MARKET NOTE

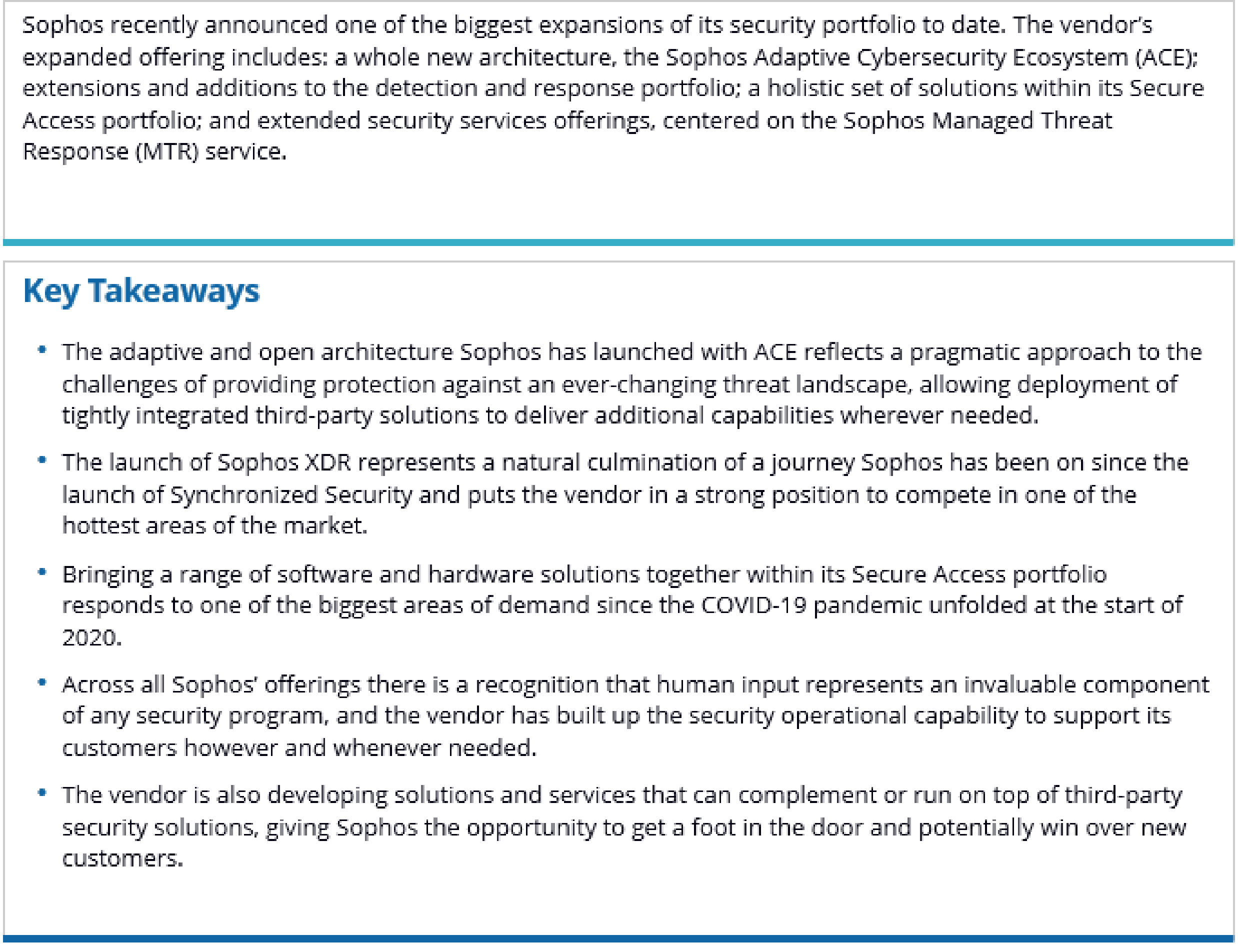
Sophos Plays a Quartet of Aces

Mark Child

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Sophos Plays a Quartet of Aces



Sophos recently announced one of the biggest expansions of its security portfolio to date. The vendor's expanded offering includes: a whole new architecture, the Sophos Adaptive Cybersecurity Ecosystem (ACE); extensions and additions to the detection and response portfolio; a holistic set of solutions within its Secure Access portfolio; and extended security services offerings, centered on the Sophos Managed Threat Response (MTR) service.

