Enterprise Strategy Group | **Getting to the bigger truth.™**

Solution Showcase

The Shift Toward Cybersecurity Technology Platforms

Date: February 2019 **Author:** Jon Oltsik, Senior Principal Analyst and ESG Fellow

Abstract: Since the late 1990s, enterprise security infrastructure grew organically as CISOs added independent security controls as countermeasures to new or growing threats. This tactical strategy was adequate in the past, but it is a mismatch for today's dangerous threat landscape and growing attack surface. In fact, a point tools-based security infrastructure often leads to high costs, complex security operations, unacceptable levels of cyber risk, and data breaches. ESG research indicates that many organizations have had enough. As an alternative to point tools, CISOs are embracing tightly coupled security technology platforms offering advanced threat protection, central management, and coverage across endpoints, networks, and clouds.

Overview

Organizations face several daunting cybersecurity issues today. For example, there are more sophisticated threats aimed at large and small firms than there were in the past. Many organizations face a mix of state-sponsored hackers, ransomware (which has been especially impactful for health care organizations and public sector agencies), and attacks that leverage IoT devices like the Mirai botnet. Along with evolving cyber-attacks, there's also an expanding attack surface at a lot of organizations, driven by public cloud, SaaS, and IoT adoption. An expanding attack surface equates to more vulnerable assets that require monitoring, scanning, patching, and security controls for protection.

Today's Security Infrastructure Is Inadequate for Addressing Requirements

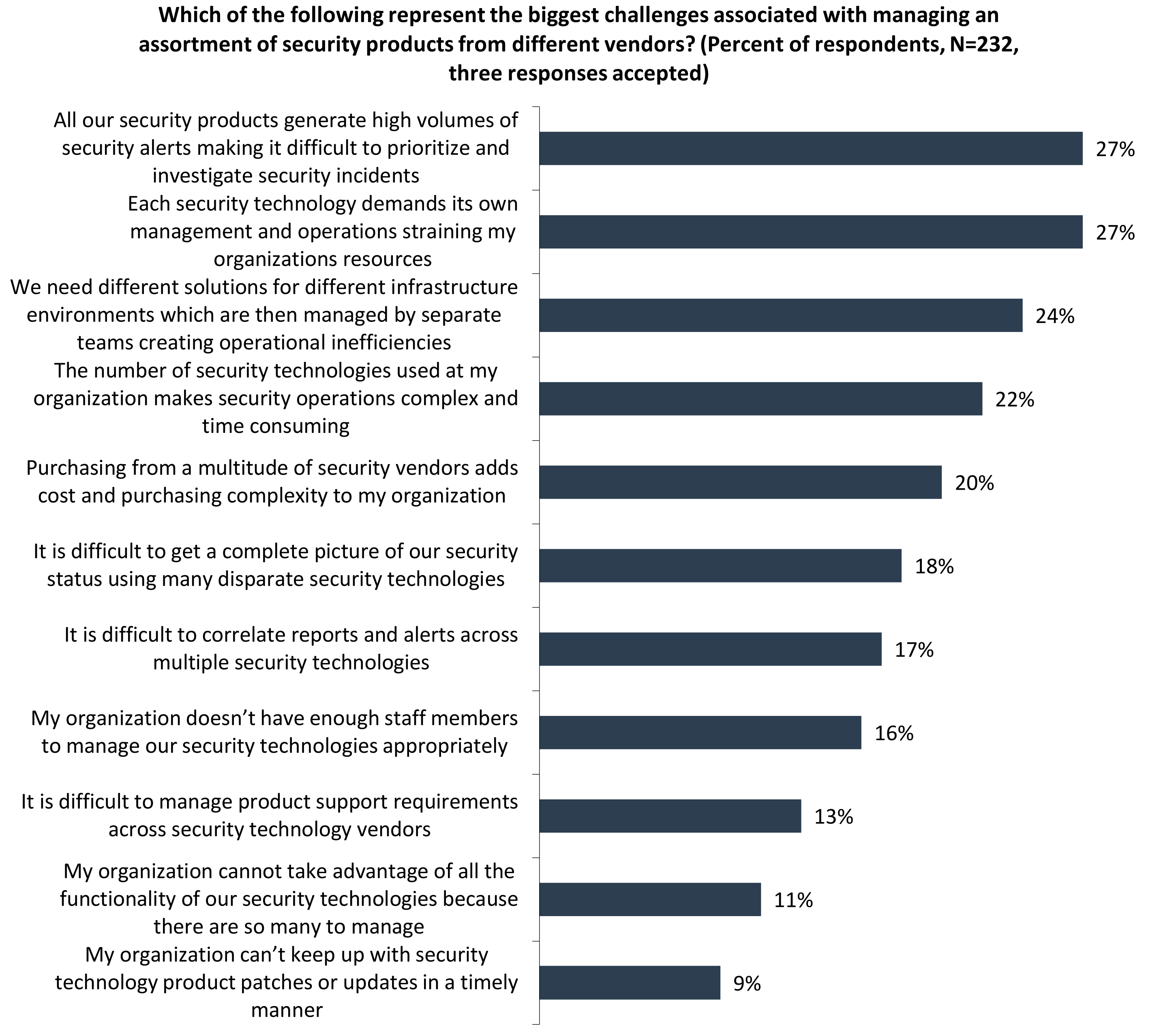
At most enterprise organizations, cybersecurity infrastructure grew organically over the past 20 years. The security team implemented numerous security controls in response to particular threats as they arose. To combat spyware, viruses, and worms, antivirus software appeared on desktops. Firewalls and IDS/IPS were deployed to protect networks and detect network-based threats. Email and web gateways were added as countermeasures to spam, phishing attacks, and malicious URLs. Sandboxes were deployed to execute and detect malicious files, etc.

