2024

MASTERING RANSOMWARE DEFENCE

YOUR ESSENTIAL GUIDE THAT CICONTINUITY CAN HELP PROTECT AGAINST

CiContinuity

CONTENTS

EXECUTIVE SUMMARY

This guide explores the evolution of ransomware, highlighting the increasing threats and sophisticated tactics employed by cybercriminals. It analyses the most recent ransomware variants, defence strategies, and the essential measures organisations must adopt to safeguard their data and systems.

Ransomware Evolution:

Ransomware attacks have escalated, targeting not only traditional sectors like healthcare, government, and education but also large corporate entities.

Modern ransomware tactics include data exfiltration and extortion, where cybercriminals extract sensitive information and threaten public exposure if ransom demands are not met.

Cybercriminal Strategies:

Ransomware as a Service (RaaS): Cybercriminals offer their ransomware code to affiliates, expanding their operations and sharing profits. This has industrialised ransomware attacks involving multiple parties for maximum gains.

Code Variants and Evasion: Constantly evolving ransomware code includes the use of open-source components and different programming languages to evade detection by security software.

Operational Resilience: When detected, cybercriminals disband and re-emerge under new identities, complicating efforts to track and stop them.

Ransomware Variants:

Ryuk: Known for targeting enterprise environments using email and social media platforms.

SamSam: Exploits vulnerabilities in unpatched servers.

Maze: Combines encryption and data theft for double extortion.

Dharma: Utilizes stolen credentials and targets RDP ports.

REvil and Sodinokibi: Targets antivirus software and leverages sophisticated infection vectors.

Netwalker: Notable for targeting the healthcare sector and employing double extortion.

LockBit: Operates under a RaaS model, is frequently updated, and employs double extortion tactics.

Defensive Measures:

Backup Solutions: Incorporate immutability features, air-gapped storage, and encryption to protect backups from ransomware.

Multifactor Authentication (MFA): Essential for securing user logins and preventing unauthorised access.

Patch Management: Regular updates and patching to close known vulnerabilities.

Network Segmentation: Limiting the spread of ransomware within an organisation.

Employee Training: Educating staff on recognising phishing emails and safe online practices.

CiContinuity's Role:

Providing robust backup solutions with features like immutability, encryption, and air-gapped storage.

Offering comprehensive cybersecurity measures and support to protect against and recover from ransomware attacks.

This guide underscores the necessity for proactive and multi-layered defence strategies to combat the persistent threat of ransomware. Organisations are advised to continually update their security measures, educate their employees, and maintain secure, reliable backup systems to mitigate risks and ensure swift recovery in case of an attack.

DYNAMICS OF RANSOMWARE EVOLUTION

Ransomware attacks are on the rise, posing an increasing danger to organisations worldwide. Due to their weaker cyber defences, cybercriminals initially targeted sectors like healthcare, government, and education, but they have now turned their attention to larger corporate entities. Recent years have seen ransomware incidents impact prominent publicly traded companies like CommScope, Dole, and Western Digital.

These attacks have evolved beyond simple data encryption and ransom demands. Cybercriminals are now extracting sensitive information from compromised systems and using it to extort higher payments from their victims, threatening public exposure of the data if demands are not met. Despite organisations bolstering their cybersecurity efforts, these sophisticated attacks persist.

Key insights from these incidents include the understanding that:

Victims may be more willing to pay substantial ransoms when they see no alternative, often surpassing what is publicly reported.

Many organisations heavily rely on backups for data recovery.

The threat of data exfiltration and public exposure adds another layer of complexity to ransomware response strategies.

Staying ahead of cyber threats demands not only robust cybersecurity measures but also a proactive approach to mitigate risks and respond effectively to emerging tactics employed by cybercriminals.

THE MATURING STRATEGIES OF CYBER BANDITS

As cybercriminals refine their methods to target larger organisations with deeper pockets, they've developed three key strategies to be more effective.

Firstly, they've embraced Ransomware as a service (RaaS), offering their ransomware code to 'affiliates' who carry out attacks on their behalf. This setup lets the original creators expand their operations, offering technical support and tools in exchange for a share of the ransom. This arrangement has turned ransomware attacks into a profitable industry where multiple parties collaborate for maximum gains.

