SOPHOS
Cybersecurity delivered.

Endpoint Protection Best Practices to Block Ransomware

Practical guidance on configuring your endpoint solution to provide optimum protection

A Sophos Whitepaper. September 2022

Ransomware attacks have increased in volume over the last year, and the repercussions are widespread.

66% of respondents in our State of Ransomware 2022 survey reported that their organization were hit by ransomware in the previous year — a 78% increase from the year before. In nearly two-thirds of these incidents (65%), attackers encrypted data.

Overall, the average cost to remediate a ransomware attack was a business-crippling $1.4 million. Furthermore, 90% of victims said a ransomware attack impacted their ability to operate, while 86% of private sector organizations said it caused them to lose business/revenue.[1]

This growth in ransomware incidents was part of a broader cyber threat trend: 72% of respondents experienced an increase in the volume/complexity/impact of cyberattacks over the last year.

A properly configured endpoint protection solution represents one of the most effective methods to defend against ransomware. This whitepaper explores how ransomware attacks work, how to stop them, and best practices for configuring your endpoint solution for the strongest protection possible.

How Ransomware Attacks Are Deployed

There are many ransomware actors and many types of ransomware attacks. Some are highly targeted, while others are opportunistic. Often, adversaries scan networks looking for weaknesses that will allow them access — 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 the common exploitation of unpatched vulnerabilities by adversaries, which was the number one method of entry used in cyberattacks (N.B., not exclusively ransomware) that Sophos incident responders investigated last year.

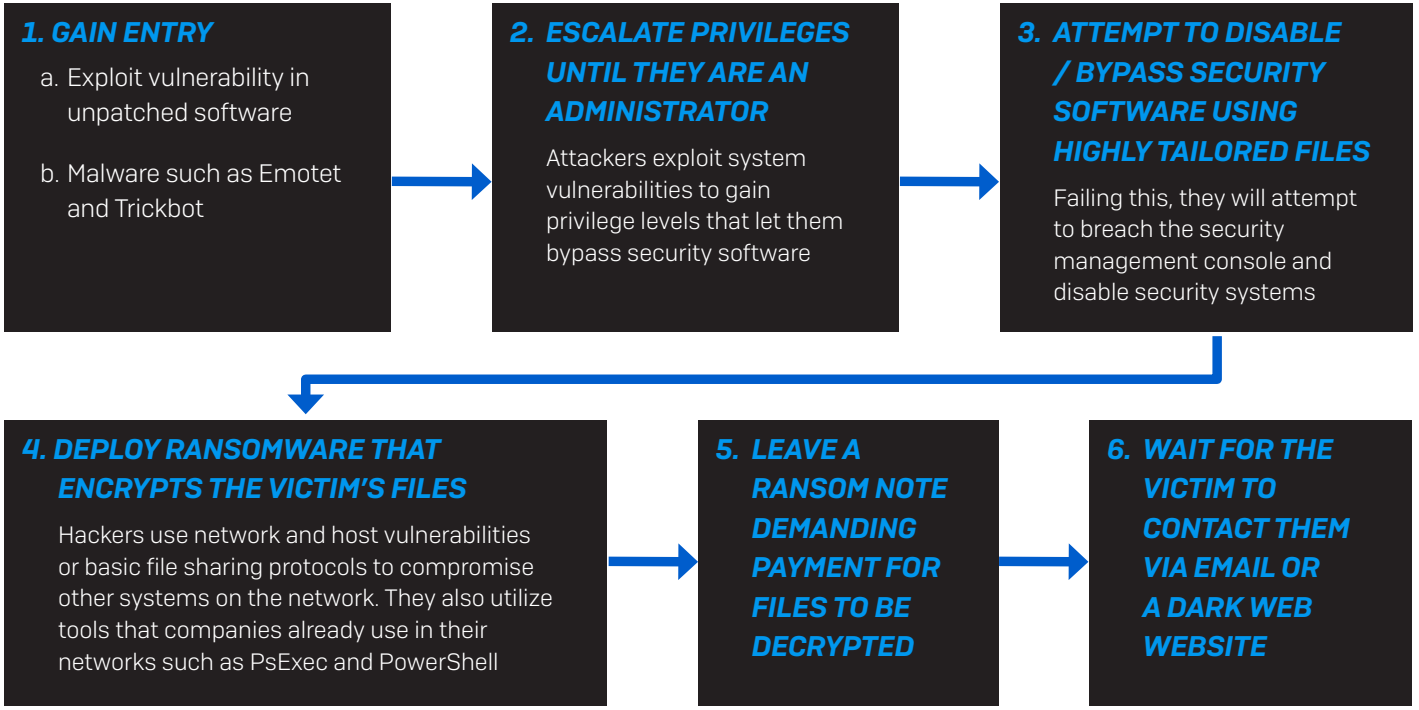
Much of the recent increase in the volume of ransomware attacks can be attributed to the growing ransomware-as-a-service (RaaS) model. There has been a shift from threat actors who make ransomware and use it to attack organizations using this model.