As the security infrastructure evolved, most enterprises were content with a potpourri of security tools rather than a security technology architecture or cohesive strategy. The tactical approach has created a situation where almost two-thirds of large enterprises (organizations with 5,000 or more employees) currently have at least 25 cybersecurity products in use.[1]

[1] Source: ESG Master Survey Results, *Cybersecurity Landscape: The Evolution of Enterprise-class Vendors and Platforms*, October 2018. All ESG research references and charts in this solution showcase have been taken from this master survey results set, unless otherwise indicated.

The lack of a cohesive security technology strategy may have been adequate 10 or 15 years ago, but it has led to real problems over time. Recent ESG research illustrates some of the challenges associated with managing an assortment of security products from different vendors, including (see Figure 1):

Figure 1. Challenges with Managing Assorted Security Point Tools



Source: Enterprise Strategy Group

- **Too many security alerts.** Numerous threat detection tools generate independent security alerts that must be investigated, prioritized, and remediated. When there are too many alerts, security analysts are forced to quickly assess alerts, prioritize a handful, and ignore the rest. This can lead to false positive/false negative situations where analysts waste time chasing dead ends, or disregard serious events. This is exactly what happened at Target when overwhelmed SOC personnel ignored alerts that eventually led to a data breach and over $160 million in unexpected costs.

- **Management and operations overhead.** Each individual security tool must be researched, tested, deployed, and operated. This alone can be difficult due to the impact of the global cybersecurity skills shortage. According to ESG research, 53% of organizations report a problematic cybersecurity skills shortage, resulting in an overwhelming and growing workload for the cybersecurity staff.[2]

- **Security complexity.** As the saying goes, complexity is the enemy of cybersecurity. Organizations need different solutions for different infrastructure environments that are managed by separate teams, creating operational inefficiencies. In other words, they have security tools for data centers, endpoints, virtual servers, public cloud workloads, etc. Coordinating policy and control across these areas is no walk in the park. These issues make security operations complex and time consuming.

