

Endpoint Security Buyer's Guide

As cyberthreats become more complex, the pressure to find the right endpoint solution has increased. However, the endpoint security market has become saturated with so many different solutions and unsubstantiated marketing claims that making an informed decision for your organization is becoming increasingly difficult.

This guide provides clarity by walking you through the key capabilities of an endpoint protection solution and what you need to guard against today's advanced threats. Armed with these insights, you'll be better equipped to make a decision for your organization.

Today's Security Threat Landscape

Our independent survey of 3,000 leaders responsible for IT/cybersecurity across 14 countries revealed that today's reality is a two-speed cybersecurity system with adversaries and defenders moving at different speeds. Slowed by multiple headwinds, defenders fall behind while adversaries accelerate.

The Evolution of the Cybercriminal Economy

One of the most significant changes in the threat landscape in recent years has been the transformation of the cybercriminal economy into an industry with a network of supporting services and well-established, professional approaches to operations.

As technology companies have shifted to "as-a-service" offerings, the cybercrime ecosystem has done the same. This has lowered the barriers to entry for would-be cybercriminals and enabled threat actors to accelerate the volume, speed, and impact of their attacks.

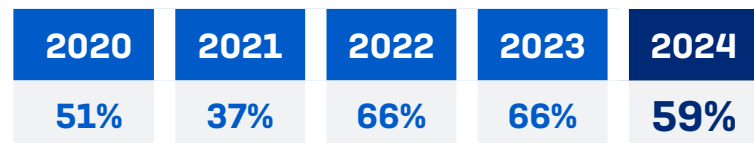
As a result, adversaries can now execute a wide range of sophisticated attacks at scale. 94% of organizations experienced a cyberattack in the last year. While ransomware was the most widely reported attack, organizations experienced many other types of threats, including:¹

| | | |
|-----------------|-------------------------------------|---------------------------------|
| 27% | 27% | 26% |
| Malicious Email | Phishing (including spear phishing) | Data Exfiltration (by attacker) |
| 24% | 24% | 21% |
| Cyber Extortion | Business Email Compromise | Mobile Malware |
| 18% | 24% | 14% |
| CryptoMiners | Denial of Service (DDoS) | Wipers |

Read our report, [The State of Cybersecurity 2023: The Business Impact of Adversaries](#), to learn more.

Ransomware Continues to Plague Organizations

On ransomware, 59% of organizations said they fell victim to an attack in the last year.



In the last year, has your organization been hit by ransomware?
Yes. n=5,000 (2024), 3,000 (2023), 5,600 (2022), 5,400 (2021), 5,000 (2020).

While the rate of attack reported in 2024 has reduced compared to the 2023 figure, data encryption from ransomware remains high, with adversaries succeeding in encrypting data in 70% of attacks.

Ransomware has also become more costly than ever before, with organizations reporting an average recovery cost of \$2.73 million — an increase from the \$1.82 million reported in 2023.²

Read our annual ransomware study, [The State of Ransomware 2024](#), to learn the reality facing organizations in 2024, including the frequency, cost, and root cause of attacks.

¹ The State of Cybersecurity 2023: The Business Impact of Adversaries, Sophos - An independent study of 3,000 leaders responsible for IT/cybersecurity across 14 countries conducted in January and February 2023.

² The State of Ransomware 2024, Sophos - An independent vendor agnostic study of 5,000 leaders responsible for IT/cybersecurity across 14 countries conducted in January-February 2024.

Legacy Approaches Lead to Poor Security Outcomes

The business environment has changed for many organizations in recent years. End-users may be in the office, working remotely, or constantly moving between customers and partners. Company data is no longer held solely on-premises; it can be on-premises, in the cloud, and on end-user devices, all while being accessed locally and remotely to address the needs of geographically dispersed employees. As a result, continuing to follow legacy cybersecurity approaches often results in poor security outcomes.

