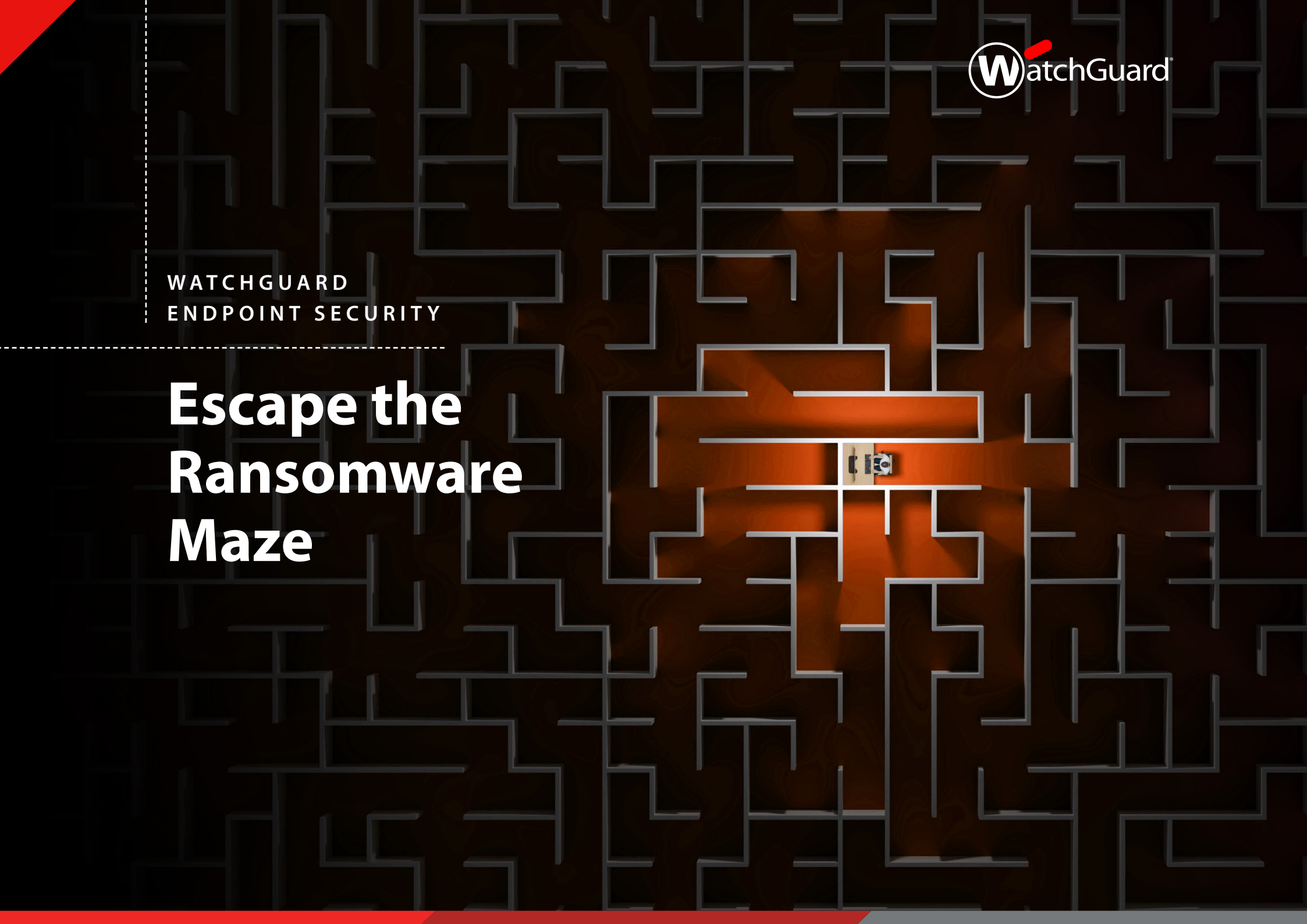
WATCHGUARD
ENDPOINT SECURITY

Escape the Ransomware Maze



Ransomware is an ever-evolving form of malware designed to steal business-critical data and then sell it or encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.

Ransomware attacks are dramatically increasing in number and frequency year over year, with high-impact, headline-making incidents continuously growing in volume and scope. Ransomware gangs are also looking at their primary victim's business partners to pressure them into paying a ransom to prevent data leakages or business disruptions caused by the attack.

Conventional endpoint protection tools just aren't the best defense anymore

+150%

the frequency and the complexity of ransomware increased by more than 150% in 2020[1]

≈1 in 2

ransomware attacks use a combination of encryption and data theft to pressure victims to pay ransom demands[2]

