SOPHOS

Sophos Guide to Cyber Insurance

How strong cyber controls can improve insurability and reduce premiums.

The cyber insurance market continues to change, and conditions remain tough in response to the increase in the number and cost of claims in recent years. While most organizations already have some cyber insurance, many are finding that the level of cybersecurity they need to qualify for coverage is now higher, policies are more complex, and premiums continue to go up.

Cyber insurance coverage is available, however providers are selective about who they insure and typically avoid high risk applicants. By investing in strong cyber defenses, organizations can reduce their cyber risk which, in turn, improves their insurance position. From facilitating access to coverage, to lowering premiums, and enabling higher limits, strong cyber defenses deliver multiple insurance advantages.

This guide provides an overview into the state of the cyber insurance market and explains the different ways that cybersecurity can positively impact cyber insurance. It also details the Sophos technologies and services that can help you lower your cyber risk and optimize your insurance position.

A Sophos Whitepaper. December 2023

The basics

Why have cyber insurance

Cyber insurance, also commonly known as cyber risk insurance and cyber liability insurance, protects you from the impact of cybercrime (though not from the crime itself). Broadly speaking, there are four main benefits to having cyber insurance:

1. **Financial.** The insurance covers costs in the event of a cyber incident
2. **Commercial.** Cyber insurance coverage is increasingly a pre-requisite for doing business with many organizations
3. **Operational.** The insurance team provides immediate access to experts in the event of an incident, including IT forensics specialists, privacy lawyers, and PR pros
4. **Peace of mind.** Having cyber insurance gives confidence to your customers, partners, suppliers, and employees that you are prepared and covered should a cyber incident strike

Causes of cyber insurance claims

While cyber insurance claims can be triggered by a wide range of incidents, the most frequent cause of claims according to NetDiligence's Cyber Claims Study 2023 Report are:

1. Ransomware
2. Business Email Compromise
3. Hackers
4. Theft of Money
5. Staff mistakes[1]

1 NetDiligence Cyber Claims Study 2023 Report

What cyber insurance covers

Cyber insurance covers the costs incurred as a result of a cyberattack. While individual policies vary, they typically cover:

- Business interruption costs
- Forensic analysis to identify the attack source
- Ransom demands and specialists to handle ransom negotiations
- Costs to regain access or restore your data from backups or other sources
- Legal costs
- Public relations services
- Notification of clients and/or regulatory bodies
- Credit monitoring services for affected individuals

When sourcing policies and comparing costs, it's worth noting that the costs of business interruption, such as loss of income or additional costs of work due to the cyberattack, are included in some policies, but not others.

In the event of a cyber incident, the insurance provider will step in and provide experts to help deal with the situation. For a ransomware attack, they will typically:

- Appoint a consultant to advise on the handling and negotiation of the ransom demand
- Identify the lowest cost way to restore the data (ransom payment, backups etc.)
- Bring in the necessary experts to deal with the issue

First-party vs. third-party coverage

Many policies include both first- and third-party coverage. First-party coverage is direct costs associated with the response to the attack, for example legal fees, forensic fees, customer notification fees, PR fees, and so on. Third-party coverage is primarily costs associated with lawsuits.

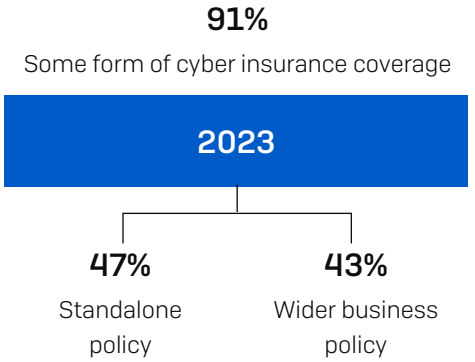
Within a policy, there may be specific sub-limits for first-party coverage, and even for specific items of first-party coverage. For example, first-party coverage may be limited to $500,000, which includes a limit of $50,000 for PR costs.