Some of the most common issues for IT security teams are:

- ▶ **Shortage of skills** – Skilled IT employees continue to be hard to recruit. A lack of experience means employees may not have the skills to determine if a security alert is malicious or benign.
- ▶ **Noise overload** – Too many alerts from many different systems overwhelm operators who often don't know how to prioritize which signals/alerts to investigate, potentially missing indicators of an attack.
- ▶ **Siloed data** – Threat signals/alerts are limited to specific technologies, preventing IT teams from seeing the big picture and remediating malicious alerts or incidents promptly.
- ▶ **Lack of integration** – Security tools don't integrate with each other or a business' IT infrastructure, increasing complexity.
- ▶ **Manual processes** – IT teams spend many hours correlating events, logs, and information to understand what is happening. This effort delays attack identification and response.
- ▶ **Reactive response** – Due to the points above, many IT teams are on the back foot, responding to threats only after they've caused the damage rather than stopping them earlier in the attack chain.

- ▶ **Focus on firefighting** – Day-to-day efforts to stop threats prevent long-term enhancements. When IT teams are firefighting they often don't have the opportunity to identify the root cause of the incident, or keep accurate records of the attack and actions taken. This hampers efforts to address structural issues.
- ▶ **Distributed data** – Users and devices are everywhere. As a result, data is everywhere — on premises, in the cloud, on devices, accessed locally, and via remote access solutions.

One way to counter many of these challenges is to deploy a best-in-class endpoint protection solution.

Endpoint Protection Essentials

Endpoint security solutions should work for and with you, adapting your defenses in response to an attack. At a bare minimum, a modern endpoint security solution should operate with a prevention-first approach that:

Reduces threat exposure – Blocking malicious content and web-based threats and controlling access to applications, websites, peripheral devices, and more.

Blocks malicious activity – Preventing exploitation and techniques that malicious coders and ransomware use to achieve their goals, identifying this specific activity and stopping it before it becomes a problem.

Facilitates adaptive and automated responses – Your defenses should automatically respond to threats and adapt to changing attacker behavior. This not only disrupts an attacker, but can also alert your team to their presence and provide valuable time for your team to respond.

Serves as a conduit for threat hunting (either in house or managed) – High quality signals enriched with security insights can dramatically accelerate threat detection and response. The better the inputs, the faster the resolution.

Delivering Optimal Security Outcomes

Now that we've outlined what an endpoint protection solution should do at a functional level, it's essential to take a broader view of how it can benefit your organization. Strong endpoint protection should work to deliver optimal security outcomes.

Reduced Cyber Risk

Strong endpoint protection reduces your cyber risk and protects you from myriad cyberthreats.

A Prevention-First Approach

The sooner you stop an attack the less work there is, if any, to do later. Superior endpoint protection uses multiple layers to protection to defend against cyberthreats and attacks that target computers, laptops, mobile devices, and servers. Endpoint protection secures these devices and their data from malware, viruses, ransomware, and other malicious activities.

Identifying Drifts in Security Posture

Security posture will drift over time for a number of reasons. In a recent vendor-agnostic survey, security tool misconfiguration was IT managers' top perceived security risk in 2023.²

Looks for endpoint security solutions that constantly evaluate your security posture and optimize your configuration. This automated approach is critical to achieving a strong security posture, reducing your cyber risk, and alleviating the headache of doing so manually.

² The State of Ransomware 2024, Sophos - An independent vendor agnostic study of 5,000 leaders responsible for IT/cybersecurity across 14 countries conducted in January-February 2024.

Streamlined Management

A centralized management console allows IT administrators to monitor and manage security settings, policies, exclusions, and threat alerts across all endpoints from a single location. This simplifies security management, reduces the risk of misconfigurations, and ensures consistent protection. Some centralized management consoles go one step further by automatically checking the "health" of your posture and flagging any activity or policy changes that could compromise it.

Accelerating Detection & Response

Every second counts when an adversary is in your environment. High-quality endpoint protection that starts with a prevention-first approach reduces the amount of noise and delivers high-fidelity alerts. Endpoint detection and response (EDR) and extended detection and response (XDR) technologies can be used to investigate these alerts.

Some solutions go one step further, leveraging artificial intelligence (AI) and threat intelligence to automatically prioritize detections. These solutions ensure that your team knows where to focus its time and accelerate human-led threat response.

Increased IT Efficiency

64% of businesses want their IT teams to spend less time firefighting cyberattacks and more time on strategic issues.³ Automated, easy-to-use endpoint protection helps IT teams realize this goal.