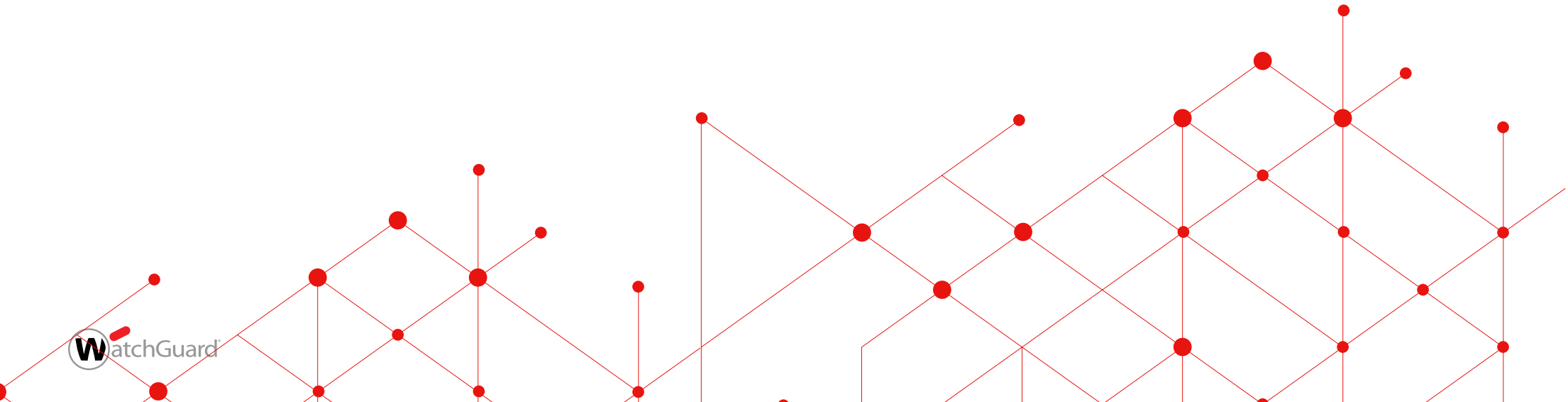
10-15 times

the cost of recovery and the resulting downtime of a ransomware attack can be 10 to 15 times more than the ransom[3]

#1

ransomware had been assessed as the prime threat for 2020-2021. The market for ransomware became increasingly "professional" in 2021[4]

1. ENISA Threat landscape report 2021 | European Union Agency for Cybersecurity (ENISA)
2. How to Prepare for Ransomware Attacks | Gartner
3. Nearly 40% of new ransomware families use both data encryption and data theft in attacks and CISA
4. ENISA Threat landscape report 2021 and CISA - 2021 Trends Show Increased Globalized Threat of Ransomware



WatchGuard

Is your Business Adequately Protected?

Ransomware is perhaps the most lucrative method of cybercrime encountered to date, and this makes a distinct shift in how cybercriminals derive value from their victims' data. With ransomware, attackers no longer need to focus on stealing data they can easily resell but rather exploit the importance of that data to the victim.

Even though the data may not be sensitive in its content, it may be business-critical for the organization.

By holding the data hostage and demanding a ransom for its return, attackers can monetize data for which they may have had no other use.

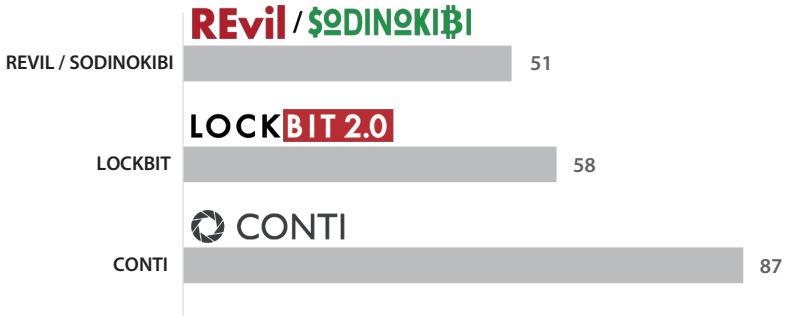
This paradigm shift places a host of organizations, many of whom have long felt themselves too small to be an appealing target for cyberattacks, firmly in the crosshairs of cybercriminals.

With ransomware, attackers no longer need to focus on stealing data they can easily resell but rather exploit the importance of that data to the victim.

Ransomware: Behind the Scenes

Today's cyberattackers use sophisticated tactics to bypass traditional ransomware detection measures and hide in the everyday nature and complexity of their target's environment. They move through the network seeking to steal data, installing ransomware, encrypting data and wreaking havoc. Once they have what they need, they threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid.

Top Ransomware Variants Victimizing Critical Infrastructure:



FBI – Internet Crime Report 2021

Ransomware as a service, spear phishing, attacks on unpatched systems, double extorsion, and supply chain attacks emerged as the top five initial infection vectors that were used to deploy ransomware on compromised networks.[5]

5. Joint advisory highlights increased globalised threat of ransomware

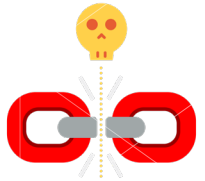
Top Ransomware trends:

Ransomware as a service

Spear phishing

Attacks on unpatched systems

Double extortion



Supply chain attacks

Lifecycle of a Ransomware Attack I

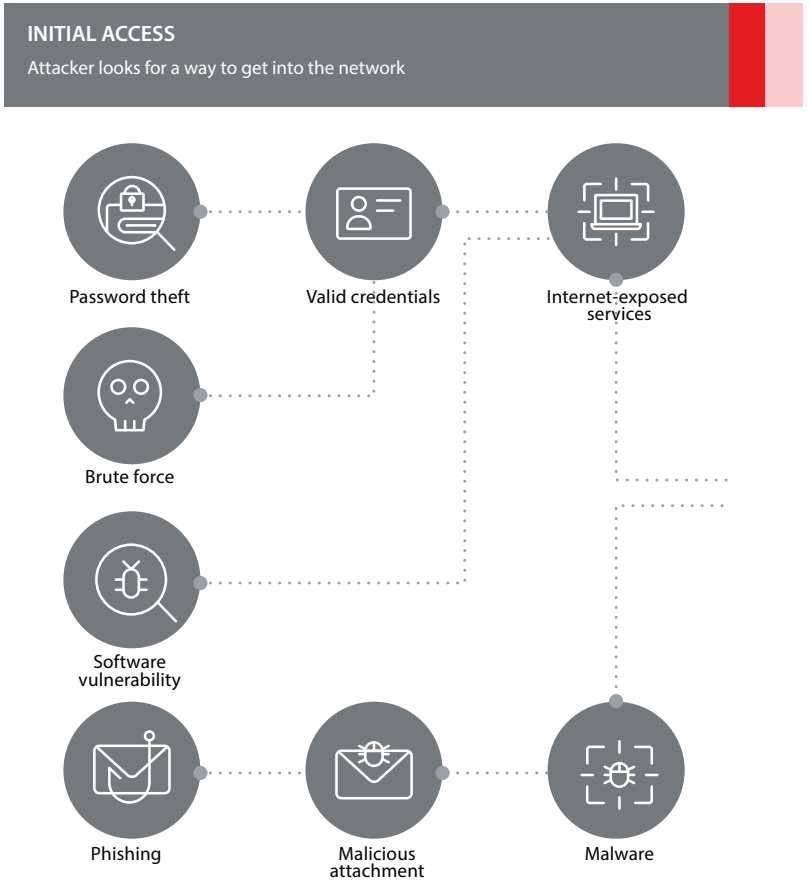
Ransomware follows attack patterns[6] included in the following stages. In most cases, it takes just a few minutes to execute. Even the most harmless action can make the endpoint become a victim of ransomware, and the sensitive data or business-critical files become hostage to extorsion.

Initial access

In the first stage of the attack, cybercriminals are looking to gain a foothold in the organization's network. In most incidents, access is acquired using one of the following infection vectors: password theft, brute force, software vulnerability, or phishing. After sneaking in, the attacker will try to discover critical identities and obtain login credentials that let them keep moving forward, bypassing traditional protection.

Common ransomware attacks use different forms of malware, such as off-the-shelf or custom malware (downloaded for reuse or purchased). Malware is usually propagated through spear-phishing emails that have malicious attachments. These attachments are often trojans in the form of Office or PDF documents but have the ransomware embedded within them. Once opened, and if macros execution is allowed, it can run its payload and attempt to load malware on the computer where the document was opened. Ransomware often seems to come from legitimate sources, including financial institutions, government entities, or users within the organization.

We also have seen many ransomware incidents that started with attackers exploiting vulnerabilities in Internet-exposed services. These have often been in remote access systems such as Remote Desktop Protocol (RDP), virtual private networks (VPNs), and other operating systems or third-party software vulnerabilities. Some attackers also attempt brute forcing credentials to target weak and easy-to-guess usernames and passwords. Most ransomware variants use multiple infection vectors.



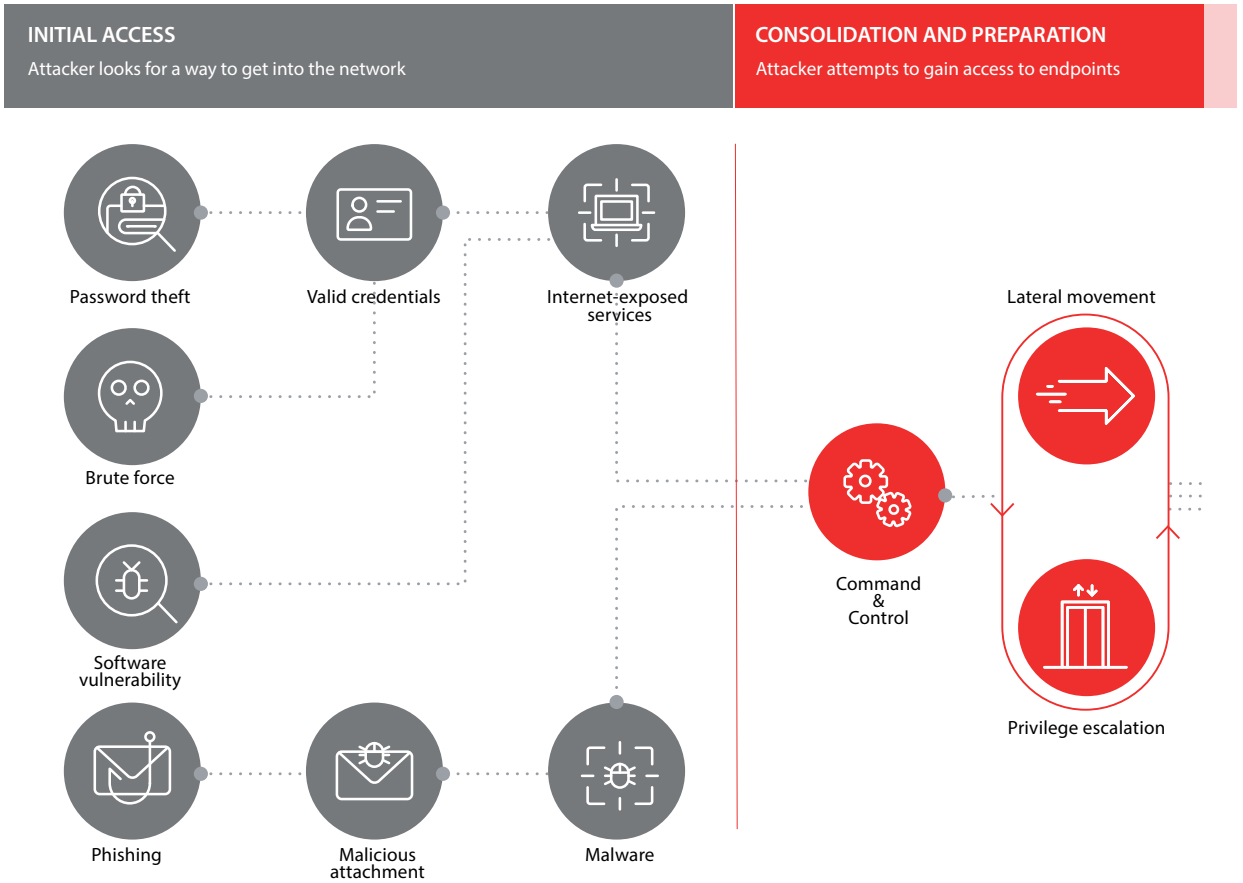
6. How ransomware happens and how to stop it - certnz