Secondly, cybercriminals constantly tweak their ransomware code to create new variants. They use open-source components or rewrite the code in different programming languages to dodge detection by antivirus software and firewalls.

When law enforcement or cybersecurity firms catch onto their activities, cybercriminals don't just give up. Instead, they dissolve their current operations and resurface under new identities. This makes it harder for authorities to track and stop their activities.

Despite these evolving tactics, cybercriminals still rely on the same vectors to execute attacks. Recognising these methods is crucial to understanding the threats they face and implementing suitable defences. By safeguarding against these tactics and ensuring secure backup solutions, businesses can shield themselves and recover swiftly from any breaches.


Ransomware as a Service (RaaS)
Offering ransomware code to affiliates for a share of the ransom, which helps expand their operations.
STRATEGIES OF THE RANSOMWARE CYBERCRIMINAL
Dissolving and Resurfacing
Dissolving operations and resurfacing under new identities to evade law enforcement.
Constant Code Tweaks
Creating new variants of ransomware to avoid detection by antivirus software and firewalls.

SPOTTING THE THREAT

The table below provides an overview of seven types of ransomware, their targets, attack methods, and their impact.

RANSOMWARE STRAIN(S)	TARGETING
1 Ryuk	Large organisations, public sector
2 SamSam	Healthcare, government
3 Maze	High-value targets
4 Dharma	Various industries
5 REvil	High-profile targets
6 Netwalker	Healthcare, education
7 LockBit	Businesses, public sector

ATTACK METHOD	POTENTIAL CONSEQUENCES	DEFENCES
Phishing, malware (TrickBot, Emotet)	High ransom demands, double extortion	Implement multi-factor authentication (MFA)
RDP vulnerabilities	Operational downtime, financial loss	Modify systems relying of RDP
Double extortion, data theft	Increased ransom pressure, data leaks	Strong email security
Phishing, RDP vulnerabilities	Persistent threat, frequent updates	Close port 3389
Phishing, exploit kits	Severe financial losses, data breaches	Good IT hygiene
Phishing, remote access vulnerabilities	Critical sector disruptions	Phishing awareness
Automated vulnerability	Fast encryption, extensive damage	Regular patching

1 Ryuk

Ryuk is a sophisticated strain of ransomware that first emerged in August 2018. Unlike some other ransomware variants, Ryuk is not distributed indiscriminately. Instead, it is typically deployed in targeted attacks against large organisations, particularly those in sectors such as healthcare, government, finance, and critical infrastructure. Ryuk is believed to be operated by a highly organised cybercriminal group, possibly based in Eastern Europe or Russia.

The modus operandi of Ryuk involves gaining unauthorised access to a network, often through phishing emails or exploiting vulnerabilities in poorly secured systems. Once inside the network, the attackers conduct reconnaissance to identify critical assets and sensitive data. They then deploy the ransomware selectively, encrypting files and demanding payment in exchange for decryption keys. Ryuk's ransom demands are often exorbitant, running into hundreds of thousands or even millions of dollars, making it financially devastating for victim organisations.

PROTECTING YOUR BUSINESS FROM RYUK*

Regular software updates and patch management:

Keep all software and systems up to date with the latest security patches. Software vulnerabilities can often be exploited by cybercriminals to gain access to your network.

Employee training and awareness:

Educate your employees about the dangers of phishing emails and other social engineering tactics commonly used to distribute ransomware. Encourage them to be cautious when opening email attachments or clicking on links from unknown or suspicious sources.

Implement multi-factor authentication (MFA):

Enforce the use of multi-factor authentication wherever possible, especially for remote access to sensitive systems and applications. MFA adds an extra layer of security by requiring additional verification beyond just a password.

Data backup and recovery:

Regularly back up your data and ensure that backups are stored securely and offline. Recent backups can significantly reduce the impact of a ransomware attack by enabling you to restore your systems and data without paying the ransom.

Network segmentation and least privilege access:

Segment your network to restrict access to sensitive systems and data only to those who need it. Implement the principle of least privilege, ensuring that users have only the permissions necessary to perform their job functions.

