

# Best Practices for Securing Your Network from Ransomware

Elevate your protection against ransomware and other network attacks

# Ransomware Attacks Are Increasing in Volume and Severity

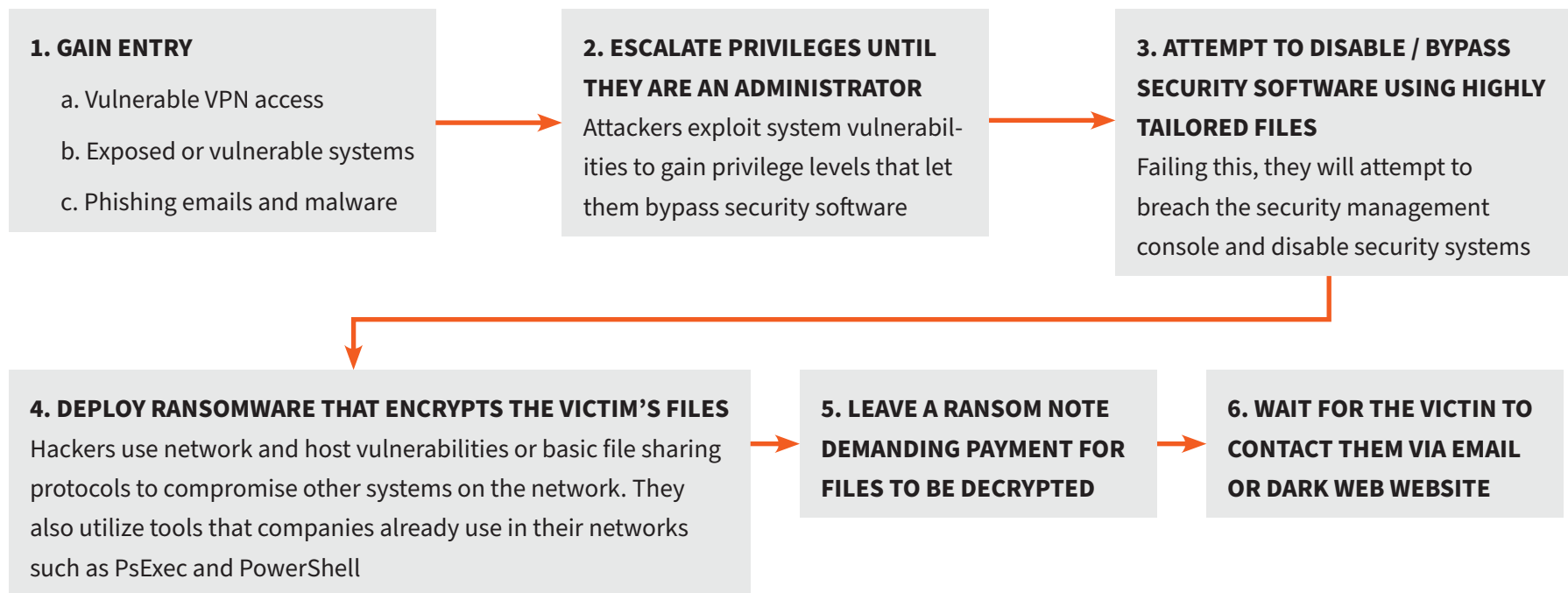
---

66% of organizations were hit by ransomware last year, up from 37% in 2020.<sup>1</sup> This is a 78% year-over-year increase, demonstrating that adversaries have become considerably more capable at executing attacks at scale than ever before. The surge in ransomware likely also reflects the growing success of the ransomware-as-a-service model, which extends the reach of ransomware by reducing the skill level required to deploy an attack.

## How Ransomware Attacks Work

---

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



Modern ransomware attacks often use legitimate IT and end-user tools such as a VPN or Remote Desktop Protocol (RDP) to gain access. 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.

# How to Prevent Ransomware Attacks

---

There are three network security measures that can help mitigate the risk of a ransomware attack.

## 1. Eliminate Exposure from Remote Access

Many believe a Virtual Private Network (VPN) protects against ransomware attacks. This myth is incorrect, and VPN is an easy-to-use attack vector for malicious actors. Of course, this vector of attack has gained even more appeal recently through the enormous proliferation of remote-access VPN use, as millions of employees have transitioned to working from home over the last two years. Attackers realize these home networks are poorly protected and vulnerable, making them easy targets.

One of the highest profile ransomware attacks in 2021 involved a U.S. pipeline organization that saw fuel delivery disrupted for most of its customers in the eastern and southern portions of the country. During the attack, cybercriminals exploited a remote-access VPN.

Most outdated VPN clients also contain vulnerabilities that can be exploited, further compounding the challenge of securing your network against external threats. This has prompted law enforcement organizations like the FBI, Department of Homeland Security, and CISA (Cybersecurity & Infrastructure Security Agency) to issue warnings about the possibility of attacks on remote-access VPN infrastructure.

### Best Practice — 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 in comparison 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. It is so important that the White House created a zero trust architecture mandate that all federal agencies must comply with by 2024.

### Eliminate exposure via exposed Remote Desktop Systems (RDP) and other systems

Remote management tools like RDP, Virtual Network Computing (VNC), and other remote management solutions allow remote staff to access and manage systems. Unfortunately, without the proper safeguards in place, these tools also provide convenient in-roads for attackers to launch ransomware attacks.

Not securing RDP and other remote management solutions can leave you open to ransomware attacks. Cybercriminals often use bulk scanning and brute-force hacking tools, which try hundreds of thousands of username and password combinations until they get the right one. Sometimes, they will use those credentials to immediately launch an attack. Other times, they may sell those credentials to another group of attackers.