Lifecycle of a Ransomware Attack II

Consolidation and preparation

Once they have gained initial access to the network, threat actors require a variety of tools to conduct the attack. They either enter with malware containing a package of all the tools necessary for the attack or, after the intrusion, they download the required tools by establishing communication with a command and control (C2) server to move forward with the next attack steps. This communication is mostly done over trusted traffic like DNS.

C2 tools may also be used to direct the discovery of other endpoints on the network, establish persistence on devices and obfuscate these activities.



Lifecycle of a Ransomware Attack II

Hackers use many tools to carry out the attacks such as:

- Reconnaissance tools that help the attacker understand where they are in the network and what accounts can be targeted further. Examples: Nmap, Process Hacker, and BloodHound
- Credential dumping tools that help compromise the login credentials of other privileged accounts, which the attacker can use to move laterally within the network. Examples: Mimikatz and ProcDump
- Built-in programs such as PowerShell, Windows Management Instrumentation (WMI), and PsExec. Security researchers found that WMI and PSExec commands were being used to delete local backup copies, and PowerShell was being used to create malicious backdoors.

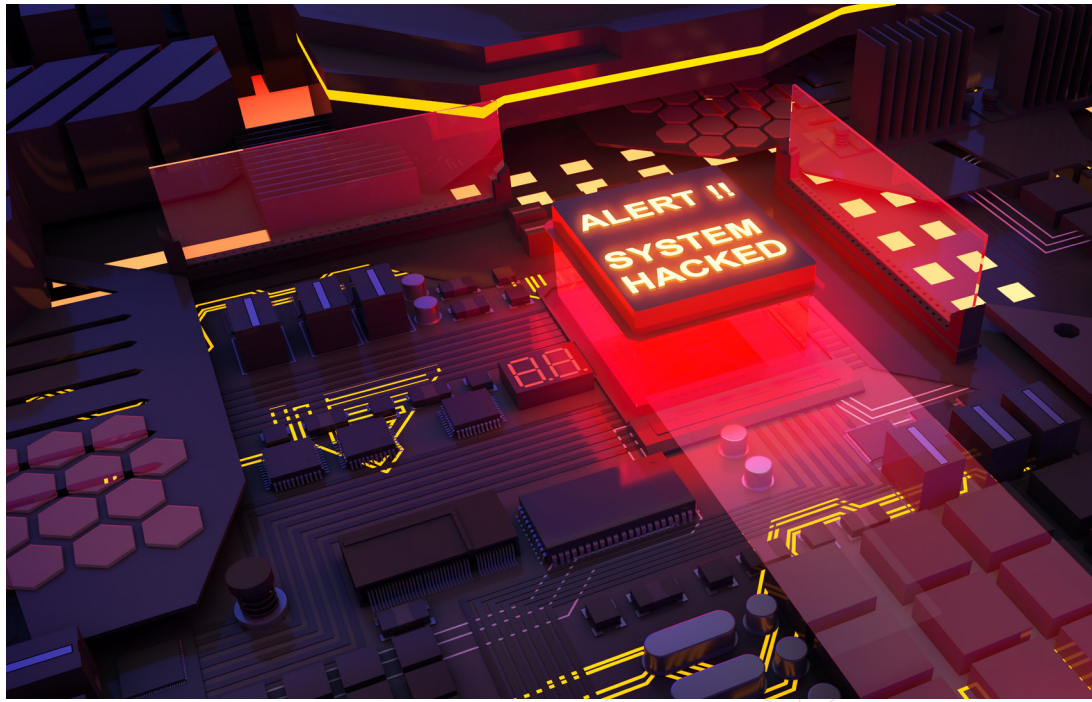
Lateral movement and privilege escalation

Cybercriminals move laterally within the network to find vulnerable privileged accounts. Once the attacker gets access to an account, network, or resource, they escalate the attack by leveraging that access to move through the infrastructure. In this stage, attackers typically carve themselves a path to the most critical data by breaking through security layers and gathering additional privileges.

One of the most common techniques observed in ransomware attacks is the exploitation of administrator accounts. Admin accounts are critical targets because organizations tend to have one common password for all their local admin accounts. By gaining admin privileges, attackers could tamper with security configurations in traditional AV and EDR solutions to disable security controls, avoid detection, and download and install a payload to the victim's endpoint.

Access to domain controllers will also enable them to release malware to all the systems in the network in one shot. Attackers have a range of tactics for gaining domain admin rights, including techniques like Kerberoasting, pash-the-hash attacks, and stealing passwords stored in the SYSVOL folder.

To ensure victim organizations can't easily recover data from their backups, most ransomware attacks involve the destruction of backups.

