SOPHOS

Sophos Guide to Cyber Insurance

How strong cybersecurity controls can help reduce premiums and lower risk

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

Good cybersecurity can help with cyber insurance in multiple ways: from facilitating access to a policy approved through underwriting to lowering premiums and reducing the likelihood of making a claim.

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

A Sophos Whitepaper. April 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 three main benefits to having cyber insurance:

1. **Financial**. The insurance covers costs in the event of a cyber incident

2. **Operational**. The insurance team provides immediate access to experts in the event of an incident, including IT forensics specialists, privacy lawyers, and PR pros

3. **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 2022 Report are:

1. Ransomware

2. Hackers

3. Cyber events

4. Business Email Compromise

5. Staff mistakes[1]

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 Ì 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.

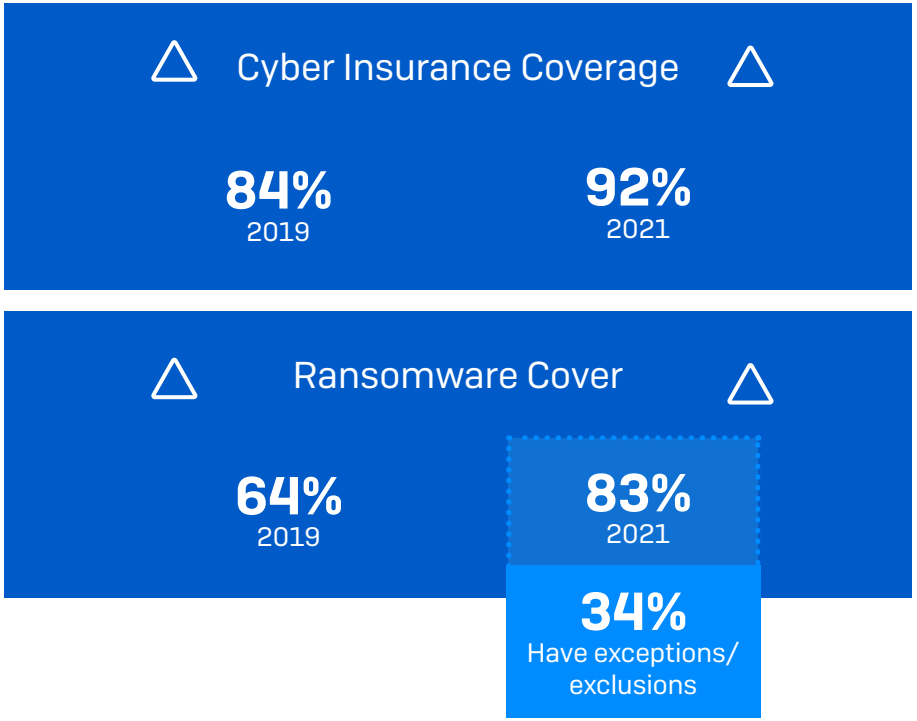
1 NetDiligence Cyber Claims Study 2022 Report