There are also risk management consequences like increased cost and poor ROI from using fragmented tools. In a recent ESG research project on cyber risk management, survey respondents indicated that purchasing security technologies from a multitude of security vendors added cost and purchasing complexity. The research also specified that 35% of organizations consider ROI on cybersecurity one of the top cyber risk management metrics.[3] This means that, while organizations are willing to increase cybersecurity spending, they also want a better understanding of what they get for their money. Clearly, they aren't getting the benefits they are seeking from their existing security infrastructure based upon independent point tools.

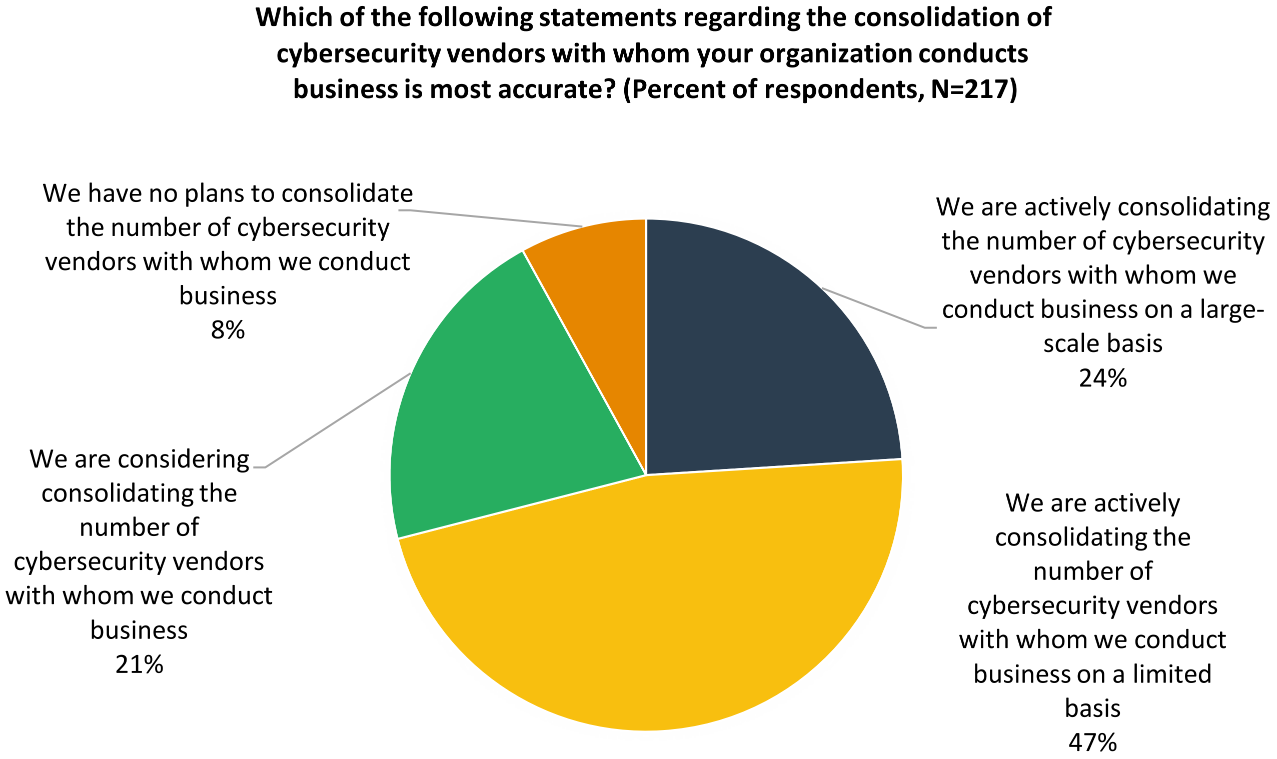
Toward Integrated Cybersecurity Technology Platforms

Too many security tools and not enough time to use them correctly is not a new problem, but the ramifications of this situation are growing increasingly worse all the time. This explains why CISOs are looking to consolidate and integrate their security infrastructure with platforms and architectures.

