IDC PERSPECTIVE

How SMBs Leverage Their Security Services Providers to Drive Outcome-Based Security

Cathy Huang

THIS IDC PERSPECTIVE EXCERPT FEATURES SOPHOS

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: How SMBs Leverage Their Security Services Providers to Drive Outcome-Based Security?

The pursuit of more effective outcomes from the security investment is never exclusive to large enterprises. This IDC Perspective excerpt discusses a small and medium-sized business (SMB) organization in detail as an example of how SMBs select and leverage their security services vendors to address the most common pain points faced by many SMBs and, more importantly, achieve outcome-based security.

Key Takeaways

- Despite being in regulated industries or not, the drive to maximize the security investment among SMBs is as genuine as that of their large counterparts.
- Every security technology vendor that an organization uses has an array of soft costs that need to be considered. Relationship time, training time, and ongoing operations come with a cost.
- The concept of an intuitive and highly integrated security platform resonates among SMBs, given that many SMBs are challenged by hiring seasoned security practitioners and rising labor costs.

Recommended Actions

- Cybersecurity teams need to work with the right security partners to identify the right metrics to track the security value creation.
- One crucial factor to determine is whether the security services vendor can deliver a promise of customer centricity, including being flexible and trustworthy.
- Cybersecurity leaders need to speak and explain cybersecurity strategy and program in a manner that matters to the board in order to secure the required investments and cooperation needed to defend their expanded attack surface.

Source: IDC, 2023

February 2023, IDC #US48547922e

SITUATION OVERVIEW

In this year's *IDC FutureScape: Worldwide Future of Trust 2023 Predictions* (IDC #US49755022, October 2022), IDC predicts that by 2025, 45% of CEOs, fatigued by security spending without predictable ROI, will demand security metrics and results measurement to assess and validate investments made in their security program. This prediction does apply to not only large enterprises but also small and medium-sized businesses (SMBs). In conversations with SMB organizations, whether in regulated industries or not, the drive to maximize their security investment is as genuine and eager as their large counterparts.

Primary considerations when SMBs determine security solutions as well as security providers include the following:

- **Affordability and cost-effectiveness:**
  - Recent macroeconomics headwinds — including inflation, rising labor costs, and a likely recession — have significantly increased pressure on SMBs, with many having to shut down. SMBs often cannot afford to pay as much as their enterprise counterparts.
  - When it comes to small and medium-sized businesses, there is always this problem of lack of sufficient resources, budget, trained personnel, and expertise in their cybersecurity programs.
- **Consolidation and value maximization:**
  - Given the fact that SMBs do not have the resources or skills to assemble so many "best of breed" security providers, it is understandable that SMBs cannot have many security controls in their environment.
  - Every security technology vendor that an organization uses has an array of soft costs that need to be considered. Relationship time, training time, and ongoing operations come with a cost. Conversely, fewer security controls mean fewer vendor relationships to manage across buying cycles, support, and required training time.
- **Intuitive and integrated:**
  - For many SMBs, the preference is to have a smaller number of tools that can be used to the maximum level possible (e.g., 80%+ of the security capabilities) compared with having a large number of tools yet only using 20% or less of their capabilities.
  - The concept of an intuitive and highly integrated security platform resonates among SMBs, given that many SMBs are challenged by hiring seasoned security practitioners and/or a senior cyberleader and rising labor costs.

The original IDC Perspective discussed two SMB organizations in detail as examples of how SMBs select and leverage their security services vendors to address the most common pain points faced by many SMBs and, more importantly, achieve outcome-based security. This excerpt features only the Sophos example.

Customer Example

Why We Chose Sophos' MDR Services

Back in 2018, one of the largest custom upholstery manufacturers in the world experienced significant management changes. Its IT team became very lean as the result of the change. The company had neither the budget nor the human resources to have 24 x 7 monitoring of its systems.

For a long time, the company had been using Sophos for its endpoint and server security. When Sophos introduced its managed threat response services (later upgraded and rebranded to managed detection and response [MDR] services) to the client company in late 2019, to its surprise, it has been a highly smooth, effective, and satisfactory experience.

"Enrolling into Sophos' MDR service settings was just a click away**.** The enrollment process is surprisingly simple. The onboarding of over 900 systems to Sophos' MDR services took a couple of days. Technically speaking, I probably could have enrolled all the systems in a single day but wanted to stage the deployment," said the company's seasoned IT lead who has been with the firm for 12 years.

Besides the simple and smooth onboarding process, according to the client, what works well from the technology perspective is the Sophos Central platform that is "intuitive and easy to change because of the underlying SaaS platform" and a "true single pane of glass for managing key components of our security stack."

The client's familiarity of using the Sophos Central platform is one thing. (The company was already using Sophos Central to manage and monitor its endpoints, servers, and Android tablets for many years.) Sophos' conscious effort in pushing the company's technology and dashboard to be highly integrated and intuitive is another important factor. For instance, the latest acquisition of SOC.OS, a privately held United Kingdom–based firm that was spun out of BAE Systems Digital Intelligence in 2020 and acquired by Sophos in April 2022, is a good example. SOC.OS has an impressive list of integrations and a correlation engine. This benefits Sophos to further expand its Adaptive Cybersecurity Ecosystem, which underpins all of Sophos' security solutions. This will include providing alerts and events from third-party endpoint, server, firewall, identity access management, cloud workloads, email, and mobile security products. This level of integration allows Sophos to claim to "meet clients where they are with technology and operations" because its MDR service supports more than its own technology stack.