The realities of cyber insurance

The prevalence of cyber insurance

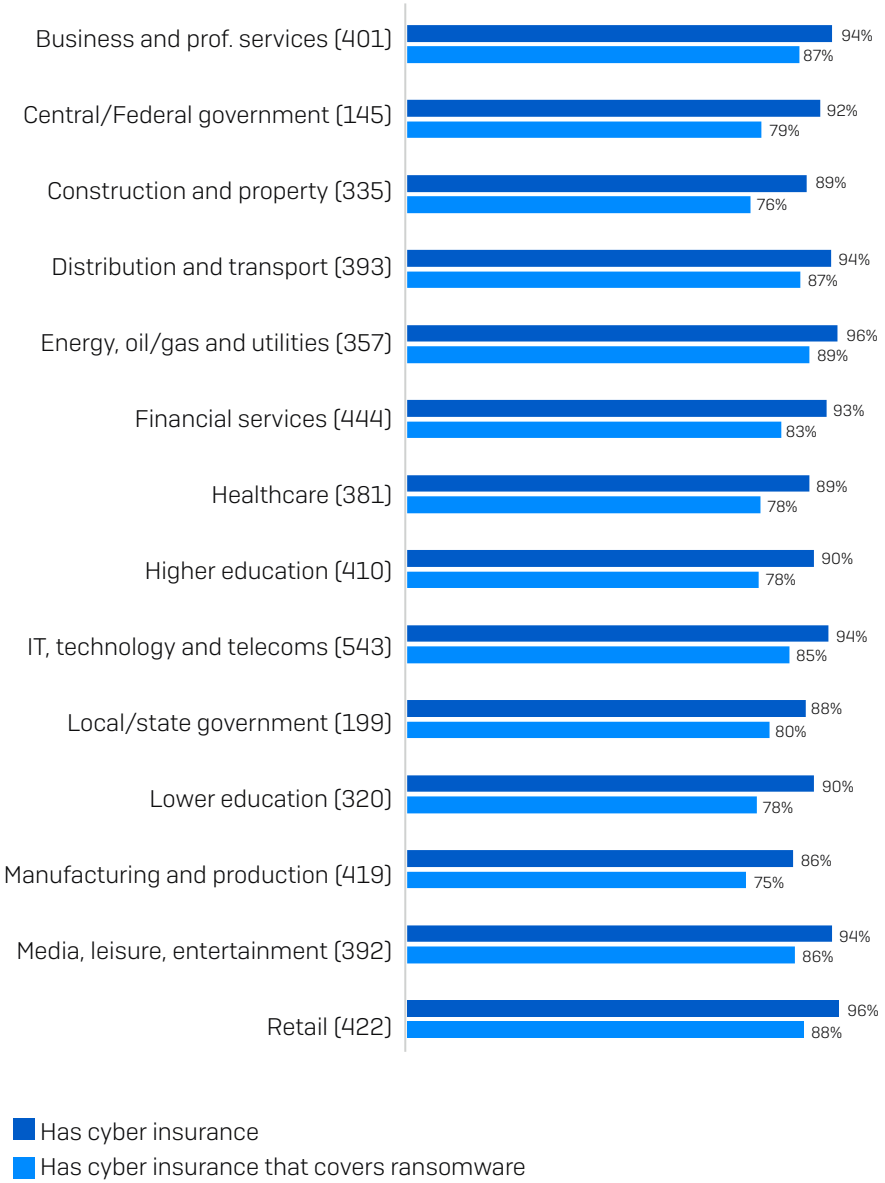
92% of organizations have some form of cyber insurance according to an independent survey of 5,600 IT decision-makers in mid-sized organizations commissioned by Sophos (up from 84% the year before)[2]. Some have standalone cyber policies while others include cyber coverage in broader business insurance policies.

Cyber insurance is commonplace across all industries, however the energy, oil/gas and utilities sector has both the joint highest level of cyber insurance coverage (96%), together with retail, and the highest level of coverage against ransomware (89%). This is unsurprising given that this sector is a major target for attacks (for example, the Colonial Pipeline ransomware incident of 2021), and also has high levels of legacy infrastructure that is often hard to keep up to date, increasing exposure to attack. Encouragingly, 83% of respondents have cyber insurance that covers ransomware (up from just 64% in 2020), although 41% of them (34% of all respondents) say there are exceptions and exclusions in their ransomware coverage. The takeaway here is to make sure that you're fully aware of the details of your policy and what it covers.



