A Unified Security Approach to Ransomware Resilience

236.1 MILLIONS

ransomware attacks occurred globally in the first half of 2022

Ransomware is malicious software (malware) that infiltrates computer systems or networks, encrypts valuable data, and demands a ransom from the victim in exchange for the decryption key needed to regain access to the compromised data. It's typically executed by cybercriminals seeking financial gain and can target individuals, businesses, or even critical industrial or government infrastructure. These attacks can result in data loss, operational disruptions, and significant financial damages, making it one of the most serious threats in the world of cybersecurity.

How does ransomware work?

Once a computer system or network is infiltrated, ransomware encrypts files using complex algorithms, locking them away from users. After the encryption process, a ransom note is displayed, informing the victim of the attack and demanding payment, often in cryptocurrency, in exchange for the decryption key required to regain access to the compromised data. The victim is usually given instructions on how to make the payment, and upon receiving it, the cybercriminals are to provide the decryption key, allowing the victim to unlock their files.

3.5 WEEKS

Average time to recovery after a ransomware attack

Ransomware typically gains entry via one of these methods:

- **Human error.** The most common way ransomware spreads is through phishing emails that trick the recipient into opening an infected attachment or clicking a malicious link. Once the ransomware is executed, it can spread to other devices on the network.
- **Unpatched vulnerabilities.** Attackers often exploit known vulnerabilities in software to gain access to a victim's computer. This is an easy entry point if the software is not updated with the latest security patches.
- **Malvertising.** This is a type of online advertising that is used to deliver malware. Attackers can infect victims with ransomware once they click on a malicious ad.
- **Drive-by downloads.** In these attacks, malware is downloaded to a victim's computer without their knowledge or consent when a victim visits a compromised website or clicks a malicious link.
- **Unsecured removable devices.** Ransomware can also spread through removable devices, such as USB drives, that aren't secure. Once a victim inserts an infected removable device into their computer, the ransomware can be copied to the computer and spread to other network devices.

Ransomware attackers are constantly looking for new ways to spread their malware. By understanding these common ways that ransomware spreads, you can take steps to protect against it.

58
ACTIVE
ransomware groups

101
KNOWN
types of ransomware

Why is ransomware spreading?

Ransomware is spreading for several reasons. First, profitability is key. Ransom payments, often demanded in cryptocurrencies that provide a degree of anonymity, have proven to be lucrative. This financial incentive encourages established criminal organizations and individual hackers to invest in developing and distributing even more ransomware.

Second, the increasing interconnectedness of our digital world creates more opportunities for ransomware to propagate. The growing popularity of Cloud computing makes it easier for attackers to target victims, as they can access files stored on Cloud servers.

Furthermore, the relative ease with which ransomware can be deployed and the availability of ransomware-as-a-service (RaaS) platforms on the dark web enable even those with limited technical expertise to launch attacks. RaaS providers offer user-friendly interfaces, customer support, and detailed instructions, allowing users to customize the ransomware for specific targets. When deployed, users collect ransoms from victims and split profits with the RaaS provider, resulting in a profit-sharing arrangement.

In the end, combatting the spread of ransomware is challenging due to its global and decentralized nature. Criminals from different countries employ anonymous communication methods, making it difficult for law enforcement to track and apprehend them.

How should you respond to a ransomware attack?

If you believe you've encountered a potential ransomware attack, don't panic. Instead, follow these steps:

- Advise the company against paying the ransom. Paying up does not guarantee the attacker will return the data, and it only provides further incentives to continue ransomware attacks.
- Contact authorities to report the attack so they can investigate and track down attackers..
- Try to recover the data from a backup. Having an up-to-date backup is the best insurance for business continuity.
- Get specialists involved. If you cannot recover the data from a backup, consider bringing in a data recovery specialist.