The realities of cyber insurance

The prevalence of cyber insurance

Having cyber insurance is very much the norm: 91%[2] of organizations had some form of cyber insurance in 2023, according to an independent survey commissioned by Sophos – a notable increase from the 84% reported in 2020[3], and in line with the 92% of organizations that said they had coverage in 2022. Of the organizations that reported having coverage in 2023, some had standalone cyber policies (47%) while others included cyber coverage in broader business insurance policies (43%).

However, these numbers don't tell the whole story. Policies vary and not all policies cover ransomware – the leading cause of cyber insurance claims. Close to one in ten organizations that had cyber coverage in 2022 were not insured for ransomware, leaving them fully exposed to the high costs and challenges of recovering from these types of attack.



2 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption, Sophos
3 The State of Ransomware 2021, Sophos

Cyber insurance adoption by sector

At an industry level, the survey revealed that the education sector (both higher and lower) reported the highest overall level of cyber insurance coverage (96%) although these organizations are more likely to have cyber as part of a wider business insurance policy than to have a standalone policy.

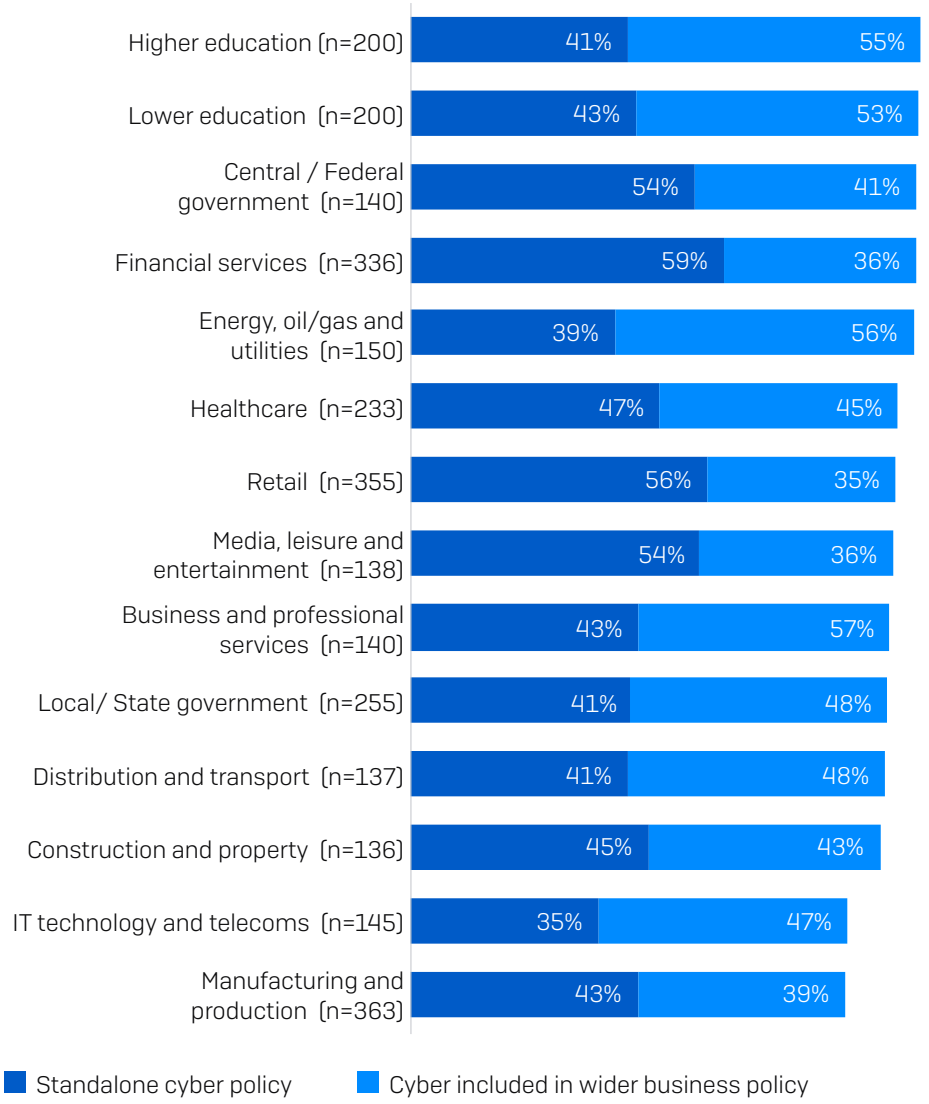
This high level of coverage is understandable given that this sector reported the highest rate of ransomware attacks in our State of Ransomware 2023 study when 80% of higher education providers and 79% of lower education providers said they had been hit by ransomware in the previous year). Financial services reported the highest propensity to have a standalone cyber policy (59%), closely followed by retail (56%).