## 2. Limit Lateral Movement

During a network attack, it's absolutely vital that your network security solution limit its ability to move around the network — or move laterally.

Unfortunately, most networks resemble a medieval fortification — with a proverbial castle wall and moat forming a secure perimeter around network resources. A VPN provides the equivalent of a secure gatehouse for authorized users to enter a safe perimeter. But, once cybercriminals access a network, they have full access to everything within its perimeter. This same freedom of movement within a network also applies to threats like ransomware.

Cybercriminals use RDP and other management systems, as well as unmanaged devices, as entry points. They also use these entry points to move laterally across a network.

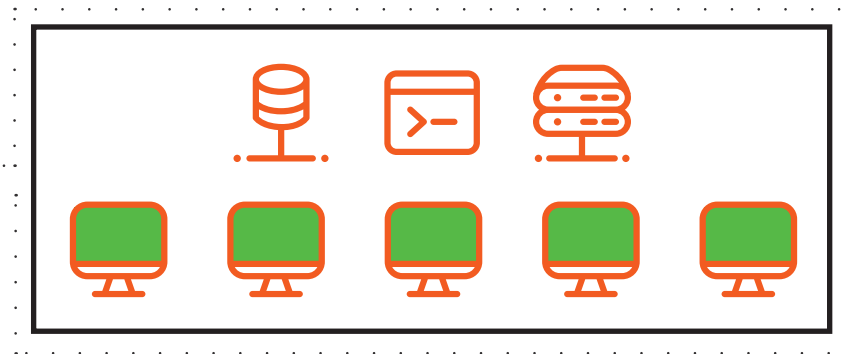
### Remote Access VPN Clients



### VPN Concentrator and Firewall



### Network Perimeter



### Best Practice — Micro-Segment Your Network

This is critical in modern networks, along with zero trust. There are three best practices you should use to architect your network:

1. **Segment Your Network.** Create small zones or VLANs and connect them via managed switches and a firewall to apply anti-malware and IPS protection between segments. This lets you identify and block threats attempting to move laterally on your network.
2. **Use ZTNA.** Micro-segment your network applications and only allow authorized users to access the resources they need. That way, if a user device is compromised and a threat goes undetected, the threat can quickly be eliminated. Sophos ZTNA goes one step further by completely removing access if a device is compromised.
3. **Utilize Technology Like Sophos Synchronized Security.** Synchronized Security lets you automatically respond to an active threat on your network, isolate it, and prevent it from moving laterally. It can immediately identify a threat and notify healthy devices to ignore any traffic from a compromised host while Sophos Switches automatically drop packets from an affected device and Sophos Firewall further limits access by the compromised host to other parts of the network.

# Network Security Best Practices to Protect Against Ransomware

---

In summary, here are best practices that you can use to protect your network against ransomware and other cyber threats:

- **Micro-Segment Your Network.** This allows you to limit lateral movement of threats. Use Sophos ZTNA to micro-segment access to your network applications. On top of that, use Sophos Firewall and Sophos Switch to micro-segment your internal network resources. And, use Sophos SD-WAN to segment and securely connect remote devices and locations.
- **Replace Remote-Access VPN with ZTNA.** Eliminate a common attack vector by removing potentially vulnerable old VPN clients. Upgrade to a modern ZTNA solution such as Sophos ZTNA, which integrates with Sophos next-gen endpoint protection to properly secure your user device, their identities, access to your apps and data, and your network with a single agent managed from a single console, from a single vendor.
- **Implement the Strongest Protection Possible.** You should implement the highest level of protection on your firewall, endpoints, servers, mobile devices, and remote access.
  - Ensure your firewall has TLS 1.3 inspection, next-gen IPS, and streaming DPI with machine learning and sandboxing for protection from the latest zero-day threats. Sophos Firewall includes all of these technologies and tightly integrates them to deliver powerful protection and performance so you're getting the most value out of your firewall investment.
  - Also, ensure your endpoints have modern next-gen protection capabilities to guard against credential theft, exploits, and ransomware. Sophos is consistently rated as the top provider of next-gen endpoint protection solutions. We cover your endpoints, mobile devices, and servers and let you manage them from the same cloud-management console as the rest of your Sophos products.
- **Reduce the Surface Area of Cyberattack.** Review your firewall rules and eliminate any remote access or RDP system access through VPN, NAT, or port-forwarding. And, ensure that any traffic flows are properly protected. Sophos Firewall makes this easy with its superior visibility, dashboards, reporting, and rule management capabilities.
- **Keep Your Firmware and Software Patched and Up to Date.** This is particularly important for any network infrastructure like a firewall or remote-access software or clients but equally important for all your systems, since every update includes important security patches for previously discovered vulnerabilities. Sophos enables you to keep all your cybersecurity products up to date automatically.
- **Use MFA.** Ensure your network operates on a zero-trust model where every user and device has to continually earn trust by verifying their identity. Also, enforce a strong password policy and consider adopting authentication solutions like Windows Hello for Business. All Sophos products support MFA from your preferred authentication provider.
- **Instantly Respond to Cyberattacks.** Use automation technologies and human expertise to speed up cyber incident response and remediation.
  - Ensure your network security infrastructure helps you automatically respond to active attacks so you can isolate a compromised host before it can cause serious damage. Only Sophos Synchronized Security is able to provide the level of response you really need, when you need it.
  - Deploy a managed detection and response (MDR) service such as Sophos MDR. With Sophos MDR, a team of threat experts is constantly monitoring and responding to incidents before they become problems, so you don't need to worry.