Flexibility and Level of Response Actions

According to the same client, Sophos' MDR service stood out from the competition in the level of response actions because the MDR team would be able to act on the client's behalf to contain or neutralize active threats. Other vendors the client reviewed at the time did not offer comparable response actions like what Sophos' team did.

Moreover, the client can change the response actions at any time. Trust is earned. Depending on the level of comfort, the client can choose the level of involvement when an active threat is happening in their environment. The client can choose to be notified by Sophos' team when there is an active threat, so they can respond directly or choose to fully authorize Sophos' team to resolve the active threat and then inform the client. According to Sophos' own statistics, the average MDR threat response time is 1 minute of detection, 25 minutes of investigation, and 12 minutes of remediation.

Put in the client's words, "Knowing we have the option to change the threat response level when we need/want reduces stress and worry." A specific scenario perfectly illustrates the benefit of the said flexibility — "Imagine if all three server admins took a week off at Christmas, we could change the threat response level to authorize, allowing the MDR team to take immediate action to respond to active threats. They would notify us after. Peace of mind."

Very often, client organizations choose to collaborate with Sophos' MDR operations team, meaning authorize Sophos' MDR team to respond only if the client's contacts cannot be reached. According to the client, "The interaction with Sophos' MDR team is very effective. Working with them allows us to focus on other security projects and sleep better."

The client also commented on the effectiveness of escalated cases. The format of case escalation is consistent and, more importantly, the escalated cases already have received a thorough investigation. This allows the client to focus on reviewing recommendations and implementing them where they can.

Working with Sophos' team for this client provides clear reporting and important visibility to the environment, which enables effective communication to the C-suite.

ADVICE FOR THE TECHNOLOGY BUYER

Select the Customer-Centric Security Services Vendor

Cybersecurity is complex and difficult, and it moves fast. Most organizations, especially SMBs, simply cannot manage it effectively on their own. Cybersecurity teams need to work with the right security partners to identify the right metrics to track the security value creation.

While many vendors' marketing messaging may sound similar — for instance, the use of artificial intelligence, a dedicated threat research team, or a global network of security operation centers (SOCs) — one crucial factor to determine is whether the security services vendor can deliver a promise of customer centricity. This includes the following:

- Does the provider understand the client organization's business?
- How flexible is the security services vendor?
- Does the vendor focus on technology/tools or outcomes?
- Is the proposed approach effective for my environment?
- Can the thought of a "trusted partner" or "they have my back so I can sleep better and focus on other things" be properly attributed to the provider?

Focus on Outcomes and Efficiency

In 2022, the SEC proposed a regulation on cybersecurity risk management, strategy, governance, and incident disclosure by public companies. This is expected to drive significant change in terms of the accountability and the relationship between cybersecurity leaders and the board. It will have a ripple effect on SMBs because SMBs very often need to demonstrate strong security posture and compliance as being part of the supply chain.

In the discussed customer case, productivity gain is one of the most mentioned outcomes. Because of the reduced time required to monitor the central dashboard as well as the simplified administration, precious time is freed up for internal security resources to focus on other projects. This is critically important for SMB organizations that often struggle for time, resources, and skills.

From a technical aspect, key metrics also include the number of cybersecurity incidents, mean time to detect, mean time to remediate, and other key metrics. Heightened cybersecurity awareness from the board translates to cybersecurity becoming a top-of-mind topic for the C-suite. Cybersecurity leaders need to speak and explain cybersecurity strategy and program in a manner that matters to the board in

order to secure the required investments and cooperation needed to defend their expanded attack surface.

LEARN MORE

Related Research

- *IDC FutureScape: Worldwide Future of Trust 2023 Predictions* (IDC #US49755022, October 2022)
- *IDC FutureScape: Worldwide Small and Medium-Sized Business and Digital-Native Business 2023 Predictions* (IDC #US49772322, October 2022)
- *IDC PlanScape: Future of Trust – Implementing Automated Compliance Management for Better Efficacy and Efficiency* (IDC #US49617722, September 2022)

Synopsis

The IDC Perspective document excerpt prepared for Sophos discusses an SMB organization in detail as an example of how SMBs select and leverage their security services vendors to address the most common pain points faced by many SMBs and, more importantly, achieve outcome-based security. The pursuit of business outcomes from the security investment is never exclusive to large enterprises. In conversations with SMB organizations, whether in regulated industries or not, the drive to maximize their security investment is as genuine as that of their large counterparts.

IDC defines the worldwide SMB market as follows:

- **Small business (1-99 employees):** All regions
- **Medium-sized business (100-999 employees):** The Americas region and Japan
- **Medium-sized business (100-499 employees):** The rest of the world

"The pursuit of more effective outcomes from the security investment is never exclusive to large enterprises. The mindset of 'to do more with less' will never go out of fashion. It implies the preference of an easy-to-use, effectively integrated platform with fewer interfaces to manage. Thus it reduces the required training time and monitoring efforts and lowers the risk of user errors," says Cathy Huang, research director, Worldwide Security Services at IDC.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com