27% of organizations feel underprepared to deal with ransomware

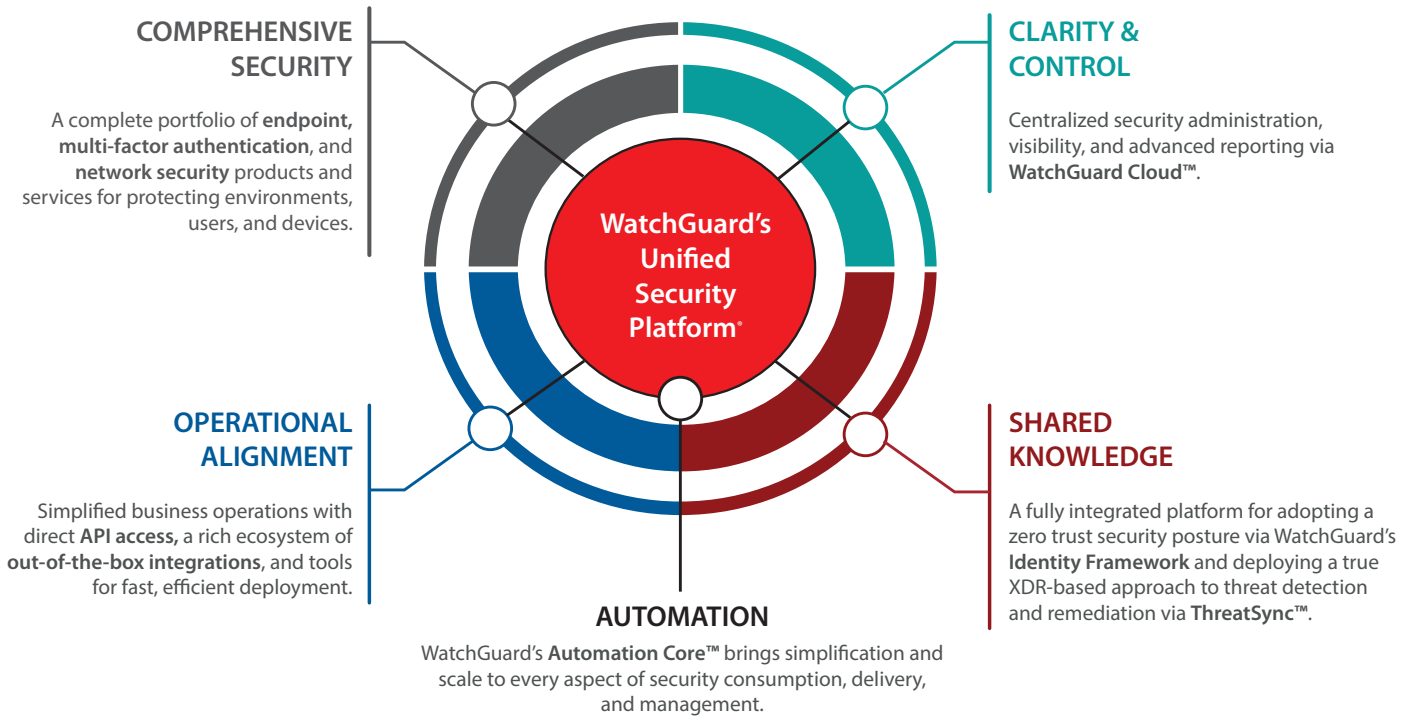
How do you protect yourself from ransomware?

The FBI emphasizes a multifaceted strategy prioritizing prevention, business continuity, and remediation. Ransomware's continually evolving and sophisticated nature demands a comprehensive approach. Contingency and remediation planning ensure swift business recovery and uninterrupted operations. This involves implementing proactive measures like application whitelisting and virtualized environments, categorizing data by its value, and enforcing network separation, all of which contribute to a robust defense against ransomware.

In the broader context, individuals and organizations must remain vigilant and proactive in safeguarding against attacks. Being aware of the risks and taking proactive steps are key. Individuals, as well as organizations, can significantly enhance their resilience against this pervasive cyber threat by adopting best practices and employing robust cybersecurity measures, such as:

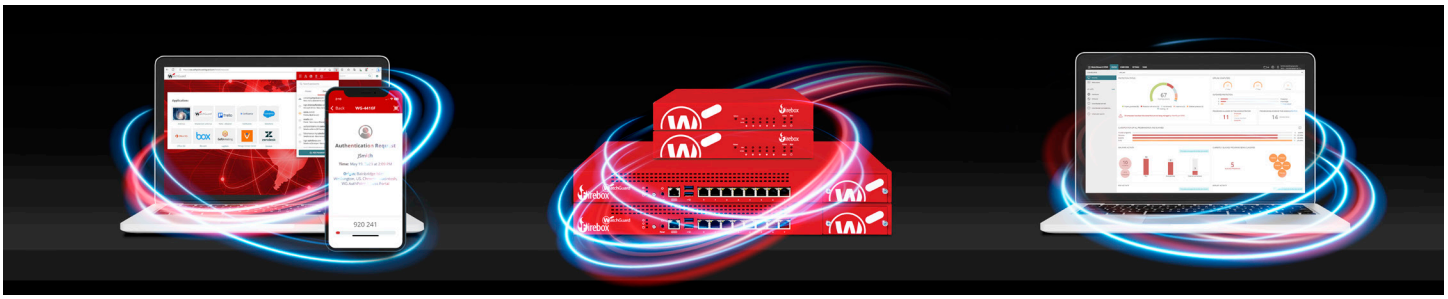
- Regularly back up important data and files so that you can restore them if they get encrypted.
- Scan email attachments and links; only allow trusted emails to be delivered.
- Keep operating systems and software up to date with the latest security patches and updates.
- Use antivirus software and update it regularly.
- Disable unnecessary services and applications not required for a customer's work.
- Use firewalls to block unauthorized access to a network.
- Limit user privileges so only authorized users can install or make changes to software.
- Educate yourself and your customers about ransomware and how to avoid it.
- Implement strict security policies and procedures to ensure a safe and secure working environment.
- Have a plan for responding to a ransomware attack, including who to contact and what steps to take.

