SOPHOS
Cybersecurity evolved.

Sophos Adaptive Cybersecurity Ecosystem

The Sophos Adaptive Cybersecurity Ecosystem (ACE) is a broad system built to optimize prevention, detection, and response. It protects the new reality of interconnected business systems, and defends against the shifting cyberattack landscape that now combines automation with live human hacking.

Sophos ACE leverages automation and analysts, as well as the collective input of Sophos products, partners, customers, and developers to create protection that continuously improves – a virtuous cycle that is constantly learning and advancing. And best of all, you can start small and grow. Begin with Sophos endpoint or firewall technology and build off that foundation.

A Sophos Whitepaper. May 2021

A shifting landscape

The landscape in which cybersecurity operates is constantly evolving, and there have been significant shifts in both business environments and the nature of attacks in recent years.

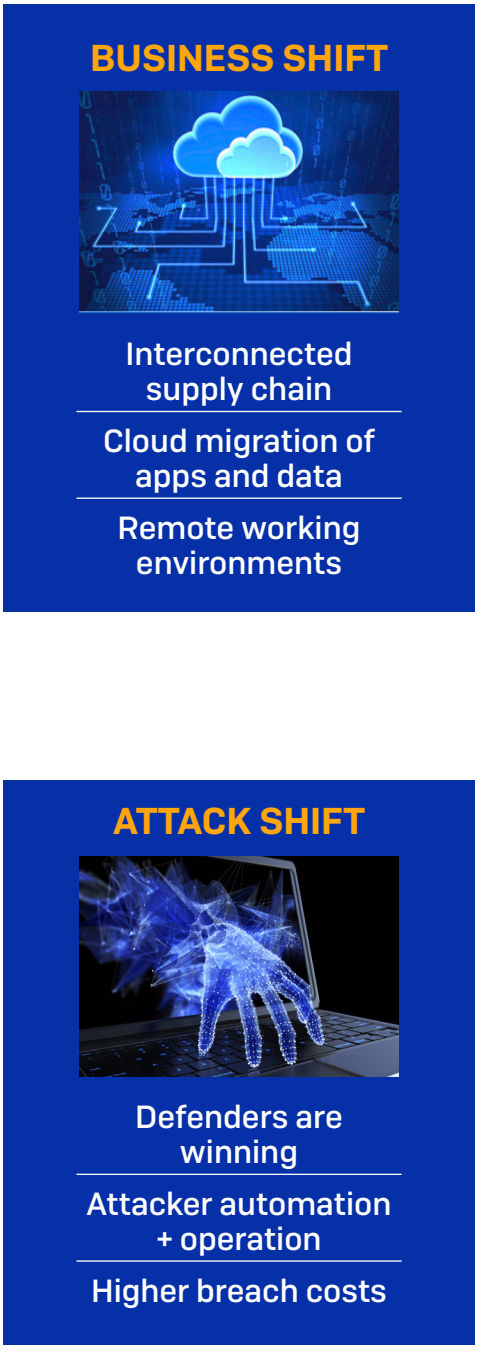
Business shift: Interconnectivity

In the constant search for ways to improve productivity and efficiency, organizations have created a very interconnected supply chain, along with the infrastructure and technology to support it. The migration of data and applications to the cloud has delivered many benefits, like the ability to work from anywhere, lower costs of operation, and improved performance and scalability, while also catalyzing the growth of the global, digital supply chain.

In parallel, COVID-19 rapidly accelerated the shift to home/remote working, and in doing so shattered any remaining myth of an organizational perimeter. It should be assumed that people, applications, devices, and data can be found anywhere.

While these interconnected and dispersed systems serve us well, they also create new security challenges. Many organizations struggle to map the reach of their network, let alone secure all the systems connected to it.

Intelligent, adaptive adversaries persistently target these systems, lured by the opportunity of scale they offer. A recent, but not the only, testament to this was the SolarWinds attack in December 2020 which impacted victims ranging from major technology vendors and smaller businesses to public sector entities at the highest levels.



Attack shift: From automated to operational

When you work in cybersecurity, it's easy to lose sight of an important but under-appreciated fact: in the battle over our critical systems and data, the defenders are winning.

