Research Report

The Shifting Cybersecurity Landscape

Rise of Enterprise-class Vendors

By Jon Oltsik, ESG Senior Principal Analyst; Doug Cahill, Senior Analyst; and Bill Lundell, Director of Syndicated Research

April 2017

Contents

List of Figures

Executive Summary

Report Conclusions

ESG conducted an in-depth survey of 176 IT and cybersecurity professionals responsible for evaluating, purchasing, and managing security technologies for their organizations. Survey participants represented large midmarket (500 to 999 employees) and enterprise-class (1,000 employees or more) organizations in North America (United States and Canada). Based on the data collected from this survey, ESG concludes that:

- **Best of breed is the norm, but integration and architectural compatibility are important product requirements.** Organizations favor cybersecurity products that align with their broader integration strategies based on an architectural approach to alleviate the complexity associated with siloed processes and solutions. While best-of-breed product selection criteria remains intact, product selection is now highly influenced by integration capabilities.
- **Cybersecurity vendor consolidation is happening.** Driven by users' prioritization for integrated products, the industry continues to move toward vendor consolidation. Organizations prefer to first and foremost purchase security products from vendors that they already work with as opposed to using a new vendor for procurement, support, and operational efficiencies.
- **Vendor consolidation increases the influence of the CISO.** The stated intent of enterprise organizations to consolidate the number of vendors from whom they procure cybersecurity solutions will result in CISOs being more involved in strategic briefings with vendors. In these discussions with vendors, CISOs will look to vet the alignment of the current capabilities and product roadmap of a given vendor with their own cybersecurity initiatives and technology adoption plans.
- **The concept of cybersecurity platforms resonates, but needs further refinement.** IT professionals are aware that vendors are increasingly eager to offer "platforms," but there are some gaps in communication and messaging between vendors and customers. The majority of respondents have only a vague idea of what their vendors are offering in regard to a platform and what they are planning with respect to their roadmap. The onus is on vendors to clearly communicate their plans and the benefits of their platforms to gain customers' buy-in.
- **Enterprise-class cybersecurity vendors are emerging.** Enterprise-class cybersecurity vendors are those vendors positioned to offer a broad array of increasingly integrated products and services to large organizations. Or put another way, they are vendors that can serve as a primary source for a wide variety of cybersecurity products and services. Pairing this with the theme of cybersecurity vendor consolidation provides a clear picture of the future: Organizations will work with fewer vendors over time, with preference given to those that meet criteria that characterizes them as "enterprise-class," or those remaining point-tools vendors that latch onto enterprise cybersecurity vendor ecosystems.
- **SIEM is key for enterprise-class security consideration.** Organizations continue to rely heavily on SIEMs as the hub of their security operations. Indeed, nearly half of respondents report that SIEM is very important as part of an enterprise-class security architecture or platform. IT professionals have high standards and broad requirements for their SIEMs, and for prospective enterprise-class security vendors, so offering a feature-rich SIEM will remain paramount.
- **Cisco, IBM, and Microsoft are most commonly perceived as enterprise-class security vendors.** The cybersecurity landscape is packed with vendors, but very few have the portfolio breadth to be considered truly enterprise-class. Among that small group, IT professionals currently view Cisco, IBM, and Microsoft as the leaders. It is noteworthy that Microsoft and Amazon, two vendors only peripherally involved in the cybersecurity technology market, both garnered significant mindshare as enterprise-class security providers. ESG attributes this to the strategic relationships both these organizations have in IT infrastructure.

Introduction

The cybersecurity industry is populated with a plethora of vendors offering discrete solutions representing a fragmented market, historically absent of dominant leaders. The influx of venture capital funding, and, more recently, the participation of private equity firms, have contributed to a growing number of players vying for buyer mindshare and budget. However, notable M&A activity, including Symantec's acquisition of BlueCoat, and the TPG Capital-led spinout of Intel Security, coupled with anecdotal customer feedback about point tool fatigue, indicate the cybersecurity market is at a tipping point, one that could lead to centers of power, vendor-centric ecosystems, and the emergence of a small group of enterprise-class cybersecurity vendors. These dynamics were the impetus for ESG to conduct research on both the rise of enterprise-class cybersecurity vendors and the requirements of enterprise-ready cybersecurity platforms.

Research Objectives

In order to further investigate and assess these trends, ESG surveyed 176 IT and cybersecurity professionals representing large midmarket (i.e., 500 to 999 employees) and enterprise (i.e., 1,000 or more employees) organizations in North America, though it is worth noting that more than 90% of respondents are employed at organizations with at least 1,000 employees. The survey was designed to provide insight into the following questions:

- How are IT decision makers approaching cybersecurity product purchasing decisions when it comes to best of breed, integrations, and single sourcing?
- What do IT and security professionals view as the most important characteristics of an enterprise-class cybersecurity vendor?
- Which vendors are perceived to be "enterprise-class" cybersecurity vendors?
- What changes have organizations undergone in regards to their cybersecurity processes and product selection decisions?
- Are vendors succeeding in messaging their platforms to customers and prospects?
- Are organizations opting for cybersecurity vendor consolidation initiatives?
- How do IT decision makers view "enterprise-class" cybersecurity vendors? What defines them? Who are the leaders?
- How will vendor consolidation affect the CISO's influence in product purchasing decisions?
- How have integration requirements altered the evaluation, the purchase, and the deployment process for cybersecurity technologies?
- How do organizations view SIEM technology? How important is SIEM technology to their overall strategy and operations?

Survey participants represented a wide range of industries including financial services, manufacturing, health care, and retail. For more details, please see the *Research Methodology* and *Respondent Demographics* sections of this report.

Research Findings

Best of Breed Is the Norm, but Architectural Integration Is an Important Product Requirement

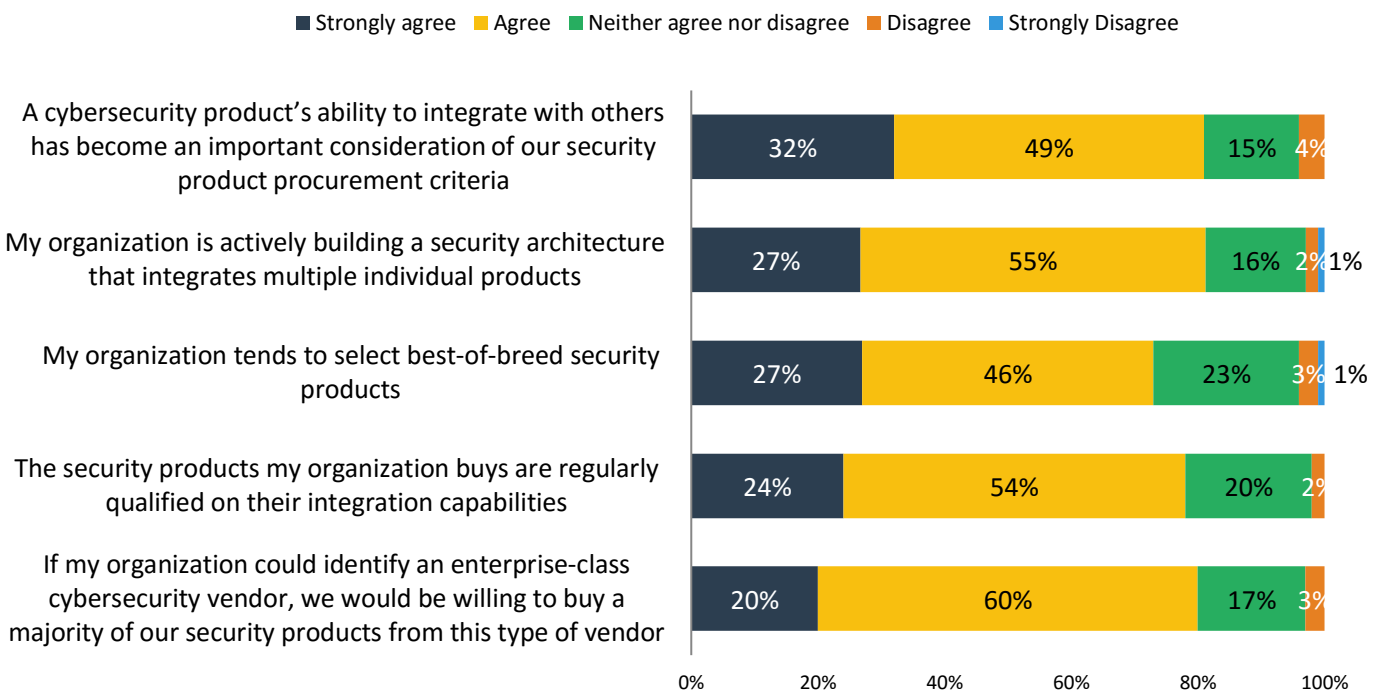
Organizations increasingly need to do more with less when it comes to cybersecurity. The well-documented cybersecurity skills shortage that ESG has tracked for the last several years continues to impact organizations in that most cannot hire their way to better security; they must instead make the most of the technology and staff at their disposal. In practical terms, this means that integrating various cybersecurity products and technologies is now a central factor in purchasing decisions.

