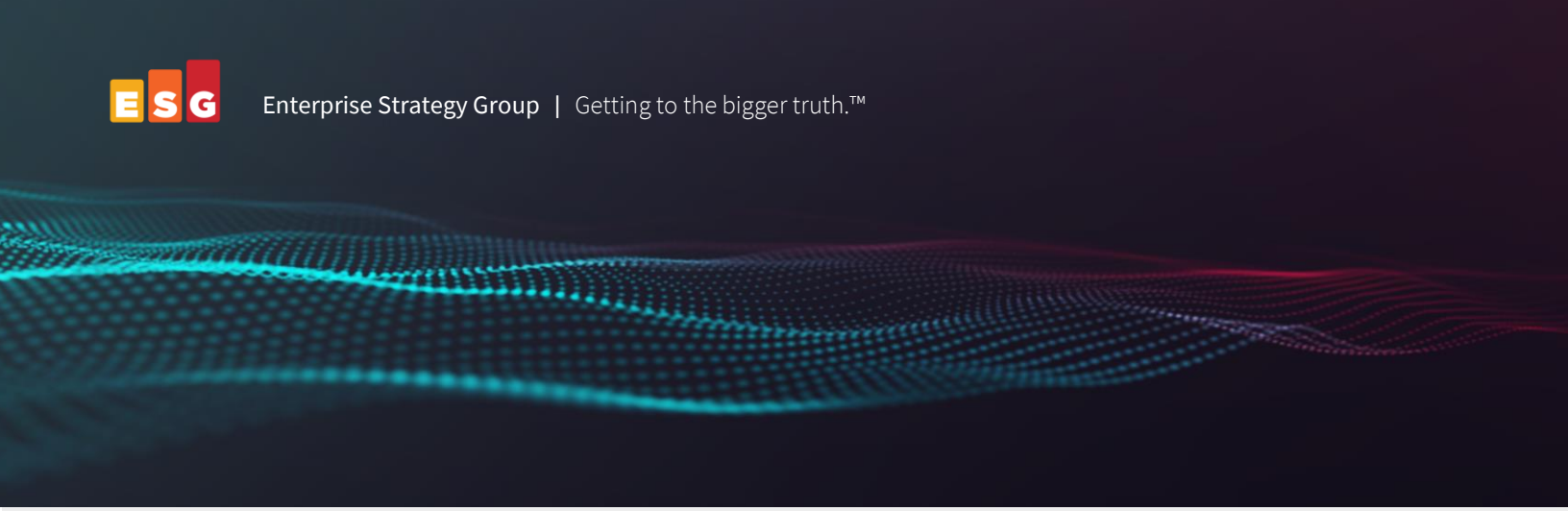


ESG RESEARCH INSIGHTS PAPER

Toward Enterprise-class Cybersecurity Vendors and Integrated Product Platforms

By Jon Oltsik, ESG Senior Principal Analyst and Fellow

February 2020

This ESG Research Insights Paper was commissioned by Cisco and is distributed under license from ESG.

Contents

Executive Summary

Famed physicist, Albert Einstein, is attributed with this famous quote: "The definition of insanity is doing the same thing over and over again and expecting different results."

Based upon ESG research, Einstein could have been talking about enterprise cybersecurity. Many organizations continue to address cybersecurity challenges with finite tactical changes, like adding a new network security control or force-fitting some type of backend analytics tool. In this scenario, any improvement in security efficacy is often offset by technical complexity and operational overhead. This can also lead to increasing cyber-risk, security incidents, and costly data breaches.

Fortunately, organizations are digging deeper, looking for the roots of their problems, and then exploring new types of cybersecurity solutions. This ESG Research Insights paper concludes:

- Security point tools represent a foundational problem. Cybersecurity professionals have long held a cultural belief in the benefits of best-of-breed security products. Unfortunately, this has led to silos of best-of-breed security tools everywhere—strong individual products and a disconnected collective security infrastructure. Scarce security professionals are forced to monitor and manage security on a product-by-product basis and use their knowledge, skills, and intuition to piece together a holistic security picture—an operationally challenging situation. CISOs can't hire their way out of this predicament due to the global cybersecurity skills shortage. Given the scale, scope, and sophistication of cyber-threats, a point tools-based piecemeal approach has become a liability.
- Organizations are consolidating vendors and integrating technologies. To address this situation, organizations are actively consolidating security vendors and integrating security products. The goals? Improve threat prevention/detection, streamline operations, encourage faster time to resolution, and receive greater support from vendors. The research points to a clear direction—enterprise organizations will spend more money with fewer vendors. This change is already happening and will become even more significant moving forward.
- Leading vendors are responding to demand-side requirements. To address customer requirements, leading vendors are integrating products, opening interfaces, driving industry standards, and creating partner ecosystems. ESG believes a few leaders will separate themselves from the pack to become enterprise-class cybersecurity vendors, offering technology platforms for threat prevention, detection, and response across areas like application, endpoint, network, and cloud security. The best platforms will also feature advanced analytics, world-class threat intelligence, security operations process automation, and a common UI/UX. Cybersecurity technology platform competition will be fierce. Leaders in this space will have solid offerings, strong future roadmaps, and services capabilities to help customers succeed.

