Solution Showcase

Modernizing Midmarket Cybersecurity

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

Abstract: The growing number of cyber-attacks and the resulting increase in regulatory requirements and consumer demand for security have spurred significant investment in security products and services. For many large enterprises and government agencies, this has also meant greater investment in IT and security staffing. Despite facing the same challenges as a large enterprise, a majority of midmarket organizations can't keep up with investments in security technology *and* staffing. These businesses are at a disadvantage, with limited skills, staff sizes, and resources. To address this imbalance, midmarket organizations must think creatively and define a new model for cybersecurity built around integrated cybersecurity technology architectures, external partners, and continuous training for business, IT, and security.

Overview

Midmarket companies continue to face cyber-attacks from both external and internal sources. According to ESG research from 2018, 66% of midmarket cybersecurity professionals described experiencing one or more security incidents over the previous two years, including system compromises, malware incidents, DDoS attacks, targeted phishing attacks, and data breaches. Of those organizations that experienced a security incident, 46% reported that it led to lost productivity, 37% said it resulted in disruption of a business application or IT system availability, 37% claimed it led to disruption of business processes, and 31% admitted that a security incident required significant time and or personnel for remediation.[1]

The research indicates that many factors contributed to these breaches, including human error by end-users (35%); a general lack of organizational understanding of cybersecurity risk (28%); and new IT initiatives, such as cloud computing, and mobile computing, that were implemented without proper cybersecurity oversight and controls (27%). Commonly, as midmarket organizations forge ahead with IT expansion, their security platforms, skills, and awareness don't keep pace with the changes.

Midmarket Cybersecurity Challenges

Midmarket organizations manage cybersecurity as best they can. While some firms employ dedicated cybersecurity personnel, many simply ask IT to add infosec tasks to their existing capacities. Meanwhile, organizations large and small face a global cybersecurity skills shortage—ESG research indicates that 53% of survey respondents report a problematic shortage of cybersecurity skills in 2019,[2] and 74% believe that their organization has been negatively impacted by the cybersecurity skills shortage.[3]

[1] Source: ESG Master Survey Results, *Cybersecurity Trends at SMB Organizations*, August 2018. All ESG research references and charts in this solution showcase have been taken from this master survey results set unless otherwise indicated.
[2] Source: ESG Master Survey Results, *2019 Technology Spending Intentions Survey*, March 2019.
[3] Source: ESG Research Report, *The Life and Times of Cybersecurity Professionals 2018*, May 2019.

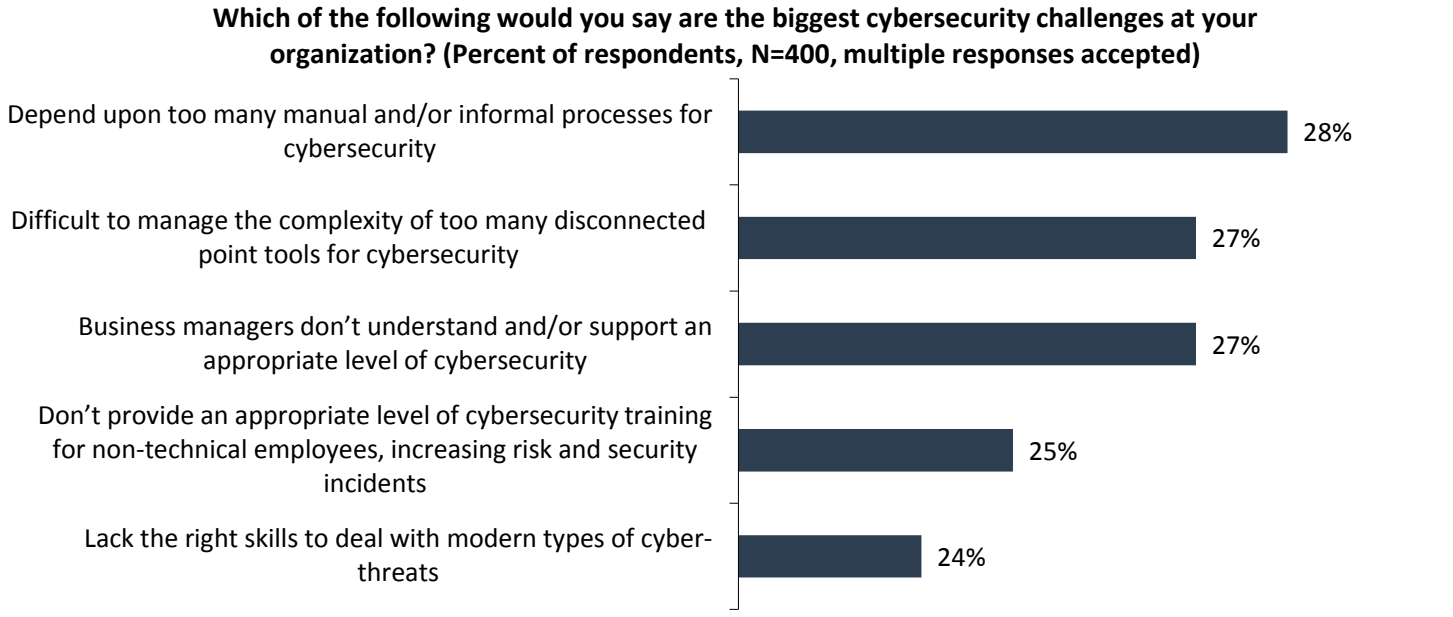
What are the implications of the cybersecurity skills shortage? An increase in the workload of existing staff (with associated high "burn-out" rates), an inability of cybersecurity staff to fully learn or utilize some of the security technologies to their full potential, and a need to recruit and train junior personnel rather than hire experienced cybersecurity professionals.