Superior endpoint solutions automatically block and clean-up the majority of threats upfront. This frees up IT capacity, enabling IT teams to prioritize business initiatives. Technologies such as XDR work to reduce signal fatigue, further freeing up time for important projects.

This increased efficiency ultimately allows IT teams to shift from reactive to proactive cybersecurity. It gives these teams the time to seek out threats before they cause long-lasting problems. This, in turn, also reduces cyber risk.

³ The State of Cybersecurity 2023: The Business Impact of Adversaries, Sophos - An independent study of 3,000 leaders responsible for IT/cybersecurity across 14 countries conducted in January and February 2023.

Improved Cybersecurity Return on Investment

Strong cybersecurity should protect organizations from the financial and operational consequences of a major security incident.

Investing in superior endpoint protection is key. Prevention, done well, costs far less than remediation. Strong endpoint protection blocks the majority of threats upfront, reducing the chance of falling to an attack and having to deal with its associated costs.

Furthermore, best-in-class endpoint protection solutions can integrate/communicate with your existing security investments to extend your protection, reduce complexity, and make your existing protection technologies (such as email, firewall, network, identity, and cloud) work smarter and harder than ever before.

All of these things improve your cybersecurity ROI while simultaneously reducing your total cost of ownership.

Optimized Cyber Insurance Position

Cyber insurance premiums have risen significantly in recent years, and policy applications have become more complex and time-consuming. Insurers are demanding stronger cyber controls – in fact, 95% of organizations that purchased insurance in the last year said the quality of their defenses directly affected their insurance position⁴.

The key to optimizing your insurance position is to minimize your cyber risk. Investing in strong defenses, including 24/7 security services and leading detection and response tools, delivers multiple insurance benefits:

1. Makes it easier to obtain cyber insurance coverage (i.e., improves insurability)
2. Helps reduce premiums and enhance terms
3. Reduces the likelihood of a claim – and the resulting higher premiums
4. Reduces the risk of non-payment in the event of a claim

Best-in-class endpoint protection technologies serve as a conduit for detection and response capabilities, so make sure the vendors on your radar offer them. Endpoint detection and response (EDR) is now a prerequisite for coverage for most cyber insurers and organizations and organizations without this capability typically struggle to obtain a policy.

Services that optimize detection and response and therefore minimize the risk of a cyber incident occurring are considered the 'golden standard' by cyber insurers. Organizations that use managed detection and response (MDR) services in particular are often considered "Tier 1" customers by insurers, as they represent the lowest level of risk.

That said, seek out vendors that offer a seamless upgrade path from an endpoint protection solution to a 24/7 fully managed threat hunting, detection and / or incident response service that integrates with existing products and third-party security controls.

⁴ The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption - Sophos.

Evaluating Endpoint Security: Top 10 Questions to Ask

Now that you have a clearer idea of what a best-in-class endpoint security solution looks like, here are suggested questions to ask of a potential vendor.