Cybersecurity technology platforms have the potential to simplify and automate security operations, giving time back to overwhelmed security teams. In this way, CISOs can focus on enabling secure business processes rather than just blocking cyber-attacks.

Security Point Tools Pitfalls

According to recent ESG research, 76% of organizations claim that threat detection and response is more difficult today than 2 years ago.[1] This increasing difficultly is driven by external and internal changes. Externally, security professionals must address a dynamic and sophisticated threat landscape while monitoring and maintaining security over a growing attack surface (i.e., cloud, IoT, mobile, SaaS, etc.) driven by new IT initiatives like digital transformation. These conditions

[1] Source: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019.

are outside the control (i.e., external) of the security team. Internally, many CISOs are addressing cybersecurity challenges with a reliance on manual informal processes, an understaffed cybersecurity team, and an army of disparate point tools from an assortment of vendors.

This last point is illustrated by recent ESG research: 31% of organizations use more than 50 different security products while 60% use more than 25[2]. Managing a wide assortment of security tools creates numerous challenges like (see Figure 1):

- Monitoring and securing different infrastructure. 40% of those surveyed said that they need different (security) infrastructure environments which are then managed by separate teams, creating operational inefficiencies. For example, SOC personnel may monitor application, endpoint, network, and cloud security using different teams and tools, making it difficult to compare data or coordinate actions across different IT infrastructure environments. These security silos can get in the way of efficient operations across a modern hybrid cloud IT infrastructure.

- Purchasing complexity. Security teams are hired to prevent, detect, and respond to security incidents—not manage vendors and service contracts. Unfortunately, 40% of security professionals say that purchasing from a multitude of security vendors adds cost and purchasing complexity to their organization. Since CISOs aren't measured on purchasing proficiency, this is overhead they don't need.

- Intricate and time-consuming security operations. In another recent ESG research report, 75% of organizations claim that the global cybersecurity skills shortage has impacted their security operations.[3] Regrettably, the impact of the cybersecurity skills shortage is exacerbated when too few staffers are confronted with too many security point tools. As the research indicates, 35% say that managing an assortment of security products leads to complex and time-consuming security operations. In other words, threat detection and response take far longer than optimal, resulting in higher levels of cyber-risk, security incidents, and data breaches.

- Assessing the big picture through a series of little pictures. 35% of respondents say that managing an assortment of security products makes it difficult to get a complete picture of their security status. Again, this makes it problematic to understand cyber-risk or track an attack across the kill chain when a compromised system scans the network to steal administrator passwords, downloads malware payloads, or reaches out to a command-and-control (C2) server for instructions. Understanding the totality of this type of malicious activity would require time and effort by highly trained SOC analysts piecing together analysis from several different security technologies.

[2] Source: ESG Master Survey Results, *Enterprise-class Cybersecurity Vendor Sentiment Survey*, February 2020. All ESG research references and charts in this research insights paper have been taken from this master survey results set, unless otherwise noted.
[3] Source; ESG/ISSA Research Report, *The Life and Times of Cybersecurity Professionals 2018*, May 2019.

