SOPHOS

Endpoint protection best practices to block ransomware

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

A Sophos Whitepaper. October 2024

Introduction

Ransomware ranks among the most significant cyberthreats, with far-reaching and often catastrophic consequences. 59% of respondents in the Sophos State of Ransomware 2024 survey reported that their organization was hit by ransomware in the previous year. In 70% of these incidents, data was encrypted by the attacker.

Overall, the average cost to remediate a ransomware attack was a business-crippling $2.73 million – a 50% increase from the year before. Furthermore, over one-third (34%) of organizations took over a month to recover from attacks, underscoring the increasing complexity and severity of these incidents.

The extended recovery timelines highlight the need for more comprehensive response efforts. This growing complexity also places considerable strain on internal security teams, with 95% of organizations reporting difficulties delivering essential security operations tasks[1].

These findings emphasize the urgent need for organizations to strengthen their ransomware defenses and recovery strategies, as the rising costs, prolonged recovery times, and increasing strain on security teams make ransomware a formidable threat to business continuity. A well-configured endpoint protection solution is one of the most effective defenses against ransomware. This whitepaper delves into the mechanics of ransomware attacks, strategies to prevent them, and best practices for optimizing your endpoint protection to ensure maximum security.

How ransomware attacks are deployed

There are many threat actors and many types of ransomware attacks. Some are highly targeted, while others are opportunistic. Often, adversaries (sometimes called cybercriminals or attackers) scan networks for weaknesses or vulnerabilities that will provide them access to your environment. 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."*

This quote also highlights adversaries' common exploitation of unpatched vulnerabilities, which was the the leading root cause of ransomware attacks in 2024.[2]

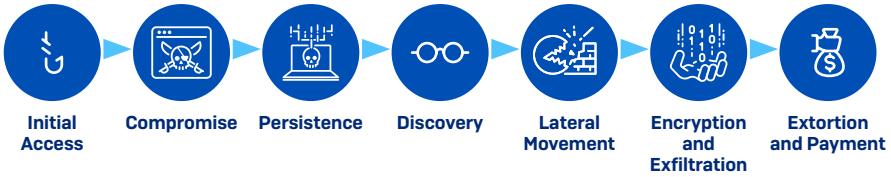
Much of the increase in ransomware attacks over recent years can be attributed to the growing ransomware-as-a-service (RaaS) model. With RaaS, a cybercrime group builds ransomware and leases it out to other adversaries. This approach lowers the barrier to entry, making ransomware accessible to more threat actors than ever.

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 2023, the average dwell time in ransomware attacks was six days[3]. This gives defenders a window to identify and stop intruders before an attack.

1 Addressing the cybersecurity skills shortage in SMBs - Sophos

2 The State of Ransomware 2024 - Sophos
3 It's Oh So Quiet (?): The Sophos Active Adversary Report for 1H 2024 - Sophos

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. Ransomware attacks often occur on Fridays or Saturdays to exploit potentially reduced IT monitoring over the weekend.

Analysis by Sophos X-Ops incident responders shows that 43% of ransomware attacks in 2023 were timed for these days, and 91% of attacks began outside regular business hours (8am to 6pm Monday to Friday) in the victim's time zone, taking advantage of periods when the likelihood for detection and response was lower[4].

Remote ransomware

Microsoft's 2023 Digital Defense Report states that around 60% of human-operated ransomware attacks involve remote encryption. Also known as remote ransomware, remote encryption occurs 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.

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

Remote Desktop Protocol or ransomware deployment protocol?

Remote Desktop Protocol (RDP) played a part in 90% of cyberattacks investigated by the Sophos incident response team in 2023, up from 83% the year before[5].

RDP and desktop sharing tools like Virtual Network Computing (VNC) are useful for remote system management, but without proper safeguards, ransomware actors 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 access, internal access, and lateral movement. While organizations have made progress in ensuring RDP is not exposed externally, adversaries widely use it to move laterally inside an organization.

4 Stopping Active Adversaries: Lessons From The Cyber Frontline - Sophos

5 It's Oh So Quiet (?): The Sophos Active Adversary Report for 1H 2024 - Sophos

Best IT practices to protect against ransomware

Staying secure against ransomware and other threats requires more than having the latest security solutions. Good IT security practices, including regular employee training, are essential. While not a complete list, make sure you're following these best practices.

1. Patch early and often

Did you know?
While all ransomware attacks have negative outcomes, those that start by exploiting unpatched vulnerabilities are particularly brutal. Organizations hit by attacks that began in this way reported 4x higher recovery costs and longer recovery times compared to those starting with compromised credentials.

Exploiting unpatched vulnerabilities was the leading root cause of ransomware attacks in 2024[6]. Malware and adversaries exploit security vulnerabilities in popular applications. The earlier you patch your endpoints, servers, mobile devices, and applications, the fewer holes adversaries can exploit.[7]

2. Use strong passwords

It sounds trivial, but it isn't. A weak and predictable password can give hackers access to your network in seconds. We recommend making passwords unique, consisting of at least 12 characters, using a mix of uppercase and lowercase letters, and adding a random punctuation Ju5t.LiKETh1s!

3. Enable multi-factor authentication (MFA)

MFA provides an additional layer of security after the first factor, which is often a password. Enabling MFA across all applications and services that support it is critical. Adversaries often purchase valid credentials from the dark web or actively attempt to obtain credentials once they are inside your environment.

MFA places an additional roadblock for an adversary and stops them from authenticating as a valid user without challenge. Finally, where applications support them, use phish-resistant passkeys.