Advanced threat detection and response:

Deploy advanced security solutions such as endpoint detection and response (EDR) tools, intrusion detection systems (IDS), and security information and event management (SIEM) platforms to monitor suspicious activities and respond swiftly to potential threats.

Incident response plan:

Develop and regularly update an incident response plan that outlines the steps to take in the event of a ransomware attack. This should include procedures for containing the attack, communicating with stakeholders, and restoring operations.

Engage with cybersecurity professionals:

Consider working with cybersecurity experts who can assess your organisation's security posture, identify vulnerabilities, and provide recommendations for mitigating risks associated with ransomware and other cyber threats.

2 SamSam

SamSam is a type of ransomware that was first detected in late 2015. Unlike many other types of ransomware that spread through phishing emails or malicious downloads, SamSam typically infiltrates networks by exploiting known vulnerabilities in systems that have not been patched or updated.

Once it gains access to a network, SamSam attempts to escalate its privileges to gain control over the entire network. It then systematically encrypts files on servers and workstations. The attackers behind SamSam carefully select their targets, often choosing organisations like hospitals, schools, and government agencies, which are more likely to pay the ransom due to the critical nature of their work.

One of the most notable attacks by SamSam was on the city of Atlanta in the United States in March 2018. The attack disrupted numerous city services, causing significant delays and forcing many functions to be carried out manually.

SamSam is known for its high ransom demands, often asking for tens of thousands of dollars, paid in Bitcoin. The group behind SamSam was indicted by the U.S. Department of Justice in 2018.

TO PROTECT AGAINST SAMSAM RANSOMWARE, CONSIDER THE FOLLOWING MEASURES:*

Modify systems relying on RDP:

- Remote Desktop Protocol (RDP) is often exploited by SamSam ransomware. Make necessary changes to systems that rely on RDP for remote communication.[01]

Use firewalls:

- Protect open RDP ports with firewalls to prevent unauthorised access.[02]

Two-factor authentication (2FA):

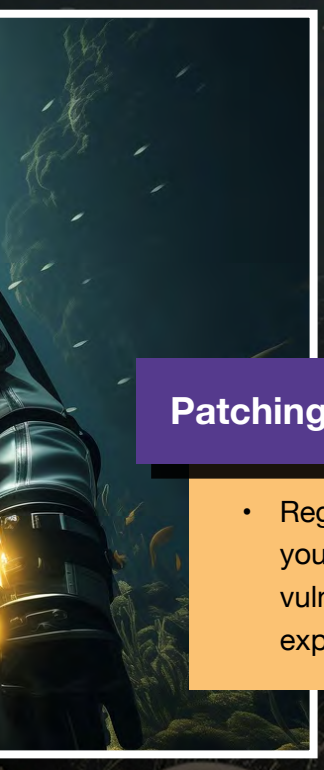
- Require 2FA on all externally-facing applications. This can prevent attackers from gaining easy access.[15]

Implement a password hygiene policy:

- Use strong passwords that are frequently and randomly changed. This can limit the success of brute force attacks.[04]

Secure main attack vectors:

- Ensure that the main attack vectors used by SamSam ransomware, such as RDP and weak passwords, are secured.[05]



Be a small target:

- The best way to avoid trouble is not to be there when it starts. So far, the SamSam attacker has entered networks through exposed RDP servers, so ensure these are well-protected.[06]

Patching and updating:

- Regularly update and patch your systems to fix any known vulnerabilities that could be exploited by the ransomware.[07]

Strong passwords and account lockout policies:

- Implement strong passwords and account lockout policies to defend against brute force attacks. Apply two-factor authentication where possible.[08]

3 Maze

Maze is a sophisticated ransomware first identified in May 2019, notorious for its dual-threat extortion tactics. Unlike traditional ransomware, which solely encrypts data, Maze also exfiltrates data and threatens to release it publicly if the ransom isn't paid. This approach significantly increases pressure on victims to comply with the ransom demands.

Maze typically infiltrates systems through phishing emails with malicious attachments or links, exploiting software vulnerabilities and using compromised Remote Desktop Protocol (RDP) connections. Once inside, it encrypts files, appending a unique extension, often containing the word 'maze,' and then displays a ransom note demanding payment in cryptocurrency, usually Bitcoin.