Figure 1. Challenges Associated with Managing an Assortment of Security Products

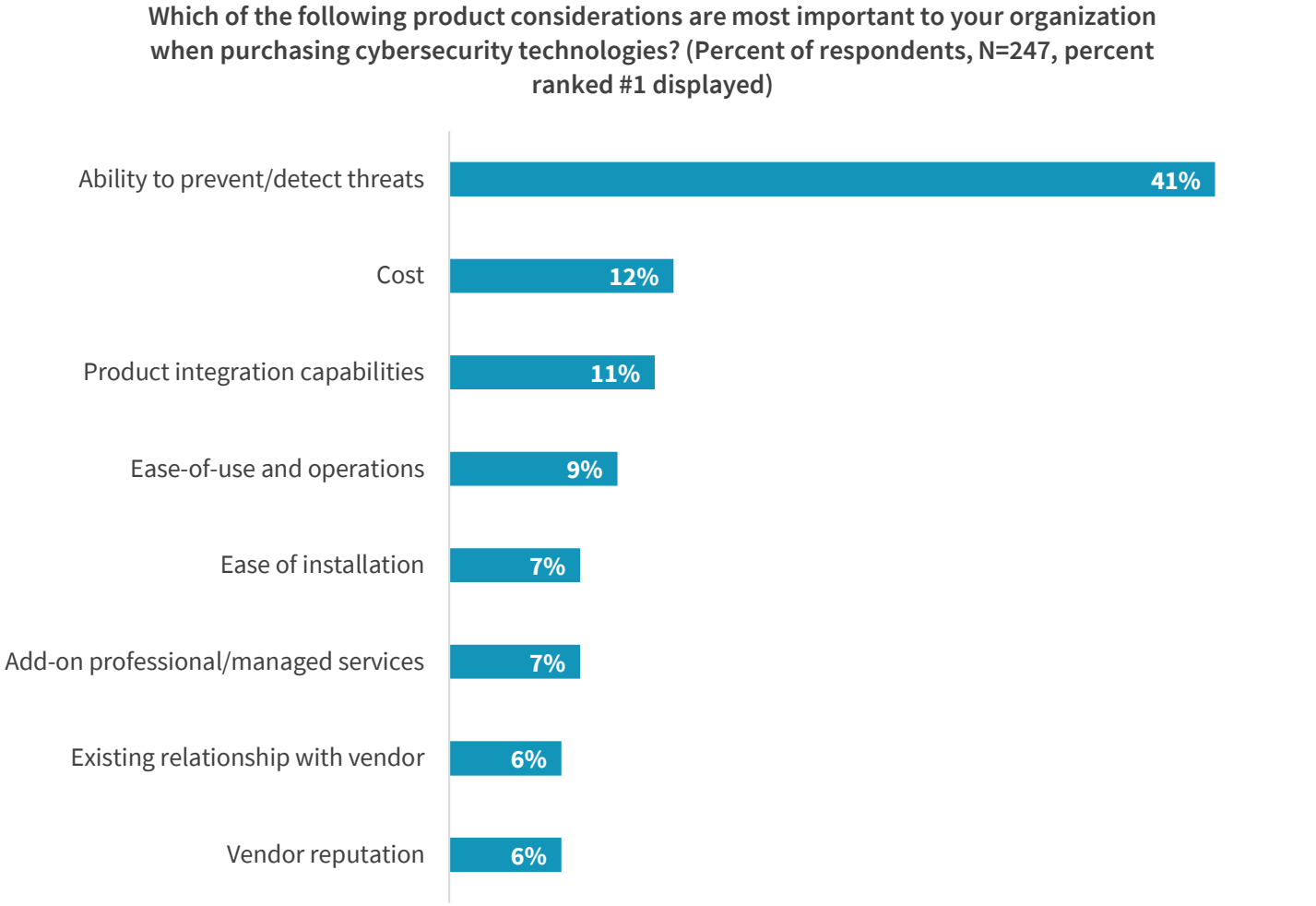
Source: Enterprise Strategy Group

Organizations are Changing Security Product Purchasing Behavior

Over the last few years, many CISOs recognized that a point tools-based security infrastructure is unsustainable—the problems associated with a lack of integration and operational overhead outweigh any benefits accompanying individual tools. As a result, organizations have changed their approach to buying, deploying, and operating security products.

While purchasing, deployment, and operations strategies are evolving, security professionals still demand excellence from individual security products. This attitude is clearly evidenced in Figure 2. When asked to identify the most important security product considerations, 41% of survey respondents opted for a product's ability to prevent/detect threats. Thus, a security technology architecture must be anchored by a foundation of best-of-breed threat prevention and detection tools.

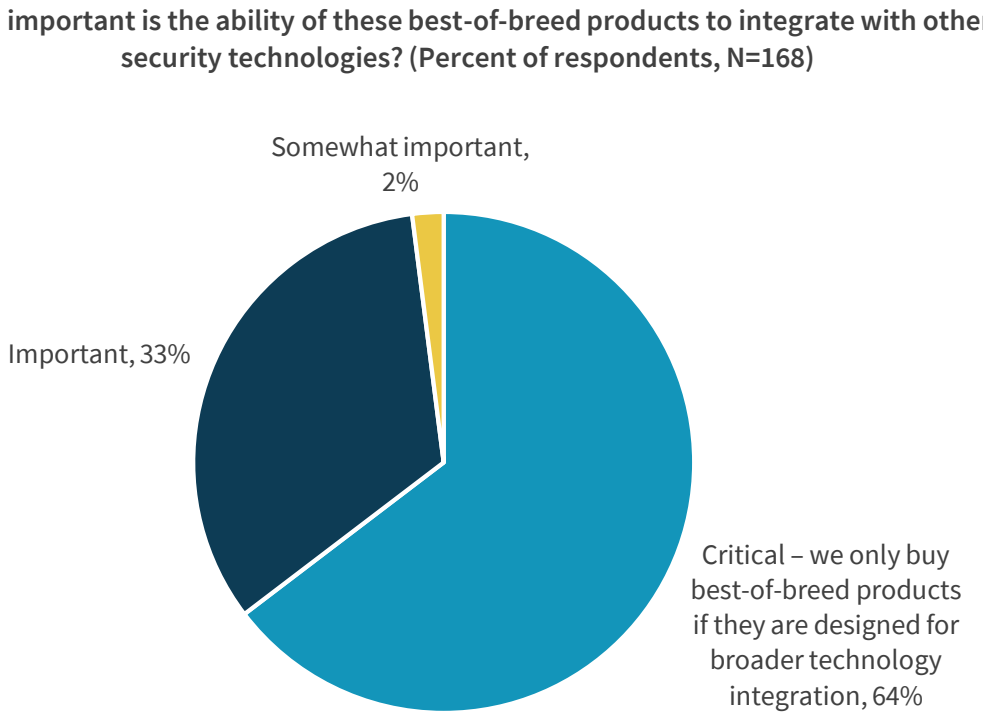
Figure 2. Important Cybersecurity Technology Considerations



Source: Enterprise Strategy Group

Beyond best-of-breed threat prevention/detection, however, security professionals want to move beyond silos of disconnected point tools toward an integrated security technology architecture. This desire is clearly illustrated in Figure 3—64% of survey respondents say that it is critical that security products integrate with other security technologies while another 33% say it is important that best-of-breed products integrate with other security technologies. Clearly, CISOs want it all—a best-of-breed security tools foundation AND interoperability across technologies.