Cyber insurance adoption by revenue

Perhaps unsurprisingly, cyber insurance adoption increases with revenue. 96% of organizations with $5 billion + annual turnover have some form of cyber coverage compared with 79% of those reporting revenue of less than $50 million.

Larger revenue organizations also have a greater propensity to have a standalone cyber policy than smaller revenue ones: 58% of organizations reporting an annual revenue of over $5 billion have a standalone policy compared with 34% of those reporting annual revenue of less than $10 million. Overall, our research reveals a steady increase in standalone policy adoption with revenue[4].

Cyber insurance adoption by sector, 2023



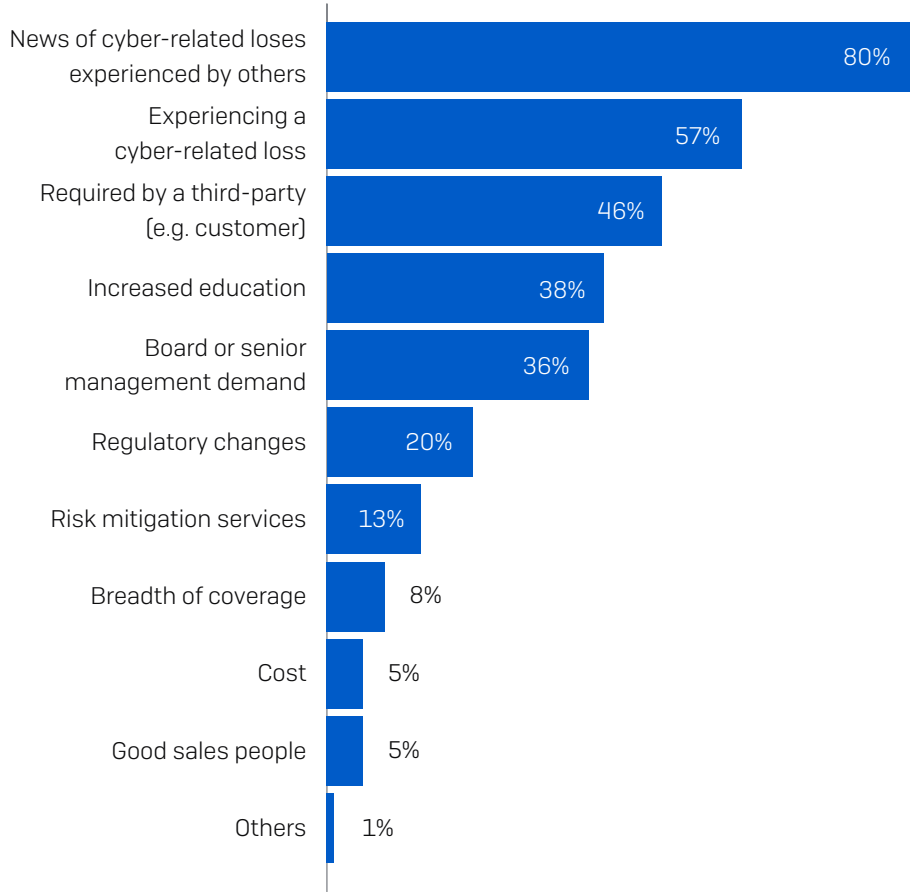
Does your organization have cyber insurance? Yes, we have a standalone cyber insurance policy, Yes, we have cyber insurance as part of a wider business insurance policy (e.g. a general liability policy). Base numbers in chart