Maze has targeted various sectors including healthcare, finance, and manufacturing, demanding substantial ransom amounts. It gained notoriety for publicly shaming non-compliant victims by publishing their names and leaking portions of their data on a dedicated website. Despite the group's announcement of shutting down operations in November 2020, the techniques and code used by Maze continue to influence other ransomware groups, highlighting the need for robust cybersecurity measures.[09,10]

TO PROTECT AGAINST MAZE RANSOMWARE, CONSIDER IMPLEMENTING THE FOLLOWING STEPS:*

Strong email security:

- Use email filtering to block phishing emails and malicious attachments.

Regular patching:

- Update and patch software and systems regularly to close security gaps.

Multi-factor authentication (MFA):

- Adds an additional layer of security, making it harder for attackers to gain access.

Frequent backups:

- Maintain secure, frequent backups of all critical data, stored offline or in a separate network.

Network segmentation:

- Limit the spread of ransomware by segmenting your network and restricting access to sensitive areas.

Employee training:

- Educate staff on recognising phishing attempts and other common attack vectors used by ransomware.

4 Dharma

Dharma is a type of ransomware that has been active since 2016. It is known for its high number of variants and its widespread distribution. Dharma ransomware typically infiltrates systems through exposed Remote Desktop Protocol (RDP) connections, using brute-force attacks to gain access.

Once inside a system, Dharma encrypts files and appends a unique extension to the encrypted files, often including the word ‘dharma’. A ransom note is then displayed, demanding payment in Bitcoin in exchange for the decryption key.

Dharma is particularly dangerous because it often targets businesses and organisations, encrypting critical files and demanding high ransom payments. It’s also worth noting that Dharma’s source code was leaked in 2020, increasing the number of attacks as more cybercriminals gained access to the ransomware’s code.

As with all ransomware, the best defence against Dharma is to maintain up-to-date backups of all important files, update systems and software, and educate users about the dangers of phishing emails and unsafe downloads.

PROTECT AGAINST DHARMA RANSOMWARE, CONSIDER THE FOLLOWING MEASURES:*

Close port 3389:

- Dharma often gains access through this port. Shutting it down can prevent the ransomware from entering your system.

Password requirement:

- Set up a password requirement to stop Dharma from gaining access.

Firewall utillisation:

- Use Microsoft Defender Firewall and your network firewall to prevent RPC and SMB communication among endpoints whenever possible.

Regular backups:

- Maintaining regular, up-to-date backups is the best way to avoid damage from ransomware infections.

Isolate infected devices:

- If a device is infected, isolate it from the rest of your network to stop the ransomware from spreading.

Secure remote desktop services:

- Brute forcing remote desktop services is a common attack vector for Dharma Ransomware. Ensure that these services are secure to protect yourself from attack.

For more detailed information, you can refer to the following resources: 11,12,13,14,15

5 REvil or Sodinokibi

REvil, also known as Sodinokibi, is a sophisticated strain of ransomware that first appeared in April 2019. It's believed to be the successor of the infamous GandCrab ransomware, as it appeared shortly after GandCrab was retired and shares many similarities in its code and operation.

REvil is a ransomware-as-a-service (RaaS), meaning its developers rent it out to "affiliates" who carry out attacks and share a portion of the profits. This business model allows for a high volume of attacks and makes it difficult for law enforcement to track down the individuals responsible.

The ransomware typically infiltrates systems through phishing emails, exploit kits, or by exploiting vulnerabilities in remote desktop services. Once inside a system, REvil encrypts files and leaves a ransom note demanding payment in Bitcoin or other cryptocurrencies for the decryption key.

One of the distinguishing features of REvil is its double extortion tactic. Not only does it encrypt files, but it also steals data and threatens to leak it online if the ransom isn't paid. This puts additional pressure on victims to pay, even if they have backups of their encrypted files.

REvil has been responsible for several high-profile attacks, including the attack on Travelex in late 2019 and the attack on the law firm Grubman Shire Meiselas & Sacks in 2020, where confidential data related to numerous celebrities was stolen.