Key Takeaways

- The adaptive and open architecture Sophos has launched with ACE reflects a pragmatic approach to the challenges of providing protection against an ever-changing threat landscape, allowing deployment of tightly integrated third-party solutions to deliver additional capabilities wherever needed.
- The launch of Sophos XDR represents a natural culmination of a journey Sophos has been on since the launch of Synchronized Security and puts the vendor in a strong position to compete in one of the hottest areas of the market.
- Bringing a range of software and hardware solutions together within its Secure Access portfolio responds to one of the biggest areas of demand since the COVID-19 pandemic unfolded at the start of 2020.
- Across all Sophos' offerings there is a recognition that human input represents an invaluable component of any security program, and the vendor has built up the security operational capability to support its customers however and whenever needed.
- The vendor is also developing solutions and services that can complement or run on top of third-party security solutions, giving Sophos the opportunity to get a foot in the door and potentially win over new customers.

Source: IDC, 2021

IN THIS MARKET NOTE

In May 2021, cybersecurity vendor Sophos announced one of the biggest expansions of its portfolio to date. The announcements covered four major pillars: the launch of the Sophos Adaptive Cybersecurity Ecosystem (ACE); new features for Sophos Endpoint Detection and Response (EDR) and a newly launched Extended Detection and Response (XDR) solution; an expanded Secure Access portfolio; and extended security services offerings, centered on Sophos Managed Threat Response (MTR).

IDC'S POINT OF VIEW

In recent years, IDC has detected a shift in focus from best-of-breed security point solutions to a best-in-platform approach. This responds to the challenges that many organizations face in terms of managing an overpopulated security estate and integrating too many disparate point solutions, all while trying to keep up with digital transformation (DX) and an evolving threat landscape. The benefits of a platform or ecosystem approach include a unified architecture with natively integrated proprietary components, which can be enriched or extended with dedicated offerings from select third parties. Those third-party components, tailored to fit the platform, can then be easily deployed by the customer, integrated through APIs, and rapidly configured to provide cutting-edge security add-ons.

Another fundamental factor is the way in which the arms race between cybercriminals and security vendors has driven shifts in attackers' behavior and how their targets seek to defend themselves. Traditionally, security has been somewhat rigid and mechanical, in the sense that solutions apply security policies according to the configurations set by security administrators. Once those solutions have been deployed, it is often expected that – to a certain extent – they will run themselves, conferring the desired protection. The reality is that as cybercriminals have become more sophisticated and innovative, they are often able to evade defences and persist within corporate networks for a considerable time, "living off the land". This has driven an evolution in the approach of the defenders, who now look to combine security technologies with advanced analytical capabilities and, critically, human intervention in the form of a security operations approach.

Sophos Plays Its ACE

The security ecosystem approach is the path that Sophos has taken. Of course, the vendor already had a robust security portfolio of its own, with key pillars of endpoint and network security bridged by the Sophos Central unified management console, and extended with components for email, web, mobile, and cloud security. The launch of Sophos ACE builds on the vendor's Project Darwin development, which sought to create an adaptive architecture to underpin the entire Sophos ecosystem and drive security operations. There are multiple elements to this.

Underlying the whole of ACE is the Sophos Data Lake, fed by telemetry from a diverse set of software and hardware sources, as well as Sophos' services and threat intelligence feeds. Above this is a threat intelligence layer that includes Sophos Labs and Sophos Security Operations and applies data science and AI to process and analyze the huge volumes of security data and derive context and insights. On top of that sits the Sophos portfolio of software and hardware solutions, as well as services. One of the key endeavors, implicit in the ACE name, is that the insights from the threat intelligence layer be channeled up to the security infrastructure to adapt response accordingly. Speed of response is paramount; hence the vendor has also put a heavy focus on automation.

An important aspect to note is the human element to this. Sophos Labs and Sophos Security Operations each comprise large teams of analysts that conduct advanced threat hunting across thousands of customer environments, as part of the vendor's Managed Threat Response service. That collective and curated threat intelligence is invaluable in guiding responses and adaptation throughout the ecosystem.

Another key characteristic is that Sophos has designed the system to be open. Every single product in the Sophos portfolio is now API-enabled. APIs allow Sophos' customers and partners to develop tools and components that integrate with the system and can be managed through the Sophos Central management platform. This could include anything from tools that check device health status or conduct security monitoring and management through to threat hunting tools and threat intelligence and feeds.

Sophos actively seeks to expand this range of extensions through its Sophos Technology Alliances Program. Integrations to date include Splunk, SumoLogic, LogRhythm, Rapid7, ConnectWise, Kaseya, and Aruba. From an ease of use perspective, this open and integrated approach is crucial, enabling security teams to get the benefits of operating all the capabilities they need through a single pane of glass.