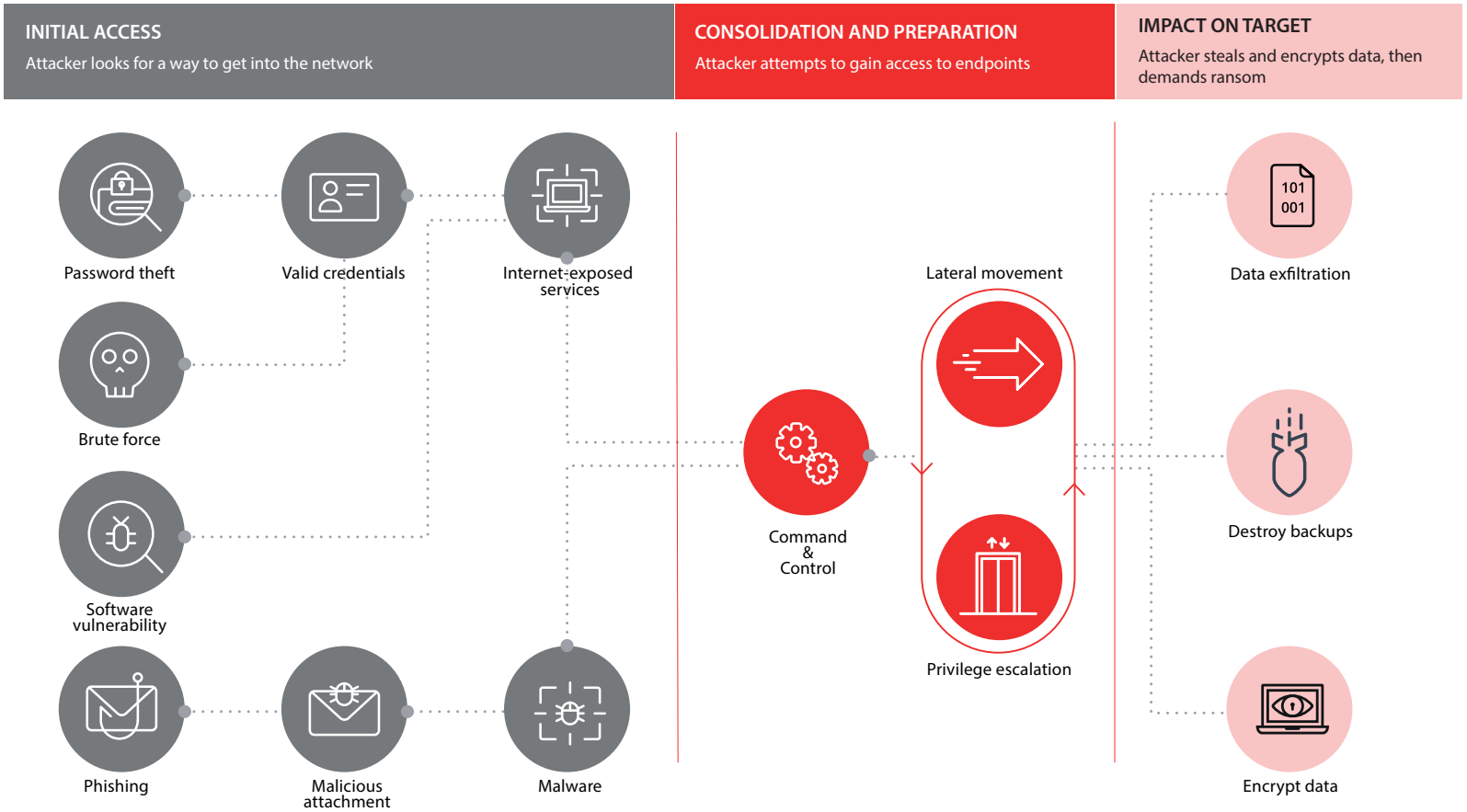


Lifecycle of a Ransomware Attack III

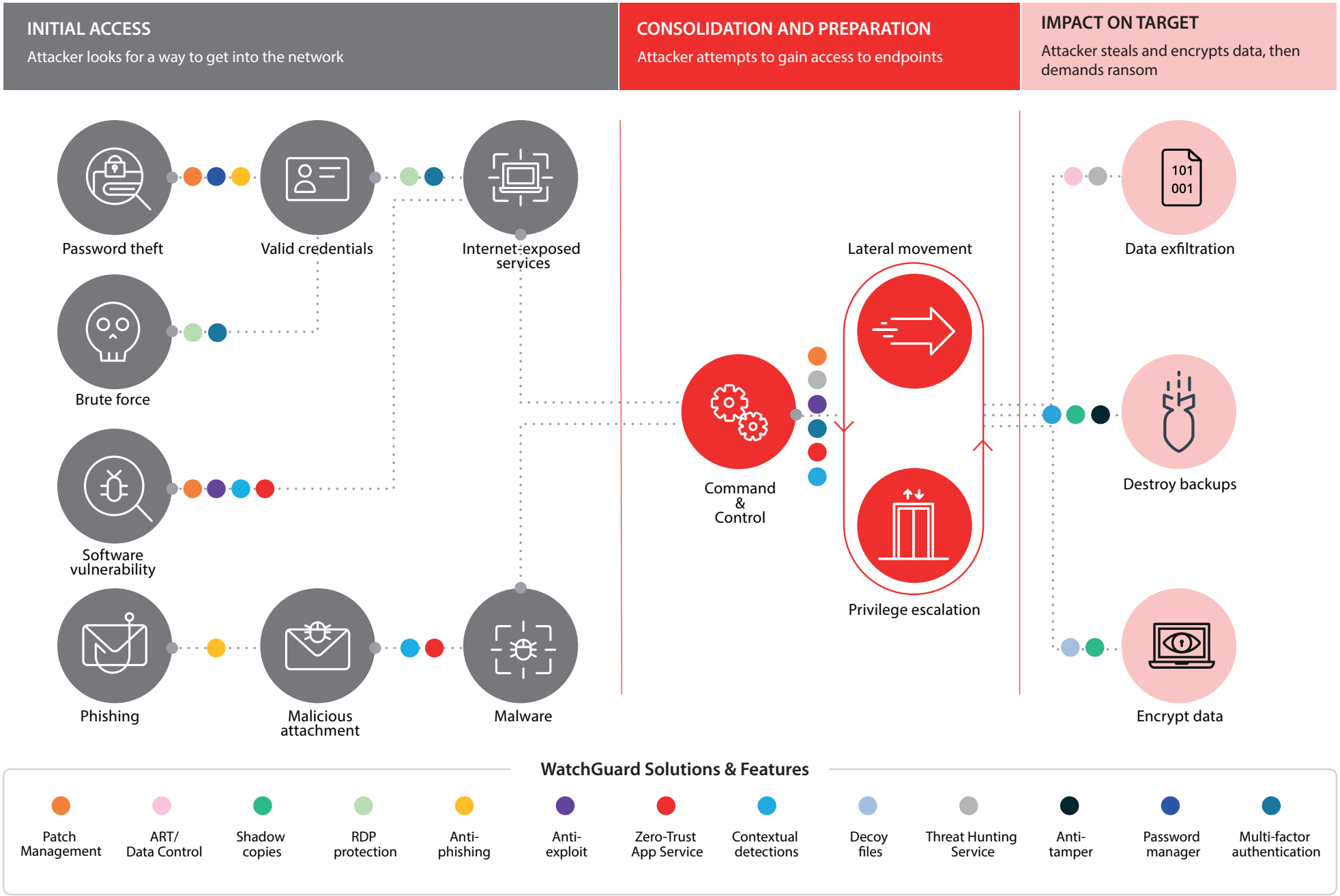
Impact on target

In this final stage of the attack, the ransomware has been downloaded and installed on the victim's system and now starts doing what it was designed to do. Once the attacker has disabled the system's critical protection, it will seek to exfiltrate sensitive information on the endpoint, destroy organization backups and finally encrypt systems and data.

At this point, ransom notes or lock screens direct the victim to the hacker's demand for payment (usually cryptocurrency) and other details to ensure the victim complies with the hacker's instructions. These details will often include an amount of cryptocurrency in exchange for access to the victim's files or a second payment to prevent the attacker from leaking or selling the data.



Stopping Ransomware with WatchGuard Endpoint Security



Prevent incidents before they happen

With ransomware attacks is especially important to prevent the attack before it happens. Once the ransomware is in your organization and starts encrypting the files in your laptops, computers and servers can be too late. The costs associated with a ransomware attack are huge, so the best defense is prevention.

Our unique protection layer contains different protection layers and tens of advanced technologies to protect against ransomware.

Use a strong password manager system

Password security is essential to protecting your organization's data, but many companies fail to implement proper password use and management across their teams. This simple line of defense can drastically reduce the chances of a ransomware attack or any other cyberattack. Organizations that prioritize a robust password management system will be more successful in preventing an attack.

With Password Manager, admins manage all their passwords under one master key, auto-fill forms for speed and ease, synchronize passwords, update passwords, avoid duplications, and provide military security level keys.

Implement multi-factor authentication (MFA)

Ransomware attacks typically start with the theft of a user credential that gives an attacker access to the network or a sensitive business account. AuthPoint, our multi-factor authentication (MFA) solution ensures that attackers can't get where they don't belong with stolen credentials alone by requiring additional factors to prove a user's identity. This minimizes the impact of lost and stolen passwords while giving transparency into user access.