The daily headlines that report new security breaches serve an important purpose: as cautionary tales to remind us to take preventative action and stay vigilant. But these stories are the exception to the rule. There are no headlines for the businesses that successfully defend themselves against thousands of breach attempts every day.

Not only has cybersecurity effectiveness dramatically improved, but the latest tools and managed security services are more accessible and cost effective than ever before. Technologies like anti-ransomware, exploit prevention, behavioral detection, and anti-phishing are available to all.

These capabilities – which are facilitated, improved, and accelerated by artificial intelligence and machine learning –are addressing the known adversarial tactics, techniques, and procedures documented in the MITRE ATT&CK framework as well as new and novel attacks never before seen in the wild. By closing holes, closing paths and blocking techniques, these

improvements have made some attacks so cost prohibitive that attackers have had to adapt. The improvements in security are so significant that the old adage "the attacker only needs to be correct once" is no longer true. In order to make money, attackers need to be correct many times during an attack.

In fact, it has shifted their approach from automated malware to a more comprehensive approach that combines automation with hands-on hacking. The adversaries' main goal is to remain undetected, and the best way to do that is to act like an employee – using local tools, local devices, and typical traffic patterns.

These sophisticated attacks, which require significant human investment, are all the more costly for the victims. The attackers are able to exploit their in-depth knowledge of the victim's environment to cause maximum damage – and demand maximum return.

The IT security shift to security operations

Such business and attack shifts necessitate an evolution in IT security. Organizations face an intelligent adversary that continually moves the objective as they progress toward it, requiring IT security teams to develop countermeasures that improve their chances of winning.

Firstly, it requires a step-change shift from **security management to security operations**. Gone are the days of "set it and forget it" security policy; as attackers move to hands-on-keyboard, IT security needs to do the same to hunt and detect suspicious behavior and events before they become a breach.

Security teams need to look for suspicious activity as early in the attack chain as possible in order to give defenders the ability to respond before damage is done. Even stealthy attackers will leave breadcrumbs, and security teams need to find and follow that trail to stop the attack early in the process. It's no longer just a matter of finding the signal amongst the noise, but of identifying critical weak signals before they become strong signals. The stronger the signal, the closer you are to a breach. With proper tools, IT issues can be proactively detected and remediated before an adversary is able to discover and use them in an attack.

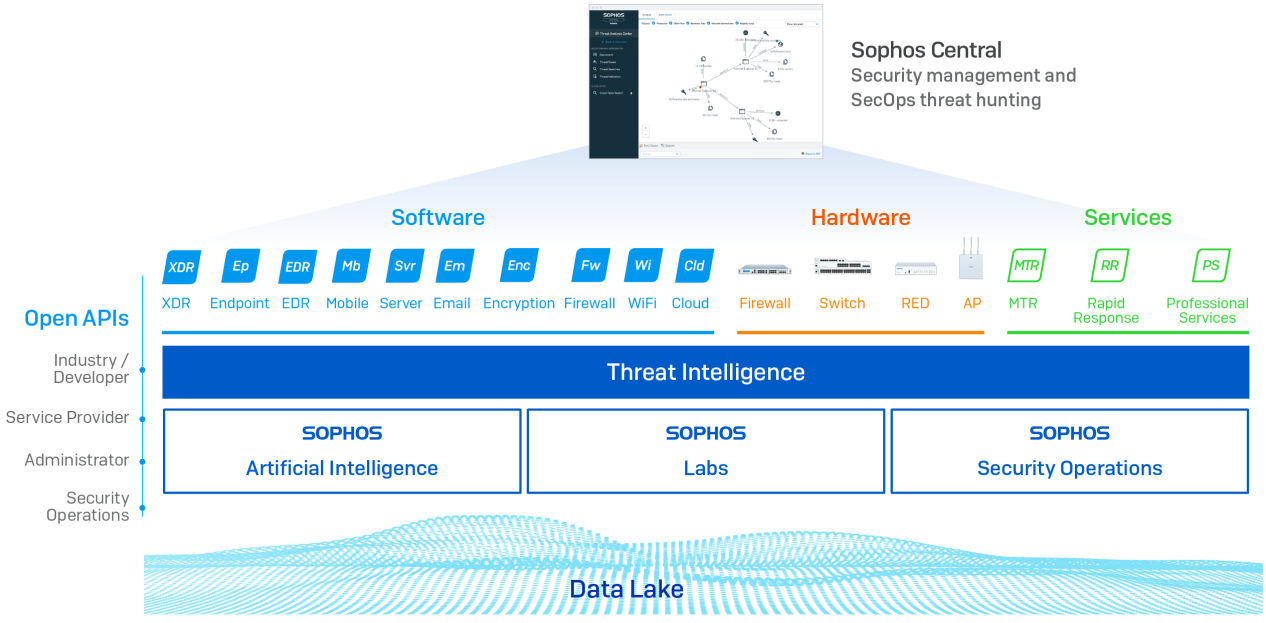
With business now so interconnected, security needs to follow suit. IT security teams need to move from unintegrated security point products to an **adaptive security system** that automatically prevents as much as possible, while enabling operators to search and detect weaker signals – such as suspicious behaviors and events – and prevent them from becoming breaches.