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

Cyber Insurance Adoption by Sector



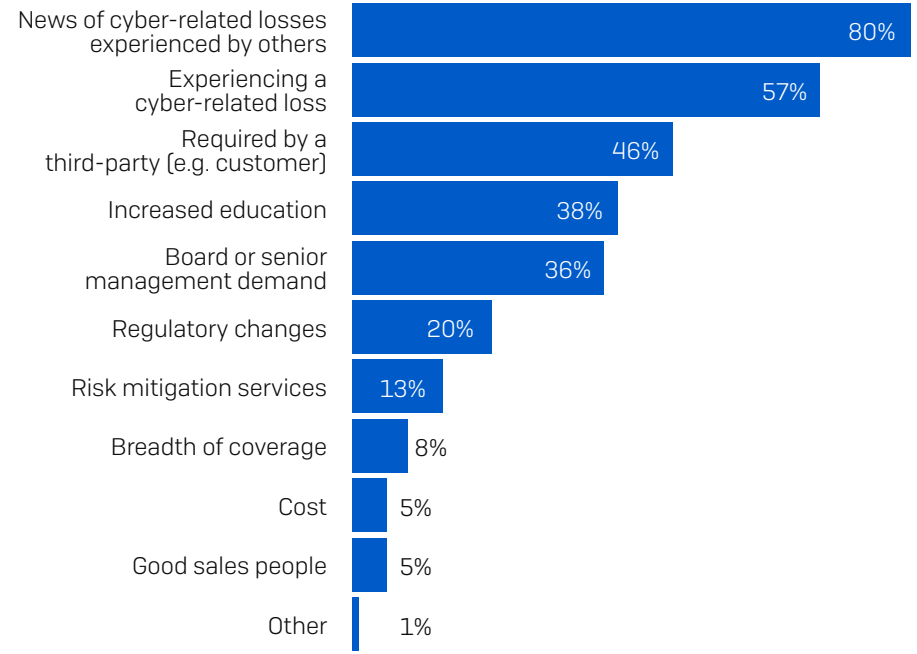
At the other end of the scale, manufacturing and production has both the lowest level of cyber insurance coverage (86%) and the lowest level of coverage against ransomware (75%).This is concerning as it leaves many organizations exposed to the high costs of ransomware recovery. In fact, the sector reported the highest average (mean) ransom payment of all sectors at an eye-watering US$2.04M.[3]

3 The State of Ransomware in Manufacturing and Production 2022

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%) 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

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**

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 vendors/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 vendors/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 vendors/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.

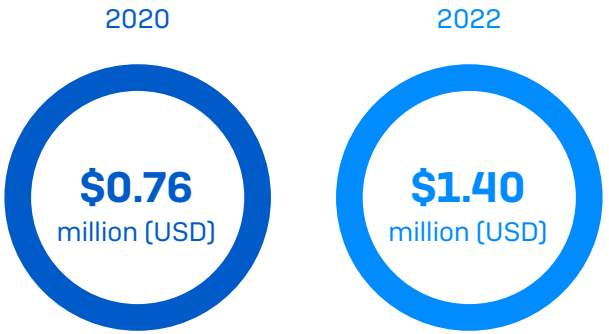
If your preferred supplier is not 'on-panel' with your insurance provider, you can request to use them. Early communication with your insurance provider is paramount so your preferred supplier's cyber insurance team can engage with the insurance provider for the appropriate approvals.

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 2021 was US$1.4M[4] - up from US$0.76M in 2019. Interestingly, this is a welcome drop from US$1.85M in 2020 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.

Ransomware costs are soaring



The high recovery costs are driven in large part by the growing complexity of many cyberattacks. Adversaries are increasingly combining automation and tools with hands-on hacking, leading to far more destructive attacks that are harder to recover from. We should also remember that a large part of the recovery costs is restoring IT systems to the level they should have been before the attack with advanced protection on all devices, not just returning to status quo.

4 The State of Ransomware 2022, Sophos

The cyber insurance market

Cyber insurance conditions are getting harder

Cyber insurance was for many years a 'soft' market, characterized by high capacity and low premiums. However, the market has now hardened for the first time in its 15-plus year history as a standalone policy, as insurers see their payouts rising faster than the income from premiums: the industry's loss ratio rose steadily from 2018, rising to 72.8% in 2020[5]. (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 have driven this hardening of the market:

- Cyberattacks have increased in both volume and complexity –
  - **57%** of IT managers say they have experienced an increase in volume of cyberattacks over the last year[6]
  - **59%** said they experienced an increase in the complexity of attacks over the last year[7]
- The costs to recover from a cyberattack have increased – as already mentioned, the average cost to remediate an attack in 2021 was a crippling US1.4M

The result of this market hardening is that it is now 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%** say the level of cybersecurity they need to qualify is now higher
- **47%** say policies are now more complex
- **40%** say fewer companies offer cyber insurance
- **37%** say the process takes longer
- **34%** say it is more expensive[8]

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

"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 creates 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 are 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.