Even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and they will not be able to access the targeted physical space, computing device, network, or database.

Note: Companies looking for cyber insurance will be required to prove they are protecting emails, servers, remote access, and sensitive data with MFA.

Contextual detections

Our Endpoint Security products include behavioral detection to prevent and block fileless attacks based on scripts embedded in Office files as well as attackers using living-off-the-land (LotL) techniques.

It spots the misusage of existing applications at the endpoint that try to bypass the security control and gain access to the system or move laterally to other endpoints. This is a highly effective protection against exploits taking advantage of web browser vulnerabilities and other commonly-targeted applications such as Java, Adobe Reader, Adobe Flash, Office, etc.

Our products include hundreds of contextual detections to stop attacks based on the context. All of these detections are proactive as they are not based on signature files or any other reactive technology.

Part of the context is obtained from Windows AMSI (Anti-malware Scan Interface). The use of AMSI provides our solutions with telemetry and additional information about script and macro execution, improving protection without negatively impacting computer performance.

Decoy files

Decoy files are a honeypot to monitor if some specific files deployed by our solutions are modified. If these files are changed, an event is sent to our behavioral detection engine. It is likely that this action will be classified that ransomware is the root process killed, preventing the file's encryption on the endpoints.

Anti-exploit technology

Anti-exploit technology is an important protection to prevent lateral movements by adding virtual patching capabilities to our EDR solutions. It complements Patch Management solutions by protecting against unpatched applications or those applications that have reached the end of their maintenance period, such as Windows XP or Windows 7.

Unlike other solutions, our anti-exploit includes generic detections based on the anomalous behavior of exploited processes.