From EDR and Synchronized Security to XDR

Another major focal point of Sophos' announcements is in the field of detection and response. The vendor launched an update to its EDR solution, version 4.0. This adds new features such as scheduled queries and reports (the number one addition requested by Sophos' customers) and live query and live response functions for individual devices. EDR 4.0 also allows customers to store data from endpoints and servers in the Sophos Data Lake and access it even when a device is offline (for example, if a device is lost or has been knocked offline by an attack). Data is retained in the data lake for seven days under the standard EDR offering. These developments allow much richer context and insights from Sophos' EDR, increasing customers' ability to detect suspicious activity before it impacts their organization.

Sophos also announced several updates and additions to its core Intercept X endpoint security solution. These included a new IPS Engine to provide additional endpoint protection separately from what is provided by firewalls and an Anti-Malware Scan Interface (AMSI) to protect against malicious or obfuscated scripts. Output from AMSI is sent to Sophos' XDR and managed threat response (MTR) teams for additional investigation to feed detection capabilities. One of the newest additions is a Dynamic Shellcode tool that prevents programs from executing malware in memory, a crucial capability for protecting against remote access trojans (RATs). Finally, the vendor updated its behavioural engine to enhance detection and protection.

Perhaps the biggest development in the detection and response area, however, is the launch of Sophos XDR. In some respects, Sophos predated the XDR market with its Synchronised Security approach, launched in 2015. This sought to derive enriched context and insights from the combination of endpoint and network telemetry via Sophos Central. Other vendors, such as Trend Micro and Palo Alto Networks, stole a march on Sophos by going to market with XDR solutions that drew telemetry from multiple sources.

Sophos is now ready to compete in this burgeoning field, with Sophos XDR, backed by the Sophos Data Lake. Telemetry sources include Intercept X (endpoint), Intercept X for Servers, Sophos Firewall, and Sophos email security. The vendor is also working towards bringing in cloud and mobile data to further enrich its XDR telemetry. Under the XDR offering, data is retained in the data lake for 30 days, as well as for 90 days on the device itself. As with Sophos EDR, this enables the security team to conduct investigations even when a device is knocked offline.

Key capabilities of Sophos XDR include identification of unprotected devices on the network, as well as guest and IoT devices within the company's environment. It also correlates indicators of compromise (IoCs) from multiple sources to identify and neutralize potential threats. Fundamentally, a key requirement for any XDR solution is to enable proactive security and orchestrate responses. Sophos has focused on ensuring that it provides a platform for threat hunting and investigations across different components, while enabling remediation of threats across different products. The vendor expects its XDR to become the basis for security interactions across the whole Sophos ecosystem, including its third-party solution partners.

Addressing Secure Access

Secure access has become a top priority for all European organizations since the COVID-19 pandemic unfolded in 2020. As noted above, Sophos already had a strong offering in the network security space and is using this to pull together a robust secure access offering.

A key element of this is zero trust network access (ZTNA), through which Sophos will enable end users to securely access to their corporate networks from anywhere, using any device, with all connections monitored through Sophos Central. Sophos ZTNA comprises three main components:

- The **ZTNA Client**, which will aim to provide a transparent user experience and ensure safe access through monitoring device health, user identity, and Synchronized Security Heartbeat, if the customer has it enabled. The ZTNA Client can be deployed alongside Intercept X or even third-party endpoint solutions. The initial launch will support Windows, with Mac and mobile support on the roadmap.
- The **ZTNA Gateway**, which is both SW-based and VM-based, for on-premises and cloud environments. The ZTNA Gateway provides continuous verification of device health, enforcement of policies, and shares login and event data with Sophos Central.
- **Sophos Central** is the vendor's established cloud management platform, which will enable granular access control through the ZTNA Gateway and Client.

Sophos is also expanding access options for its customers with a new range of Switch hardware products, with the vendor's Security Heartbeat feature built in. Security Heartbeat enables network components to communicate with Sophos Central if unexpected system activity is detected, allowing customers to isolate network segments if that behavior is determined to be malicious. As noted above, Sophos ZTNA also uses Heartbeat and can deny access to corporate applications and data if a device is found to be compromised. The combination of network and device access data through Sophos Central ultimately provides more context, more insights, and more control to enable secure access. Finally, the vendor has also re-engineered its XGS Firewall hardware to improve performance and provide scalable architecture, with multiple models available depending on customer needs.

