WHITE PAPER

Endpoint protection best practices to block ransomware

Practical guidance on configuring your endpoint security solution to provide optimum protection.

SOPHOS

Introduction

Ransomware remains a widespread threat with severe financial, operational, and human consequences. In 2024, ransomware accounted for 70% of Sophos Incident Response cases among small businesses and over 90% among midsized organizations, underscoring its dominance as today's most disruptive cyberthreat.[1] 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 is $1 million.[2] 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 the return on investment (ROI) of investing in prevention.

Robust, well-configured endpoint protection remains one of the most powerful defenses against ransomware and its escalating consequences. This paper explores the mechanics of ransomware attacks, strategies to prevent them, and best practices for optimizing your endpoint protection to ensure maximum security.

90%

The percentage of cyberattacks targeting midsize businesses that were ransomware.

70%

The percentage of cyberattacks targeting small businesses that were ransomware.

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 exploiting vulnerabilities, leveraging stolen or compromised credentials, sending malicious emails and phishing, conducting 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:

1 The Sophos Annual Threat Report: Cybercrime on Main Street 2025
2 The State of Ransomware 2025 - Sophos

> "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."

This quote also highlights adversaries' common exploitation of unpatched vulnerabilities, which was the leading root cause of ransomware attacks in 2025.[3]

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. Throughout 2024, 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.[4]

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 2024, the median dwell time for ransomware attacks was four days[5] — 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 often race to discover and compromise Active Directory servers, generally within 11 hours of a breach.[6] 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 the backups just before starting the ransomware attack. If you cannot restore the data from a backup, you may be motivated to pay the ransom.

?

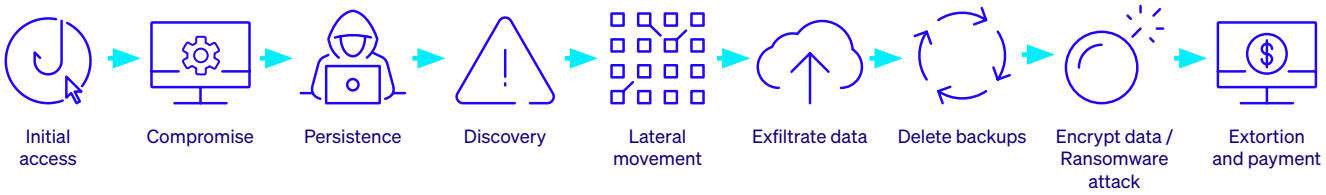
?

4 days

The median dwell time for ransomware attacks

3 The State of Ransomware 2025 - Sophos
4 The Sophos Annual Threat Report: Cybercrime on Main Street 2025
5 It takes two: The 2025 Sophos Active Adversary Report
6 It takes two: The 2025 Sophos Active Adversary Report

A typical ransomware attack might look like this:



It's important to note that adversaries strategically target organizations at times when they're less likely to be detected. 88% of ransomware attacks remediated by Sophos Incident Responders occur outside of regular working hours in the victim's time zone (i.e., outside 8 a.m. to 6 p.m. Monday to Friday)[7] to exploit potentially reduced IT monitoring.

Remote ransomware

According to Microsoft's 2024 Digital Defense Report, remote encryption was present in 70% of successful ransomware attacks, with 92% traced back to unmanaged devices within victim networks.

Also known as remote ransomware, remote encryption attacks occur when a compromised endpoint is used to encrypt data on other devices on the same network.

A key factor driving the increasingly widespread use of this approach is its scalability: One unmanaged or under-protected endpoint can expose the entire organization to malicious remote encryption, even if other devices have advanced security solutions installed.

Another factor driving remote ransomware is that protection technology has not kept pace with the evolving threat. While endpoint protection solutions are typically effective at detecting ransomware executed locally on the victim's device, many solutions lack robust protection against remote ransomware, thereby increasing the adversary's chances of success.

Organizations need to be acutely aware of the threat of remote ransomware attacks, as not all endpoint security solutions can effectively protect against them.