Figure 3. Importance of Integration Across Security Products and Technologies



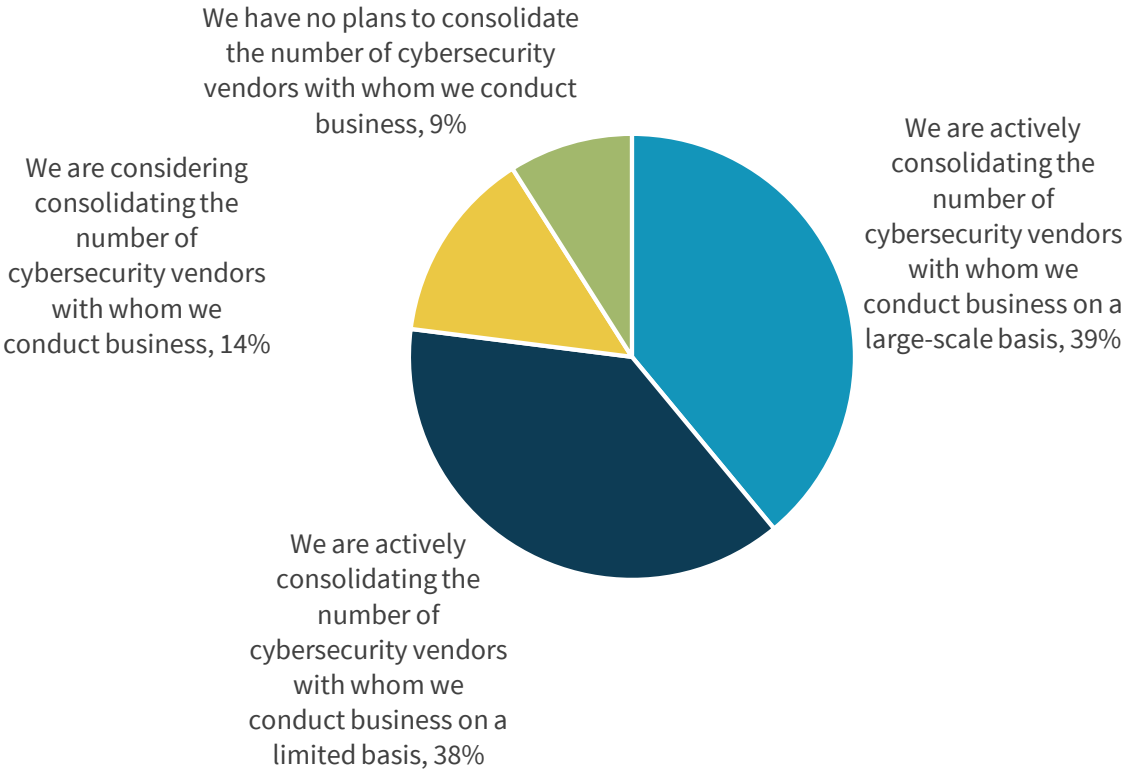
Source: Enterprise Strategy Group

Cybersecurity Vendor Consolidation

Given the trend toward product integration, it is not surprising then that companies may be inclined to buy more products and technologies from fewer vendors. Why? Enterprise-class cybersecurity technology vendors can do a lot of the grunt work by tightly integrating their best-of-breed products into scalable and interoperable technology architectures. Based on this industry trend, many organizations are taking an active approach to vendor consolidation. ESG research indicates that 39% of organizations are actively consolidating the number of cybersecurity vendors they do business with on a large-scale basis while another 38% are actively consolidating the number of cybersecurity vendors they do business with on a limited basis (see Figure 4).

