SONICWALL®

8 WAYS TO PROTECT YOUR NETWORK AGAINST RANSOMWARE

Steps to prevent ransomware attacks and save your money

Sometimes old becomes new again. Such is the case with ransomware attacks, which have become popular once more.
First released in 1989, ransomware infects a system and “locks out” the user from accessing the device or files on it. Only
when the victim agrees to pay a ransom, usually in the form of bitcoins, can the system be unlocked and accessed again.

The following e-book provides eight ways you can protect your network against ransomware attacks and avoid giving your money to cybercriminals.

Ransom amounts vary, but are often in the $200-$400 range.[1]

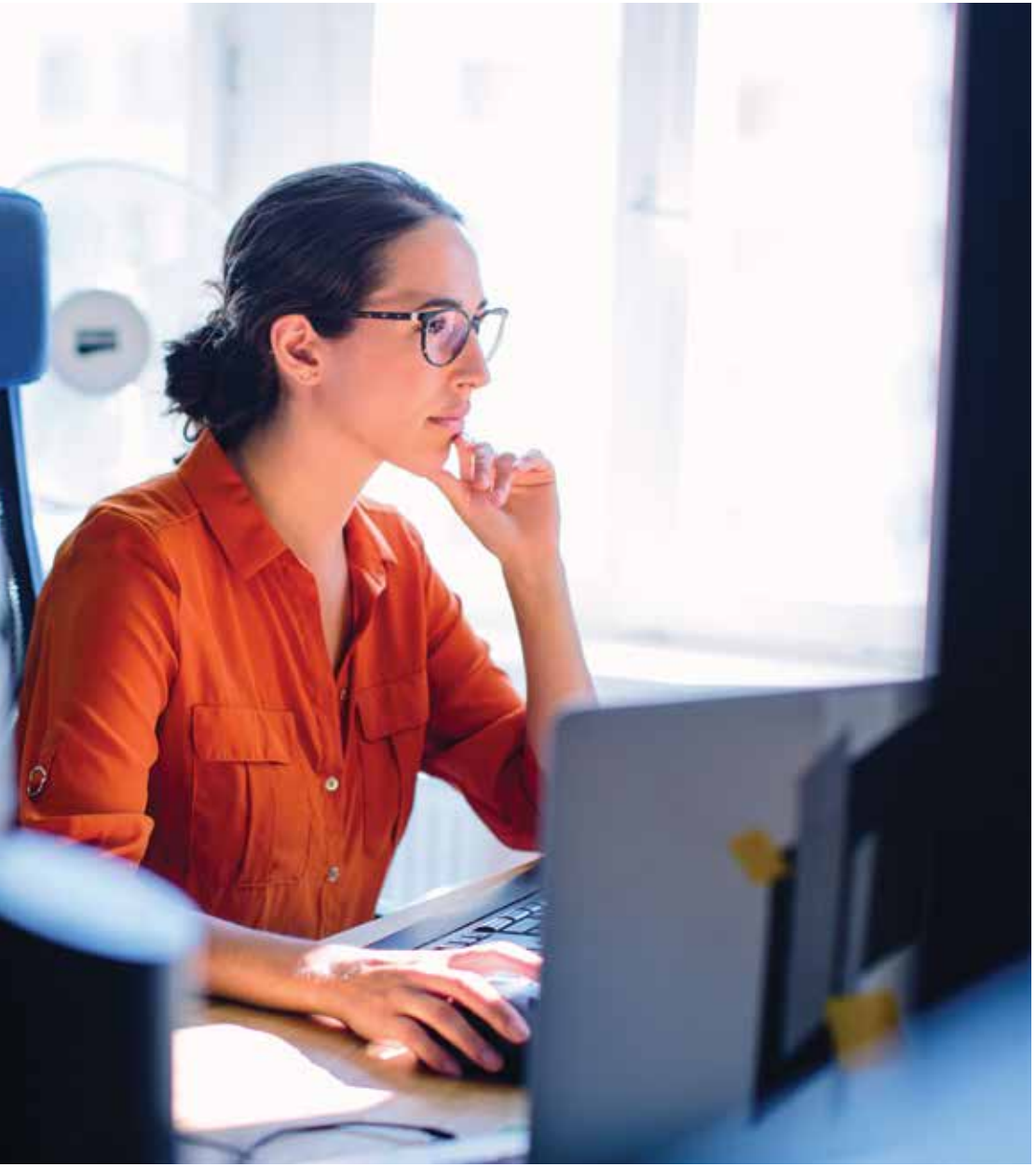
1. Educate your employees

User education and awareness are critical when it comes to defeating ransomware. Treat suspicious emails with caution. Look at the domain name that sent the email. Check for spelling mistakes, review the signature and the legitimacy of the request. Hover over links to check where they lead to.

2. Use a multi-layered approach to network security

Protection from ransomware and other forms of malware doesn’t begin and end at the gateway. Extending security through the use of anti-virus, anti-spyware, intrusion prevention and other technologies on devices at the network perimeter is critical. Adopt a layered approach to stop ransomware by avoiding a single point of failure in your security architecture.

1 US Computer Emergency Readiness Team Alert (TA16-091A)



3. Back up your files regularly

Another safeguard against having to pay ransom is a robust backup and recovery strategy. Depending on how quickly the compromise is detected, how widely it has spread and the level of data loss that is acceptable, recovery from a backup could be a good option. However, this calls for a smarter backup strategy that is aligned to the criticality of your data and the needs of your business around recovery point objectives (RPO) and recovery time objectives (RTO).

4. Make sure your endpoints are protected

Since most users primarily interact with personal and corporate devices, the endpoints are particularly at risk if they are not managed or don't have the right anti-malware protection. Most anti-virus solutions are signature-based and prove ineffective if not updated regularly. The newer ransomware variants are uniquely hashed and thereby undetectable using signature-based techniques. Many users also turn off their virus scans so that it doesn't slow their system down.

Implement a layered security strategy for greater network protection.

5. Patch your systems and applications