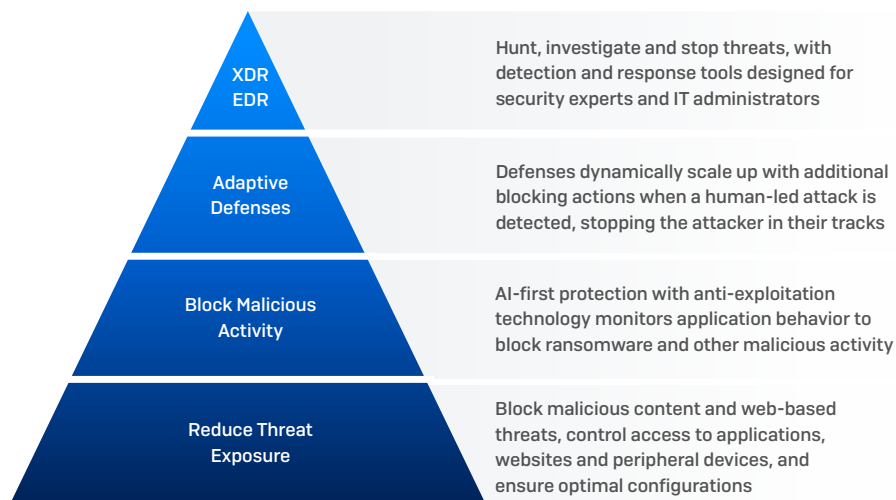
1. Does the product take a multi-layered prevention-first approach? Or does it rely on a detection-first approach? Which specific features are core to the technology?
2. Does the product have the functionality to detect and automatically rectify a drift in security posture? Can it highlight changes in policy settings that increase risk?
3. Does the product automatically respond to a threat? Can it automatically clean up a threat and respond to an incident?
4. Does the product have defenses that automatically adapt when a hands-on-keyboard attack is detected?
5. Does the product have strong anti-ransomware and anti-exploitation capabilities, including real-time protection against remote ransomware attacks? Are these capabilities enabled by default? Do these capabilities need to be activated and trained before they work in your environment?
6. How many consoles are needed to manage the product? Is/Are the console(s) cloud-hosted or do they require on-premises installation?
7. Does the product allow for a seamless transition to EDR/XDR using the same management console and the same agent on the endpoint/server?
8. Does the XDR functionality integrate and incorporate alerts from native and third-party security controls to provide a complete picture of my environment?
9. Does the product offer a seamless upgrade path to a 24/7 fully managed threat hunting, detection, and incident response service that integrates with my existing products and third-party security controls?
10. Does the vendor have third-party testing organizations, analyst, and customer testimonials that validate their approach to endpoint security?

The Sophos Approach

Let's now look at the Sophos approach to endpoint protection. Sophos Endpoint provides unparalleled protection against advanced cyberattacks. Airtight ransomware protection and a comprehensive defense-in-depth approach stop the broadest range of threats before they impact your systems. Powerful EDR and XDR tools enable your team to hunt, investigate, and respond to threats with speed and precision.

Prevention-First Approach

Sophos Endpoint takes a comprehensive approach to protecting all endpoints without relying on a single security technique. By stopping more threats upfront, resource-stretched IT teams have fewer incidents to investigate and resolve.



Reduce Threat Exposure

Sophos Endpoint reduces your threat exposure and the opportunities for attackers to penetrate your environment. It blocks malicious web content and web-based threats and lets you control access to applications, websites, and peripheral devices.

Blocking web-based threats and controlling web access

There are many web-based threats. Organizations often use next-generation firewalls to protect their users working from offices against phishing, malicious websites, and other web-based threats. While this protects endpoints on office networks, endpoints can be used at home, on the road, in coffee shops, etc. where a firewall cannot protect them.

Sophos Endpoint blocks access to phishing and malicious websites by analyzing files, web pages, and IP addresses. It ensures that endpoints are constantly protected against threats, regardless of location.

In addition, SophosLabs and the Sophos MDR team provide real-time threat intelligence to protect Sophos customers against emerging threats.

Controlling web, peripherals, and applications

Sophos allows you to restrict endpoint activities. These controls are generally used with an organization's acceptable use policy.

The first control is monitoring and/or blocking access to categories of websites (gambling, social media, etc.). Sophos Endpoint allows you to monitor and block categories of websites, and the enforcement occurs on and off of office networks.

Controlling access to removable media or other peripheral devices can further reduce your attack surface. Think about times when a user attaches a printer or USB storage device or charges their mobile phone from a USB port. Are any of those actions allowed? This functionality not only blocks an attack vector from getting malicious code onto an endpoint, but it can also help block the exfiltration of company data.

Applications are another category to consider. With application control, you can block applications or browser plug-ins from running on work devices. Following the data exfiltration theme, consider applications like OneDrive or Google Drive for cloud storage. Alternatively, think about torrent programs, TOR browsers, etc. and whether their usage should be allowed on your endpoints. There is a wide range of web browser plug-ins. Many of them have legitimate and beneficial uses, while others do not.

Block Malicious Activity

The next layer of defense involves the use of artificial intelligence, behavioral analysis, anti-ransomware, anti-exploitation, and other technologies to stop threats fast before they escalate.

Sophos uses AI-first protection, starting with AI classification of executables. It utilizes a model trained on millions of good and bad executables. This model can quickly and effectively identify malicious executables based on their properties and does not require any signatures.

