

WHITE PAPER

Best practices for securing your network from ransomware

Elevate your protection against ransomware and other network attacks.

SOPHOS

Ransomware remains a top cyberthreat

Ransomware remains a widespread threat with severe financial, operational, and human consequences. The 2025 Sophos Threat Report found that ransomware made up 70% of Sophos Incident Response cases for small businesses and more than 90% for midsized organizations, underscoring its dominance as one of today's most disruptive cyberthreats. The financial impact is severe. Our annual State of Ransomware survey revealed that the average cost of recovering from a ransomware attack is now $1.53 million, while the average ransom payment comes in at $1 million.[1] In addition to these costs, attacks cause serious operational disruption and human consequences, ranging from lost productivity to increased stress for IT and cybersecurity teams. These impacts highlight the scale of the threat and underscore the urgent need for stronger ransomware defenses and recovery strategies. Alongside endpoint protection, an optimized network security stack is one of the most effective defenses against ransomware. Use this guide to explore ransomware attack mechanics, prevention strategies, and how to optimize your network stack for maximum security.

90%

The percentage of cyberattacks targeting midsize businesses that were ransomware.

$1.0M

The average ransom payment made by organizations in 2025.

How ransomware attacks work

There are many types of threat actors and ransomware attacks. Some campaigns are highly targeted, while others are purely opportunistic. Adversaries — often referred to as cybercriminals or attackers — typically use a range of techniques to infiltrate organizations. These include identity-based techniques, such as using stolen or compromised credentials, as well as other methods of attack, including exploiting vulnerabilities, sending phishing emails, carrying out brute-force attacks and delivering drive-by downloads through compromised websites. Consider the quote below from a ransomware gang that attacked a Canadian education organization:

> "You had an old critical Log4j vulnerability not fixed on Horizon, this is how we were able to get in initially. It was a bulk scanning; not like we were targeting you intentionally."

1 The State of Ransomware 2025 - Sophos

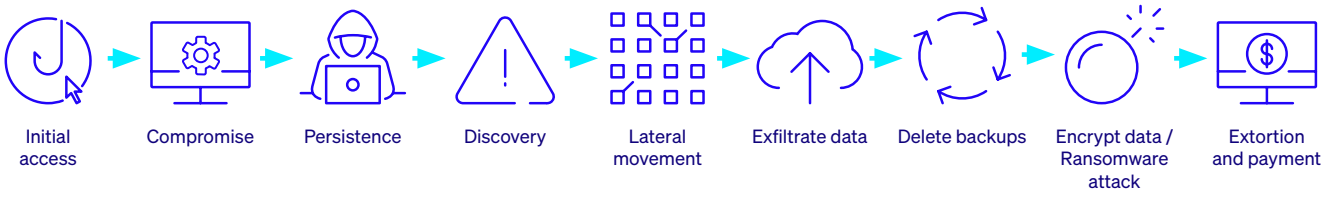
This quote also highlights adversaries' common exploitation of unpatched vulnerabilities, which was the leading root cause of ransomware attacks in 2025.[2]

Much of the increase in ransomware attacks over recent years can be attributed to the growing ransomware-as-a-service (RaaS) model. With RaaS, a cybercrime group builds ransomware and leases it out to other adversaries. This approach lowers the barrier to entry, making ransomware accessible to more threat actors than ever. Law enforcement agencies worldwide have tried to disrupt ransom-as-a-service providers. However, much like a hydra, when one group is disrupted, others pop up to take their place.

Once adversaries are inside their victims' environments, they often spend many days, weeks, or months exploring the network, escalating privileges, exfiltrating data, and installing malware. In 2025, the median dwell time for ransomware attacks was three days[3] — offering defenders a crucial window to detect and evict intruders before they strike.

However, when it comes to specific objectives, adversaries don't waste time. They move quickly to locate and compromise Active Directory servers, and that speed is increasing year on year. In 2025, attackers accelerated this phase by 70% compared to the previous year, reducing the median time to just 3.4 hours.[4] A compromised Active Directory server can provide them with elevated privileges and a way to deploy ransomware and other tools from "a trusted source." Another asset attackers actively seek out is the location of backups. If found, they will attempt to gain access and delete and disable the backup process just before starting the ransomware attack. If you cannot restore the data from a backup, you may be motivated to pay the ransom.

A typical ransomware attack might look like this:



Exploited vulnerabilities

The leading root cause of ransomware attacks in 2025.