This situation is not without a historical precedent. In the 1990s, many organizations abandoned departmental applications in favor of tightly integrated ERP software designed for enterprise business processes and scale. While this transition wasn't easy, consolidating applications and data into a central platform drove new business processes, augmented decision making, and led to higher revenue and lower costs. In a cybersecurity context, organizations believe that integration and consolidation can promote enhanced threat prevention while accelerating threat detection and incident response. These anticipated benefits are driving behavioral changes—91% of enterprises are actively consolidating or considering consolidating the cybersecurity vendors with whom they are conducting business (see Figure 2).

[2] Source: ESG Research Report, *2019 Technology Spending Intentions Survey*, February 2019.
[3] Source: ESG Research, *Cyber Risk Management Trends Survey,* October 2018.

Figure 2. Cybersecurity Technology Consolidation Trends



Source: Enterprise Strategy Group

Beyond simple point tools consolidation, many enterprises are seeking security technology platforms where tightly integrated security tools share data, coordinate on threat prevention, and report up to a central management plane for things like configuration management, policy management, and monitoring/reporting.

What features and functions should a cybersecurity technology platform support? According to ESG research, the top priorities include:

1. **Coverage that includes major threat vectors (like endpoint, email, web, and cloud).** Cybersecurity platforms should be able to prevent, detect, and respond to threats across an enterprise IT infrastructure (i.e., endpoints, networks, servers, or cloud-based workloads). Prevention, detection, and response capabilities should be tightly coupled so that security and IT operations teams can monitor activities or take actions across any and all security technology controls regardless of location.

2. **Central management and reporting across all products and services.** All security controls should report to a central management plane providing configuration management, policy management, monitoring, and remediation capabilities. Central management must be built for scale, support role-based access control, and offer multiple UIs and functions, customized for different security and IT operations profiles.

3. **Threat prevention, detection, and response capabilities.** Cybersecurity platforms should have strong defenses (i.e., rules, heuristics, behavioral algorithms, threat intelligence integration, etc.) used for blocking and/or detecting threats with close to 100% efficacy. When threats are detected, cybersecurity platforms should have low false positive rates and provide clear and concise forensic evidence to analysts that includes a breadcrumb trail of events that led to an alert. Finally, cybersecurity platforms should include simple mitigation techniques like

quarantining a system, halting a process, or securing a network connection. Users should be able to automate these remediation actions if they choose to do so.

4. **An open architecture, ease of integration, and third-party support.** Security platforms must be built for integration by supporting common messaging buses and open APIs. Vendors offering best-in-class cybersecurity platforms will also support third-party developers and security vendors with developer support resources, partner ecosystems, technical support services, and go-to-market programs. A unified/consolidated agent can help enable openness and integration by minimizing software contention.

ESG believes that initial cybersecurity platform implementation will tend to focus on improving security efficacy and streamlining security operations, making security vector coverage, central management, and threat lifecycle support top priorities. As cybersecurity platform deployments mature, organizations will want greater coverage and flexibility. Therefore, security professionals will likely look to supplement initial cybersecurity platforms by adding things like cloud-based services (as opposed to on-premises options) and integrating third-party tools and services. Given this evolution, CISOs should approach cybersecurity platforms with a long-term strategy and project plan that spans a 24 to 36-month timeframe.

The Bigger Truth

In the past, security professionals sought out best-of-breed point tools, but the overall market is undergoing a profound change. It's increasingly clear that disconnected point tools can no longer support enterprise security requirements. Moving forward, security technology integration and architectural considerations are equally or more important than best-of-breed product functionality. What's better? A platform comprising best-of-breed products. Security professionals should seek out strategic cybersecurity partners with integrated technology platforms, as they have the potential to help improve security while streamlining security operations. For investment protection and flexibility, CISOs should insist on platforms with open architectures, developer support, and partner ecosystems with ample existing third-party integrations.

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