Airtight Ransomware Protection




Sophos Endpoint is the most robust zero-touch endpoint defense against local and remote ransomware. It includes advanced CryptoGuard technology that detects the signs of encryption, regardless of the source. This universal approach stops new variants and both local and remote ransomware. It inspects changes to file content in real-time to detect malicious encryption and blocks remote ransomware running on a different device that attempts to encrypts files over the network. Files encrypted by ransomware are automatically rolled back to their unencrypted state, regardless of size or file type. This minimizes any impact on business productivity. It also protects the Master Boot Record (MBR) from encryption used in some ransomware attacks.

Anti-Exploitation

Anti-exploitation technology stops the behaviors and techniques that attackers rely on to compromise devices, steal credentials, and distribute malware. Sophos deploys novel on-device anti-exploitation approaches at scale for all applications. Straight out of the box, Sophos builds on top of the basic protection offered in Microsoft Windows, adding at least 60 proprietary, pre-configured, and tuned exploit mitigations. The result is that Sophos keeps your organization secure against fileless attacks and zero-day exploits by stopping the techniques used throughout the attack chain.

Adaptive Defenses

These additional dynamic defenses are an industry-first initiative that provides a step-up automated protection that adapts to the context of an attack. Sophos Endpoint blocks actions that aren't inherently malicious in an everyday context but are dangerous in the context of the attack. This functionality dynamically responds to and disrupts active attacks where attackers may have gained a foothold without raising red flags or using malicious code.

| | BEHAVIORAL PROTECTION | ADAPTIVE ATTACK PROTECTION | CRITICAL ATTACK WARNING |
|----------|---|---|--|
| SCOPE | INDIVIDUAL DEVICE | INDIVIDUAL DEVICE | INDIVIDUAL DEVICE |
| BENEFITS | Behavioral engine stops early stages of active adversary attacks | Elevates protection sensitivity to prevent damage | Alerts customer to attack requiring immediate incident response |
| TRIGGER | Behavioral rules | Hacking toolsets detected | High-impact active adversary indicators, including org-level correlations and thresholds |
| ANALOGY |  "SHIELDS ON!" |  "SHIELDS UP!" |  "RED ALERT!" |

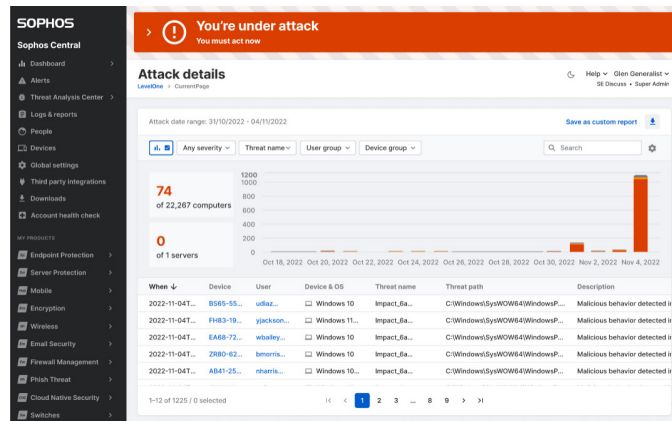
Adaptive Attack Protection

Adaptive Attack Protection dynamically enables heightened defenses on an endpoint when a hands-on-keyboard attack is detected. This removes the attacker's ability to take further actions, minimizes the attack surface, disrupts and contains the attack, and buys valuable time to respond.

Endpoint Security Buyer's Guide

Critical Attack Warning

A Critical Attack Warning alerts you to a severe estate-wide attack if adversary activity is detected across multiple endpoints or servers in your environment with additional high-impact indicators. This is a red-alert situation, and you're under attack! Automated technology informs you of the situation, providing attack context and details. You can respond using Sophos XDR, seek assistance from your partner, or engage the Sophos Incident Response team to help respond to the threat.



