SOPHOS

Best practices for securing your network from ransomware

Elevate your protection against ransomware and other network attacks

A Sophos Whitepaper. October 2024

Ransomware remains a top cyberthreat

Ransomware continues to rank among the most significant cyberthreats, with far-reaching and often catastrophic consequences. 59% of respondents in our State of Ransomware 2024 survey reported that their organizations were hit by ransomware in the previous year. In 70% of these incidents, attackers encrypted data.

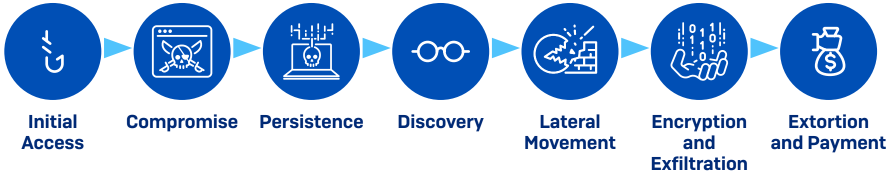
The surge in attack rates over the last few years likely reflects the growing success of the ransomware-as-a-service model which has lowered the skill barrier for attackers.

The average attack remediation cost has now soared to $2.73 million—a 50% increase over the previous year—while 34% of businesses took over a month to recover. This extended recovery period highlights the increasing complexity of attacks and the heavy strain on security teams, with 95% struggling to manage essential security operations tasks[1].

These trends 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. This whitepaper explores ransomware attack mechanics, prevention strategies, and how to optimize your network stack for maximum security.

How ransomware attacks work

To understand how to protect against ransomware attacks, we first need to examine how they work. A typical attack looks like this:



Modern ransomware actors often use legitimate IT and end-user tools such as a VPN or Remote Desktop Protocol (RDP) to gain initial access. RDP played a part in 90% of cyberattacks investigated by the Sophos Incident Response team in 2023, up from 83% the year before.[2]

These tools are used by authorized staff as part of their jobs, making initial detection of modern ransomware attacks difficult. The root of the problem is that there's too much implicit trust in the use of these tools — anyone who can access a VPN or RDP is assumed to be trusted, a practice which has proven time and time again to be unwise.

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

[1] Addressing the cybersecurity skills shortage in SMBs - Sophos

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

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. 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.

2. Patch and keep firmware up to date

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.[3]

Unpatched vulnerabilities were the leading root cause of ransomware attacks in 2024[4]. 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.

3. 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**: In today's fast-evolving threat landscape, automated hotfixes are crucial. To address emerging threats, the firewall must be capable of receiving updates instantly, without requiring major firmware updates.
- **Proactive monitoring**: Vendor-side monitoring across the entire deployed customer base can help identify and respond to attacks much faster.

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 there is nothing being exposed that's not absolutely essential. 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 multi-factor authentication (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 both ZTNA and endpoint protection.

6. Use strong passwords and multi-factor authentication (MFA)

Weak passwords and lack of multi-factor authentication (MFA) remain major vulnerabilities, leading to a significant number of successful cyberattacks. Ensure all systems on your network, even those not exposed externally, use strong passwords and are protected by MFA to prevent brute-force attacks.

[3] Unpatched Vulnerabilities: The Most Brutal Ransomware Attack Vector - Sophos
[4] The State of Ransomware 2024 - Sophos

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.

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. Additionally, 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

Despite your best efforts, 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 91% of ransomware attacks occurring outside regular business hours[5], you need a cybersecurity solution that operates around the clock to detect adversaries in real time and immediately shares 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. 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.

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, ensuring a coordinated defense that prevents lateral movement and isolates the threat.

[5] Regular business hours refer to 8am – 6pm, Monday – Friday | Stopping Active Adversaries: Lessons From The Cyber Frontline - Sophos

Layering security technologies to protect against ransomware

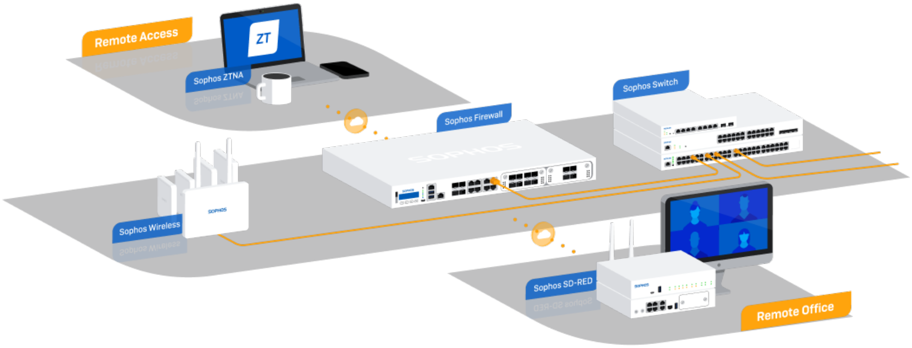
As the saying goes, "*an ounce of prevention is worth a pound of cure*." Stopping issues early is far easier than fixing the damage later. Protecting your organization from ransomware benefits from a layered IT security approach, where multiple technologies work together to create defense and visibility. 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.
- **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 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 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, your switches and access points will drop packets from the compromised host, and ZTNA can prevent any compromised device from connecting to your applications. 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.
- **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.
- **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 ZTNA

Sophos ZTNA transparently connects your users to the applications and systems they need to do their jobs, while providing enhanced segmentation, security, and visibility over 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 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 easy of management.

Sophos Email

Sophos Email provides advanced phishing and message protection to stop threats from getting in via email:

- **Phishing protection**: Sophos Email employs AI-powered natural language processing (NLP) to identify impersonation attempts that aim to trick users into believing a phishing attempt is legitimate. It also includes multi-layered malware and malicious URL analysis with time-of-click protection that rewrites URLs, forcing an additional check if they are clicked. Sophos email also utilizes several technologies to identify suspicious senders by leveraging SPF, DKIM, and DMARC as well as email header anomaly analysis.
- **Phish Threat employee training**: Sophos Phish Threat provides attack simulation and training for your employees. It can be extremely helpful in training employees how to identify suspicious email and phishing attacks, and can be used to test and identify users that need additional training.

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

2024-10-14 (WP-PC)