTarget, Inc.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.


This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188