Reduce Cybersecurity Total Cost of Ownership

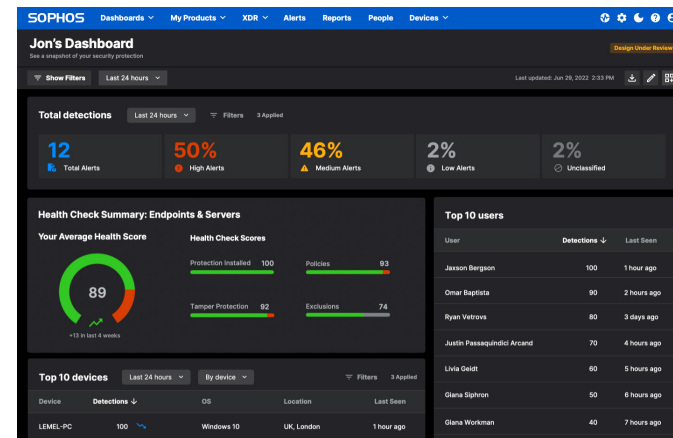
Most IT and security teams are stretched. Automation and saving time and effort are key themes with Sophos Endpoint. Anything that can be automated, reduced, or removed from IT and security teams' workloads allows these teams to focus on other business initiatives.

Sophos Central offers a cloud-based management platform for managing your Sophos products (endpoints, servers, mobile devices, firewalls, switches, access points, email, and cloud), including Sophos Endpoint. From a single location, you can create and manage policies, view detections and alerts, investigate and remediate potential threats, and perform other actions across your Sophos products.

Sophos' recommended protection technologies are all enabled by default, ensuring ease of setup and that you immediately have the strongest protection settings with no complex tuning required. Granular control is available if required.

Identify Drifts in Security Posture

An organization's security posture can drift from compliance or optimum configuration over time. Poorly configured policy settings, exclusions, and other factors pose risks to your security posture. Sophos' Account Health Check identifies security posture drift and high-risk misconfigurations, enabling you to remediate issues with a single click.