Zero-Trust Application Service

Our EDR products are the only solution on the market that classifies 100% of running processes. Any unknown application is blocked until it is validated as trustable by our machine-learning technologies (99.98%) or by our cybersecurity experts worldwide (0.02%). And all is done in real time for unknown applications with the flexibility of adding authorized software with granular rules for those organizations that build their own software.

This protection layer allows us to have malware-based attacks under control, and it is essential for already-infected organizations to stop lateral-movement attacks inside the network.

RDP protection

RDP protection is part of the Threat Hunting Service, and it is available for all customers acquiring our EDR solutions.

Among the cyberattacks that target companies, RDP brute force attacks are the most frequently used by adversaries, especially where systems are directly exposed to the Internet. Our EDR solution detects and protects network computers against attacks that use the RDP (Remote Desktop Protocol) as an infection vector.

When a computer protected by our solutions receives many RDP connection attempts that fail due to invalid credentials, the protection software puts the computer into Initial RDP attack containment mode. In this mode, RDP access to the computer is blocked from IPs outside the customer network that have sent a large number of connection attempts over the last 24 hours.

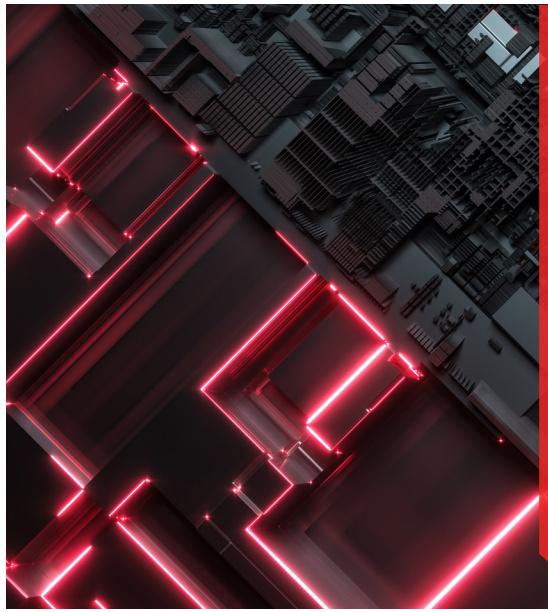
If a computer protected by our EDR solutions receives a successful login attempt from an account that previously failed due to invalid credentials, the account is considered to have been compromised. As a mitigation mechanism, all external RDP connections that have tried to connect at least once with the target computer in the previous 24 hours are blocked.

Anti-malware technologies

As many other next-gen antivirus solutions do, our Endpoint Security solutions include signature files, access to our real-time protection to our Collective Intelligence, and heuristic technologies using deep learning to prevent ransomware attacks not using LotL (living-off-the-land) techniques.

Many ransomware attacks will attempt to freeze the protection installed on endpoints before they try to spread over the network and encrypt files in the whole organization. It is crucial to include anti-tamper protection against hackers trying to stop or suspend services and processes.

Our anti-tampering protection uses proprietary technologies, and it also leverages the ELAM (Early Launch Anti-Malware) technology included in Windows 10, Server 2019, or higher operating systems.



Hackers are constantly looking for holes and backdoors to exploit. By vigilantly updating your systems, you'll minimize your exposure to known vulnerabilities.

Patch to reduce the attack surface

Hackers are constantly looking for holes and backdoors to exploit. You'll minimize your exposure to known vulnerabilities by vigilantly updating your systems.

Ransomware like WannaCry and Petya relied on unpatched vulnerabilities to spread around the globe. The Locky and Cerber ransomware attacks used a flaw in Adobe Flash to distribute themselves to victim workstations.

You can prevent many attacks by ensuring that operating systems and third-party applications are updated and patched. It is essential to patch early and patch often, at least once a month, for critical vulnerabilities.

Anti-phishing protection

Phishing via email is one of the most common methods for starting a ransomware attack. Blocking phishing URLs will help reduce the likelihood that a user clicks a link they shouldn't.

Threat Hunting service

Even a robust EDR solution can't rely on prevention technologies for all detections ...sometimes it just takes a human brain to spot a hacker, especially since the advent of fileless living-off-the-land attacks.

Our Threat Hunting Service identifies abnormal behavior and suspicious activity and their categorization as indicators of attack (IoAs) with a high degree of confidence and without false positives. Usually, they are attacks at an early or at the exploitation stage that do not use malware.

We recommend that you contain or remediate them as soon as possible.

Broad Platform Support

Your security is as strong as the weakest point in your organization's security infrastructure, so it is critical to keep every single endpoint protected.

We support legacy systems starting in Windows XP, and we support systems based on Intel and ARM-based processors.

In addition to Windows, we support macOS and a broad set of distributions in Linux, Android and iOS devices.

Isolate your endpoints to contain the attack

In the event of ransomware infection, the attacker tries to infect the entire network. You can contain the attack by isolating the endpoints affected and avoiding lateral movements from one machine to another by exploiting the vulnerability, using stolen credentials, copying itself and using the SMB protocol, etc.

It would help if you patched as quickly as possible to minimize the impact of the attack and decrease the number of files encrypted in your organization.

Isolated computers can communicate with our servers so you can still manage the security of all the endpoints. You can even add some exceptions and allow them to communicate with specific processes that you need for remediation purposes.

Activate all the prevention technologies

Ensure all the protection layers mentioned before are active and the Lock mode is activated in the advanced protection so as not to allow any unknown applications being executed regardless of where they come from.

Apply remediation actions with 'shadow copies'

Many ransomware attacks go one step further, and apart from encrypting files, they try to destroy all kinds of backups created by the customers.