Business environments and attacks are always evolving. The future of IT security is a system that enables a unique feedback loop so it can **constantly learn and improve.** New information and events detected by the operations team can be automated, improving prevention and reducing the number of new attacks that get into the system. Similarly, as automation software improves, operators can find suspicious behaviors and events faster, further reducing incidents. This virtuous cycle constantly improves overall security for an organization and its connected business.

Sophos Adaptive Cybersecurity Ecosystem

The good news is that this system already exists. Sophos's Adaptive Cybersecurity Ecosystem (ACE) addresses this new reality. It leverages the power of automation and analysts to enable the shift from security management to security operations. Automation can analyze and react faster to behaviors and events, while human analysts are better at correlating multiple suspicious signals and interpreting their meaning.

Sophos ACE was built to protect the interconnectedness of our businesses and online world. It protects systems and data wherever they exist, and constantly learns and improves to protect future shifts in technology and attacks.



Sophos ACE starts with the collective **threat intelligence** from SophosLabs, Sophos Security Operations (human analysts who conduct advanced threat hunting across thousands of customer environments via our Managed Threat Response service), and the Sophos Artificial Intelligence group. These real-time intelligence capabilities are continuously improving the next-gen technologies in our world-leading **software** and **hardware** offerings.

A single, integrated **data lake** takes information from all our products and our threat intelligence sources, with real-time analysis that enables defenders to prevent breaches by proactively finding the suspicious signals amongst the noise. In parallel, **open APIs** enable customers, partners, and developers to build tools and solutions that interact with the system. Everything is managed through the **Sophos Central management platform**. All your security in one place for unparalleled efficiency.

These five elements – threat intelligence, next-gen technologies, data lake, APIs, and central management – work together to create an adaptive cybersecurity ecosystem that constantly learns and improves. And while the power of the comprehensive ecosystem is extensive, you can use as much or as little as you like. Many customers start with our endpoint protection or firewall and then expand at their own pace.

The past year has turned many Security Operations Centers into virtual SOCs. Sophos ACE can be managed by security experts from any location, giving organizations the ability to find the best global security talent. Alternatively, our experts can manage threat detection and response as a service for you.

The evolution of Synchronized Security

Synchronized Security, the ability of Sophos products to share real-time information via a Security Heartbeat™ and automate incident response, has been a cornerstone of our protection for many years. When launched in 2015, Synchronized Security was unique in the market, and we continue to offer the most extensive integration of any security vendor with deeper cross-product insights.

"Sophos continues to lead the market with its XDR capabilities between firewall and endpoint security products."

Gartner
Gartner Magic Quadrant for Enterprise Network Firewalls,
Analyst(s): Rajpreet Kaur | Adam Hils | Jeremy D'Hoinne | November 09, 2020

The Sophos Adaptive Cybersecurity Ecosystem builds on the automation and integration of Synchronized Security, and further extends the Sophos cybersecurity system.