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 use a Zero-Trust Network Access (ZTNA) solution to access applications, services, and other organizational resources.

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 2024 survey, 68% of IT managers whose data was encrypted could 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.

7. Remove unnecessary applications

Adversaries use commonly installed applications for malicious purposes. This approach, called living-off-the-land, makes it harder to differentiate legitimate usage from malicious 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

Adversaries seek out devices without endpoint protection to remain undetected and unchallenged in your environment. These unprotected devices can be used in remote ransomware attacks.

6 The State of Ransomware of 2024 - Sophos
7 Unpatched Vulnerabilities: The Most Brutal Ransomware Attack Vector - Sophos

Best practices for your endpoint protection

An effective method for protecting against ransomware attacks is an endpoint protection, endpoint detection and response (EDR), or extended detection and response (XDR) solution that includes advanced prevention technologies and threat-hunting capabilities.

Security tool misconfiguration is considered the top cybersecurity risk to organizations[8]. Poorly configured policy settings, exclusions, and other factors can compromise 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.

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 features that detect 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 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)

If you do get compromised, you will want to know what happened, to enable you to prevent recurrence. 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 to protect against emerging threats, it's vitally important to regularly update security products with new data. Disabling product and content updates will degrade your protection over time.

2. Regularly review your exclusions

Exclusions prevent trustworthy directories and file types from being scanned for malware. 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 could take advantage of. Malware that manages to make its way into excluded directories – perhaps accidentally moved by a user – may succeed.

Regularly check 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. This prevents malware from bypassing your security and running from the same folder.

3. Enable MFA for your security console

Doing so ensures secure access to the platform that manages your endpoint protection and other security controls. This stops adversaries from deliberately changing your settings or disabling/removing protection, which can leave your endpoints and servers vulnerable to attack.

4. Maintain good IT practices and hygiene

Regularly evaluating your IT hygiene ensures your endpoints and the software installed 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, regularly check for configuration issues, monitor device performance, and remove unwanted or unneeded programs. 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.

8 Addressing the cybersecurity skills shortage in SMBs - Sophos

5. Proactively hunt for active adversaries across your environment
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 essential to identify and stop these living-off-the-land attacks. Once found, you also need to be able to take appropriate actions to stop them quickly.

Technologies like endpoint detection and response (EDR) and extended detection and response (XDR) provide threat hunting, investigation, and neutralization capabilities for 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 to internal network traffic that a firewall cannot see.
- **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 for complete visibility across your environment. MDR provides the highest level of protection against advanced, human-led ransomware attacks.
- **An external attack surface management (EASM) 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.

Sophos protects against ransomware

Sophos Endpoint takes a comprehensive, prevention-first approach to security, blocking threats without relying on any single technique. It uses sophisticated technologies that block the broadest range of attacks, including:

- **Airtight ransomware protection** protects against local and remote ransomware attacks, including new variants. It stops malicious encryption in real time and automatically rolls back any affected files to their original state, minimizing business impact.
- **Anti-exploitation technology** protects against fileless attacks and zero-day exploits by stopping the techniques used by adversaries throughout the attack chain.
- **Adaptive attack protection** is an industry-first dynamic defense that adapts in response to active adversaries and hands-on-keyboard attacks. Dynamically enabled heightened defenses prevent adversaries from taking further actions by minimizing the attack surface and disrupting the attack.

Sophos Endpoint is easy to set up and manage. Install Sophos Endpoint and go! The recommended protection technologies are enabled by default, so you immediately have the strongest protection settings with no tuning required. Granular control is also available if required.

You manage Sophos Endpoint through **Sophos Central,** the world's most trusted cybersecurity platform. This powerful, cloud-based cybersecurity management platform unifies all Sophos next-gen security solutions and enforces MFA for access.

Sophos customers manage their endpoint protection through Sophos Central and benefit from the "Account Health Check" feature. This identifies security posture drift in policies and exclusions, and other high-risk misconfigurations, enabling administrators to remediate issues with one click.

Sophos XDR – proactive threat hunting and IT hygiene tools

Sophos XDR is a unified detection and response platform built on the protection-first approach of Sophos Endpoint. It enables you to quickly detect, investigate, and respond to multi-stage threats across all key attack vectors.

Fully integrated into the Sophos XDR platform, Sophos technologies work together to seamlessly deliver the best possible security outcomes. Additionally, get more return on investment from your existing cybersecurity products using turnkey integrations with an extensive ecosystem of third-party endpoint, firewall, network, email, identity, productivity, cloud security, and backup and recovery solutions.

Sophos XDR provides tools and capabilities designed to maximize the efficiency of security analysts and IT admins.

- AI-prioritized detections across all key attack surfaces help identify suspicious activity that needs immediate attention.
- Detections and cases are automatically mapped to MITRE ATT&CK Tactics, enabling you to easily identify gaps in your defenses.
- Automated actions like process termination, ransomware rollback, and network isolation contain threats rapidly and save you valuable time.Outcome-focused Generative AI capabilities empower security analysts to neutralize adversaries faster, increasing analyst efficiency and business confidence and business confidence.

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 third-party security products for increased visibility and protection across your environment.

Sophos Incident Response Services Retainer– an incident response service on standby

Having an incident response team in place before adversaries strike is the only way to save time, reduce costs, and mitigate the impact 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.

Note: The Sophos Incident Response Services Retainer is not required if you subscribe to the Sophos MDR Complete service tier, which includes full-scale incident response as standard.

Sophos Managed Risk – vulnerability and 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

2024-10-01 (WP-NP)

SOPHOS