Cyber insurance pays out

The good news is that cyber insurance invariably delivers 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.

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[9]

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

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

Good cybersecurity helps optimize your cyber insurance position

There is a direct relationship between cybersecurity and cyber insurance, and having strong cyber defenses in place can help in a number of ways:

1. Good cybersecurity makes it easier to get cyber insurance coverage

Providers are focusing increasingly on managing – and reducing – risk. Good 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 now often 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 Protection

The sooner you stop an attack, the better. Advanced endpoint security that automatically identifies and blocks threats is a core foundational layer of strong cyber defenses.

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

EDR and XDR are tools that enable analysts to detect and investigate potential compromise, enabling them to neutralize an advanced cyberattack before damage is done. As their names suggest, EDR works with data points from endpoint protection technology, while XDR takes data sources from both endpoint solutions and the wider wide security stack, including firewall, email, cloud, and mobile security solutions to provide greater visibility and insights.

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.

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

IT technology and solution provider, global reach

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. Good cybersecurity helps reduce premiums

Just as an alarm and window locks reduce your home insurance premiums, so 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

3. Good cybersecurity reduces the likelihood of making a claim – and higher premiums in the future

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 you reduce the likelihood that you'll need to call on your policy – and help keep your premiums down.

4. Good cybersecurity reduces the risks 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. Good cybersecurity can 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.

How Sophos can help

Optimize your cyber defenses

Sophos provides the advanced threat protection that is increasingly required to qualify for insurance coverage and keep premiums down – all backed by the threat intelligence and cybersecurity expertise of Sophos X-Ops.

- **Sophos Managed Detection and Response (MDR)** is the world's most trusted MDR service, securing over 15,000 organizations around the world. 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 minimizes the risk of a major cyber incident.
- **Sophos Extended Detection and Response (XDR)** enables you to hunt for threats across your endpoints and wider environment so you can identify and neutralize an attack before the damage is done.
- **Sophos Intercept X Endpoint** gives your endpoints and servers the world's best protection against ransomware and breaches:
  - **Strongest protection (by default).** Our advanced machine learning, anti-ransomware, and anti-exploit technology is enabled right out of the box
  - **Unrivalled ransomware protection.** Multiple layers of advanced behavior-based ransomware prevention technology stop even the most advanced attacks in their tracks
  - **Accelerated, automated threat response.** Threats are automatically stopped and cleaned up, and suspicious behavior is blocked to disrupt live hands-on-keyboards attacks
- **Sophos Firewall** secures your network against advanced attacks, keeping your data safe from malicious hackers and ransomware actors:
  - **Expose hidden risks**. Sophos Firewall gives you superior visibility into risky activity, suspicious traffic, and advanced threats help you regain control of your networks.
  - **Stop unknown threats.** Powerful next-gen protection technologies like deep learning and intrusion prevention keep your organization secure.
  - **Isolate infected systems.** Automatic threat response instantly identifies, and isolates compromised systems on your network to stop threats from spreading.

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.

Sophos customer and analyst validation

Sophos solutions are widely recognized by customers and the analyst community, including:

Sophos Managed Detection and Response (MDR)

- Top rated and most reviewed vendor on Gartner® Peer Insights™ for Managed Detection and Response Services
- Top performer in the 2022 MITRE Engenuity ATT&CK Evaluation for Managed Services

Sophos Extended Detection and Response (XDR)

- Recognized as the #1 overall leader in the Omdia Universe for Comprehensive Extended Detection and Response (XDR)

Sophos Endpoint

- Named a Leader in the 2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for the 13th consecutive time
- Named a 2021 Gartner® Customers' Choice™ for Endpoint Protection Platforms with a 4.8/5 customer rating on Gartner Peer Insights

Sophos Firewall

- Named a 2022 Gartner® Customers' Choice™ for Network Firewalls with a 4.7/5 rating on Gartner Peer Insights
- Recognized as a Strong Performer on the Forrester Wave

Test drive Sophos solutions at www.sophos.com/trial

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.

© Copyright 2023. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2023-04-21 (WP-NP)

SOPHOS