More visibility

No one knows where the next attack is coming from, and it's simply impossible for human operators to monitor everything. Instead, you need a system that monitors everything, enabling you to react quickly to emerging threats. That's why we've expanded the ecosystem to include an even wider range of technologies, including new Sophos Extended Detection and Response (XDR) and our APIs. Sophos products see and record all the suspicious events, behaviors, and detections across your environment, so you have the information you need at your fingertips.

More data

The data lake combines and correlates information from all these sensors to deliver deeper cross-product insights. Operators can query the data lake directly with Sophos Intercept X with EDR and Sophos XDR, enabling identification of suspicious behaviors and events across your entire environment – and prevent issues from becoming breaches.

More intelligence

With the rapid growth of our Managed Threat Response (MTR) service, we're able to add real-time data from our expert threat hunters to complement detection data. In parallel, we continue to advance our AI models and threat detection inputs from SophosLabs.

More integration

SophosLabs, Sophos AI, and Sophos Security Operations work together, integrating their expertise for the benefit of all customers in a virtual cycle. For example, PowerShell is a legitimate tool with many good uses that is also widely abused by attackers. The MTR operators train our AI models to distinguish between 'good' PowerShell use and 'bad' PowerShell use based on their real-world experiences. The whole system is then updated with this AI learning, elevating customers' protection.

Sophos Adaptive Cybersecurity Ecosystem in action

Sophos ACE is a live system that is already elevating and extending protection in real-world scenarios. In March 2021, an adversary group called Hafnium exploited a ProxyLogon vulnerability in Microsoft Exchange. This was a zero-day vulnerability, and the attackers took advantage of inherent weaknesses in the way Exchange was designed to avoid triggering any immediate detections.

As soon as the vulnerability became known, the Sophos Managed Threat Response (MTR) service instantly updated sensor monitoring to include behaviors associated with ProxyLogon. With the information already in the data lake, Sophos MTR had instant access to all the inputs they needed to identify and remediate malicious activity related to this vulnerability.

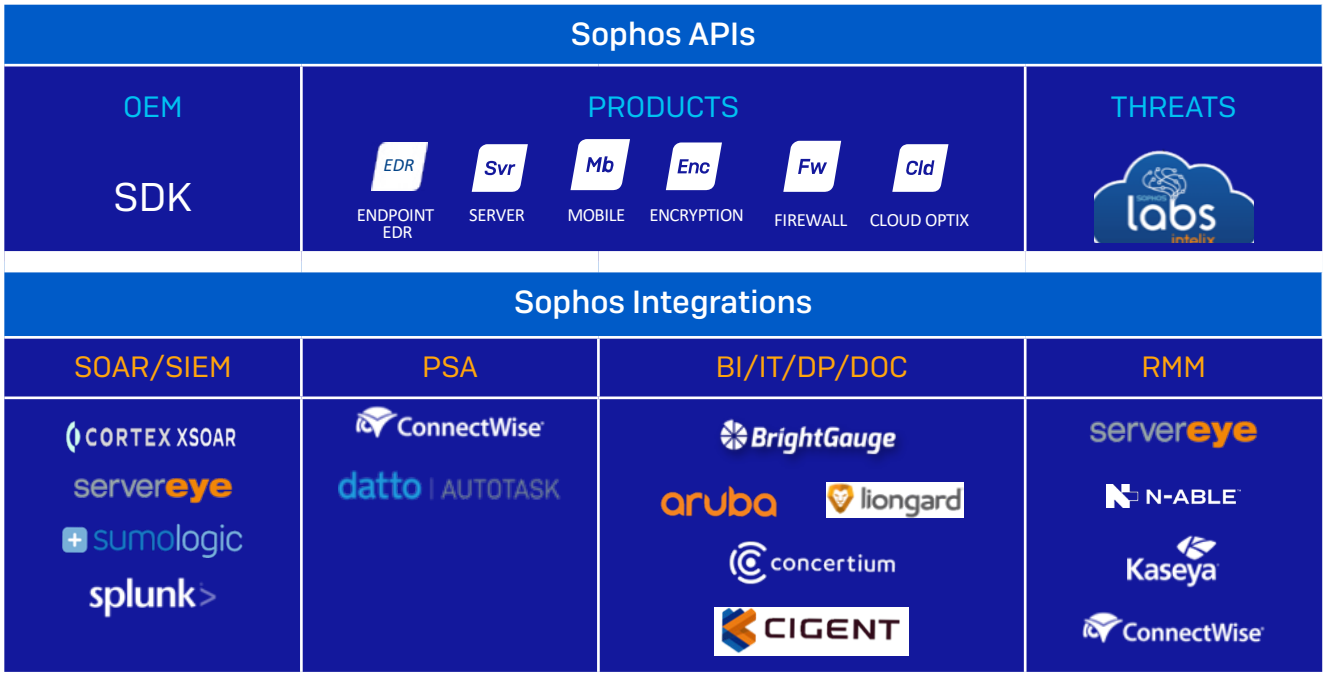
Additionally, they combined their threat hunting skills with Sophos EDR technology to uncover new artifacts or indicators of compromise (IOCs) related to the attack. These indicators were shared directly with SophosLabs who used them to publish additional IOCs related to the Exchange vulnerability, providing further protection for all Sophos customers.