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

Cyberattacks are fuelling cyber insurance

A survey of cyber insurance brokers and cyber underwriters from around the world by Advisen and PartnerRe provides insight into the top drivers of new or increased cyber insurance sales. It is perhaps unsurprising that the top two factors behind the take up of cyber insurance are news of cyber-related losses experienced by others and experiencing a cyber-related loss. However, in third place is 'required by a third party'. With the increase in supply chain attacks, organizations are increasingly required to have cyber insurance as a condition of a business engagement that covers the client if they experience a cyber incident as a result of the partnership.

Over one in three (36%[5]) cite board or senior management demand as one of the top drivers of cyber insurance purchase. This high level of demand from leadership teams reflects the cross-organization devastation that a major cyber incident can cause. Defending against the implications of a cyberattack is now a mainstream business issue, not just an IT challenge.



Cyber Insurance: The Market's View – Advisen, PartnerRe

5 Cyber Insurance: The Market's View, PartnerRe and Advisen

The cost of cyber insurance

As with all other forms of insurance, the cost depends on multiple factors, including:

- **Demographics:** Size, industry, sector, location, revenue etc.
- **Potential exposure:** Type and volume of sensitive data stored/collected/processed
- **Level of cybersecurity:** The security defenses an organization uses
- **History:** Previous claims invariably result in higher premiums
- **Policy terms:** Coverage/liability limit etc.

It is important to be aware of the distinction between deductible and retention policies. With a deductible policy, the deductible (known as 'excess' in some countries) is included in the overall policy limit. Conversely, with a retention policy, the retention amount is in addition to the policy limit.

DEDUCTIBLE	RETENTION
$100K policy limit, $10K deductible (excess)	$100K policy limit, $10K retention
You pay first $10K of claim, insurer pays $90K	You pay first $10K of claim, insurer pays $100K
Total coverage $100K	**Total coverage $100K**

Insurance towers

In the SMB market, it is not uncommon for there to be just a single carrier for cyber insurance. However, in the large enterprise market, cyber insurance towers are common, as one single insurer cannot provide all the necessary risk transfer. Insurance brokers build towers for individual customers, bringing together two, three, four, or more providers. The first provider covers cover the primary risk transfer, with the remainder covering the excess risk transfer.

Insurance panels

Cyber insurance carriers will often have pre-approved suppliers, called a 'panel', that they work with in the event of an incident. If the company experiencing the incident does not have any existing relationships with suppliers, the cyber insurance carrier will encourage or even require them to work with one of these 'on-panel' organizations.

That said, most carriers are also open to working with other reputable suppliers, especially if a pre-existing relationship and/or contractual terms exist. This is referred to as an 'off-panel' approval. Naturally, there are many financial and operational advantages to working with a supplier that already knows the organization experiencing the incident and is familiar with their IT and business set-up.

If your preferred supplier is not 'on-panel' with your insurance provider, you can request to use them. Early communication with your insurance provider is paramount so your preferred supplier's cyber insurance team can engage with the insurance provider for the appropriate approvals.

Coverage needs

When selecting a cyber insurance policy, it's important to choose the appropriate level of coverage for your organization. You need to be able to recover successfully and keep your business afloat if you experience a cyberattack – while at the same time keeping your premiums at an affordable level.