Figure 4. Cybersecurity Vendor Consolidation Trends

Which of the following statements regarding the consolidation of cybersecurity vendors with whom your organization conducts business is most accurate? (Percent of respondents, N=247)



Source: Enterprise Strategy Group

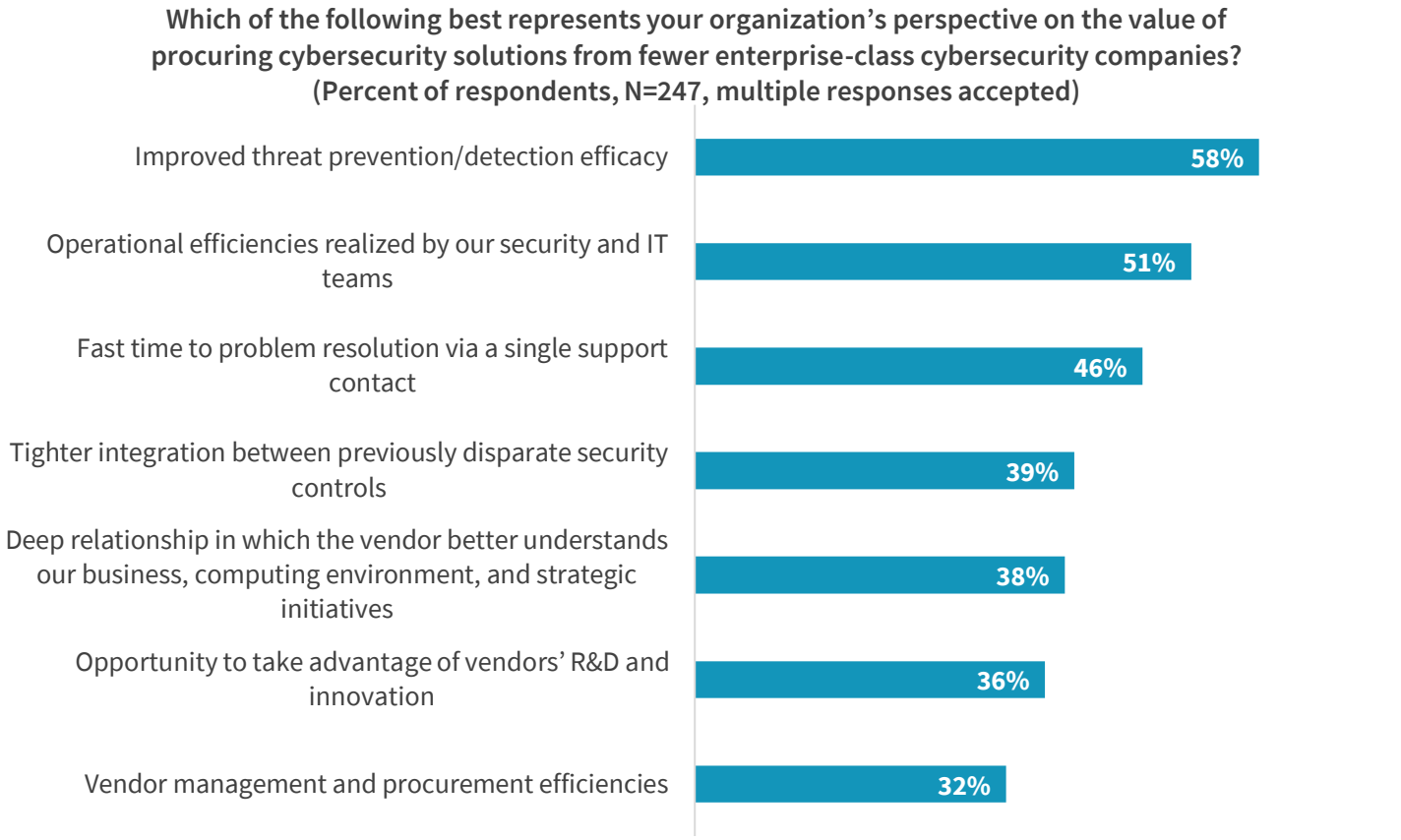
The research also indicates that cybersecurity professionals have clear expectations about the value of buying more security technologies from fewer vendors. For example (see Figure 5):

- 58% point to improved threat prevention/detection efficacy. The thought here is that individual tools will interoperate, sharing data, alerts, and pertinent threat intelligence. In this way, an integrated security platform can improve alert fidelity while enriching and contextualizing security telemetry. This can help SOC teams minimize the dead-end work of chasing false positives while streamlining security operations tasks associated with forensic investigations.

- 51% say they expect operational efficiencies realized by their security and IT teams. Strong cybersecurity practices depend upon effective communications and collaborations between SOC and IT/network operations teams. Survey respondents believe that security/IT operations coordination can be improved if both teams are working off aggregated data, enriched alerts, and common administration tools.

- 46% claim that they expect faster time to problem resolution via a single support contact. Nearly half (46%) of survey respondents believe that SOC analysts' jobs will become easier when they have a single vendor to work with for platform support. This makes sense—rather than tuning multiple individual products, SOC teams can customize rule sets and centralize configuration settings. Leading vendors can benefit here as well by dedicating trained field personnel measured on making their customers as successful as possible.

Figure 5. The Value Associated with Cybersecurity Vendor Consolidation



Source: Enterprise Strategy Group

Toward Enterprise-class Cybersecurity Vendors

Today, the industry is made up of thousands of individual vendors, many offering a single point tool. As large organizations integrate security technologies and consolidate vendors, the industry will change accordingly and lead to the rise of a handful of enterprise-class cybersecurity vendors. ESG defines the term enterprise-class cybersecurity vendor as those cybersecurity vendors offering a breadth of cybersecurity products and/or services designed for scale, integration, and support for the business process requirements of a large organization.