PROTECT AGAINST REVIL OR SODINOKIBI RANSOMWARE, CONSIDER THE FOLLOWING MEASURES:*

Good IT hygiene:

- Do not allow hosts on the internet with exposed RDP port 3389. Disable host-to-host communications as strictly as possible.[16]

Visibility and prioritisation:

- Ensure visibility of your external-facing shadow environment and prioritise resolving high-priority threats.[17]

User awareness:

- Educate your employees about the risks and signs of ransomware attacks. Advise them on safe online practices.[18]

Invest in cybersecurity:

- Use a cybersecurity programme with real-time protection designed to thwart advanced malware attacks.[19]

Multi-pronged approach:

- Implement a multi-pronged approach involving security awareness, email scanning, and regular audits of your IT infrastructure.[20]

Managed detection and response:

- Consider using a managed detection and response service to quickly identify and respond to threats.[21]

Software updates:

- Always keep software updated on all devices to prevent ransomware from exploiting vulnerabilities.[22]

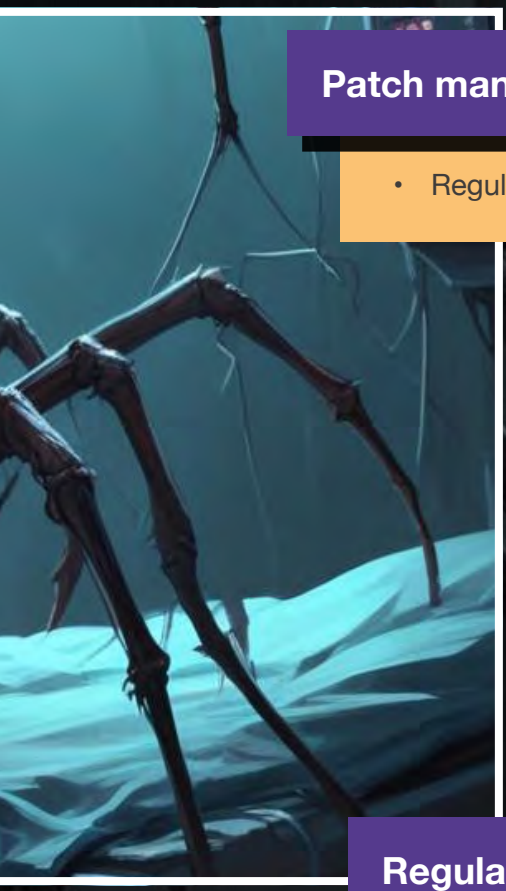
6 Netwalker

Netwalker is a highly disruptive ransomware that emerged in late 2019. It is known for targeting corporate networks, particularly those in the healthcare sector, by exploiting vulnerabilities and using phishing emails to gain initial access. Once inside, Netwalker encrypts the victim's files and demands a ransom, often in Bitcoin, for the decryption key.

Netwalker typically gains access to networks through phishing attacks or exploiting known software vulnerabilities, such as those in VPN systems like Pulse Secure and Telerik UI. Once a system is compromised, Netwalker encrypts files and appends a specific extension to them, then displays a ransom note demanding cryptocurrency payment.

Netwalker has been particularly damaging to the healthcare sector, taking advantage of the COVID-19 pandemic to launch attacks. For instance, it has been known to disrupt the operations of healthcare facilities, making it difficult for them to provide critical services. Netwalker also engages in 'double extortion,' threatening to publish stolen data if the ransom is not paid.[23,24,25]

TO PROTECT AGAINST NETWALKER RANSOMWARE, CONSIDER THE FOLLOWING MEASURES:*



Phishing awareness:

- Educate employees on how to recognise and avoid phishing emails.

Patch management:

- Regularly update and patch systems to close known vulnerabilities.

Multi-factor authentication (MFA):

- Implement MFA to add an extra layer of security.

Network segmentation:

- Segregate your network to prevent the spread of ransomware.

Regular backups:

- Maintain encrypted and offline backups of critical data.

Incident response plan:

- Develop and regularly update an incident response plan specifically for ransomware attacks.

7 LockBit

LockBit is sophisticated ransomware that has become one of the most prolific variants globally. It operates under a Ransomware-as-a-Service (RaaS) model, attracting affiliates to carry out ransomware attacks. This model has enabled LockBit to evolve and adapt continuously, making it a significant threat across various sectors.