3 days

The median dwell time for ransomware attacks.

2 The State of Ransomware 2025 - Sophos
3, 4 Nowhere, man: The 2026 Active Adversary Report - Sophos

“Remote Desktop Protocol” or “Ransomware Deployment Protocol?”

Our 2025 Active Adversary Report revealed that Remote Desktop Protocol (RDP) was involved in 91% of cyberattacks investigated by the Sophos Incident Response team.

RDP and desktop sharing tools, such as Virtual Network Computing (VNC), are helpful for remote system management. However, without proper safeguards, adversaries can exploit them to elevate privileges, steal credentials, move laterally, install backdoors, create fake accounts, and evade detection.

It is essential to prevent adversaries from using RDP for external and internal access, as well as for lateral movement. While some organizations have made progress to ensure RDP is not exposed externally, adversaries continue to use it to move laterally inside an organization.

91%

The percentage of cyberattacks where RDP was involved.

Identity is the cybersecurity frontline

Identity-based attacks now dominate the threat landscape. Our State of Identity Security 2026 report reveals that over seven in ten (71%) organizations experienced at least one identity-related breach over the last year.

Among organizations hit by ransomware in 2025, two-thirds (67%) said the ransomware incident was the same event as their most significant identity attack, establishing identity compromise, alongside exploited vulnerabilities, as a primary ransomware delivery mechanism.

Once identity is compromised, attackers can blend in as legitimate users, evade detection, and move laterally to deploy ransomware, steal data, or carry out business email compromise (BEC). Increasingly, the same pattern applies not only to human accounts, but also to the non-human and service identities that underpin cloud, SaaS, and automation.

71%

The percentage of organizations that experienced at least one identity-related breach over the last year.

Adversarial use of AI

Compounding the surge in identity-based attacks is the accelerating adoption of AI by threat actors. The telephone took 75 years to reach 100 million users. The cell phone did it in 16 years. The internet reached the same milestone in 7 years. ChatGPT reached 100 million users in just two months,[5] an adoption curve that underscores the unprecedented speed at which AI capabilities can now scale.

AI has materially shifted the threat landscape because it removes the traditional "cost and skill" barriers that used to slow attackers down. With readily available models, adversaries can now generate convincing phishing and social-engineering content at scale, rapidly tailor lures to specific targets, automate reconnaissance, and iterate on malware and exploit techniques far faster than most defenders can respond.

The result is a lower-friction attacker operating model with less delay and less oversight. In practice, this enables:

- Higher volume, more personalized, and more adaptive attack campaigns.
- Compressed detection and response windows.
- A greater impact from human error.

Defenders need to automate and modernize their operations to keep ahead of AI-enabled threats.

2 months

How quickly ChatGPT reached 100M users.

5 ChatGPT sets record for fastest-growing user base - analyst note - Reuters

Best practices to protect your network from ransomware

Now that we've taken a quick look at how ransomware attacks and threat actors operate, here are three best practices for strengthening your network security defenses:

1. Reduce exposure, i.e., your surface area of attack.
2. Inspect and protect network traffic as it enters your network.
3. Identify and stop any threats that manage to get on the network.

Reduce exposure, i.e., your surface area of attack

Any network infrastructure exposed to the public internet inherently becomes a potential target for attackers. Therefore, the first best practice is to minimize this exposure as much as possible. We recommend that you:

1. Ensure your network infrastructure is secure by design

Ensure any network infrastructure products exposed to the Internet, such as your firewall, are secure by design. Opt for a firewall that has been specifically designed and hardened to withstand attacks. Key features to look for include:

- No default internet access: The firewall should come with no out-of-the-box internet access and offer granular access controls for managing what is exposed.
- Hardened design: It should incorporate security mechanisms like multi-factor authentication (MFA) and containerization of any exposed services or portals, preventing attackers from exploiting potential vulnerabilities.
- Automated hotfixes: As mentioned above, automated hotfixes are crucial. To address emerging threats, the firewall must be capable of receiving updates rapidly, without requiring major firmware updates or scheduling downtime.
- Proactive monitoring: Vendor-side monitoring across the entire deployed customer base can help identify and respond to attacks much faster.

Key features to look for in a firewall:

- Built with Secure by Design in mind
- No out-of-the-box internet access
- Automatic patching and hotfixes
- Vendor-side monitoring access

SOPHOS

2. Consolidate your network infrastructure

Most organizations have a firewall protecting their network. Many also have a VPN concentrator, or additional network gateway products. Reduce this infrastructure as much as possible. Upgrade your firewall to one that integrates remote access, at least replacing any existing VPN concentrator you're using, but ideally enabling you to switch to zero-trust network access (ZTNA) — more on this to come.