Based upon this general definition, ESG asked cybersecurity professionals to identify the most important attributes of an enterprise-class cybersecurity vendor (see Figure 6). These include:

- Industry-specific cybersecurity expertise. Digital transformation applications, IoT device proliferation, and increasing regulations are changing cybersecurity technologies from horizontal services to vertical industry applications. This transition is reflected in the ESG data, as 35% of respondents believe that industry-centric cybersecurity expertise is one of the most important attributes for enterprise-class cybersecurity vendors.

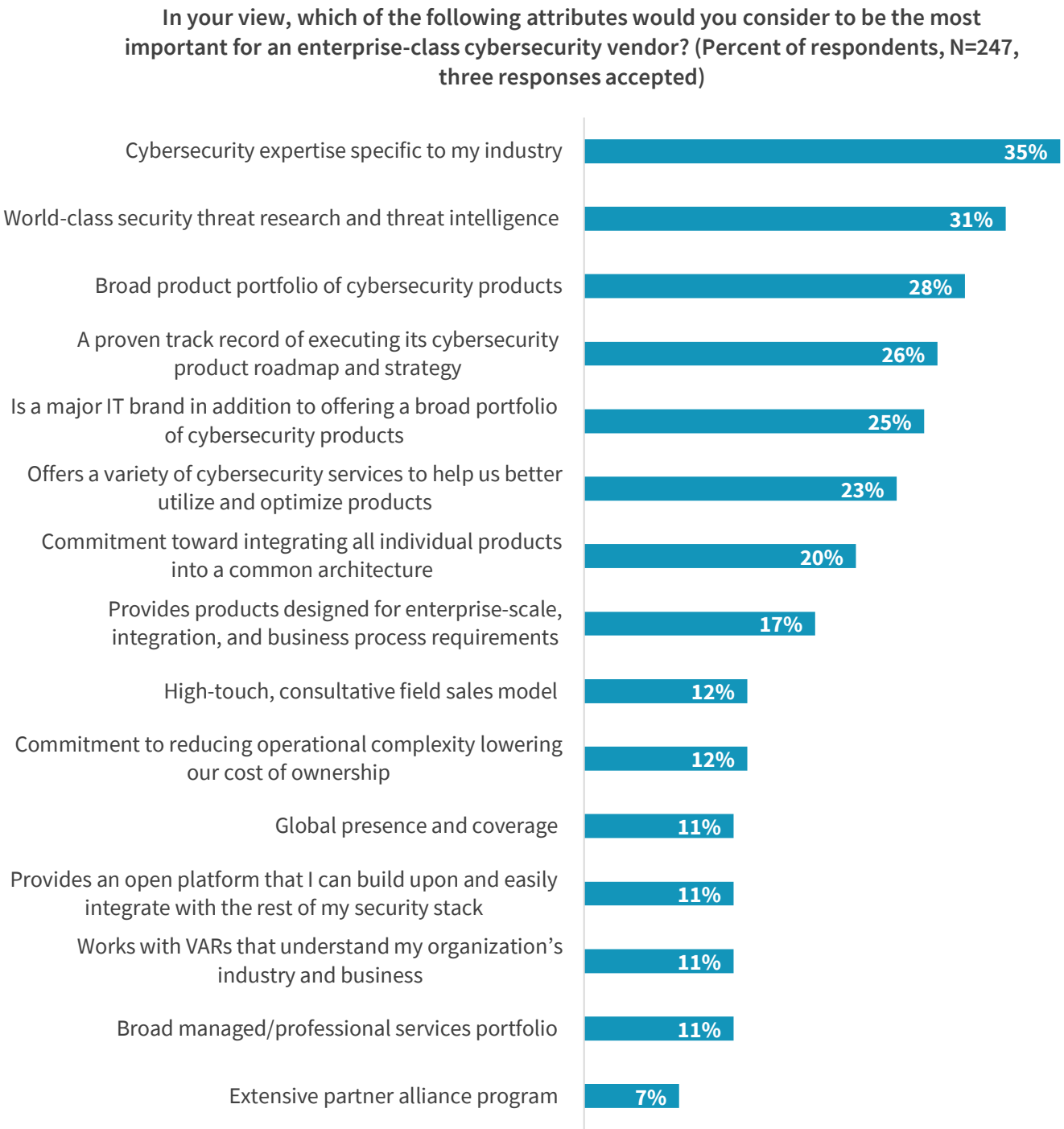
- World-class threat research and intelligence. Security operations teams need real-time intelligence about the threat landscape for forensic investigations and threat hunting. Thus, world-class security threat research and intelligence is a top attribute for enterprise-class cybersecurity vendors.

- A broad portfolio of cybersecurity products. As previously stated, CISOs want to buy more products from fewer vendors. Enterprise-class cybersecurity vendors can meet this requirement by offering a broad product portfolio to

customers. Little wonder then why 28% of survey respondents consider this an important enterprise-class cybersecurity vendor attribute.