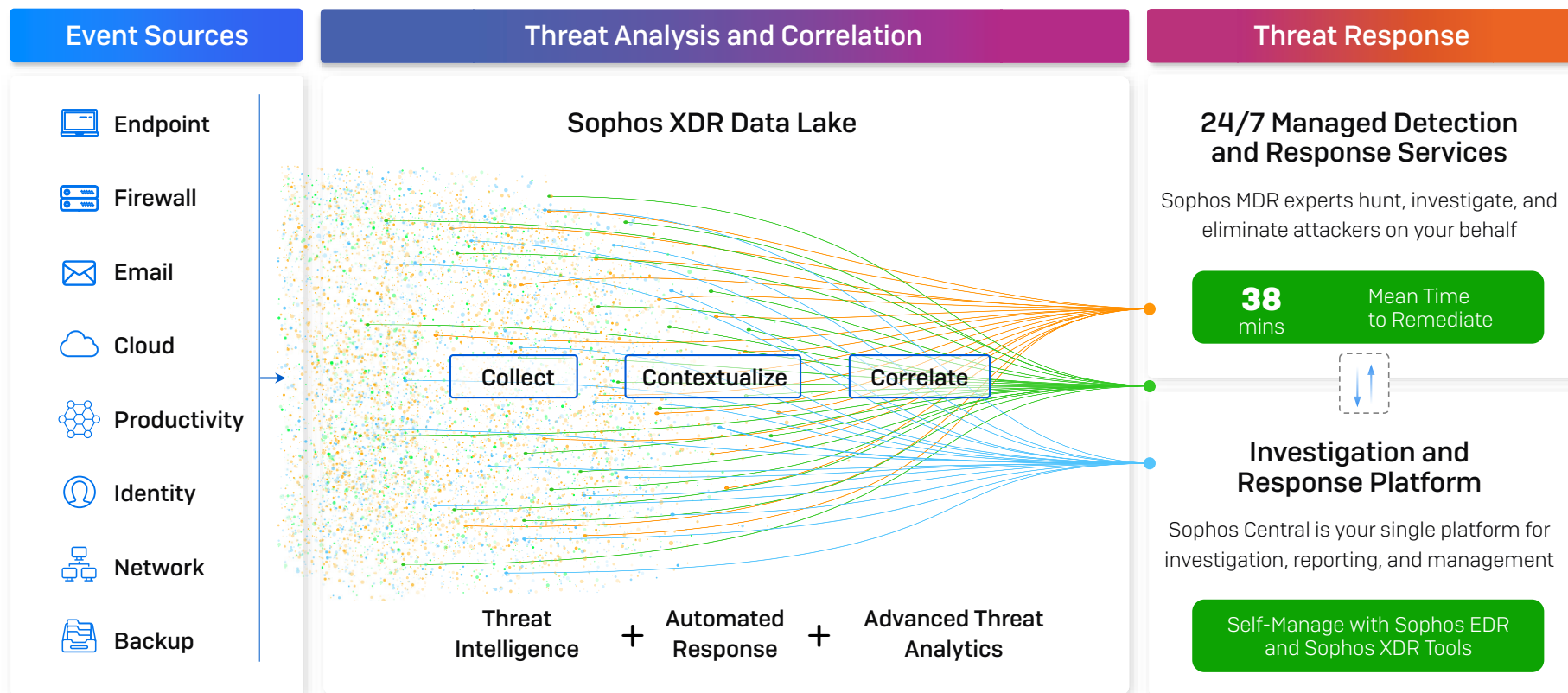


Synchronized Security

Sophos solutions work better together. Sophos Endpoint shares status and health information with [Sophos Firewall](#), [Sophos ZTNA](#), and other products to provide additional visibility into threats and application usage. [Synchronized Security](#) will automatically isolate compromised devices while cleanup is performed and then return network access once the threat is neutralized—all without administrator intervention.

Accelerate Detection and Response: EDR, XDR and MDR

Sophos' prevention-first approach automatically blocks and cleans up as many threats as possible upfront, meaning fewer high-quality detections for IT and security teams to investigate later.



The Sophos approach to prevention, detection and response.

Sophos Endpoint Detection and Response (EDR)

Sophos integrates powerful detection and response capabilities with the robust prevention-first approach of Sophos Endpoint, enabling you to hunt for, investigate, and respond to suspicious activity across endpoints and servers. Detections are prioritized with AI-driven analysis, helping you to identify where best to focus your time and energy. Operators can access devices remotely to investigate problems, install and uninstall software, and remediate any issues.

Sophos Extended Detection and Response (XDR)

For organizations seeking more comprehensive threat detection and response capabilities, Sophos XDR enables you to hunt for, investigate, and respond to suspicious activity and multi-stage attacks across your full security environment. Designed by security analysts for security analysts, it is the industry's only security operations tool that brings together telemetry from native Sophos and third-party security controls to accelerate detection and response. Sophos XDR provides turnkey integrations with an extensive ecosystem of endpoint, firewall, network, email, identity, productivity, cloud, and backup solutions, enabling you to get more ROI from your existing security tools.

Sophos Managed Detection and Response (MDR)

For organizations without the resources to manage threat detection and response in house, Sophos MDR is a 24/7 service delivered by an elite team of experienced threat hunters and incident responders. Sophos MDR leverages telemetry from both Sophos and third-party security controls to detect and neutralize even the most sophisticated and complex threats.

Both Sophos XDR and Sophos MDR meet you where you are, integrating with your existing technology investments, including email, firewall, network, identity, and cloud, and enabling you to get more ROI on your existing investments.

Sophos Incident Response Service Retainer

The Sophos Incident Response Services Retainer is an annual subscription that gives Endpoint, EDR, and XDR customers fast access to a team of incident response experts, with pre-agreed service terms, to rapidly stop active attacks and get you back to normal operations.

Why Sophos

Sophos is a worldwide leader and innovator of advanced cybersecurity solutions, including MDR, incident response, and endpoint, network, email, and cloud security technologies that help organizations defeat cyberattacks. As one of the largest pure-play cybersecurity providers, Sophos defends more than 550,000 organizations and more than 100 million users globally from active adversaries, ransomware, phishing, malware, and more. This unparalleled visibility into the threat landscape provides unparalleled threat intelligence that is used to uplevel the defensive capabilities of Sophos products and services for all customers.

Independent Testing

Reputable third-party testing is an important tool to help organizations make informed decisions about their technology stack and security investments. However, as attacks increase in volume and complexity, meaningful results can only be achieved when the tests reflect organizations' real-world realities.

SE Labs

SE Labs is one of the few security testers in the industry that simulates modern-day attack tools and tactics, techniques, and procedures (TTPs) that cybercriminals and penetration testers are currently using.