The costs to recover from a cyberattack are considerable and rising. The average cost to an organization to rectify the impact of a ransomware attack in 2023 was US$1.82M[6] - up from US$0.76M in 2020. Interestingly, this is a small but welcome drop from US$1.85M in 2021 which likely reflects that, as ransomware has become more prevalent, the reputational damage of an attack has lessened. In parallel, insurance providers are better able to guide victims swiftly and effectively through the incident response process, reducing the remediation cost.

6 The State of Ransomware 2023, Sophos

The cyber insurance market

Cyber insurance conditions have hardened

Cyber insurance was for many years a 'soft' market, characterized by high capacity and low premiums. However, the market hardened in 2021 for the first time in its 15-plus year history as a standalone policy, as insurers saw their payouts rising faster than their income from premiums: the industry's loss ratio rose steadily from 2018, rising to 72.8% in 2020[7]. (Loss ratio is insurance costs divided by total earned premiums. For example, if a company pays $80 in claims for every $160 in collected premiums, the loss ratio would be 50%.)

A number of factors were behind this hardening of the market:

- Cyberattacks increased in volume and complexity –
  - 57% of IT managers said they have experienced an increase in volume of cyberattacks [8]
  - 59% said they experienced an increase in the complexity of attacks[9]
- The costs to recover from a cyberattack increased – as mentioned, the average cost to remediate a ransomware attack in 2023 was a crippling US1.82M

The result of this market hardening is that it became much harder to secure cyber insurance coverage. This situation was confirmed by our study of 5,600 IT professionals conducted at the start of 2022 which revealed that 94% of those with cyber insurance said the process for securing cover had changed over the last year:

- 54% said the level of cybersecurity they need to qualify was higher
- 47% said policies were more complex
- 40% said fewer companies were ofering cyber insurance
- 37% said the process took longer
- 34% said it was more expensive[10]

"Our cyber insurance is up and we're having to jump through more hoops than we've ever had to before."
Corporate travel company

This hardening of the market created a particular challenge for public entities, which are often considered to be easy targets for cybercriminals due to their weaker defenses. As a result, public organizations looking to obtain or renew coverage were facing fewer providers and tougher conditions, with prices sometimes doubled year over year.

"Where [insurers] used to offer $10 million in limit, it's now $5 million."
Jack Kudale, CEO, Cowbell Cyber Inc.

The second half of 2023 has seen selective softening of the cyber insurance market. Capacity has increased as new players enter the market, however providers are highly selective about who they cover: low risk organizations are seeing improved insurance offers while higher risk companies continue to struggle to get coverage.

Cyber insurance pays out

The good news for anyone with cyber insurance is that policies invariably deliver if the worst happens and you fall victim to a cyberattack. In Sophos' State of Ransomware 2022 survey, 98% of respondents insured for and hit by ransomware said the insurance provider covered costs resulting from the attack. In nearly three quarters (73%) of incidents the insurance provider covered the clean-up costs to get the organization back up and running again. In 36% of incidents the insurance paid the ransom, and in 33% it paid other costs such as those incurred for downtime and lost opportunities.

7 S&P Global, June 1, 2021
8 The State of Ransomware 2022, Sophos
9 The State of Ransomware 2023, Sophos
10 Cyber Insurance 2022: Reality from the InfoSec Frontline, Sophos

Cyber insurance is driving improvements to defenses

In light of the hardening market, almost all organizations (97%) with cyber insurance have made changes to their cyber defenses to improve their insurance position.

- 64% have implemented new technologies/services
- 56% have increased staff training/education activities
- 52% have changed processes/behaviors[11]

But what are the changes you should make?
What will help you improve your cyber insurance position?