A nuanced look at the data bears this point out. For example, Figure 1 shows that 73% of respondents strongly agree or agree that their organization tends to select best-of-breed security products. This is consistent with historical infosec behavior where each product was evaluated and purchased based upon its overall security efficacy compared with other competitive technologies. However, 81% of those same respondents also strongly agree or agree that a cybersecurity product's ability to integrate with others (i.e., by way of standards adherence, open APIs, integration support, etc.) has become an important consideration for the procurement of cybersecurity solutions, with 82% noting they are actively building an architecture to support such integrations. Similarly, 78% of respondents strongly agree or agree that security products are regularly qualified on their integration capabilities. This supports the notion that best-of-breed *must* include technology integration support. Yet the requirement for integration does not negate the interest in a primary supplier of cybersecurity products and services as evidenced by 80% of participants noting they would buy a majority of cybersecurity products from an enterprise-class vendor.

Taken in sum, the data paints a picture: Organizations still want best-of-breed products, but favor those offering superior potential integration capabilities. This represents a possible break from the past when cybersecurity professionals often followed a best-of-breed strategy for every individual cybersecurity technology deployed on hosts and networks. While this general philosophy still remains intact today, the data suggests that because each product is now also evaluated and selected based upon its integration capabilities, the equation is no longer tilted purely in favor of technical superiority. In fact, a convincing 74% of survey respondents report that their organization selects best-of-breed *only* if the product is designed for broader technology integration (see Figure 2). This attitude was further summed up in a recent discussion with an enterprise CISO. When asked about product integration, he stated, "Product integration *is* the new best-of-breed."

Figure 1. Cybersecurity Product Considerations and Strategies

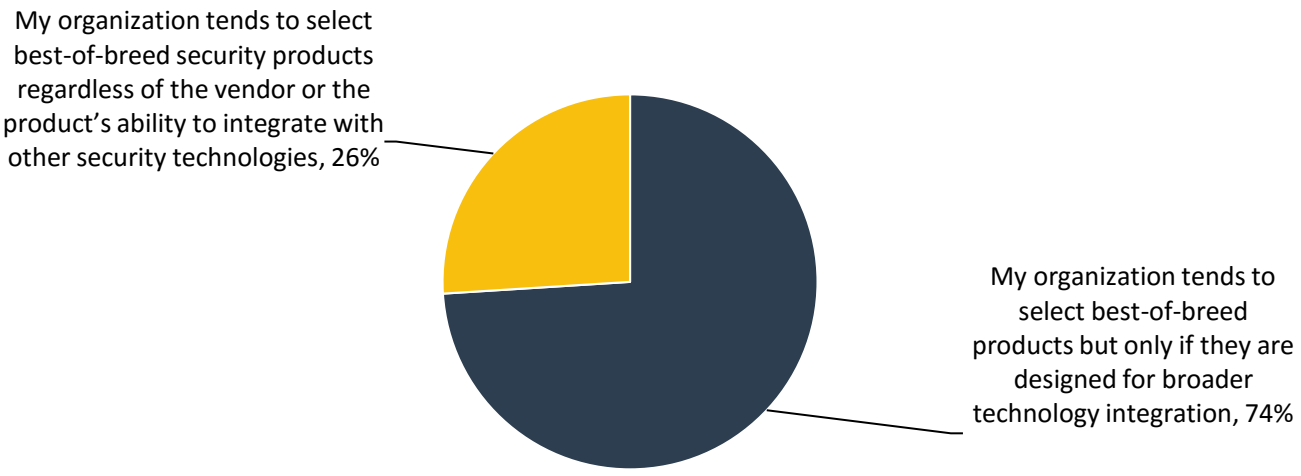
Please indicate whether you agree or disagree with each of the following statements. (Percent of respondents, N=176)



Source: Enterprise Strategy Group, 2017

Figure 2. Best-of-breed Product Outlook

Which of the following statements about best-of-breed products most closely aligns with your organization's outlook? (Percent of respondents, N=129)



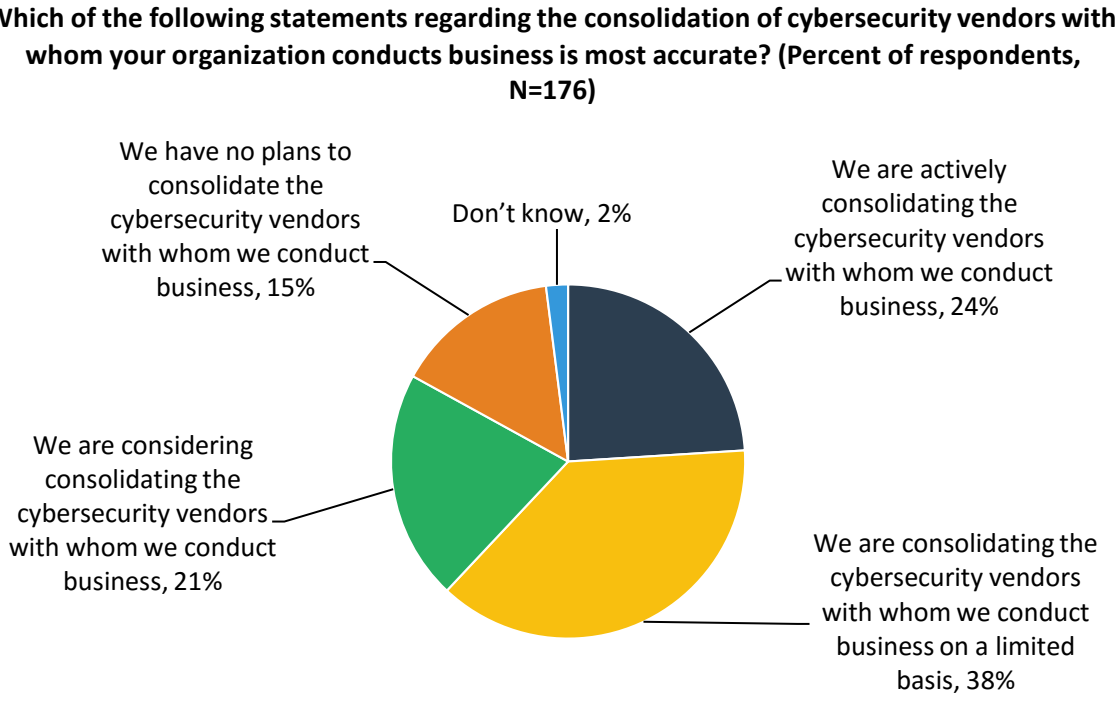
Source: Enterprise Strategy Group, 2017

Cybersecurity Vendor Consolidation Is Happening

While organizations prioritize best-of-breed security products built for integration, they are also winnowing down the total number of vendors from whom they purchase security products and services. In fact, nearly one-quarter of organizations are actively consolidating the cybersecurity vendors they conduct business with while another 38% are consolidating security vendors on a limited basis today (see Figure 3). It is worth noting that organizations of all sizes are consolidating cybersecurity vendors. This points to a general trend where CISOs will likely continue to reduce the number of security vendors they work with in the future. This data seems to indicate that there will be winners and losers in the cybersecurity industry in the near future.

These trends—the importance of integration capabilities, growing vendor consolidation, and increasing CISO involvement—indicate that organizations are likely to change the way they qualify and perform due diligence on the cybersecurity vendors they ultimately choose. Indeed, the data shows organizations have become more rigorous in their testing and more demanding in their expectations from vendors (see Figure 4). Twenty-four percent of respondents indicate that over the last 12 months they have begun performing due diligence to examine the cloud hosting environment of their security-as-a-service providers, while an equal 24% report that they have begun requiring regular roadmap reviews from their most strategic vendors. While these activities were not unheard of in the past, their practices appear to be more commonplace and rigorous than in the past. Cybersecurity vendors will have to adopt best practices for secure development, supply chain management, staff training, and field support in order to achieve "enterprise-class" status.