3. Patch and keep firmware up to date

Unpatched vulnerabilities were the leading root cause of ransomware attacks in 2025.[6] It's essential to keep your firewall and other infrastructure firmware up to date. Check regularly (at least monthly) for firmware updates and schedule them to be applied during convenient times. Ensure your firewall vendor enables automated over-the-air hotfixes that don't require downtime for important security patches.

4. Minimize servers and applications exposed to the internet

If you're using remote desktop tools (RDP or VNC) or have any system on your network directly accessible via the internet for remote management, disable such access immediately. As mentioned, this type of exposure is one of the top ways attackers get into networks. Look at your firewall's NAT rules and make sure nothing is being exposed. Use ZTNA to protect your servers and admin systems and make them invisible to attackers while still providing secure remote access to those who need it.

5. Replace remote access VPN with ZTNA

Zero-trust network access (ZTNA) is the modern replacement for remote-access VPN. It eliminates the inherent trust and broad access that VPN provides, instead using the principles of zero trust — trust nothing, verify everything. ZTNA offers improved security, easier management, better visibility, and a better user experience compared to remote-access VPN.

ZTNA eliminates vulnerable VPN clients, utilizes MFA and device health to control access, and only provides access to specific network applications, effectively micro-segmenting your network. Look for a firewall that integrates ZTNA for a single gateway solution — managed from a single console, and ideally with a single agent on your user's device for ZTNA and endpoint protection.

Ideally get a ZTNA solution that integrates with your endpoint protection, a secure browser, and DNS protection for comprehensive workspace protection for your remote and hybrid workers. This way you can easily secure your workers, apps and data with a single solution, from a single vendor, with a single management console.

6 The State of Ransomware 2025

SOPHOS

6. Enable MFA and passkeys, and use strong passwords

MFA adds a critical layer of protection beyond a password, blocking adversaries who rely on stolen or purchased credentials. Enable MFA across all applications and services, and where available, use phish-resistant passkeys.

Passkeys replace passwords with device-bound cryptographic keys, verified through biometrics or a secure PIN, making accounts both harder to compromise and easier for users to access.

If MFA and passkeys are not available, ensure you use strong, unique passwords. Weak and predictable passwords can give attackers access to your network in seconds. Always create unique passwords with at least 12 characters, mixing uppercase and lowercase letters, numbers, and symbols Ju5t.LiKETh1s!. Alternatively, consider a passphrase made from unrelated or memorable words, such as PurpleMountainRace37!.

Most importantly, never reuse the same password across websites, logins, or devices — using unique credentials limits the damage if one is compromised.

Inspect and protect your network traffic as it enters your network

Another common attack vector popular with adversaries: gaining a foothold on your network through the regular web and email traffic that traverses your infrastructure. While web and email tools are essential for any business and cannot be simply shut down, you can ensure that this traffic is adequately inspected and protected. Here are some recommended best practices for securing your network traffic:

1. Inspect encrypted traffic

More than 90% of network traffic is encrypted. This is great for privacy, but a challenge for security, as typical threat detection can't see inside encrypted traffic streams. Attackers take advantage of this security blind spot. Most firewalls will buckle under the added load of trying to decrypt and inspect that 90% of encrypted traffic. Select a firewall specifically designed for today's heavily encrypted world, capable of intelligently determining which traffic streams need decryption and which do not. It should efficiently decrypt and inspect traffic without compromising overall network performance while still being able to identify encrypted threats. Or better yet — get a firewall that doesn't need to decrypt traffic to find encrypted threats.

90%

The amount of network traffic that is encrypted, which poses a challenge for security teams.

SOPHOS

2. Utilize IPS

Many systems on your network may have unpatched vulnerabilities. These could be Windows or Linux systems, IoT devices like cameras, industrial control systems, or anything that connects to your network — either wired or wireless. Every firewall includes technology to detect network attacks attempting to exploit vulnerabilities — this is called an intrusion prevention system or IPS. Unfortunately, many organizations simply don't use it. Make sure you're using IPS on all your network traffic flows — certainly those coming from the internet, but even internally to catch potential attackers that may already be on your network.