With RaaS, a cybercrime group builds ransomware and leases it out to other attackers. This approach lowers the barrier to entry, making ransomware accessible to a greater number of adversaries than ever before.

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 2021, the average dwell time in ransomware attacks was 11 days.[2] This gives defenders a window to identify and stop intruders before an attack.

1 The State of Ransomware 2022 - Sophos
2 The Active Adversary Playbook 2022 - Sophos

A typical targeted ransomware attack might look like this:



Remote Desktop Protocol or Ransomware Deployment Protocol?

Remote Desktop Protocol (RDP) played a part in at least 83% of cyberattacks investigated by the Sophos incident response team in 2021, up from 73% the year before.[3]

RDP and desktop sharing tools like Virtual Network Computing (VNC) are legitimate and highly useful features that allow administrators to access and manage systems remotely. Unfortunately, without proper safeguards, ransomware actors commonly exploit these tools.

Interestingly, how attackers are using RDP is changing. In 70% of incidents investigated by Sophos, RDP was used only for internal access and lateral movement. Meanwhile, RDP was used for external access *only* in 1% of cases, and 12% of attacks showed adversaries used RDP for external access and internal movement.[4]

It is essential to prevent adversaries from using RDP for external access, internal access, and lateral movement.

3 The Active Adversary Playbook 2022 - Sophos
4 The Active Adversary Playbook 2022 - Sophos

Best Practices to Protect Against Ransomware

Staying secure against ransomware requires more than just having the latest security solutions. Good IT security practices, including regular employee training, are essential. Make sure you're following these nine best practices:

1. Patch early and often

The exploitation of unpatched vulnerabilities was the root cause for almost half (47%) of cyber incidents investigated by Sophos in 2021.[5] Malware often relies on security bugs in popular applications. The earlier you patch your endpoints, servers, mobile devices, and applications, the fewer holes that cybercriminals can exploit.

2. Back up regularly and keep a recent backup copy offline and offsite

In our State of Ransomware 2022 survey, 73% of IT managers whose data was encrypted were able to restore it using backups. Encrypt your backup data and keep it offline and offsite so you won't have to worry about cloud backups or storage devices falling into the wrong hands. Moreover, restore data from backups regularly.

3. Enable file extensions

The default Windows setting is to hide file extensions, meaning you must rely on file thumbnails to identify them. Enable extensions to make it easier to spot JavaScript (JS) files and other file types that aren't commonly sent to you and your users.

4. Open JS files in Notepad

Opening a JS file in Notepad blocks it from running any malicious scripts and allows you to examine the file's contents.

5. Don't enable macros in document attachments received via email

Microsoft deliberately turned off auto-execution of macros by default many years ago as a security measure. Many infections rely on persuading you to turn macros back on — so don't do it!

6. Be cautious about unsolicited attachments

Cybercriminals often rely on an ages-old dilemma: knowing that you shouldn't open a document until you are sure it's legitimate but not being able to tell if it's malicious until you open it. When in doubt, leave it out.

7. 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. And avoid browsing, opening documents, or performing other regular work activities while you have admin rights.

5 The Active Adversary Playbook 2022 - Sophos

8. Regulate internal and external network access

Don't leave network ports exposed. Lock down your organization's RDP access and other remote management protocols. Also, use two-factor authentication and ensure remote users authenticate against a VPN.

9. Use strong passwords

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

Best Practices for Your Endpoint Security Solution

Alongside network security solutions, using an endpoint security or extended detection and response (XDR) solution that includes advanced prevention technologies and threat hunting capabilities is one of the most effective methods for protecting against ransomware attacks.

However, for these technologies to provide maximum cyber protection, they need to be configured correctly.

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

1. Turn on all policies and ensure all features are enabled

It sounds obvious, but this is a surefire way to get the best protection from your endpoint solution. Policies 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. We recommend that you:

A) Enable tamper protection

This prevents unauthorized modification or removal of cyber protection software. One of the first actions malware and attackers make after they access a system is to try to locally disable or remove any security software present.