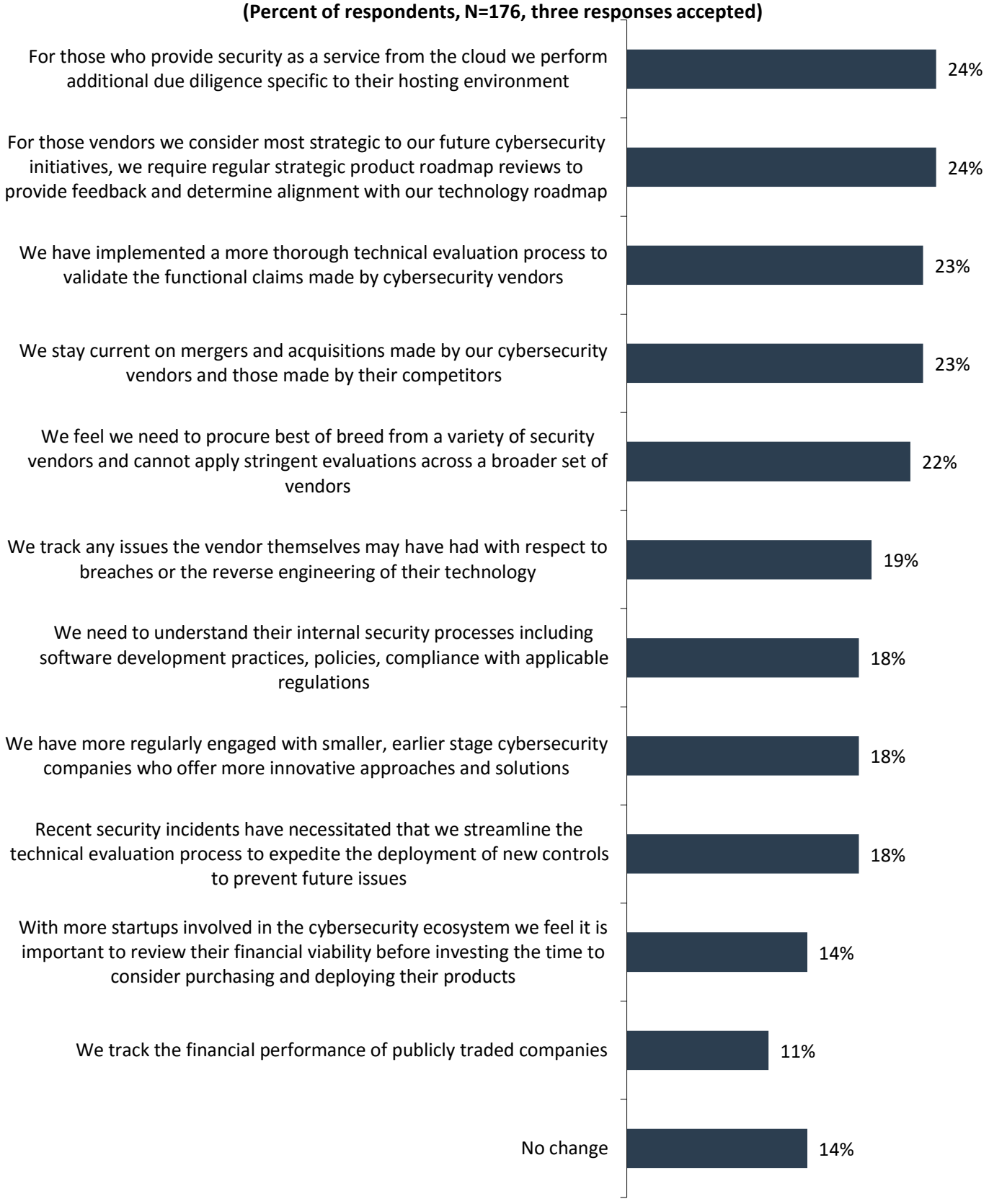
Figure 3. Cybersecurity Vendor Consolidation Sentiment



Source: Enterprise Strategy Group, 2017

Figure 4. Changes in Cybersecurity Vendor Management Over the Last 12 Months

How, if at all, has your organization's management of cybersecurity vendors changed over the last 12 months? (Percent of respondents, N=176, three responses accepted)



Source: Enterprise Strategy Group, 2017

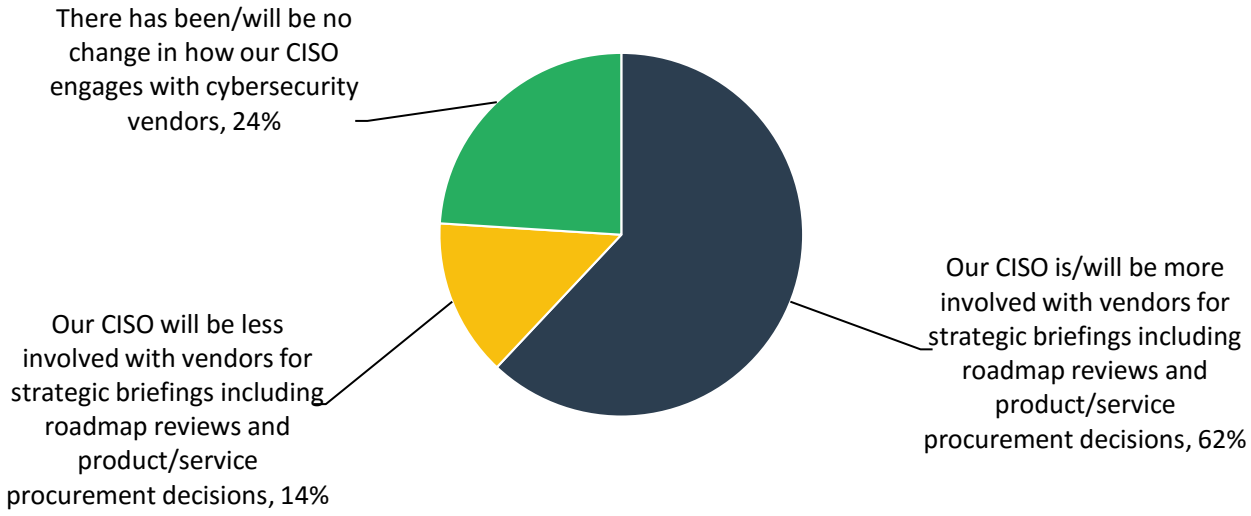
Vendor Consolidation Increases the Influence of the CISO

Vendor consolidation may simplify activities like contract management and lead to more attractive discounts, but it also comes with some risk typically associated with relying on a single vendor (i.e., putting all of your proverbial eggs in one basket). To mitigate these risks, organizations will dedicate more effort toward vendor risk management by assessing each vendor's cyber supply chain, employee background checks, and technical support capabilities. Given the gravity of these risks, it is not surprising that 62% of cybersecurity professionals claim that their CISO is/will be more involved with vendors for activities like strategic briefings, including roadmap reviews and product/service procurement decisions (see Figure 5).

With greater CISO involvement in product evaluation and selection, cybersecurity vendors must have the ability to communicate with and sell to CISOs if they hope to be viewed as enterprise-class. Selling to the CISO, however, will be challenging for security product and services vendors used to selling product feature/functionality directly to technologists rather than executives. To address changes in purchasing behavior, these vendors must hire executive level account managers or retrain direct sales and partners who can discuss cybersecurity issues in a business context.

Figure 5. Impact of Cybersecurity Vendor Consolidation on Role of CISO

What impact – if any – has your organization's cybersecurity vendor consolidation efforts had – or do you expect them to have – on the role of your CISO? (Percent of respondents, N=146)



Source: Enterprise Strategy Group, 2017

The Concept of Cybersecurity Platforms Resonates, but Needs Further Refinement

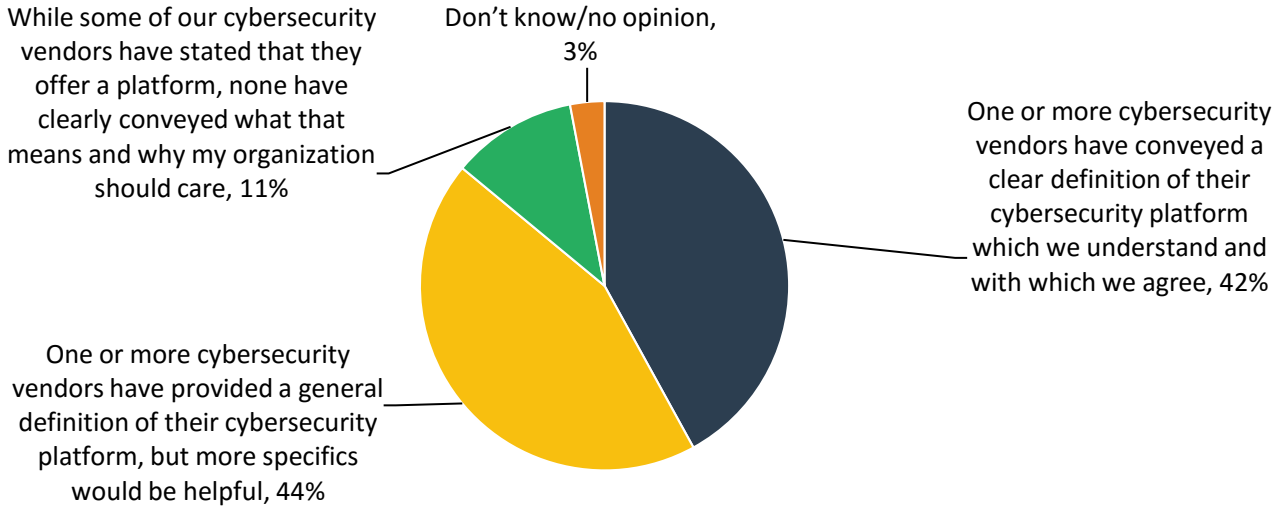
The aforementioned trends of product integration, vendor consolidation, and stringent vendor qualification collectively lend themselves to the concept of cybersecurity platforms as a means to realize these objectives. However, there exists a fundamental disconnect between vendors and customers/prospects when it comes to simply defining what a "platform" is. Fifty-five percent of respondents indicate that they either have not received enough detail from one or more vendors or they have not clearly understood platform offerings from *any* of their vendors (see Figure 6). This indicates that confusion persists, making cybersecurity "platforms" more hyperbole than reality.