[7] It takes two: The 2025 Sophos Active Adversary Report

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

Remote Desktop Protocol (RDP) was involved in 91% of cyberattacks investigated by the Sophos incident response team in 2024.[8]

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 organizations have made progress to ensure RDP is not exposed externally, adversaries continue to use it to move laterally inside an organization.

Adversarial use of AI

Adversaries have begun to utilize generative AI for creating spam and phishing emails. Large language models (LLMs), such as ChatGPT, can be used to create grammatically correct content in a format that varies from target to target, thereby defeating content filters that identify signatures. This convincing AI-generated content helps them trick a user into clicking on a link, taking them to a malicious website to capture their credentials, which the adversary can then use to access your environment in the guise of a legitimate user.

8 It takes two: The 2025 Sophos Active Adversary Report

Best IT practices to protect against ransomware

Staying secure against ransomware and other threats requires more than having the latest security tools deployed. Good IT security practices, including regular employee training, are essential. While not an exhaustive list, be sure to follow these best practices.

1. Patch and keep firmware up to date

Exploiting unpatched vulnerabilities was the leading root cause of ransomware attacks in 2025.[10] As Sophos CEO Joe Levy recently pointed out, obsolete and unpatched hardware and software constitute an ever-growing source of security vulnerabilities, a phenomenon he referred to as "digital detritus."[11]

Adversaries exploit security vulnerabilities in popular applications and legacy or end-of-support operating systems. The earlier you patch your endpoints, servers, mobile devices, and applications, the fewer holes adversaries can exploit.

Did you know?

While all successful ransomware attacks have negative outcomes, those that start by exploiting unpatched vulnerabilities are particularly brutal. In 2024, organizations hit by ransomware attacks that began in this way reported 4x higher recovery costs and longer recovery times compared to attacks starting with compromised credentials.8

2. Enable multi-factor authentication (MFA) and passkeys

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.

9 Unpatched Vulnerabilities: The Most Brutal Ransomware Attack Vector - Sophos
10 The State of Ransomware 2025 - Sophos
11 Digital Detritus: The engine of Pacific Rim and a call to the industry for action - Sophos

3. Use strong passwords

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.

4. Regulate internal and external network access

Don't leave network ports exposed. Lock down your organization's RDP access and other remote management protocols. Ensure remote users connect to applications, services, and other organizational resources via a Zero-Trust Network Access (ZTNA) solution.

5. Monitor administrator rights

Constantly review local and domain admin rights. Know who has them and remove those who don't need them. Don't stay logged in as an administrator any longer than necessary.

6. Regularly back up data in multiple locations and routinely practice restoration procedures.

In our State of Ransomware 2025 survey, 54% of IT managers whose data was encrypted were able to restore it using backups. Regularly back up your data to multiple locations, using MFA to protect cloud backups. Practice restoration from backups to ensure smooth recovery. Monitor for suspicious activity to secure backups from potential threats.

Keep in mind that attackers routinely search for and delete backups as part of their attack chain, so monitoring for suspicious activity is essential to keep recovery options safe.

7. Remove unnecessary applications

The exploitation of legitimate applications, known as "living off the land" (LoLBin abuse), surged by 126% in 2024,[12] as adversaries increasingly used trusted Microsoft binaries to blend in and evade detection, making it significantly harder for defenders to distinguish between malicious and legitimate activity. If a user does not need an application to perform their job, carefully consider whether it should be installed. If in doubt, leave it out.

8. Find unprotected devices on your network

In 40% of cases investigated by Sophos in 2024, unprotected systems were discovered.[13] Adversaries deliberately hunt for unprotected endpoints, using them to move undetected and launch remote ransomware attacks that can quickly compromise an entire environment.

12 It takes two: The 2025 Sophos Active Adversary Report
13 It takes two: The 2025 Sophos Active Adversary Report

Best practices for your endpoint protection

An effective defense against ransomware starts with a modern endpoint protection, endpoint detection and response (EDR), or extended detection and response (XDR) solution that includes advanced prevention technologies and threat investigation and remediation capabilities. However, even the best technology can be undermined by misconfiguration.