In addition to a skills shortage, midmarket organizations face other cybersecurity challenges, including (see Figure 1):

- **A dependence on manual processes.** This complicates cybersecurity operations, as personnel struggle to implement security controls, monitor critical systems, and respond to attacks. Manual processes don't scale, and problems associated with manual processes are exacerbated by inadequate skills and staff in the midmarket.
- **An overabundance of disconnected point tools.** Each cybersecurity technology must be purchased, tested, piloted, configured, and operated on an ongoing basis. Once again, midmarket organizations have neither the time nor resources to manage this situation.
- **Business management apathy and ignorance.** Too often, midmarket businesses believe they are too small or unimportant to be a cyber-attack target. In these cases, executive management may eschew good security for "good enough" security or base security investments on the bare minimum required for regulatory compliance alone. This misguided strategy greatly increases cyber-risk.
- **Shortage of cybersecurity training for non-technical employees.** This tends to result in a lack of awareness and careless behavior such as sharing sensitive data with external parties, connecting to unsanctioned public cloud services, and clicking on suspicious email attachments.

Of course, midmarket organizations are challenged by many of these factors simultaneously. The result? Extremely clumsy defenses and growing cyber-risks to business operations.

Figure 1. Top Five Midmarket Cybersecurity Challenges



Source: Enterprise Strategy Group

A Modern Cybersecurity Technology Strategy for the Midmarket

As ESG research indicates, midmarket organizations face a dangerous threat landscape while lacking the right defenses, resources, and cybersecurity talent. This haphazard approach isn't working—CEOs and cybersecurity personnel need to think outside the box and adopt more flexible security programs that align with business needs and resource realities.

ESG believes midmarket organizations need a comprehensive cybersecurity strategy based upon:

- Integrated platforms built for the midmarket. As previously stated, point tools must be operated on an individual basis, which complicates security operations and makes it difficult to prevent, detect, and respond to security incidents across the network. To alleviate this burden, midmarket organizations should start replacing independent point tools with integrated security technology platforms that provide central management in the form of policy management, configuration management, and reporting and distributed enforcement across multiple security control points like user access, network infrastructure security, and cloud security. In this case, cybersecurity technology platforms must be designed for the realities of midmarket organizations. For example, cybersecurity technology platforms should be easy to deploy and operate, with intuitive GUIs, built-in security content such as secure configuration templates and ransomware detection templates, and continuous content updates like threat intelligence and rules/signatures. Through integration, midmarket organizations should be able to improve security efficacy with increased ability to prevent, detect, and respond to incidents while streamlining operations. Furthermore, individual security applications should share data and present a holistic picture of end-to-end security at any time.
- Process automation capabilities. Given the profound cybersecurity skills shortage, midmarket organizations need to automate cybersecurity processes like generating remediation rules, gathering data for investigations, and applying security patches. Midmarket cybersecurity technology platforms must support this need with simple operations capabilities for tasks like trouble ticketing, case management, and process workflow for the cybersecurity team. Combined with tools integration, this should help midmarket firms address the burdensome manual cybersecurity processes they face today.
- Security analytics. The volume of security telemetry needed to monitor and fine-tune cybersecurity infrastructure is overwhelming for understaffed midsize enterprises. To create order from chaos, midmarket cybersecurity technology platforms must aggregate all security data into interactive dashboards and reports that identify potential threats, monitor Internet usage, and gain critical insights about related traffic trends. The best analytics tools will offer comprehensive reports and dashboards customized for key stakeholders like C-level executives, IT directors, HR managers, network operations personnel, and security analysts, while providing advanced machine learning algorithms to learn from the malicious/benign inputs it receives, aggregate threat intelligence sources, predict threats, accelerate detection, inform response, and automate remediation. Analytics reports should also support compliance needs for regulations like PCI, HIPAA, and KCSiE. In this way, midmarket cybersecurity technology platforms can improve overall security visibility and help organizations mitigate risks and accelerate incident response when need be.
- Services options. ESG research reveals that 46% of midmarket organizations worked with managed security service providers (MSSPs) in 2018 while 33% planned to do so in 2019. Given the global cybersecurity skills shortage, this data is not surprising. Some midmarket organizations need simple staff augmentation while others seek to outsource entire security areas, like threat detection and response. As they adopt cybersecurity technology platforms, midmarket organizations must assess where they need help with deployment and operations. Thus, procurement decisions should be equally guided by the technology capabilities and add-on managed services from vendors and third-party partners.