Contributing to the disconnect between customer and vendor definitions of a cybersecurity platform is likely the fact that both parties are in the early stages of considering what constitutes a platform or what is considered the most important requirements for a platform (see Figure 7). Thirty-eight percent of respondents believe that the most important attribute of a cybersecurity platform is a set of controls that span applications, hosts, and the network to coordinate threat prevention, detection, and response, while 22% of respondents cite that the most important attribute of a cybersecurity platform is an integrated product suite from a single vendor that also provides APIs for the integration of third-third party technologies.

These requirements are certainly not mutually exclusive, but the differences in the most important attribute of a cybersecurity platform make it challenging for vendors to communicate the focus of their respective platforms. Refinement of this concept can be expected moving forward on an industry-wide basis, during which time this current confusion represents an opportunity for vendors to establish and cultivate thought leadership around their notion of a cybersecurity platform. For example, Vendor A may cater to the majority seeking applications, host, and network controls, while Vendor B specializes in customers seeking open source capabilities. The important consideration for vendors is to provide clarity on the focus and differentiations of their cybersecurity platform that align with market requirements and resonate with cybersecurity professionals.

Figure 6. Cybersecurity Platform Sentiment

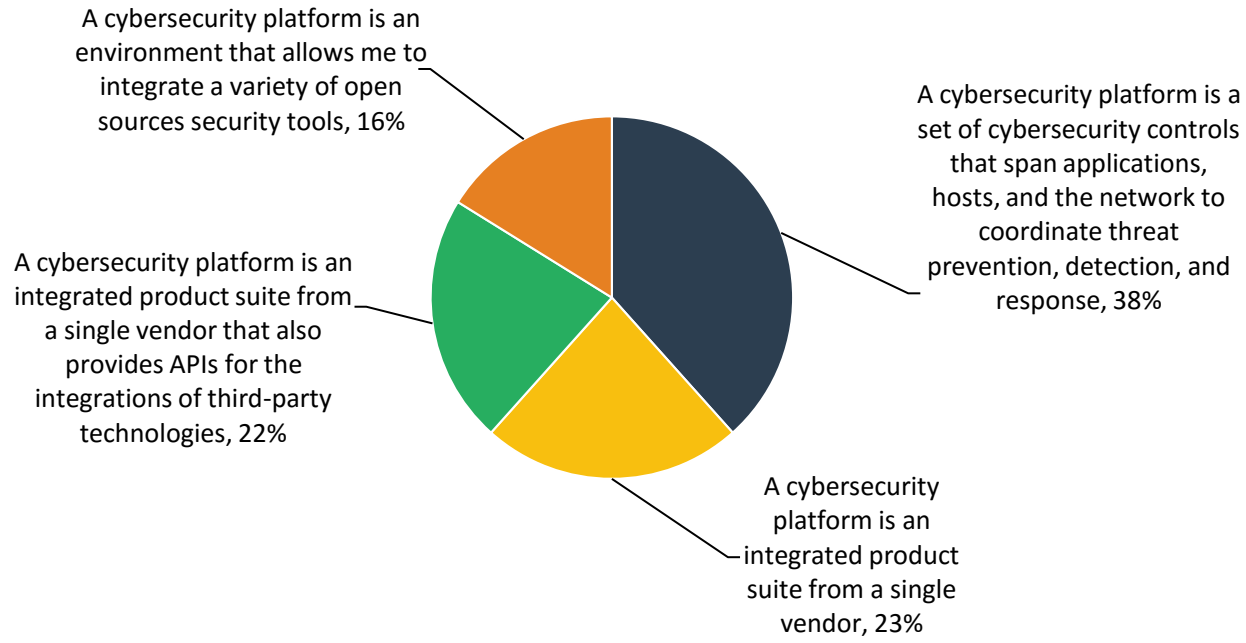
Which of the following statements most closely aligns with your opinion as to whether the cybersecurity industry has provided you and your organization a clear definition of a cybersecurity "platform"? (Percent of respondents, N=176)



Source: Enterprise Strategy Group, 2017

Figure 7. Most Important Attribute of a Cybersecurity Platform

In your opinion, which of the following is the most important attribute of a cybersecurity "platform"? (Percent of respondents, N=176)



Source: Enterprise Strategy Group, 2017

Enterprise-class Cybersecurity Vendors Are Emerging

Customer demand for integrated solutions, the desire to consolidate vendors, and other aforementioned trends point to an opportunity for a select group of enterprise-class cybersecurity vendors (i.e., vendors that can offer features like leading integrated products, central management, professional/managed services, etc.). The perceived points of value in procuring cybersecurity solutions from enterprise-class vendors include (see Figure 8):

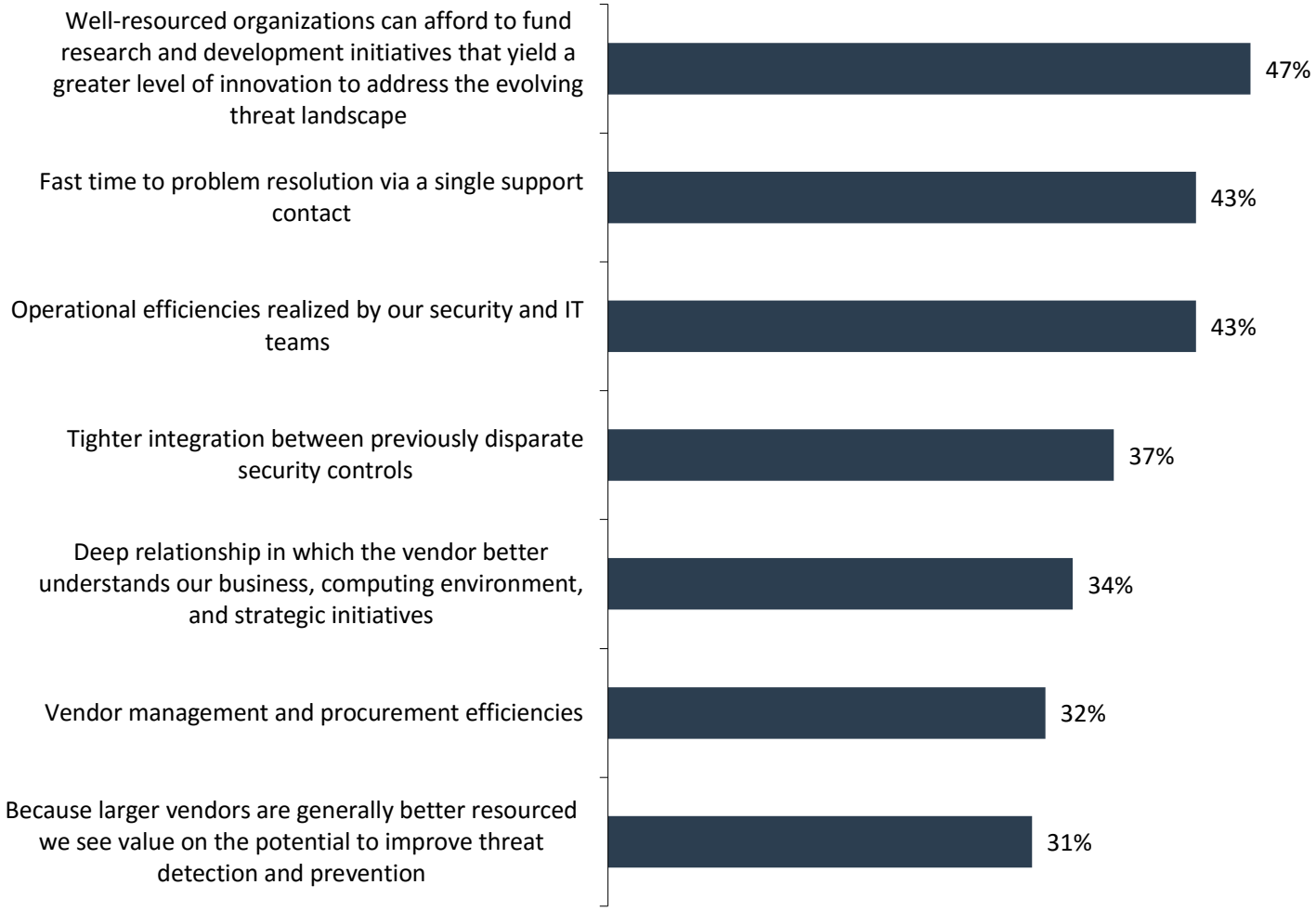
- **Continuous innovation.** Nearly half (47%) of respondents see value in enterprise security vendors that have the resources to fund cybersecurity R&D and continually innovate to keep up with user requirements and the threat landscape. This may be a function of enterprise security vendors remaining active in M&A activity to purchase innovative startups, but the data suggests that users want a combination of innovation and an integrated architecture.
- **Consolidated support.** Interestingly, 43% of respondents see value in an enterprise security vendor's ability to provide problem resolution through a single support contact. Given the global cybersecurity skills shortage and the current security operations morass, it makes sense that CISOs want to simplify security operations wherever they can.
- **Operational efficiencies.** Similarly, 43% believe that enterprise security vendors can deliver value through operational efficiencies with security and IT operations teams. Since these two groups tend to collaborate on provisioning, configuration management, and incident response, a common enterprise security platform could lead to better coordination, communications, and workflows.