Security tool misconfiguration is considered the top cybersecurity risk to organizations.[14] Poorly configured policy settings, exclusions, and other factors can compromise your security posture. Ensure your endpoint protection is configured correctly to provide maximum protection.

We therefore recommend you follow these best practices to protect your endpoint devices from ransomware:

1. Turn on all recommended policies and features

It sounds obvious, but this is a surefire way to get the best protection from your endpoint security solution. However, not all solutions have recommended protection settings enabled by default. Policies and settings are designed to stop specific threats and regularly checking that all protection options are enabled ensures your endpoints are protected against current and emerging ransomware. Ensure that features detecting fileless attack techniques and behavioral technologies are enabled. Additionally, we recommend that you:

a. **Enable tamper protection**

This prevents the unauthorized modification or removal of the endpoint protection software. One of the first actions adversaries take after they access a system is to attempt to disable or remove endpoint protection.

b. **Enable forensic logging (ideally to the cloud)**

14 Addressing the cybersecurity skills shortage in SMBs - Sophos

SOPHOS

If you do get compromised, you will want to know what happened so that you can prevent it from happening again. However, adversaries often wipe system logs to cover their tracks, removing forensic evidence that would assist in understanding the attack. You may also lose access to your device. Having a record of activity in the cloud ensures you can retain access to critical information.

c. **Ensure endpoint protection content and product updates are enabled**

To keep pace with the ever-evolving threat landscape and protect against emerging threats, it's vitally important to regularly update security products with the latest protection rules and content. Disabling product and content updates will degrade your protection over time.

d. **Ensure ransomware protection, especially remote ransomware protection, is enabled on all endpoints.**

Some solutions don't include protection from remote ransomware attacks or ship with it disabled by default, leaving a single compromised device free to encrypt data across your network.

2. Regularly review your exclusions

Exclusions prevent trustworthy directories and file types from being scanned for malware when files are created, updated, etc. They are sometimes used to reduce system delays and minimize the risk of false-positive security alerts.

Over time, a growing list of exclusions creates security holes that adversaries can exploit. Malware that manages to make its way into excluded directories — perhaps accidentally moved by a user — still poses a potential threat.

Regularly review your list of exclusions within your policy settings and remove as many as you can. For any you can't remove, ensure they're as specific as possible. For example, rather than excluding a database's directory or drive, only exclude specific files with their full path.

It is essential to note that any executable from an excluded directory should still be subjected to runtime execution and behavioral scans when it is executed.

3. Enable MFA and passkeys everywhere

Enabling MFA and, where supported, phish-resistant passkeys ensure secure access to your chosen platform for managing your endpoint protection and other critical security controls. This prevents adversaries from changing settings or disabling protection to expose endpoints and servers. Apply MFA and passkeys consistently across all applications that support them, including high-value targets such as backup and recovery systems, to close off common attack paths.

4. Maintain good IT practices and hygiene

Regularly evaluating your IT hygiene ensures that your endpoints and installed software run at peak efficiency. This mitigates your cybersecurity risk and can save you time when you remediate future incidents.

Implementing a program to maintain IT hygiene is especially critical for safeguarding against ransomware attacks and other cybersecurity threats. For example, ensure RDP runs only where you need it and expect it to, regularly check for configuration issues, monitor device performance, and remove unwanted or unnecessary programs.

NOTE: Use application control to block remote access tools and other programs on devices that do not need them. This stops them running if an attacker downloads them onto a compromised device.

An IT hygiene check may highlight the need to update software applications. It's also a surefire way to ensure your data is backed up regularly.

5. Proactively hunt for active adversaries across your environment

Sophisticated active adversaries use advanced techniques to stealthily and deliberately evade even the strongest preventive security controls.