Even with these preventive measures, ransomware could still infiltrate a network. Fully integrated layers of security are the ultimate defense. WatchGuard's Unified Security Platform architecture is crucial in combatting ransomware attacks.



Better Ransomware Protection – The WatchGuard Way

WatchGuard's security solutions provide a powerful defense against ransomware attacks. The Firebox firewall and complementary security services protect your network from external threats, while Endpoint Security defends your endpoints from internal threats. WatchGuard's Total Identity Security helps protect users from credential theft and prevent unauthorized access to your systems, a common way ransomware is introduced. This unified, layered security approach ensures that your entire network is protected against ransomware attacks, minimizing the risk of data loss and downtime.



WatchGuard Network Security

To protect your network perimeter from ransomware, you need a comprehensive security solution that provides robust protection at multiple levels. WatchGuard offers a wide range of features to help you safeguard your network, including:

- Advanced Threat Prevention: Uses real-time intrusion detection and prevention to actively identify and block ransomware attacks before they can breach your network.
- Multi-Layered Security: Combines signature-based detection, behavioral analysis, and heuristic scanning to identify known and emerging ransomware variants.
- Secure VPN and Access Control: Offers built-in VPN and access control features to safeguard remote connections and reduce the risk of ransomware infiltrating your network through remote or mobile devices.
- Early Detection: Provides real-time alerts and reports to enhance user awareness and promptly address suspicious activities.
- Rapid Response: Isolates affected devices and helps recover data during ransomware attacks, minimizing downtime and financial losses.
- Scalability: WatchGuard's security solutions can be scaled to protect businesses of all sizes, from small enterprises to large corporations.
- Continuous Updates: WatchGuard regularly updates its security solutions to keep you ahead of emerging ransomware threats.

Stay one step ahead with WatchGuard network security.

WatchGuard Endpoint Security

Ransomware detections on endpoints increased by 627% last year. WatchGuard endpoint security solutions can detect ransomware attacks early by monitoring for suspicious behavior, such as large numbers of files being encrypted at once or attempts to communicate with known ransomware command and control servers. To stay safe, your endpoints need the latest advances in endpoint protection, including:

- Real-time threat detection: Our Threat Hunting Service monitors systems and networks for threats in real time, proactively identifying and blocking ransomware attacks before they can gain a foothold.
- Behavioral analysis: The Zero Trust Application Service uses behavioral analysis to detect ransomware activity, even from new variants. Monitoring the behavior of processes and files can identify and quarantine suspicious actions, stopping potential attacks.
- Anti-ransomware signatures: WatchGuard continuously updates its signatures to ensure known ransomware strains are promptly identified and blocked.
- Web reputation filtering: This prevents users from accidentally visiting malicious websites that are known to host ransomware distribution, reducing your attack surface.
- Centralized management: WatchGuard Cloud allows administrators to easily oversee and configure security policies across all endpoints, ensuring that all devices on your network are uniformly and reliably protected.
- Quarantine and remediation: In a ransomware incident, our endpoint security can isolate infected devices and assist in recovering encrypted data, minimizing downtime and losses.
- Multi-platform support: Our endpoint security supports various platforms, including Windows, macOS, and Linux, making it suitable for diverse IT environments.

Get complete endpoint protection with WatchGuard.

WatchGuard Multi-Factor Authentication (MFA)

AuthPoint is a multi-factor authentication (MFA) solution that enhances security by requiring users to authenticate their identities through multiple factors, such as passwords, one-time passwords (OTPs), push notifications, and biometrics. This significantly reduces the risk of unauthorized access and ransomware infiltrations. AuthPoint is delivered entirely from the Cloud, making it easy to set up and manage. It offers a variety of benefits, including:

- Improved access security: AuthPoint provides strong access control by requiring multiple authentication factors and using mobile device DNA to identify and block unauthorized devices.
- Protection from stolen credentials: Ransomware attacks often begin with stolen or compromised credentials. AuthPoint mitigates this risk by requiring users to authenticate their identities using two or more factors, even if their login credentials have been stolen.
- Compliance with industry regulations: Many regulatory standards and compliance frameworks now mandate MFA to protect sensitive data. Implementing AuthPoint not only enhances security but also ensures compliance with industry regulations.
- Versatility: AuthPoint supports a variety of authentication methods, allowing organizations to choose the most suitable approach for their users and security needs.
- Scalability: Authpoint easily scales to meet the needs to meet the needs of organizations of all sizes.

Protect your credentials with WatchGuard AuthPoint

You need a comprehensive cybersecurity solution to protect your networks from ransomware. WatchGuard's Unified Security Platform architecture **layers network, endpoint, and identity security** to seamlessly protect your organization from all angles and establish a robust defense against the relentless ransomware threat.

Check out the ransomware tracker powered by WatchGuard Threat lab.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit **WatchGuard.com**.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 WEB www.watchguard.com