Aside from the general value, survey respondents were asked to identify the most important attributes of an enterprise security vendor. These results were especially interesting (see Figure 9). The highest percentage (35%) say the most important attribute for an enterprise cybersecurity vendor is expertise specific to their industry. In other words, enterprise cybersecurity vendors must have knowledge and experience with industry business processes, specific technologies, and regulations. Nearly one-third (32%) of respondents chose three other important attributes:

- **Offer cybersecurity products/services that align with IT initiatives.** This means that enterprise cybersecurity vendors must have products and services that support projects like cloud computing, digital transformation, mobile applications, and IoT.
- **Lead with a commitment to streamlining security operations and cutting costs.** CISOs are overwhelmed today by factors like security alert volume and manual processes. Thus, they are looking for enterprise security vendors that can help them overcome these challenges and make operations more efficient, effective, and productive.
- **Provide products built for integration, scale, and business processes.** This equates to a broad portfolio of products, a commitment to scale and performance, and an architectural approach where multiple products act as force multipliers.

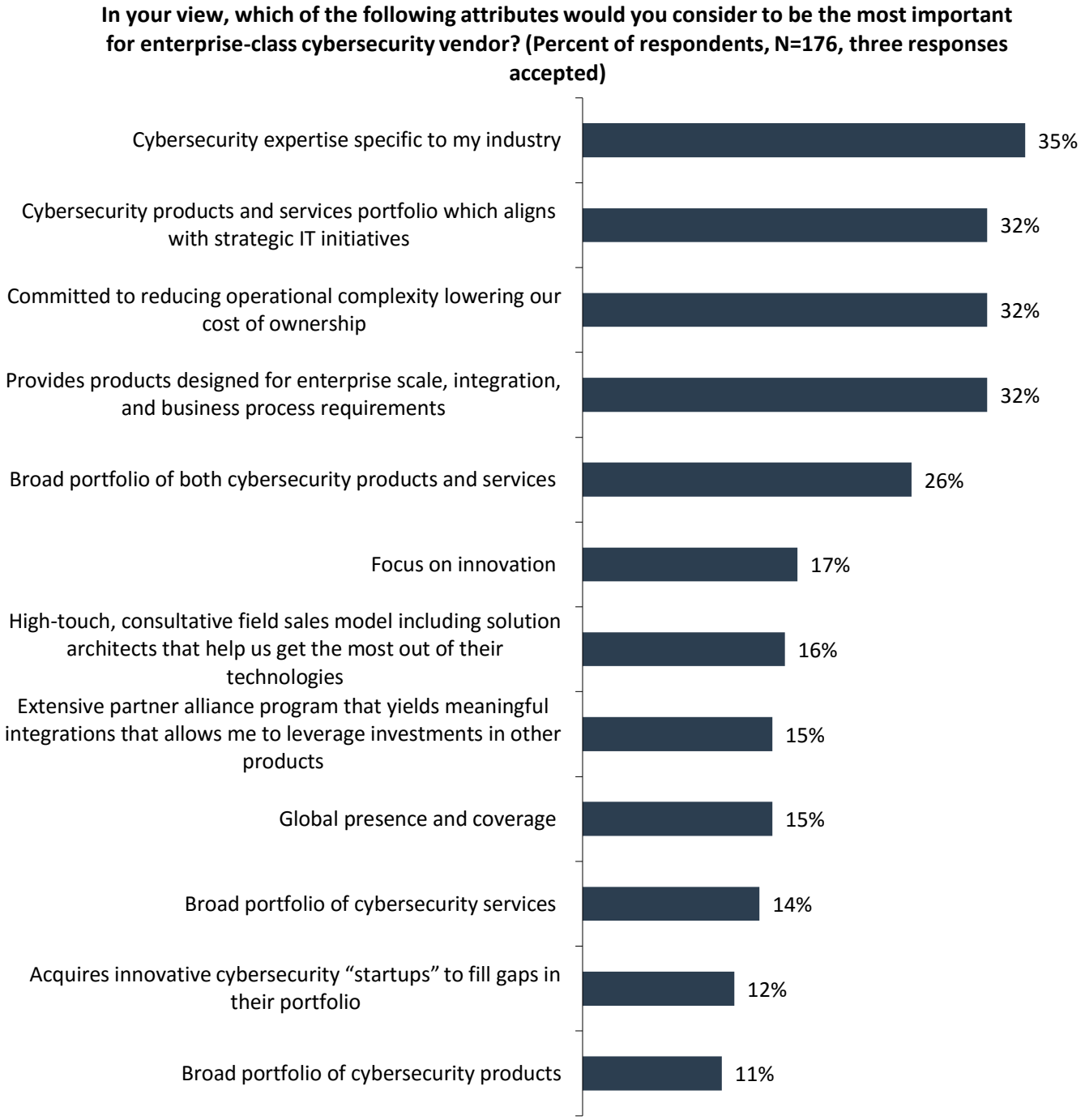
Figure 8. Value of Procuring Cybersecurity Solutions from Fewer Enterprise-class Vendors

Which of the following best represents your organization's perspective on the value of procuring cybersecurity solutions from fewer enterprise-class cybersecurity companies? (Percent of respondents, N=176, multiple responses accepted)



Source: Enterprise Strategy Group, 2017

Figure 9. Most Important Attributes for Enterprise-class Cybersecurity Vendor



Source: Enterprise Strategy Group, 2017

SIEM Is Important for Enterprise-class Security Consideration

The role of security information and event management (SIEM) solutions has evolved from compliance use cases to incident response, security analytics, and threat hunting. For many organizations, their SIEM remains the center of the security operations center (SOC), receiving, aggregating, processing, and correlating logs and events from sensors across their environment. The central role of SIEM is reflected in the fact that nearly half of respondents (48%) report that SIEM is very important as part of an enterprise-class security architecture or platform, with an additional 45% reporting that SIEM is somewhat important as part of an enterprise-class security architecture or platform (see Figure 10).

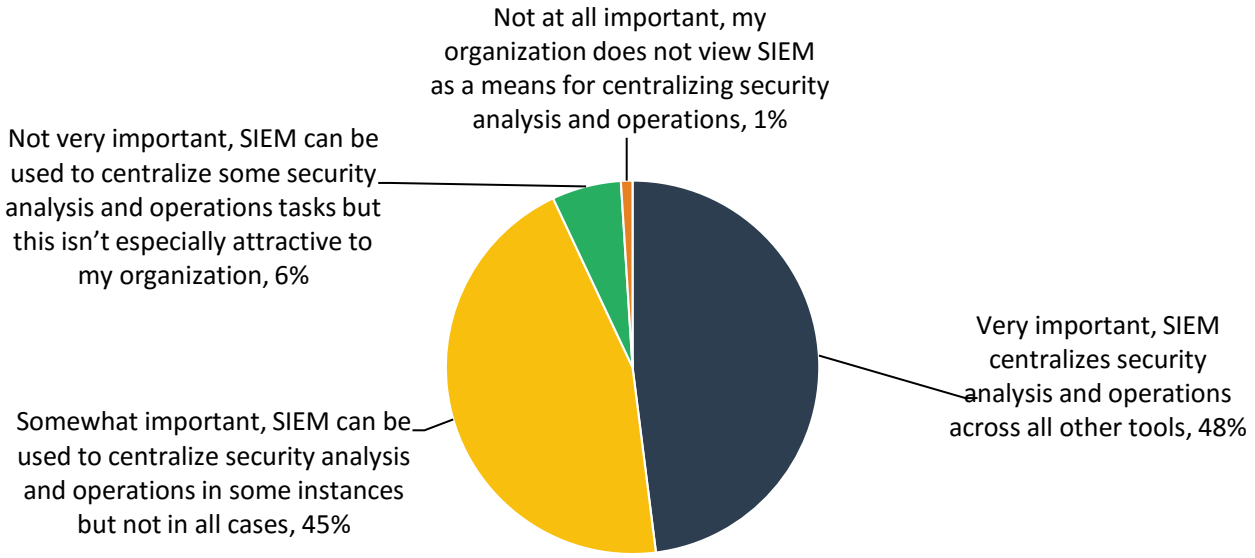
Given the overall importance of SIEM to many organizations' overall cybersecurity operations, it is not surprising that IT professionals largely consider it important for an enterprise-class cybersecurity vendor to offer a SIEM product as part of its portfolio. In fact, an overwhelming 90% of respondents stated that it is either very important or important for a vendor to offer its own SIEM product in order to even be *considered* enterprise-class (see Figure 11). Vendors that do not offer a SIEM product will need to partner with SIEM leaders while conveying how they enable SIEM use cases with other solutions in their portfolio.

Furthermore, it is important for vendors offering a SIEM to understand how cybersecurity professionals are using the technology. Respondents indicate that the capabilities they consider most important to an enterprise-class cybersecurity portfolio include threat intelligence integration (36%), which is often sourced from another vendor, and the centralization of security data collection (30%) (see Figure 12). ESG research participants also indicated that they look to their SIEM to enable a variety of important use cases including incident response automation for remediation tasks (26%) and integrated vulnerability scanning (23%).