In today's threat landscape, adversaries are more cunning than ever, often deploying legitimate tools and stolen credentials to avoid detection. Proactively hunting for advanced threats and active adversaries is crucial for identifying and stopping these living-off-the-land attacks. Once identified, you also need to be able to take swift action to stop the attack and eject the adversary from the environment.

Technologies such as endpoint detection and response (EDR) and extended detection and response (XDR) offer threat hunting, investigation, and neutralization capabilities to support your in-house security team. However, as adversaries often start their attacks outside of office hours, your security team may not be around to stop them. Many organizations struggle to maintain round-the-clock coverage to defend against advanced ransomware attacks — that's why managed detection and response (MDR) services are essential for many organizations.

Layering security technologies to protect against ransomware

The saying "Prevention is better than cure" highlights that stopping an issue early is 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 endpoint protection, organizations can add more layers as needs change, enhancing protection and visibility over time.

Examples include:

- **A firewall** to identify and block suspicious network traffic and stop threats from entering your environment. A firewall has visibility on network traffic entering and leaving your organization. It does not have visibility of network traffic inside the environment.

- **A network detection and response (NDR)** product can detect unprotected devices and identify adversaries moving laterally in your network. NDR provides visibility into internal network traffic that a firewall cannot see, potentially revealing unprotected devices.

- **An 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 against ransomware

Sophos Endpoint is the industry's most sophisticated AI-powered endpoint security solution, delivering unparalleled defense against advanced cyberattacks.

A prevention-first approach stops the broadest range of threats quickly before they impact your endpoints and servers. Deep learning AI models protect against known and never-before-seen attacks. Control features reduce your threat surface, while behavioral analysis, anti-ransomware, anti-exploitation, and other advanced technologies stop threats fast before they escalate.

- Industry-leading CryptoGuard technology provides the strongest zero-touch defense against both local and remote ransomware. It detects encryption attempts, regardless of the source. Maliciously encrypted files are automatically rolled back to their unencrypted states, minimizing the impact to your business.

- Over 60 proprietary and pre-configured anti-exploitation mitigations identify and block the techniques adversaries use in their attacks.

- Industry-first, dynamic defenses automate protection by adapting in real time to an attack. Adaptive Attack Protection dynamically enables heightened defenses when a hands-on-keyboard attack is detected, disrupting and containing the attack and buying you valuable time to respond.

Sophos Endpoint is easy to set up and manage. Sophos Endpoint comes with our recommended protection technologies enabled by default, immediately providing you with the strongest protection from the moment of installation. There's no need for complicated configuration or tuning. However, if you need it, you also have the option for more granular control.

Sophos Central is an AI-native, open platform for managing Sophos Endpoint and all your other Sophos products and services. Sophos Central users must authenticate with MFA using a TOTP authenticator app (like Google Authenticator or Microsoft Authenticator) or a passkey.

Poorly configured policy settings, exclusions, and other factors can compromise your security posture. The account health check feature, in Sophos Central, identifies security posture drift and high-risk misconfigurations and enables you to remediate issues with a single click.

Sophos Endpoint Detection and Response (EDR)

Sophos EDR includes Sophos Endpoint and extends it with detection and response tools. Designed for security analysts and IT generalists, Sophos EDR enables you to respond to evasive threats with speed and precision, making it the ideal solution for organizations looking to up-level their endpoint defenses.

- Prioritized threat detections score and highlight suspicious activity requiring immediate attention.
- Analyze activity in real time with access to rich on-device data and telemetry from the Sophos data lake, including historical activity, even when devices are offline.
- Outcome-focused AI tools streamline investigation and response.

- AI Search uses natural language to accelerate day-to-day tasks and lower the technology barrier to security operations.
- AI Case Summary provides an easy-to-understand overview of detections, helping you make smart decisions, fast.
- AI Command Analysis analyzes complex command-line arguments to uncover their intent and impact, providing explanations in plain language.

Sophos EDR also includes powerful tools that enable you to conduct extensive IT operational tasks quickly and easily. You get direct, secure, and audited shell access to your endpoints and servers, allowing you to investigate and remediate potential issues directly from your Sophos console. Remotely access devices to install and uninstall software, run scripts and programs, edit configuration files, and more.