3. Make use of zero-day threat protection

Many attacks use bespoke malware embedded in files that are unknowingly downloaded from the web. These threats have never been seen before and are thus called "zero-day." You can't rely on traditional AV scanning to detect these zero-day threats, you need threat scanning that leverages AI or machine learning that has been trained on millions of past samples to identify new and emerging threats.

Make sure your firewall inspection includes zero-day analysis — ideally performed real-time in the cloud to offload this intensive processing from your firewall and to instantly benefit from global sharing of threat intelligence.

4. Implement robust email security measures and educate users on spotting phishing emails

We all know someone who has experienced unknowingly clicking on a malicious link in an email that appeared legitimate. While this will remain a popular attack vector for cybercriminals, there are effective protections and educational measures available to combat this challenge.

Look for an email security solution that can proactively filter malicious emails from users' inboxes. Even if some emails do get through, the solution should have the capability to retroactively remove them or rewrite the URLs to enable time-of-click checks. Seek an email security product that includes features to test users' ability to recognize phishing attacks and provides training on what to watch for.

Identify and stop any threats that manage to get on the network

Against the backdrop of a rapidly evolving threat landscape, the domination of identity-based threats and increasing adversarial use of AI, it is prudent to assume that at some point, an attacker will breach your network. At this point, identification and response time becomes critical, yet this is where most network security solutions fall short. You should look for solutions that can help you to:

1. Segment your network

If an attacker does somehow breach your network, one thing they will look to do is move around it. Micro-segmenting your network enables you to limit any movement and detect an attacker earlier. Make sure your network is segmented into multiple granular zones or VLANs that are connected via managed switches and access points, and through your firewall where IPS is inspecting this flow of traffic. Also use ZTNA for remote access, which effectively microsegments your applications as well.

2. Instantly identify adversaries across multiple vectors

When an attacker breaches your network, rapid detection is essential. With 88% of ransomware attacks occurring outside regular business hours,[7] you need a cybersecurity solution that operates around the clock to detect adversaries in real time and immediately share threat intelligence. This capability must go beyond merely alerting administrators — it should enable seamless communication across all security products to ensure a swift, coordinated response and containment. Choose a fully integrated suite of solutions, including firewalls, endpoints, switches, wireless, ZTNA, and email security. Also ensure your firewall integrates network detection and response (NDR). These tools should share threat intelligence both with your security team and with each other, empowering automated responses to neutralize attacks — even in the dead of night.

88%

The percentage of ransomware attacks that occur outside of regular business hours.

3. Automatically adapt and respond to active threats

When a threat is detected — whether by you, a security analyst, your endpoints, firewall, or any other part of your cybersecurity system — you need an immediate, coordinated response to contain and neutralize it. To achieve this, choose a firewall (and integrated security solutions) that can:

- **Automatically respond to active threats** without manual intervention, containing the attack as soon as it's discovered.
- **Block threats dynamically** without requiring new firewall rules or administrator input.
- **Work seamlessly with other security tools** like endpoints or ZTNA and a secure browser, to identify attacks and provide a coordinated response that prevents lateral movement and isolates the threat before it can move across the network.

7 Nowhere, man: The 2026 Active Adversary Report - Sophos

Layering security technologies to protect against ransomware

As the saying goes, "an ounce of prevention is worth a pound of cure." Stopping issues early is far easier than fixing the damage later. Protecting your organization from ransomware benefits from a layered IT security approach, where multiple technologies work together to create defense and visibility. Starting with a firewall and endpoint protection, organizations can add more layers as needs change, enhancing protection and visibility over time.

Examples include:

- **A network detection and response (NDR) product** can detect unprotected devices and identify adversaries moving laterally in your network. NDR provides visibility to internal network traffic that a firewall cannot see. Make sure your next firewall integrates NDR capabilities.

- **An extended detection and response (XDR) platform** can provide threat-hunting, investigation, and neutralization capabilities. It can also integrate with your other IT security solutions, providing visibility across all security controls from a single platform.

- **An MDR service** provides 24/7 monitoring and threat hunting delivered by experts specializing in detecting and responding to cyberattacks that technology solutions alone cannot prevent. Your MDR service should offer a full-scale incident response to disrupt, contain, and fully eliminate adversaries without additional costs. An MDR service must integrate with your existing cybersecurity tools to provide complete visibility across your entire environment. MDR provides the highest level of protection against advanced, human-led ransomware attacks.