Threat Response Services

Sophos first entered the security services market at the end of 2019, with the launch of its Managed Threat Response (MTR) service. This was enabled through a series of acquisitions during 2019 (Avid Secure, Rook Security, and DarkBytes) that provided capabilities in the fields of telemetry for public cloud environments, managed detection and response (MDR) services, and additional endpoint protection and threat detection tools, along with orchestration capabilities.

Sophos entered the MDR market with a compelling proposition, including elements in its standard tier that are normally found in premium offerings, competitive pricing, and flexible response modes for engagement. The vendor put a strong emphasis on its willingness to conduct threat remediation on behalf of its clients. That offering seems to be paying off: As of May 2021, the vendor has over 3,000 customers for MTR worldwide, making it one of the fastest-growing offerings in the company's history.

Nevertheless, the vendor is not resting on its laurels. Sophos has also launched a service called Rapid Response, which is open to all organizations, regardless of whether they are an existing Sophos customer or not. If a company is struggling to deal with a security incident and needs external assistance, they can engage Sophos to provide an emergency incident response team that will provide immediate assistance to neutralize an active threat.

Sophos Rapid Response comprises three phases. In the initial onboarding and deployment phase, the team deploys Sophos service solutions and begins incident triage and impact assessment. Phase two, neutralization, covers cutting off attacker access and control within the network and ensuring that any data exfiltration has been halted. In phase three, they transition to monitoring mode, which includes delivering a post-incident report and recommendations to improve the customer's security posture and ensure there is no recurrence of the incident. The whole service is managed by a remote team with no requirement for Sophos staffing on the customer's premises. This allows resources from anywhere in the world to be allocated to incidents, with customers getting 24x7 service.

A notable characteristic of Sophos Rapid Response is its fixed term of 45 days, which removes the cost uncertainty associated with some comparable services, wherein the customer does not know how many days or hours it will take to resolve the threat and, consequently, what the ultimate cost will be. Note that there is a further important consideration for companies that engage Rapid Response: In the initial onboarding and deployment phase, it is necessary for Sophos' team to remove any incumbent solutions before deploying Sophos' own tools. Consequently, by the end of the 45 days, the customer needs to make a decision on whether to fully adopt Sophos, re-deploy their previous solution, or take another path altogether. According to the vendor, more than half of clients that have used Rapid Response to date have gone on to take a full Sophos MDR service.

Another addition to Sophos' services portfolio, which will go live in the summer, is Managed Threat Detection (MTD). This service can even be deployed on top of third-party endpoint protection solutions, so a company running, for example, Symantec or McAfee, will be able to deploy Sophos MTD and benefit from the additional protection provided by that service. That includes 24x7 monitoring and investigation, AI-assisted detection and triaging, case validation by security analysts before incidents or alerts are escalated to the customer, and recommendations for addressing the threat.

Closing Note

Sophos has built up a broad and comprehensive portfolio of security software, hardware, and services. However, the vendor emphasizes that organizations do not need to sign up for the entire Sophos portfolio to reap the benefits of its solutions. New customers can simply deploy the Intercept X endpoint security solution or Sophos Firewall and enable Sophos Data Lake and start getting the advanced threat mitigation provided by Sophos' security insights.

The new solutions and services launched in this round of releases considerably expand the protection Sophos can offer to its customers. A few things stand out and are worth mentioning in conclusion:

- The adaptive and open architecture Sophos has launched with ACE reflects a pragmatic approach to the challenges of providing protection against an ever-changing threat landscape, allowing deployment of tightly integrated third-party solutions to deliver additional capabilities wherever needed.
- The launch of Sophos XDR represents a natural culmination of a journey Sophos has been on since the launch of Synchronized Security and puts the vendor in a strong position to compete in one of the hottest areas of the market.
- Across all of its offerings there is a recognition that human input represents an invaluable component of any security program, and Sophos has built up the security operational capability to support its customers however and whenever needed.

LEARN MORE

- *Sophos Goes the Extra Mile with New Managed Detection and Response Service* (IDC #lcEUR245593319)
- *Thoma Bravo Makes Offer to Acquire Sophos: Private Equity Companies Becoming More Invested in Security* (IDC #lcUS45610919)
- *European Endpoint Security Forecast, 2020-2024* (IDC #EUR145782220)

Synopsis

This IDC Market Note covers Sophos' recent launch of a range of additions and updates to its portfolio, including hardware, software, and services offerings, as well as a whole new platform architecture to enable customers to develop and refine their security as both business processes and the threat landscape evolve.

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.

IDC CEMA

Male namesti 13
110 00 Prague 1, Czech Republic
+420 2 2142 3140
Twitter: @IDC
blogs.idc.com
www.idc.com