An open platform with powerful integrations and open APIs

In our interconnected world, it's essential that cybersecurity can integrate with the wider business environment. Cybersecurity is multi-faceted, and the Sophos Adaptive Cybersecurity Ecosystem supports a wide range of security needs, including:

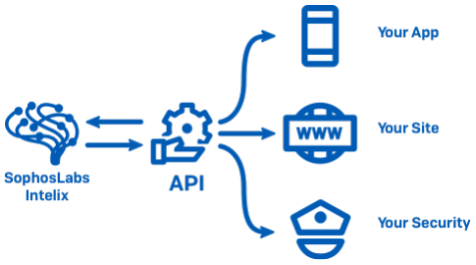
- MSSPs – supporting the delivery of advanced cyber defenses to their customers
- Channel partners – streamlining their business processes
- ISPs – enabling them to ensure the security of the internet services they deliver
- Small and mid-sized enterprises – facilitating the creation of custom tools to control and enable security

Myriad APIs and integrations are already in place – and there are more to come – with Sophos ACE already handling over five million API requests every day.



API showcase: SophosLabs Intelix™

Intelix is a suite of simple and rapid-response RESTful APIs that enables apps to identify, classify, and prevent threats, augmenting their security. Sophos ecosystem customers, partners, and developers can use these APIs to do cloud threat lookups, static file analysis, and dynamic file analysis. More information on the SophosLabs Intelix APIs is available at https://www.sophos.com/en-us/labs/intelix.aspx.



Sophos ACE: Delivering real business impact

The benefits of the Sophos Adaptive Cybersecurity Ecosystem add up. Combining next gen technologies: threat intelligence from SophosLabs, Sophos AI, and Sophos Security Operations; an integrated, adaptive, always-learning system; and centralized management through the Sophos Central platform makes a huge impact, to both protection and efficiency.

Next-gen technologies	+	**Threat intelligence**	+	**Integrated, adaptive system**	+	**Centralized management**

Customers running Sophos Firewall and Sophos Intercept X together already tell us that they would need to double their security headcount to maintain the same level of protection if they didn't have a Sophos cybersecurity system. They also tell us that they experience fewer security incidents and can identify and respond quicker to issues that do occur. Sophos ACE builds on this, further transforming cybersecurity TCO as well as protection.

Getting started

The Sophos Cybersecurity Ecosystem is very flexible, and getting started is as simple as deploying one of the Sophos protection products or services. Organizations immediately benefit from the combined threat intelligence expertise of Sophos AI, SophosLabs, and Sophos Security Operations. You can expand your ecosystem at any time, aligned to the needs of your business. The most popular starting points include:

Sophos Intercept X for your endpoints or servers (with the option to add EDR or XDR functionality)

Sophos Firewall – hardware, software, or virtual

Sophos Managed Threat Response (MTR) service

To learn more, speak with your Sophos representative, check out our website, or start a free trial.

Gartner Magic Quadrant for Enterprise Network Firewalls,
Analyst(s): Rajpreet Kaur | Adam Hils | Jeremy D'Hoinne | November 09, 2020

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Learn more about ransomware and how Sophos can help you defend your organization.

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2021-04-26 (SB-NP)

SOPHOS