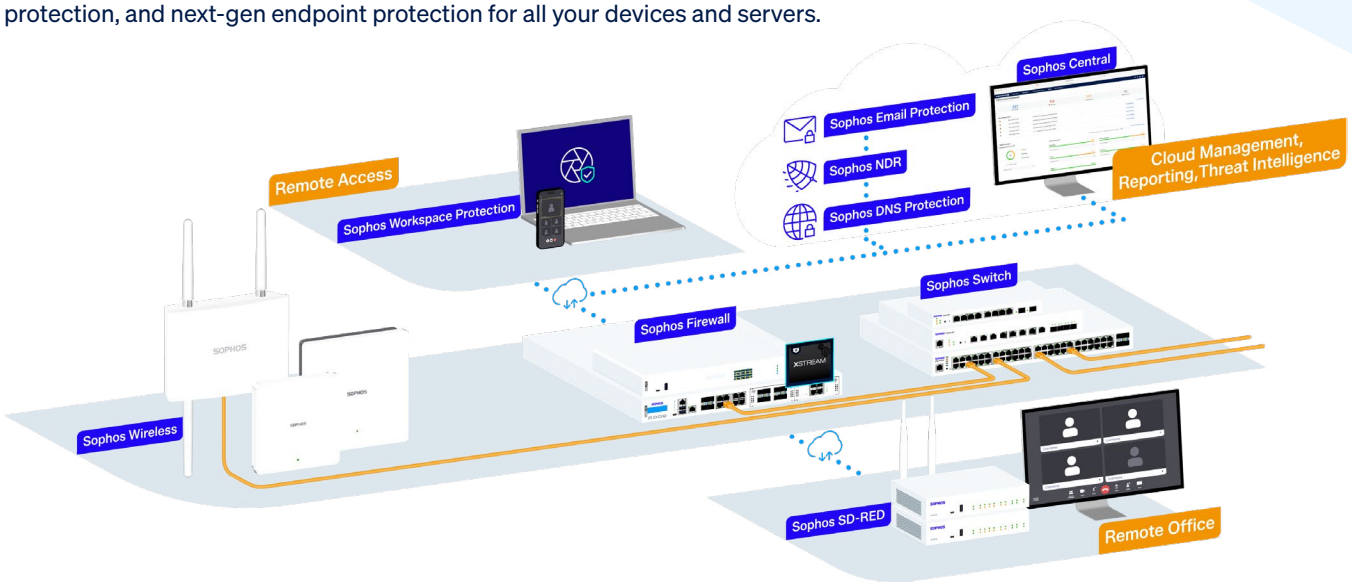
- **An attack surface management (EASM/IASM) or vulnerability management (VM) solution** can be used to identify and prioritize vulnerabilities. This allows you to identify and apply missing patches before adversaries can exploit them.

- **An identity threat detection and response (ITDR) solution** can be used to identify misconfigurations and weak policies in identity systems, as well as monitor the dark web for leaked or stolen credentials that adversaries could exploit.

- **Proactive security testing services**, such as penetration testing, evaluate controls and policies as an adversary would, helping to identify exposures in your environment, strengthen defenses, and enhance your resilience.

Sophos protects your network against ransomware

Sophos provides everything you need to secure your network from ransomware and other attacks. With Sophos, you get an integrated cybersecurity stack that includes firewalls, ZTNA, switches, wireless, remote-edge devices, messaging protection, and next-gen endpoint protection for all your devices and servers.



The best part is that it's all managed from a single cloud management platform — Sophos Central — which brings together threat insights from our solutions and expert analysts, enabling automatic threat response.

This level of integration and synchronization is unique to Sophos - you won't find it anywhere else, and it is arguably the most critical component of any active attack response.

Synchronized security in action

When a compromised host is detected, Sophos Firewall immediately isolates it while your healthy Sophos-managed endpoints automatically ignore traffic from that device. In addition, Sophos ZTNA and Sophos Protected Browser will prevent any compromised device from connecting to your applications and data. An active threat is immediately and automatically isolated on the network, with nowhere to go.

Sophos network security at a glance

Sophos Firewall

Sophos Firewall and XGS Series appliances help you protect your network from ransomware by implementing best practices out of the box:

- **Secure by design:** We've not only invested heavily in ensuring Sophos Firewall is the most secure firewall on the market, but we continuously work to make it the most difficult target for hackers, while helping keep your network and organization safe from future attacks through proactive monitoring. Sophos Firewall is unique in the industry for providing automatic over-the-air hotfixes for security patches that don't require scheduling any downtime.