Enter WatchGuard

Cybersecurity is in a state of transition as organizations try to update their people, processes, and technologies to align with modern threats and organizational limitations. The old “best-of-breed” mentality is no longer appropriate as it has led to an unmanageable army of point tools and complex security operations. As organizations replace this antiquated approach with integrated cybersecurity technology platforms and add-on services, they should seek the best solutions from vendors with cybersecurity technologies designed for the specific needs of midmarket organizations.

WatchGuard is a vendor worth consideration, as it combines a midmarket focus with a modern cybersecurity technology architecture, including network security, secure Wi-Fi, and multi-factor authentication (MFA) solutions. According to ESG research, midmarket organizations rely on security technologies like firewalls (82%), email security (77%), data security (75%), endpoint security (70%), VPNS (61%), and cloud security (61%). WatchGuard provides physical appliances, virtual appliances, or cloud-based appliances offering multifunction security capabilities across these common security controls. The company designs its products for the specific needs of midsize organizations, such as ease-of-use, centralized management, automation/orchestration, common monitoring, and reporting. Finally, WatchGuard combines its security controls with a variety of service offerings. For example, WatchGuard's Total Security Suite includes all services offered with its Basic Security Suite plus artificial-intelligence-enhanced advanced malware protection, DNS-level protection, next-generation cloud sandboxing, data loss protection, enhanced network visibility capabilities, cloud-hosted threat correlation and scoring, and a network visibility platform. It also includes upgraded Gold level 24x7 support.

Beyond product, WatchGuard has spent more than 20 years building an ecosystem of IT solution providers, all proficient in WatchGuard, as well as the broader cybersecurity landscape. Access to this ecosystem of dedicated WatchGuard partners provides midmarket organizations with the ability to supplement their in-house IT with security experts for implementation, ongoing management, or break-fix services.

With its broad product and services coverage and midmarket focus, business and security executives would be wise to evaluate how working with WatchGuard can improve security, streamline operations, and unleash their limited cybersecurity resources.

The Bigger Truth

Albert Einstein is often quoted as saying that the definition of insanity is doing the same thing repeatedly but expecting different results. Regrettably, this is exactly what many midmarket organizations continue to do toward cybersecurity defenses. Firms tend to layer their security infrastructure with tool after tool and manage these tools through a series of manual processes. This increases the workload on their already overwhelmed and under-resourced cybersecurity staff, leading to poor security efficacy, complex security operations, staff burnout, and increasing cyber-risks to the business.

It's time for midmarket organizations to abandon these obsolete practices and move to a more cohesive security strategy anchored by a tightly integrated cybersecurity technology platform designed specifically for midmarket security requirements. These platforms should feature centralized management, broad security functionality, and distributed enforcement, while providing features for process automation. Midmarket organizations should also look to partner with cybersecurity technology platform providers that supplement technologies with an assortment of managed services that help midmarket organizations augment limited in-house skills and staff.

As they seek out the best solutions, midmarket business and security executives should remain openminded toward new types of vendors and solutions. Choose to partner with a vendor that understands midmarket needs, supports industry requirements, offers a well-designed platform for present and future needs, and provides a portfolio of add-on services (on its own or through partners).