With our endpoint security solution, you can create shadow copies leveraging the operating system technology, and we will protect them using our anti-tampering technology so you will be able to recover the information after a ransomware infection.

IT professionals use the shadow copies to recover files from critical system failures, but it is also an excellent technology for recovering files encrypted by ransomware.

Contrary to other solutions that make copies of each encrypted file consuming a lot of disk space, shadow copies are optimized only to save the differences. So, the chances of running out of disk space are minimal. Our solution allows you to configure the percentage of disk space dedicated to shadow copies, although the 10% allocated by default should be sufficient in most cases.

10 Ways to Defend Against a Ransomware Attack

1

Perform frequent backups of critical data, system images, and configurations regularly. Test your backups and maintain them offsite and offline where attackers can't find them.

2

Use multi-factor authentication (MFA). Set and enforce strong passwords, managed through a password manager.

3

Limit access to resources over internal networks and enforce time-based access for privileged accounts. Restrict permissions, remove local administrator rights from end users, and block application installation by standard users.

4

Make sure your security solutions are up to date. UTMs with sandboxing can detect malicious files coming into the network.

5

Patch everything, patch early and patch often to keep all operating systems and software up to date. Ransomware attacks like WannaCry and NotPetya relied on unpatched vulnerabilities to spread around the globe.

6

Implement robust anti-phishing protection with different security layers at the endpoint and perimeter.

7

Lock down accessible services at the firewall. If you don't need it, turn off RDP, and use rate limiting, 2FA, VPN, or other remote access tools.

8

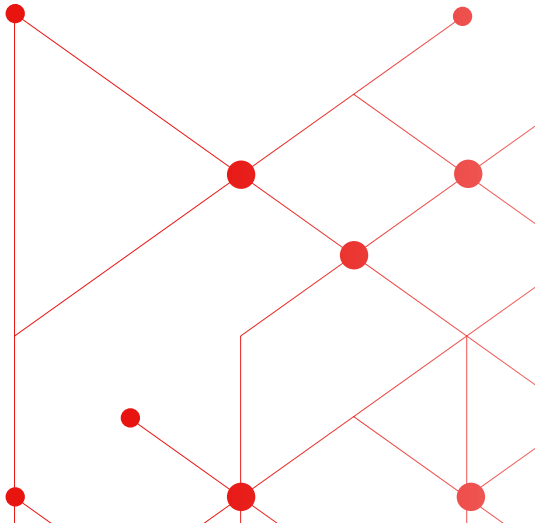
Ensure anti-tamper protection is enabled – Ryuk and other ransomware strains attempt to disable your endpoint protection.

9

Monitor and respond to alerts. Consider implementing advanced endpoint security solutions such as an EDR that includes a zero-trust protection model approach with multiple layers of defense.

10

Raise awareness among users about the risks of phishing and educate them about the dangers of social engineering as part of the best cybersecurity practices.



WatchGuard

Ransomware attacks are growing and more sophisticated than ever. They are a sustainable and lucrative business model for cybercriminals. In some cases, it is easier and cheaper to pay the ransom than to recover from backup, but paying the ransom also does not guarantee that a victim's files will be recovered, or the system will be accessible, and the endpoint will still be infected.

Traditional protection methods relying on malware signatures are not enough against ransomware threats. Indeed, attackers design their ransomware to bypass conventional protection layers. These threats should be managed with a comprehensive security solution that responds to the latest threats.

Now is the time to secure your organization with WatchGuard Endpoint Security from these threats – before the next ransomware attack impacts you.

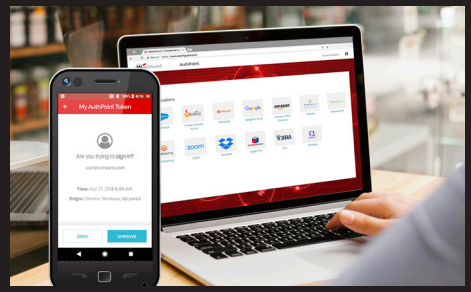
WatchGuard Portfolio

Network Security

WatchGuard Network Security solutions are designed from the ground up to be easy to deploy, use, and manage – in addition to providing the strongest security possible. Our unique approach to network security focuses on bringing best-in-class, enterprise-grade security to any organization, regardless of size or technical expertise.

Secure Wi-Fi

WatchGuard's Secure Wi-Fi solutions, true game-changers in today's market, are engineered to provide a safe, protected airspace for Wi-Fi environments, while eliminating administrative headaches and greatly reducing costs. With expansive engagement tools and visibility into business analytics, it delivers the competitive advantage businesses need to succeed.



Multi-Factor Authentication

WatchGuard AuthPoint® is the right solution to address the password-driven security gap with multi-factor authentication on an easy-to-use Cloud platform. WatchGuard's unique approach adds the "mobile phone DNA" as an identifying factor to ensure that only the correct individual is granted access to sensitive networks and Cloud applications.

Endpoint Security

WatchGuard Endpoint Security is a Cloud-native, advanced endpoint security portfolio that protects businesses of any kind from present and future cyberattacks. Its flagship solution, WatchGuard EPDR, powered by artificial intelligence, immediately improves the security posture of organizations. It combines endpoint protection (EPP) and detection and response (EDR) capabilities with zero-trust application and threat hunting services.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by more than18,000 security resellers and service providers to protect more than 250,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.

NORTH AMERICA SALES 1.800.734.9905 INTERNATIONAL SALES 1.206.613.0895 WEB www.watchguard.com

Part No. WGCE67583_052322