11 Cyber Insurance 2022: Reality from the InfoSec Frontline, Sophos

Strong cybersecurity helps optimize your cyber insurance position

There is a direct relationship between cybersecurity and cyber insurance - in fact, 95% of organizations that purchased insurance in 2023 said the quality of their defenses directly affected their insurance position[12]. Investing in strong defenses, delivers multiple insurance benefits:

1. Facilitate access to coverage

60% of organizations with cyber insurance said that the quality of their defenses impacted their ability to get coverage[13]. Providers are focusing increasingly on managing – and reducing – risk. Strong cybersecurity enables you to reduce your cyber risk which, in turn, makes you a more attractive prospect for cyber insurance coverage. While each insurer's specific requirements will vary, several cyber controls are commonly looked for across the market:

Multi-factor authentication

Multi-factor authentication is an essential requirement to secure coverage as insurers look to close a common security gap before they absorb risk.

"Our cyber insurance renewal is predicated on us enabling MFA for remote access."

IT support and services provider, USA

"I was told that if we don't get MFA within a year, our cyber insurance will be dropped."

Healthcare provider, USA

Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR)

High quality endpoint protection that automatically blocks threats is a core foundational layer of strong cyber defenses. However, as adversaries continue to evolve their attacks by exploiting legitimate IT tools, compromised credentials and unpatched vulnerabilities, endpoint protection alone is no longer enough. To stop advanced ransomware and breaches (and the resulting claims) it's essential to also proactively monitor for, investigate and respond to suspicious activities before threat actors can deploy their attacks.

EDR and XDR are tools that enable security specialists to detect and investigate potential compromise, and neutralize an advanced cyberattack before damage is done. As their names suggest, EDR works solely with data points from endpoint protection technology, while XDR takes data sources from endpoint solutions and the wider wide security stack, including firewall, email, cloud, and mobile security solutions, to provide greater visibility and accelerate detection and response. EDR in particular is often a prerequisite for coverage for most cyber insurers and organizations without this capability typically struggle to obtain a policy.

Managed Detection and Response (MDR)

MDR is a fully managed, 24/7 service delivered by experts who specialize in detecting and responding to cyberattacks that technology solutions alone cannot prevent. It provides the highest level of protection against cyberthreats, minimizing the risk and the likelihood of making a claim. While rarely a make-or-break requirement for coverage, organizations that use MDR services are often considered "Tier 1" customers by insurers, as they represent the lowest level of risk.

"Legal wants to get ransomware insurance and [MDR] is the step we need to get it done."

IT technology and solution provider, global reach

12 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption, Sophos
13 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption, Sophos

Incident response plan

The best way to stop a cyberattack from turning into a full breach is to prepare in advance. Often, after an organization experiences a breach, they realize they could have avoided a lot of cost, pain, and disruption if they had had an incident response plan in place. Having a detailed plan that enables you to minimize the impact of an incident will reduce your cyber risk, making you a more attractive prospect to insurance providers

2. Reduce premiums

62% of organizations with cyber insurance said that the quality of their defenses impacted the cost of their coverage[14]. Just as an alarm and window locks reduce your home insurance premiums, having advanced cyber defenses helps reduce your cyber insurance costs. While the insurers' exact premium calculation algorithms are a closely-guarded secret, customers consistently say that the quality of their protection impacts their premiums.

"Because we didn't have EDR installed on 100% of our appliances, the insurance [costs] doubled."

Web hosting company, USA

"With Measured, customers who have implemented Sophos MDR or Sophos Endpoint products can reduce their cyber insurance premium by as much as 25%."

Measured Insurance, USA

3. Reduce the likelihood of making a claim

As with other forms of insurance, if you make a claim, you may struggle to renew your policy. Organizations that have made claims also experience a significant increase in their premiums in subsequent years. By minimizing your risk of being impacted by a cyberattack through strong cyber defenses you reduce the likelihood that you'll need to call on your policy – and help keep your premiums down.

4. Reduce the risk of non-payment

Poor IT security hygiene can prevent you receiving financial support in the event of an incident. If the insurer believes that you 'left the door open' through weak practices, they may have grounds to not pay out. By eliminating these gaps, you can help ensure that, should the worst happen, the insurance company will step in.

"We do not pay for any claims, losses, breaches, privacy investigations or threats due to the use of outdated or unsupported software or systems."