In the latest SE Labs Endpoint Security Report (January to March 2024), Sophos again ranked as the industry's best protection, achieving AAA ratings across the board in both the Enterprise and SMB categories. The Q1 2024 SE Labs reports can be found here:

[Endpoint Security: Enterprise | Endpoint Security: Small Business](#)



MITRE Engenuity ATT&CK Evaluations

Sophos excelled in the 2023 MITRE Engenuity ATT&CK Evaluations for Enterprise (Turla). Sophos XDR detected 99% of the adversary behaviors in the evaluation, reporting 141 out of 143 adversary attack substeps. And, demonstrating its ability to provide security teams with rich context on the what, why and how of adversary behavior, Sophos XDR recorded rich analytic coverage for 98% of the substeps in the evaluation.

MITRE Engenuity ATT&CK Evaluations are among the world's most respected independent security tests, due in large part to the thoughtful construction and emulation of real-world attack scenarios, transparency of results, and richness of participant information.



Awards and Analyst Reports

Gartner

- ✓ A Leader in the Gartner Magic Quadrant for Endpoint Protection Platforms for 14 consecutive reports
- ✓ A Customers' Choice in the Gartner® Peer Insights™ Voice of the Customer for Endpoint Protection Platforms (EPP) 2022, 2023 and 2024 reports

IDC

- ✓ A Leader in the 2024 IDC MarketScape for Worldwide Modern Endpoint Security for Small and Midsize Businesses

G2

- ✓ Overall Leader | Endpoint Protection Suites: Spring 2023 and Fall 2023 Grid Reports
- ✓ Overall Leader | EDR: Spring 2023 and Fall 2023 Grid Reports
- ✓ Overall Leader | XDR: Fall 2023 Grid Report
- ✓ Overall Leader & #1 Solution | XDR: Spring 2023 Grid Report

Omdia

- ✓ Overall Leader | November 2022 Comprehensive Extended Detection and Response (XDR) Platforms

CRN Tech Innovators Awards 2023

- ✓ Sophos Intercept X named the best endpoint protection

ChannelPro Readers' Choice Awards

- ✓ Sophos Intercept X named Gold Winner for Best Endpoint Security Vendor

Customer Testimonials



"The most valuable feature of Sophos Endpoint Protection is its advanced threat protection as Sophos utilizes a combination of advanced technologies, such as machine learning, behavioral analysis, and signature-based detection, to detect and block malicious threats."

Software Developer | Finance (non-banking) | [Read the full review on Gartner Peer Insights](#)



"A single pane of glass solution for advanced cybersecurity threats."

Network Administrator | Education | [Read the full review on Gartner Peer Insights](#)



"My experience was industrially satisfying. It reduces the attack surface and prevents attacks from spreading within our organization's network. With its anti-ransomware and deep learning AI, it stops attacks before they impact the system, which is its vast upside."

ICT Security Office | Broadcast Media | [Read the full review on G2 Reviews](#)



"Sophos is an extremely user-friendly yet potent endpoint solution."

IT Operations Manager | Mid-Market Organization | [Read the full review on G2 Reviews](#)



"Sophos Endpoint helps reduce our vulnerability to attackers and provides peace of mind that our customer's systems are secured from bad actors."

Manager of Systems Management and Backup & Recovery | Enterprise Organization | [Read the full review on G2 Reviews](#)

Conclusion

Cybersecurity is highly adversarial and moves quickly. Attackers constantly evolve their techniques to bypass defenses — and security vendors and organizations must adapt.

To do so, it is critical to use security tools that leverage a prevention-first approach. These tools offer automated and adaptive defenses to block or slow down attackers and buy you additional time to respond to cyberattacks.

Meanwhile, understanding what to look for in an endpoint security solution and what optimal security outcomes look like can help you make an informed decision. It also gives your organization the best protection against today's attacks.

At Sophos, we protect organizations against current and evolving threats. Our solutions help organizations achieve the best-possible security outcomes. To learn more, please contact us today.

To learn more about Sophos Endpoint and how it delivers unparalleled protection against advanced attacks, visit [Sophos.com/endpoint](https://sophos.com/endpoint)

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.