Key characteristics and techniques

- **RaaS model:** LockBit functions as a RaaS, allowing affiliates with varying technical skills to deploy ransomware using a simplified, point-and-click interface. This democratisation of ransomware has led to a wide range of attacks across different sectors.
- **Double extortion:** LockBit employs a double extortion strategy, where attackers first encrypt the victim's data and then exfiltrate it. They threaten to release the stolen data publicly if the ransom is not paid, increasing pressure on victims.
- **Frequent updates:** LockBit has undergone multiple iterations, including LockBit 2.0 and LockBit 3.0, each introducing new features and capabilities to enhance its effectiveness and bypass defences.[26,27,28]

LockBit has targeted various critical infrastructure sectors, including healthcare, financial services, education, and manufacturing. The ransomware has been involved in numerous high-profile incidents globally. For instance, in 2022, it was the most deployed ransomware variant, and its affiliates have continued to attack organisations in 2023.[29,30]

TO PROTECT AGAINST LOCKBIT RANSOMWARE, ORGANISATIONS SHOULD IMPLEMENT THE FOLLOWING MEASURES:*

Regular patching:

- Keep all systems and software up to date to close known vulnerabilities.

Employee training:

- Educate staff about phishing attacks and safe online practices to reduce the risk of initial infection.

Multi-factor authentication (MFA):

- Implement MFA to add an extra layer of security and reduce the risk of unauthorised access.

Network segmentation:

- Segregate networks to limit the spread of ransomware if an infection occurs.

Backup strategies:

- Maintain regular, secure backups of critical data, stored offline or in a separate network, to ensure recovery in case of an attack (CISA) (CISA).

DEFENDING AGAINST THE ATTACK VECTORS

Ransomware has been around for over 20 years, but its evolution continues to challenge organisations. Learning from early versions isn't always helpful in stopping today's attacks. The most dangerous ransomware strains started emerging in 2018.

As ransomware evolves, it finds increasingly cunning ways to infiltrate organisations and launch attacks. Here are six common attack vectors ransomware uses to breach or target organisations:

Email/Social media

Email and social media platforms are major entry points for ransomware into organisations. They both exploit open Internet ports used by staff for web access and email. Cybercriminals often send spam emails with attachments or phishing links to lure unsuspecting recipients. They use similar tricks on social media, utilising email and messaging features. Ryuk was the first ransomware to use email within organisations, but now, most variants use this tactic.

Once inside, ransomware behaviour has evolved. Cybercriminals tailor their code for enterprise environments and specific targets.

Antivirus software

Some ransomware strains, like REvil and Sodinokibi, target antivirus software. They enter organisations through phishing emails and then attempt to compromise the antivirus software. The recommended defences are the same as for the first vector: air-gapped backups, immutable storage, and instant restores.

Critical server processes

Strains that target critical server processes, enter through spam emails and then terminate server services and processes. The recommended defences include air-gapped backups, encrypted backups, immutable storage, instant restores, and multi-factor authentication (MFA) for backup login.

Usernames and passwords

Some ransomware strains, like Dharma, use stolen usernames and passwords for their attacks. They often target Windows RDP TCP port 3389. The recommended defences include air-gapped storage, immutable storage, and MFA for backup login.

Unpatched servers

Strains like SamSam exploit known vulnerabilities in unpatched servers. They enter organisations through Windows RDP in conjunction with usernames and passwords. The recommended defences include air-gapped backups, encrypted backups, immutable storage, instant restores, and MFA for backup login.

Endpoint devices

Some ransomware strains target endpoint devices such as cell phones, tablets, and Internet-enabled devices. The recommended defences include air-gapped backups, encrypted backups, immutable storage, instant restores, and MFA for backup login.

In addition to these specific defences, we also recommend general best practices for combating ransomware, such as using secure storage, authenticating backup solution logins, and having robust restore and recovery options.

THE UNAVOIDABLE THREAT

These six attack vectors are just a few of the ones discussed by law enforcement and cybersecurity firms. There may be other undetected vectors or ones that agencies are only starting to disclose. For example, in 2021, researchers found a new ransomware strain that targets and encrypts Linux systems. It has been active since at least March 2022.