- A proven execution track record. More than one-quarter (26%) believe that enterprise-class cybersecurity vendors must have the ability to execute on their product roadmaps and strategies. In other words, CISOs want to work with vendors seen as "safe bets" for the long term.

Figure 6. Most Important Attributes of an Enterprise-class Cybersecurity Vendor



Source: Enterprise Strategy Group

Enterprise-class cybersecurity technology vendors with these attributes are highly attractive to enterprise organizations. Indeed, 80% of organizations indicated that they would consider buying a significant amount of their security technologies from a single enterprise-class cybersecurity vendor.

The Rise of Cybersecurity Technology Platforms

In 2020, enterprise-class cybersecurity vendors will compete for business by offering cybersecurity technology platforms. ESG defines this term as:

A tightly integrated suite of products offered by a single vendor with third-party product integration capabilities through APIs, industry standards, and partner ecosystems.

The much-anticipated cybersecurity "platform wars" will lead to ferocious competition, industry hyperbole, and user confusion. Nevertheless, cybersecurity professionals have a clear idea of what they want from a cybersecurity platform. The top five platform attributes include:

1. Security coverage across major threat vectors and access points. Most cyber-attacks still rely on two primary threat vectors: email and the web. Therefore, cybersecurity platforms must include monitoring and controls designed to block and/or alert on suspicious/malicious activities across these common channels.

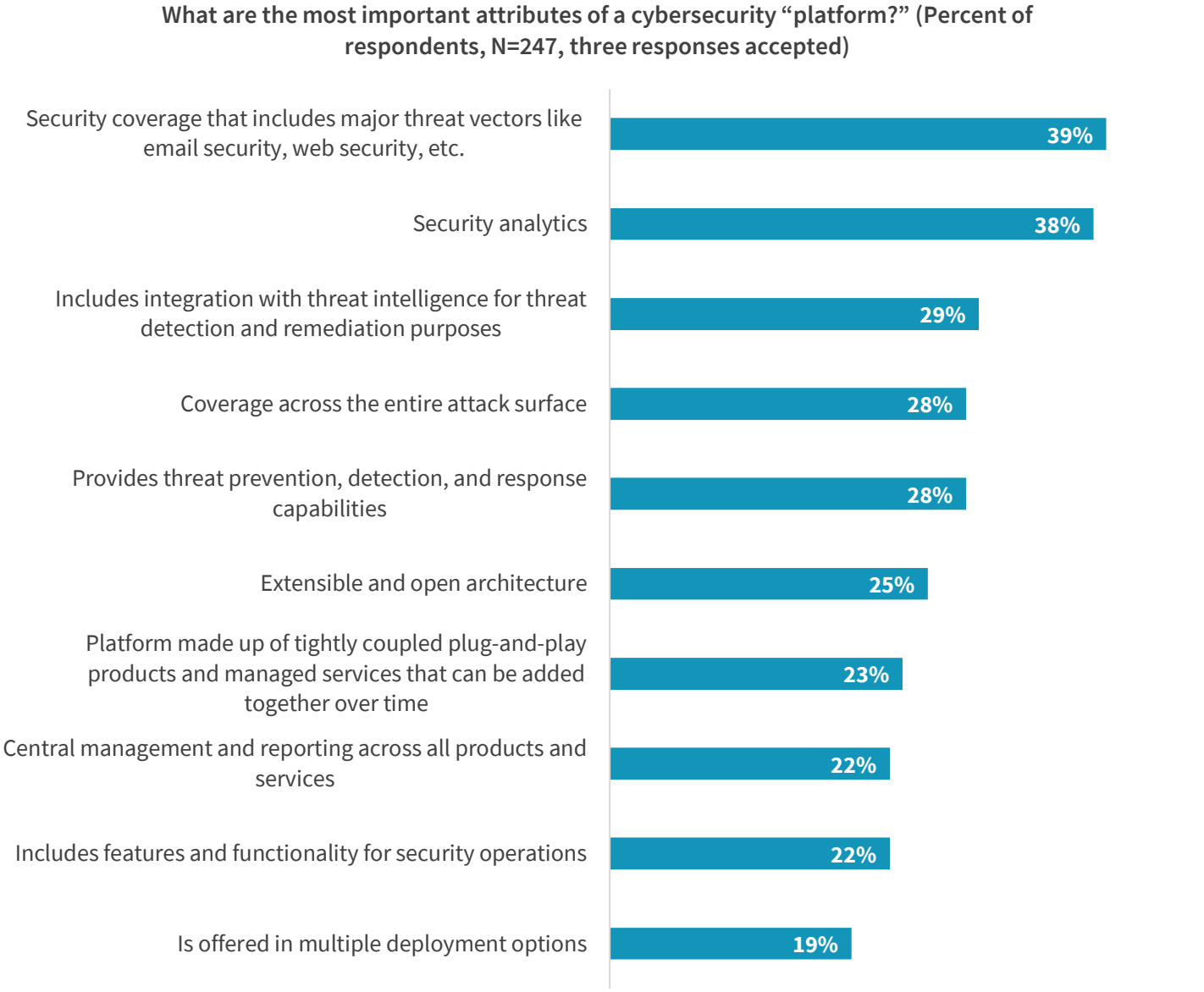
2. Analytics. Cybersecurity platforms must be back-ended by advanced analytics for behavioral analysis, file analysis, and risk scoring. The goal? Eliminate false positives and provide high fidelity and actionable alerts.