It is worth noting that these use cases can be part of a single product like SIEM or part of an overall security operations and analytics platform architecture (SOAPA). In other words, functions like threat intelligence integration could be performed on a dedicated threat intelligence platform (TIP), while incident response automation and orchestration could be delegated to an incident response platform (IRP) designed to track IR workflows throughout their lifecycles. Enterprise cybersecurity professionals demand this functionality *and* tight integration with SIEM. In this way, enterprise security vendors lacking a SIEM can partner with SIEM vendors and then effectively surround the SIEM with add-on capabilities through individual products and a comprehensive architecture.

Figure 10. Importance of SIEM as Part of Enterprise-class Security Architecture/Platform

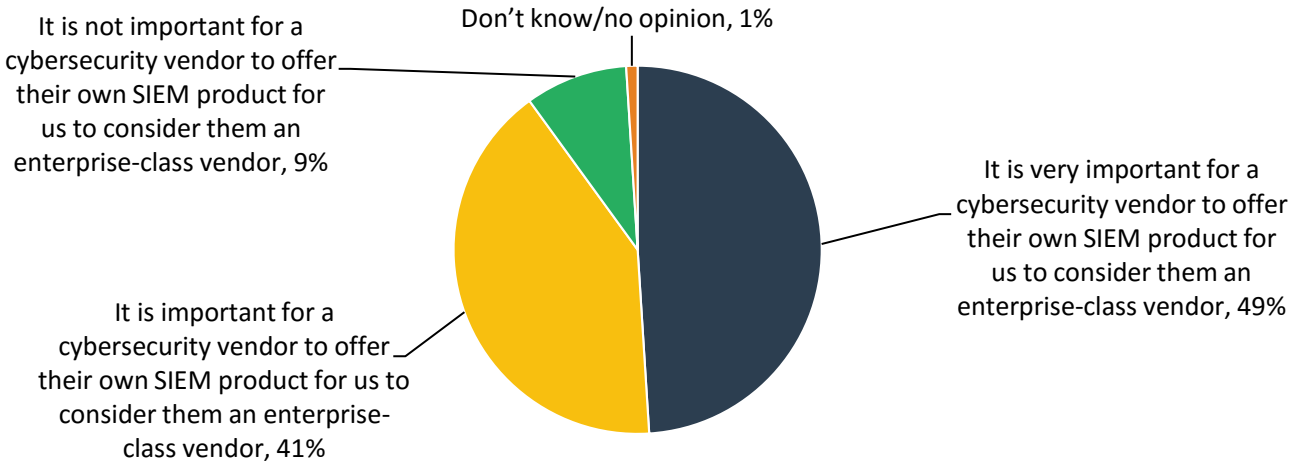
In your opinion, how important is a security information and event management (SIEM) system as part of an enterprise-class security architecture or platform? (Percent of respondents, N=176)



Source: Enterprise Strategy Group, 2017

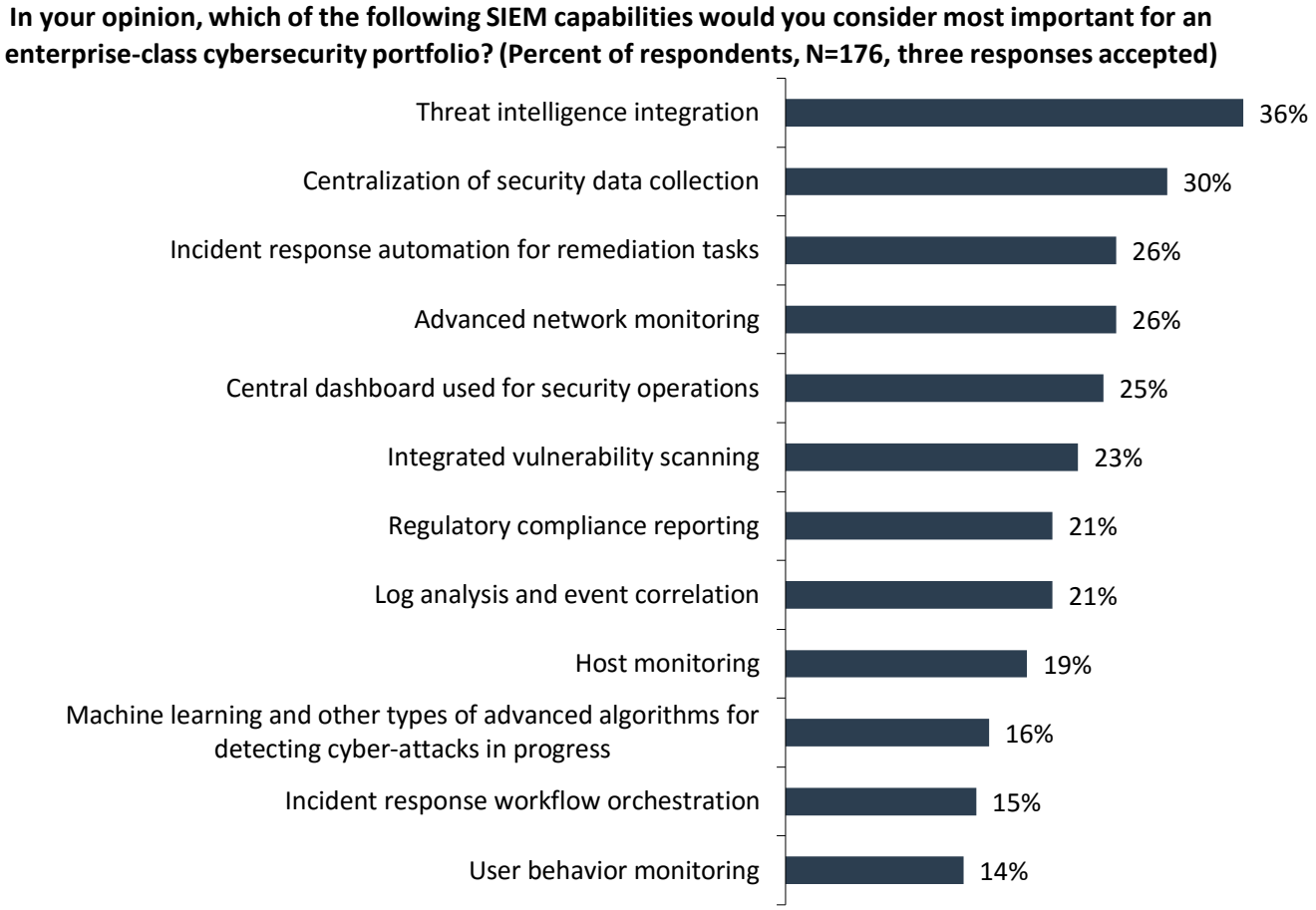
Figure 11. Importance of Enterprise-class Cybersecurity Vendor Offering SIEM Product

In your opinion, how important is it for an enterprise-class cybersecurity vendor to offer a SIEM product? (Percent of respondents, N=176)



Source: Enterprise Strategy Group, 2017

Figure 12. SIEM Capabilities Considered Most Important to Enterprise-class Cybersecurity Portfolio