Hiscox Cyberclear™ policy wording, UK, June 2021

5. Minimize the impact and cost if an incident occurs

Responding quickly and appropriately to a cyberattack can significantly reduce the impact and cost of the incident. Having a malware incident response plan in place and being able to call on experienced incident responders will help you minimize the fall-out from the attack.

14 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption, Sophos

How Sophos can help

Optimize your cyber defenses

Sophos enables organizations to achieve many of the cyber controls that are increasingly required to both qualify for insurance coverage and access the best pricing and policy terms – all backed by the threat intelligence and cybersecurity expertise of Sophos X-Ops.

Sophos Endpoint Detection and Response (EDR)

Sophos EDR combines the robust prevention-first approach of Sophos Endpoint with powerful detection and response capabilities that enable security analysts and IT administrators 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, terminate active processes, run scripts or programs, edit configuration files, and more..

Sophos Extended Detection and Response (XDR)

The more you see, the faster you can act. Sophos XDR leverages telemetry from your existing Sophos and non-Sophos security investments so you can detect, investigate, and respond to suspicious activity across your full security environment.

- **Detect:** AI-powered detections provide instant visibility of suspicious activity across all key attack surfaces, and our simple SQL-less search lets you hunt threats at speed
- **Investigate:** Automatically created cases and prioritized detections make it easy to focus on what's important, while our analyst-designed UX gives you the information and tools you need to carry out investigations easily
- **Respond:** Extensive case management tools and response actions empower you to collaborate with team members and quickly neutralize attacks

Sophos Managed Detection and Response (MDR)

Sophos MDR is the world's most trusted MDR service, securing more organizations than any other vendor. Providing 24/7 threat detection, investigation, and response delivered by an expert team as a fully-managed service, Sophos MDR gives you the ultimate protection. With an average incident closure time of just 38 minutes, Sophos MDR greatly minimizes the risk of a major cyber incident and optimizes your insurance position.

Reduce likelihood of making a claim

Sophos gives you world-leading protection against ransomware, malicious hacking, and other advanced threats. Our solutions help you minimize the risk of experiencing a major cyber incident, reducing the likelihood of needing to make a claim and helping keep premiums down in the future.

"We can't stop everything that comes in, that's why we rely on Sophos."

Vancouver Canucks, Canada

Sophos customer and analyst validation

Sophos solutions are widely recognized by customers , the analyst Community and independent testers, including:

Sophos Managed Detection and Response (MDR)

- Named a 2023 Gartner® Customers' Choice™ for Managed Detection and Response (MDR) with a 4.8/5 customer rating on Gartner Peer Insights
- Named an Overall Leader for Managed Detection and Response (MDR) in the G2 Grid ® Fall 2023 reports
- Top performer in the 2022 MITRE Engenuity ATT&CK Evaluation for Managed Services

Sophos Extended Detection and Response (XDR)

- Named an Overall Leader for XDR in the G2 Grid ® Fall 2023 reports
- Top performer in the 2023 (Turla) MITRE Engenuity ATT&CK Evaluations
- Recognized as the #1 overall leader in the Omdia Universe for Comprehensive Extended Detection and Response (XDR)

Sophos Endpoint Detection and Response (EDR)

- Named a Leader in the 2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for the 13th consecutive time
- Named a 2023 Gartner® Customers' Choice™ for Endpoint Protection Platforms for the second consecutive year with a 4.8/5 customer rating on Gartner Peer Insights
- Named an Overall Leader for Endpoint Protection Suites and EDR in the G2 Grid ® Fall 2023 reportsTop performer in the 2023 (Turla) MITRE Engenuity ATT&CK Evaluations
- AAA ratings and 100% Total Protection scores in the Q3 2023 SE Labs Endpoint Security Report in both the Enterprise and SMB categories.

For more information on Sophos solutions click here

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.

2024-01-12 (WP-PC)

SOPHOS