B) Enable forensic logging (ideally to the cloud)

If you do get compromised, you will want to know what happened. However, most data won't be available since attackers often wipe system logs to cover their tracks. Or, you may lose access to your device. Having a record of activity in the cloud, such as the Sophos Data Lake, ensures you can retain access to important information.

In addition, enable features that detect fileless attack techniques and ransomware behaviors to stop criminals from infiltrating your endpoints and deploying harmful ransomware strains.

Sophos customers managing their endpoint protection through Sophos Central benefit from the "Account Health Check" tool, which automatically assesses your account configuration to identify potential security gaps and helps you change them to optimize protection. You can access the tool here.

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 excluded directories and file types can impact many people across a network. Malware that manages to make its way into excluded directories — perhaps accidentally moved by a user — will likely succeed.

Regularly check your list of exclusions within your threat protection settings and limit the number of exclusions. For any you can't remove, make sure 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 multi-factor authentication (MFA) within your security console

MFA provides an additional layer of security after the first factor, which is often a password. Enabling MFA across your applications is critical for all users who have access to your security console. Doing so ensures access to your endpoint protection solution is secure and not prone to accidental or deliberate attempts to change your settings that can otherwise leave your endpoint devices vulnerable to attacks. MFA is also critical to secure RDP.

4. Ensure every endpoint is protected and up to date

Check your devices regularly to find out if they're protected and up to date. A device not functioning correctly may not be protected and could be vulnerable to a ransomware attack. Endpoint security tools often provide this telemetry. An IT hygiene maintenance program is also helpful for regularly checking for any potential IT issues.

5. Maintain good IT hygiene

Regularly evaluating your IT hygiene ensures your endpoints and the software installed on them 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 is running 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, including your security software. It's also a surefire way to ensure your data is backed up regularly.

6. Proactively hunt for active adversaries across your network

In today's threat landscape, malicious actors are more cunning than ever, often deploying legitimate tools and stolen credentials to avoid detection. To identify and stop these "living-off-the-land" attacks, it's essential to proactively hunt for advanced threats and active adversaries. Once found, you also need to be able to take appropriate actions to quickly stop them.

Endpoint technologies such as endpoint detection and response (EDR) and XDR provide threat hunting and neutralization. Organizations with these technologies should take full advantage of 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 key. MDR services provide 24/7 threat hunting delivered by experts who specialize in detecting and responding to cyberattacks that technology solutions alone cannot prevent. They also provide the highest level of protection against advanced, human-led ransomware attacks.

Sophos Protects Against Ransomware

We offer multi-layered threat protection technology (Sophos Endpoint Protection)

Sophos Intercept X Endpoint detects and stops 99.98% of attacks before they can run. It uses advanced, multi-layer protection, including:

- Anti-ransomware behavioral technology that detects malicious encryption processes and rolls files back to their safe states.
- Anti-exploit capabilities that detect fileless attack techniques
- AI-powered deep learning models that identify and block ransomware before it can run.

The built-in Account Health Check tool automatically assesses your account configuration to identify potential security gaps, such as policies that are not turned on or features that are not enabled. It also provides practical guidance to remediate any issues found and optimize your cyber protection.

Plus, the Sophos Central management platform automatically enforces MFA for access, increasing the security of your console.

Proactive threat hunting and IT hygiene tools (Sophos XDR)

Sophos XDR provides professional-grade tools that enable you to hunt for threats and maintain good IT hygiene across your entire estate. It empowers your team to ask detailed questions to identify advanced threats, active adversaries, unprotected devices, and potential IT vulnerabilities and quickly stop them.

With access to live device data, up to 90 days of on-disk data, 30 days of data stored in the Sophos Data Lake cloud repository, and an automatically generated list of suspicious items, you have all the information you need at your fingertips to start a forensic investigation and hunt down active ransomware threats.

24/7 MDR service (Sophos MDR)

Sophos MDR provides a 24/7 team of elite threat hunters that detects and remediates attacks on your behalf. With thousands of hours of collective experience, our experts have seen and dealt with anything a ransomware attacker can throw at you and deliver the ultimate ransomware protection.

Conclusion

Ransomware continues to evolve. While we may never be able to eradicate ransomware, our endpoint protection best practices give your organization the best chance to protect against the latest threats.

In summary:

1. Turn on all policies and ensure all features are enabled.
2. Regularly review your exclusions.
3. Enable MFA within your security console.
4. 4Ensure every endpoint is protected and up to date.
5. Maintain good IT hygiene.
6. Hunt for active adversaries on your network.

Learn more about Sophos XDR
at www.sophos.com/xdr

Learn more about Sophos MTR
at www.sophos.com/MDR

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.

2020-09-01 EN-WP (DD)

SOPHOS