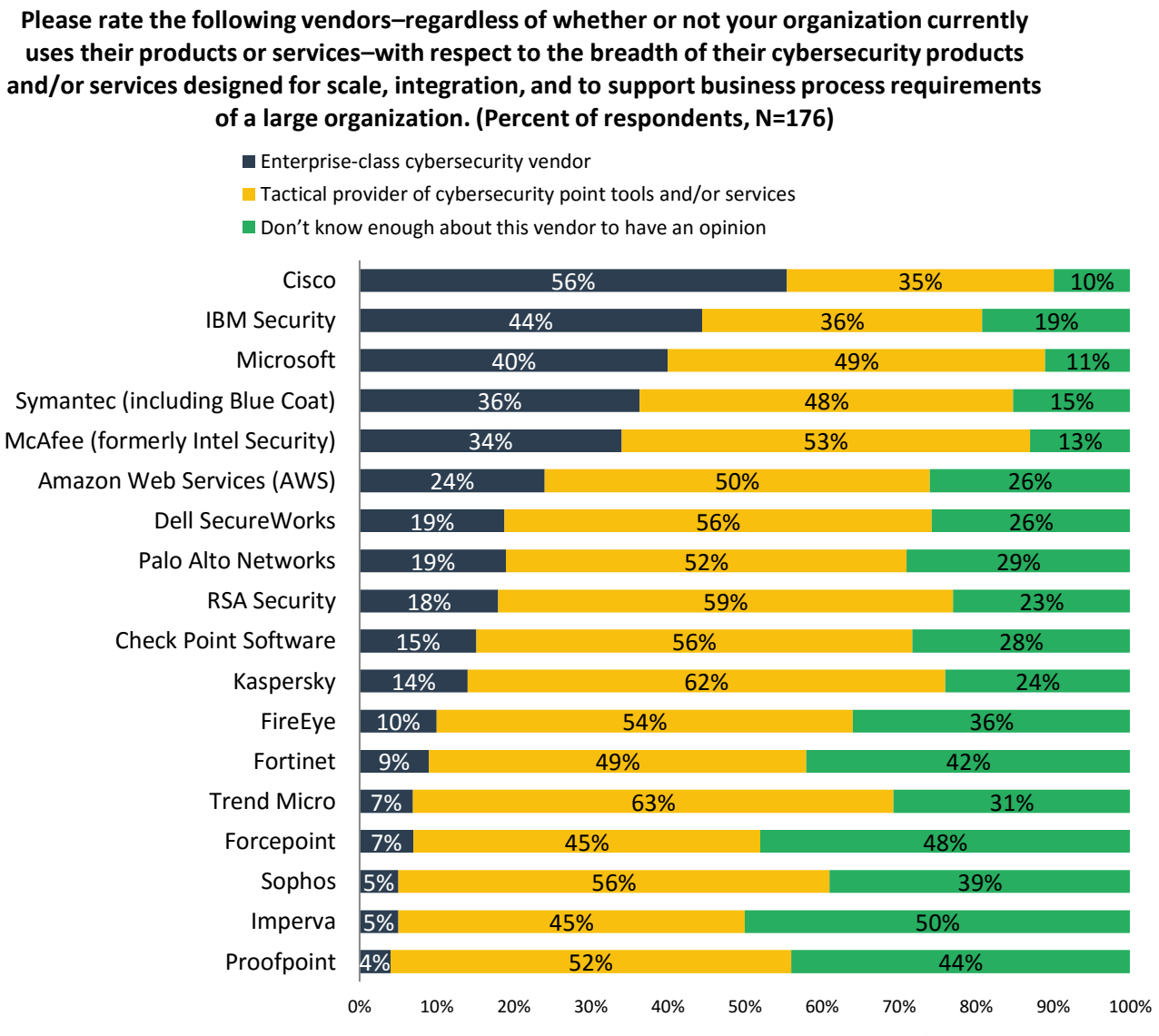


Source: Enterprise Strategy Group, 2017

Cisco, IBM, and Microsoft Are Most Commonly Perceived as Enterprise-class Security Vendors

The concept of enterprise-class cybersecurity vendors is on the rise, but the vendor profiles remain somewhat ill-defined. However, when given a loose working definition of the term, ESG found that respondents most commonly consider Cisco (56%), IBM (44%), and Microsoft (40%) to be "enterprise-class" (see Figure 13). Other established cybersecurity vendors like Symantec and McAfee were not at the very top, but they did remain in the upper echelon of responses rounding out the top five. ESG believes it is noteworthy that Microsoft and Amazon, two vendors only peripherally involved in the cybersecurity technology market, occupy the third and sixth positions respectively. ESG attributes this to the strategic relationships these organizations have in IT infrastructure. Large organizations buy numerous products from Microsoft and invest a lot of time and effort into securing these products. Furthermore, Microsoft Active Directory remains a foundational component of enterprise security for user authentication, DHCP, and policy management. Amazon's presence on this list is directly related to continuing growth in enterprise use of AWS and other cloud services. Again, this means that security teams must have the proper training, controls, and oversight to mitigate risk and respond to incidents related to AWS.

Figure 13. Respondents Rate Cybersecurity Vendors



Source: Enterprise Strategy Group, 2017

Conclusion

The well-known challenges of securing an expanding attack surface area against the ever-evolving threat landscape has necessitated the adoption of point tools. To combat multistage attacks with great efficiency, organizations are now actively building an architecture to enable the integration of disparate technologies, making integration a foundational product requirement. The fact that IT and security professionals stated they prefer to purchase security solutions from existing vendors and are actively consolidating their vendors indicates a preference to procure pre-integrated product suites based on platforms that also allow for the integration of best-of-breed tools. To meet these requirements, vendors are prescribing cybersecurity platforms, the definition of which is still a work in progress. As organizations become more dependent on a smaller number of vendors that can provide such platforms, the vendors will be more rigorously evaluated, which makes the role of the CISO even more prominent in vendor and product selections. Major IT brands—Cisco, IBM, and Microsoft—with strong cybersecurity product portfolios, along with pure-play cybersecurity vendors Symantec and McAfee, are perceived as offering the requisite level of functional breadth and integration and thus are best positioned to emerge as enterprise-class cybersecurity market leaders. All told, the dichotomy of having to purchase point tools tactically to close security gaps while taking steps toward a strategic architectural approach based on integrations and platforms represents a shift in the cybersecurity landscape.

Research Implications for Cybersecurity Vendors

Based on the findings of this research, ESG offers the following recommendations to cybersecurity vendors positioning their brand as an enterprise-class provider of cybersecurity products and services:

- **Convey a clear definition of your platform.** More than half of research participants indicated that platform definitions provided by cybersecurity vendors have not been clearly conveyed or need more specifics, representing an opportunity for vendors to establish thought leadership around the immutable attributes of a cybersecurity platform. Based on customer requirements of a cybersecurity platform, such a definition will be one that, at a high level, provides depth of threat detection, prevention, and response capabilities across the breadth of an organization's attack surface area.
- **Enable integrations and best-of-breed controls.** While participants indicated an intent to consolidate their vendor base and initiatives to define an architecture and requirement for a platform, it is also clear there will be continued demand for best-of-breed cybersecurity products. These seemingly conflicting findings should be rationalized and embraced via the delivery of platforms based on an open architecture that enables the integration of best-of-breed technologies.
- **Engage in a strategic dialog with CISOs.** CISOs at organizations consolidating vendors will be highly engaged with vendors on their product roadmap plans. To evolve from being perceived as a supplier to a trusted and strategic partner, vendors should establish a regular cadence of such conversations with CISOs to gain alignment and endorsement of the technical and business aspects of their products and services.
- **Cite your SIEM as an essential element of your portfolio or fill the gap.** Given the research finding that cybersecurity professionals view a SIEM as a product that is important for enterprise-class cybersecurity vendors to provide, the SIEM offering in a cybersecurity portfolio should be positioned as a core element of the platform. Enterprise-class cybersecurity vendors whose product portfolio does not include a SIEM will need to point to partnerships with SIEM vendors, consider acquiring a standalone SIEM vendor, and/or cite other functional capabilities to address the SIEM requirement.
- **Tout industry-specific knowledge for vertical marketing.** Vendors with expertise, knowledge of, and success in specific industry verticals should employ vertical market campaigns to leverage that domain knowledge to maximize penetration in those markets. Those vendors that have not yet developed a core competency in verticals they target, or intend to sell into, will need to make investments to better understand industry-specific

dynamics such as regulations, hire professionals from those industries and/or systems, and/or establish partnerships for credibility by proxy in those markets.

Research Implications for Cybersecurity Professionals

The learnings from this research also provides important insights for cybersecurity professionals at organizations with strategic initiatives to employ cybersecurity platforms from enterprise-class vendors including:

- Evaluate a vendor's ability to meet your enterprise-class requirements. While this research conducted by ESG revealed that capabilities such as threat intelligence integration, incident response automation, and more, are requirements of enterprise-class cybersecurity vendors, each organization will have its own set of requirements. As such, as part of consolidating vendors and establishing a cybersecurity architecture, companies should establish that set of requirements internally, and then evaluate whether vendors positioned as enterprise-class can meet those requirements today or have a credible roadmap to do so in an acceptable time frame.
- Vet the alignment of the definition of a cybersecurity platform. As more cybersecurity vendors position their solution as a platform, the functional abilities and thus definition of a platform will vary. Security professionals should work collaboratively internally to define what a cybersecurity platform is for them based on the use cases it would enable, and then vet alignment with enterprise-class vendors on that definition.
- Look for integrations with existing controls that enable use cases. To fully leverage investments in existing controls, and those that could be employed in the future, organizations evaluating offerings from enterprise-class vendors should look for meaningful levels of integrations based on an open architecture. Such integrations will go beyond simple event sharing to enable use cases such as coordinated and expedited threat detection, prevention, and remediation between network and endpoint security controls. Customers should also evaluate a vendor's commitment to maintain an open partnership program and architecture that will ensure integrations will be supported and further developed in the future.
- Require CISO involvement in roadmap reviews. Vendors positioned as enterprise-class will make their product management team and key executives available to meet with CISOs to share and discuss their strategic direction and product roadmap. Organizations should be sure their CISO is engaged in these discussions to provide a holistic, and thus strategic technical and business view of the organization's cybersecurity requirements.

Research Methodology

To gather data for this report, ESG conducted a comprehensive online survey of IT/information security professionals responsible for/familiar with their organization's cybersecurity environment and strategy, and with purchase authority or influence for cybersecurity products and services in North America (United States and Canada) between October 3, 2016 and October 13, 2016. 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 176 IT/information security 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.