3. Threat intelligence integration. As previously mentioned, SOC analysts want real-time threat intelligence so they can compare anomalous activities with what's going on "in the wild."

4. Wide coverage. Rather than purchase disparate tools, CISOs want cybersecurity platforms that span applications, endpoints, networks, and clouds.

5. Prevention, detection, and response. Platforms must be able to reduce the attack surface and easily block known threats. Leading platforms will provide advanced analytics for threat detection, and a security operations workbench, runbooks, and automation capabilities for incident response.

Figure 7. Most Important Attributes of a Cybersecurity Technology Platform



Source: Enterprise Strategy Group

The transition to cybersecurity platforms isn't some distant vision. In truth, today's cybersecurity requirements demand action, so the move to cybersecurity platforms is already underway. For example, 38% of organizations have already purchased multiple products from a single vendor rather than best-of-breed products from multiple vendors, 34% have used open source software as an integration layer between independent products, and 34% have pushed several cybersecurity technology product vendors to work together on product integration.

CISOs will continue to push vendors on product consolidation and encourage them to pursue standards, heterogeneous product integration, and industry cooperation. Enterprise-class cybersecurity vendors must anticipate these demands and take a leadership position toward facilitation. Industry leaders will offer comprehensive open cybersecurity technology platforms that can help organizations improve security efficacy while streamlining operations.

Cisco SecureX

Cisco recently announced a cybersecurity platform called SecureX. Cisco SecureX connects the breadth of Cisco's integrated security portfolio and customer's security infrastructure. This integration is intended to help customers gain more value from Cisco products and existing security infrastructure by coordinating defenses (i.e., endpoint, network, cloud, etc.), centralizing visibility and analytics, and enabling automation for threat prevention, detection, and response. SecureX is also built with a consistent UI/UX that follows the user across Cisco Security to share context between products and teams. This should help security teams rally around common reports and dashboards, eliminating the need to pivot between multiple solutions.

Overall, Cisco SecureX provides many of the important platform attributes highlighted in the ESG research. Cisco also has an aggressive roadmap for SecureX moving forward. CISOs should evaluate SecureX across current and future capabilities. Think of SecureX as a journey rather than a destination. It is also worth noting that Cisco is not charging extra for SecureX or asking customers to replace or layer on new technology. Rather, SecureX is delivered as a built-in experience across the Cisco Security portfolio.

The Bigger Truth

Given the state of cybersecurity today, most CISOs realize that they can't protect their organizations by relying on disconnected point tools, informal/manual processes, and a shortage of cybersecurity skills. One way out of this mess is through technology integration that allows independent tools to share data, correlate alerts, and enable common workflows for security operations.

Cybersecurity technology platforms can address integration complexity with turnkey interoperable product suites. Those from leading enterprise-class cybersecurity vendors will enhance cybersecurity technology platforms with world-class threat intelligence, industry feature/functionality, and enterprise quality scalability, manageability, and support. Furthermore, cybersecurity technology platforms functionality can have an immediate impact on organizational maturity. Simply stated, the cybersecurity team can be more productive and focused on protecting business-critical assets and processes.

To avoid confusion as they evaluate cybersecurity technology platforms, CISOs should:

- Assess current challenges across people, process, and technology. Leading platforms should go beyond technology alone, helping organizations increase staff productivity while streamlining operations. CISOs should look for current bottlenecks impacting areas like employee training, MTTD/MTTR, and process automation. This assessment should help produce a list of platform requirements beyond technology integration alone.

- Include IT and network operations in RFIs and product evaluations. Remember that security is a collective activity, dependent upon strong communications and collaboration between security and IT/network operations teams. Smart CISOs will work with IT peers to uncover current challenges and then seek solutions in RFIs, product evaluations, and testing/piloting that can be used effectively by both groups.

- Plan for the long-term. Cybersecurity technology platforms will likely grow organically, integrating more product categories and capabilities over time. Therefore, platform research should go beyond what's available today. CISOs should press vendors for a 24 to 36-month roadmap. Leading vendors should have comprehensive plans but also be willing to work with customers as new requirements arise. On the enterprise side, CISOs should create metrics so they

can assess progress and create programs for continual improvement as they deploy cybersecurity technology platforms more broadly through phases.

- Reach out to the community. Note to CISOs: You are not alone—just about every other enterprise organization is going through a similar transition. CISOs should seek out guidance from other industry organizations of a similar size. In this way, organizations may be able to work together to press vendors on some industry-specific nuances that can be added to cybersecurity technology platforms over time.

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