Many attacks are based on known vulnerabilities in browsers including Internet Explorer, as well as in common apps and plug-ins. Therefore it's critical to apply updates and patches promptly and reliably. Choosing a solution that is able to automate patching and version upgrades in a heterogeneous device, OS and application environment will go a long way in addressing a range of cyber threats, including ransomware.

6. Segment your network to stop the spread

Most ransomware will try to spread from the endpoint to the server/storage where all the data and mission critical applications reside. Segmenting the network and keeping critical apps and devices isolated on a separate network or virtual LAN can limit the spread.

7. Quarantine and analyze suspicious files

Technologies such as sandboxing provide the ability to move suspicious files to quarantine for analysis before they can enter the network. The files are held at the gateway until a verdict is returned. If a file is found to be malicious you can prevent follow-on attacks by implementing protective measures such as policies that block associated IP addresses or domains, or deploying signatures to security appliances across the network.

Segment your wireless LAN to separate internal from guest users for an additional level of security.

8. Protect your Android devices

Devices running the Google Android OS have become prime targets for ransomware attacks. Take the following actions to protect your Android smartphone:

- Do not root the device – it exposes the system files for modifications
- Always install apps from Google Play store – apps from unknown site/stores can be fake/ malicious
- Disable installation of apps from unknown sources
- Allow Google to scan the device for threats
- Be careful when opening unknown links received in SMS or emails
- Install third-party security applications that scan the device regularly for malicious content
- Keep an eye on which apps are registered as Device Administrators
- For corporate devices create a blacklist of disallowed apps

Malware for the Android ecosystem continued to rise in 2015, putting nearly 85 percent of smartphones at risk.

Conclusion

Ransomware attacks have become increasingly popular with cybercriminals. Make sure your network is protected. SonicWall can enhance protection across your organization by inspecting every packet and governing every identity. As a result, this protects your data wherever it goes, and shares intelligence to safeguard against a variety of threats, including ransomware.

Visit the SonicWALL Network Security Products web page.

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com

Ebook-8waysRansomware-EU-IMAG-29271-D1

SONICWALL®