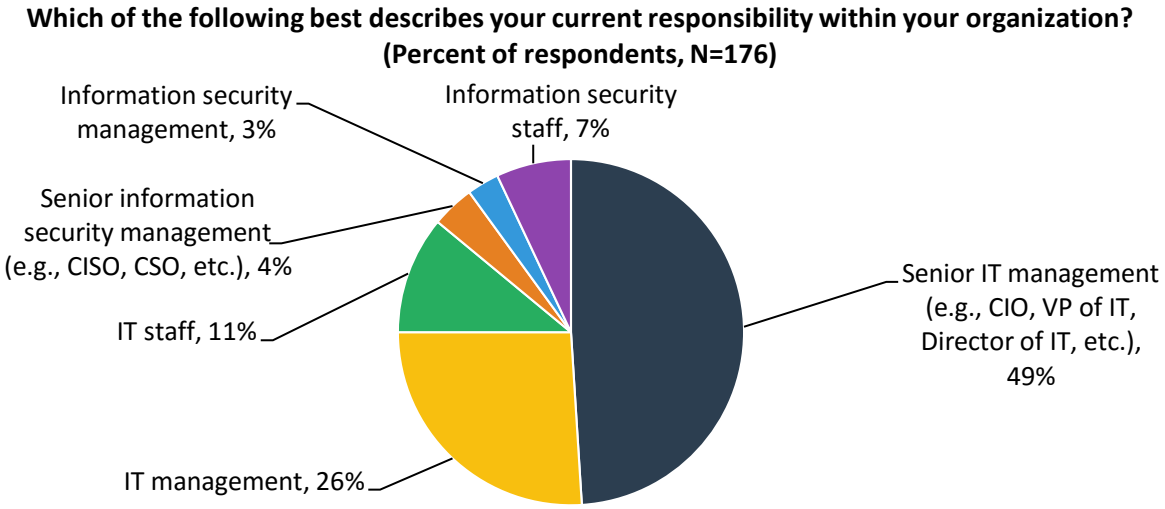
Respondent Demographics

The data presented in this report is based on a survey of 176 qualified respondents. Figures 14-17 detail the demographics of the respondent base.

Respondents by Current Responsibility

Respondents' current responsibility in shown in Figure 14.

Figure 14. Respondents by Role

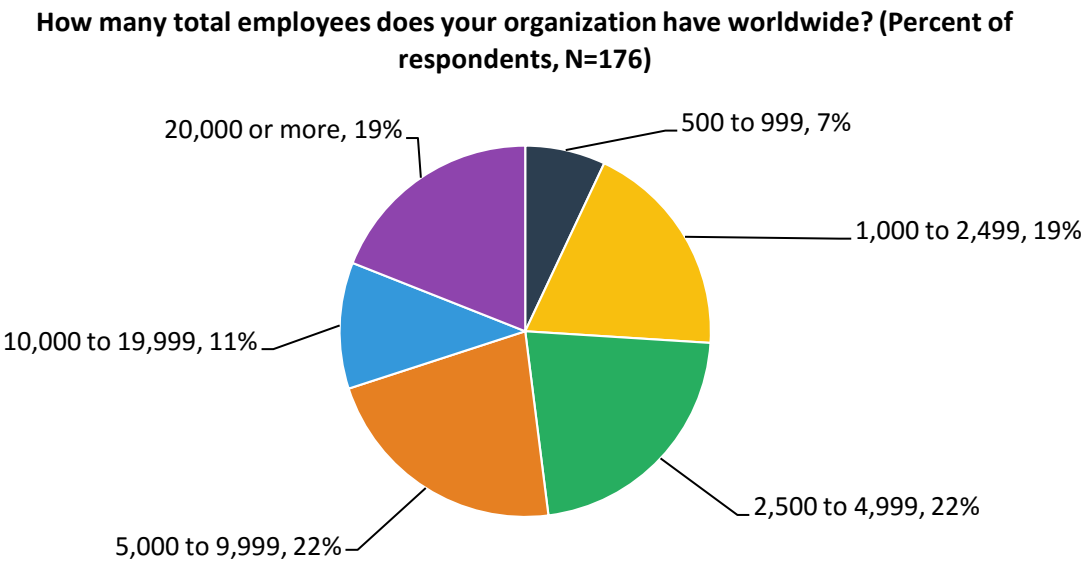


Source: Enterprise Strategy Group, 2017

Respondents by Number of Employees

The number of employees in respondents' organizations is shown in Figure 15.

Figure 15. Respondents by Number of Employees Worldwide

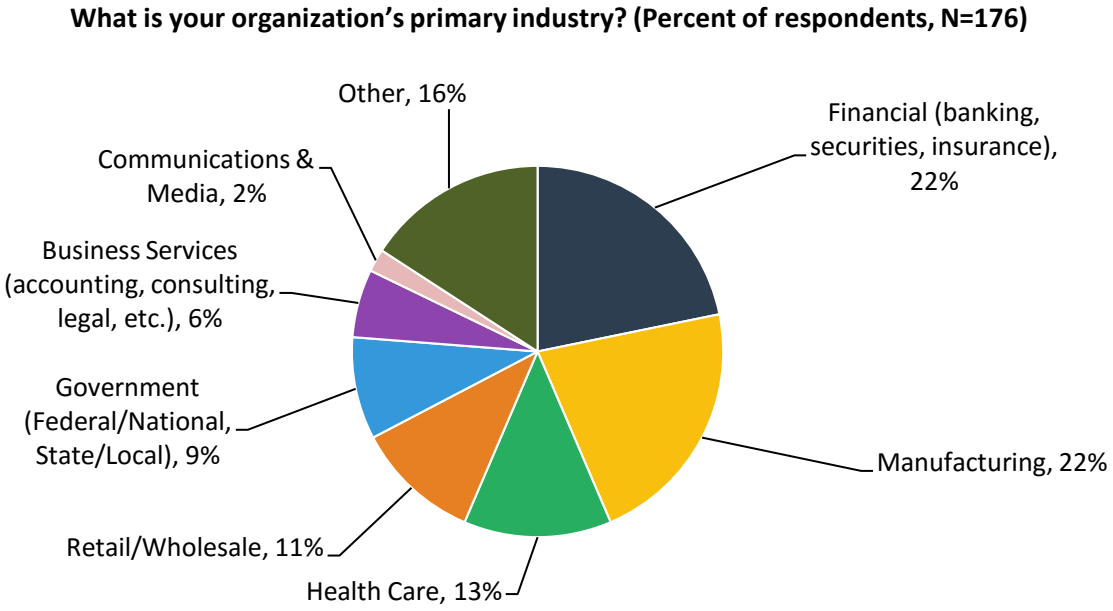


Source: Enterprise Strategy Group, 2017

Respondents by Industry

Respondents were asked to identify their organization's primary industry. In total, ESG received completed, qualified respondents from individuals in 19 distinct vertical industries, plus an "Other" category. Respondents were then grouped into the broader categories shown in Figure 16.

Figure 16. Respondents by Industry

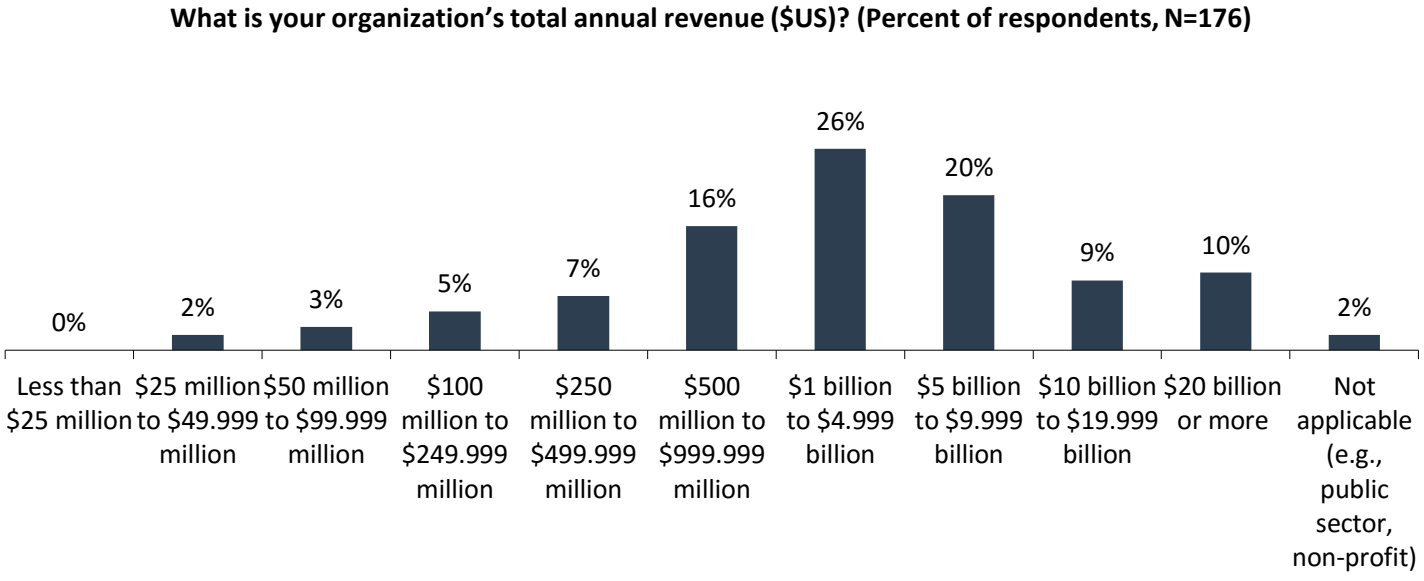


Source: Enterprise Strategy Group, 2017

Respondents by Annual Revenue

Respondent organizations' annual revenue is shown in Figure 17.

Figure 17. Respondents by Annual Revenue



Source: Enterprise Strategy Group, 2017

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

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188