- **Integrated ZTNA:** Sophos Firewall includes a built-in ZTNA gateway, enabling you to easily switch to zero-trust from old-school VPN without having to deploy anything extra. Plus, ZTNA is managed from the same cloud console as your firewall, making it easy to secure and segment your applications and remote access.

- **AI-powered zero-day threat protection:** Sophos Firewall integrates advanced AI technologies to identify bespoke ransomware attacks and stop them before they get on the network. We use a combination of advanced AI and machine learning that has been trained on millions of samples as well as real-time sandboxing to identify previously unseen threats.

- **Integrated NDR:** Sophos Firewall integrates network detection and response capabilities — an industry first. And the best part is, all the heavy AI analysis is done in the cloud, rather than on your firewall, so your active attacker detections improve without impacting your performance.

- **Active Threat Response:** Sophos Firewall can instantly identify an active adversary on the network based on a variety of threat intelligence sources and coordinate a synchronized security response to automatically isolate an active threat before it can become a real problem.

Sophos Workspace Protection with ZTNA

Sophos Workspace Protection integrates Sophos ZTNA, Sophos Protected Browser, Sophos DNS Protection for endpoints, and Sophos Email Monitoring System to protect your workers, apps, and data. It enables you to easily provide secure access for those that need it, anywhere they go, while protecting your apps and data from the outside world. It effectively micro-segments your applications, makes them invisible to the internet, and provides a hardened and secure workspace. It's a much more secure and transparent solution for remote and hybrid workers than traditional remote-access VPN.

- **Micro-segment and secure your applications:** Sophos ZTNA provides the ultimate micro-segmentation so you can deliver secure application access whether your applications are hosted on premises, in a data center, or in your public cloud infrastructure, making them invisible to the outside world.

- **Stop ransomware and threats:** The possibility for ransomware and other threats to propagate across the network from a compromised user device is no longer a concern with ZTNA. Users and devices only have explicit policy-based access to specific applications. This eliminates the implied trust and broad network access that is one of the key challenges with VPN.

- **Block access from compromised devices:** Sophos ZTNA and Sophos Protected Browser enables your remote workers to securely and seamlessly access the applications and data they need. If a user's device becomes compromised, their application access will be automatically cut off to prevent lateral movement until it's cleaned up.

Sophos Switches and Access Points

Sophos switches and access points are tightly integrated with Sophos Firewall and the rest of the Sophos cybersecurity platform, providing automated threat response and single-console management:

- **Active Threat Response:** Sophos switches and access points also support Active Threat Response to stop active adversaries dead in their tracks. A compromised device can be instantly blocked at the switch or access point to prevent lateral movement, even on the same LAN segment.

- **Single console management:** Sophos switches and access points are all managed from Sophos Central along with your firewalls, ZTNA, and other Sophos products to provide optimal visibility and ease of management.

Sophos Email

Sophos Email is a comprehensive email security solution that defends against phishing and business email compromise (BEC) attacks, securing your inboxes:

- **Phishing and BEC protection:** Sophos Email uses natural language processing (NLP) and behavioral analysis to detect phishing attempts and remove malicious messages. It further secures inboxes by proactively scanning for suspicious sender behavior, header anomalies, and spoofing attempts using SPF, DKIM, and DMARC validation.

- **Time-of-Click URL protection and malware scanning:** Multi-layered malware and malicious URL analysis protect users from email-based threats. Time-of-click protection validates URLs when they are clicked, rather than when the email is received, ensuring protection against evolving threats. Additionally, malicious payloads embedded in attachments or links are detected and blocked before they can cause harm.

- **Security awareness and training:** Sophos Phish Threat is a phishing simulation and cybersecurity awareness training platform that helps to identify at-risk users and increase security awareness through phishing simulations and actionable reporting metrics.



Conclusion

Ransomware continues to evolve and remains effective as a forcing function to encourage targeted organizations to pay a ransom. Your goal is to block adversaries from entering your organization and detect and eject them quickly if they do. Ensure you follow the network security best practices outlined in this report, continue end user education, and remain vigilant for threats and adversaries in your environment.

A layered approach to cybersecurity, with 24/7 detection and response, gives your organization the best chance to protect against ransomware and the latest threats.

To explore how Sophos can help you optimize your ransomware defenses, speak to an adviser or visit www.sophos.com.

SOPHOS

Ready to assess your cybersecurity program?

Speak to a Sophos expert today.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

© Copyright 2026. 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.

2026-04-24 WP-EN (TA)