Sophos Extended Detection and Response (XDR)

Sophos XDR builds upon the capabilities of Sophos EDR to provide full visibility of threats across your entire IT environment. It is an open, AI native, XDR platform that enables you to detect, investigate, and respond to multi-stage, multi-vector threats across all key attack vectors in your environment. It's a holistic, actionable view of your organization's entire cybersecurity posture. Leveraging AI-powered SecOps tools, Sophos XDR collects and correlates rich telemetry from your existing security tools - including non-Sophos solutions.

- Automatically generates and prioritizes detections based on risk, providing full context to easily identify suspicious activity that needs immediate attention.
- An extensive ecosystem of integrations with endpoint, firewall, network, cloud, identity, email, backup, and productivity solutions - including Microsoft 365 and Google Workspace – all included automatically with Sophos XDR.
- The bi-directional integration with Microsoft 365 lets you block users, terminate sessions, disable inbox rules, and more, directly from the Sophos XDR platform.

- Automated actions, such as process termination, ransomware rollback, and network isolation, help to contain threats quickly and save you valuable time.

- View the full attack chain and map it to the MITRE ATT&CK framework, enabling you to easily identify gaps in your defenses.

- AI tools (AI Search, AI Case Summary, AI Command Analysis) included with Sophos XDR empower your security analysts and help streamline investigations by providing real-time insights, contextualizing threat data, and offering natural language-driven recommendations.

The Sophos AI Assistant makes it easy for users of all skill levels to get the information they need to progress threat investigations. Conduct an extensive range of SecOps tasks. Analyze suspicious commands, identify impacted entities, enrich data with threat intelligence, create detailed reports, and more. Ask questions using everyday language or pre-defined prompts provided by Sophos' threat experts. Benefit from natural language summaries and recommended next steps. This technology was designed in partnership with Sophos' frontline security analysts, enabling your in-house team to benefit from real-world workflows and the experience of Sophos MDR experts.

Sophos MDR: 24/7 managed detection and response

Sophos MDR is a 24/7 managed security service, delivered by highly skilled experts that defend against novel threats and advanced active adversaries on your behalf. The Sophos MDR service delivers the ultimate ransomware protection.

With the Sophos MDR Complete service tier, you benefit from unlimited full-scale incident response with no caps or extra fees. Our experts can execute an extensive set of response actions on your behalf to remotely disrupt, contain, and fully eliminate the adversary.

Like Sophos XDR, Sophos MDR integrates and gathers telemetry from all Sophos products and integrates with the same extensive range of non-Sophos security products for increased visibility and protection across your environment.

Sophos Incident Response Services Retainer: An incident response team on standby

Having an incident response team in place before adversaries strike saves time, reduces costs, and mitigates the impact in the event of a breach (e.g., adversaries deploying ransomware).

The Sophos Incident Response Services Retainer is an annual subscription to an on-demand team of elite incident response experts that will rapidly deploy into your environment to disrupt, contain, and fully eliminate active adversaries. It also includes critical incident preparedness resources to improve your organization's security posture and reduce the likelihood of a breach.

Sophos Managed Risk: Vulnerability and internal/ external attack surface management service

Unpatched vulnerabilities are the leading root cause of ransomware attacks, making it crucial to identify, investigate, and prioritize any high-risk exposures across your environment before they become a problem. Sophos Managed Risk, powered by industry-leading Tenable technology, helps you do just that.

With Sophos Managed Risk, our experienced analysts identify high-priority cybersecurity vulnerabilities and potential attack vectors in your environment so actions can be taken to prevent attacks before they disrupt your business.

Conclusion

Ransomware continues to evolve and remains effective as a forcing function to encourage victim 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 IT and endpoint security best practices, continue end-user education, and remain vigilant for threats and adversaries in your environment. A prevention-first and 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.

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

2025-10-13 EN CRE-3415 (DD)