The constant evolution of ransomware strains and the emergence of new ones create challenges for organisations. Ideally, they want to prevent ransomware attacks rather than deal with the aftermath. However, this goal becomes increasingly difficult as ransomware evolves rapidly, with new strains appearing regularly. Additionally, human error within organisations or the addition of new endpoint devices can compromise security at any time. This means no organisation can guarantee complete immunity from a ransomware attack.

While prevention is preferable to recovery, organisations must prepare for the possibility of an attack succeeding. They can never be completely sure they've closed all cybersecurity gaps. Even if they have, cybercriminals may obtain usernames and passwords that bypass existing defences.

These reasons underscore the importance of selecting a backup solution with two key characteristics. First, it must defend against ransomware attacks and protect data. Second, it should provide features to restore data and recover applications effectively.

STRENGTHENING BACKUP SOLUTIONS AGAINST RANSOMWARE ATTACKS

To tackle the growing threat of ransomware, backup solution providers have introduced several upgrades. These enhancements are designed to safeguard the backup system and data against ransomware attacks while also offering more efficient data restoration and application recovery options.

SECURE STORAGE

Backup solutions now incorporate immutability features to protect backups from ransomware. Cloud object storage from providers and on-premises object-based storage devices support object lock functionality, ensuring backups remain unaltered. Some NAS storage devices also offer data immutability features.

Storing backups on air-gapped media like tape adds an extra layer of defence against ransomware. Despite potential drawbacks, the tape creates an air gap shielding backups from attacks. Certain disk storage devices offer logical air gap features, making stored data invisible on the network except to authorised software. This enhances security without sacrificing retrieval speed.

Encryption of backups, whether stored on standard devices or in immutable formats, is recommended. This measure prevents cybercriminals from accessing and deciphering backup data, reducing the risk of data theft or manipulation.

MULTIFACTOR AUTHENTICATION

Ransomware strains are becoming more sophisticated. They attempt to infiltrate and manipulate backup software. Once inside, they can wreak havoc by deleting or encrypting backups, altering backup jobs, or redirecting backups to cybercriminal-controlled cloud storage.

Backup solutions now offer various protection options to defend against unauthorised access. Many support multifactor authentication (MFA), requiring users to provide a second code alongside their password for login, adding an extra layer of security.

Some solutions take additional precautions to recognise the criticality of backup data. For example, when making significant changes like adjusting backup schedules or deleting backups, a second backup administrator's authorisation may be required to ensure the integrity of the process.

RESTORING AND RECOVERING DATA

Ransomware strikes can happen unexpectedly anywhere in organisations, making it difficult to gauge their impact. However, the speed and extent of data restoration and application recovery are directly affected by the encrypted data and compromised systems.

Backup solutions now provide enhanced options for data restoration and application recovery. They support storing data on multiple media types with varying performance characteristics, allowing organisations to quickly retrieve data when needed.

Some organisations cannot afford to wait for data restoration in urgent cases where production must resume immediately. Backup solutions address this need with instant restore functionality. This feature enables access to files stored on backup media or even running applications directly from backups. Additionally, some solutions facilitate live migrations of recovered production applications from backups to the production environment.

BACKUP SOLUTIONS: CRUCIAL DEFENCE AGAINST RANSOMWARE

Any organisation assuming immunity from ransomware is at risk. Ransomware evolves rapidly, making it challenging to defend against every attack. While maintaining strong cybersecurity defences is vital, organisations must also prepare for the possibility of breaches.

In the event of an attack, time is of the essence for data restoration and application recovery. Hence, having a reliable backup solution is essential. A robust backup solution should safeguard itself and backups from multiple ransomware attack vectors. This includes storing backups in an immutable format, securing user logins, and encrypting data to prevent leakage.

Furthermore, it should offer various data restore and application recovery options to swiftly restore operations.

While no organisation wants to face a ransomware attack, threats are numerous and unpredictable. Choosing a backup solution with these features equips organisations to withstand attacks and recover quickly when needed.

HOW CAN CICONTINUITY PROTECT YOU?

CiContinuity helps businesses achieve the ultimate peace of mind regarding their critical data and applications. Our range of fully managed cloud backup and disaster recovery services has enabled organisations to be secure, safe, and productive for over 25 years.

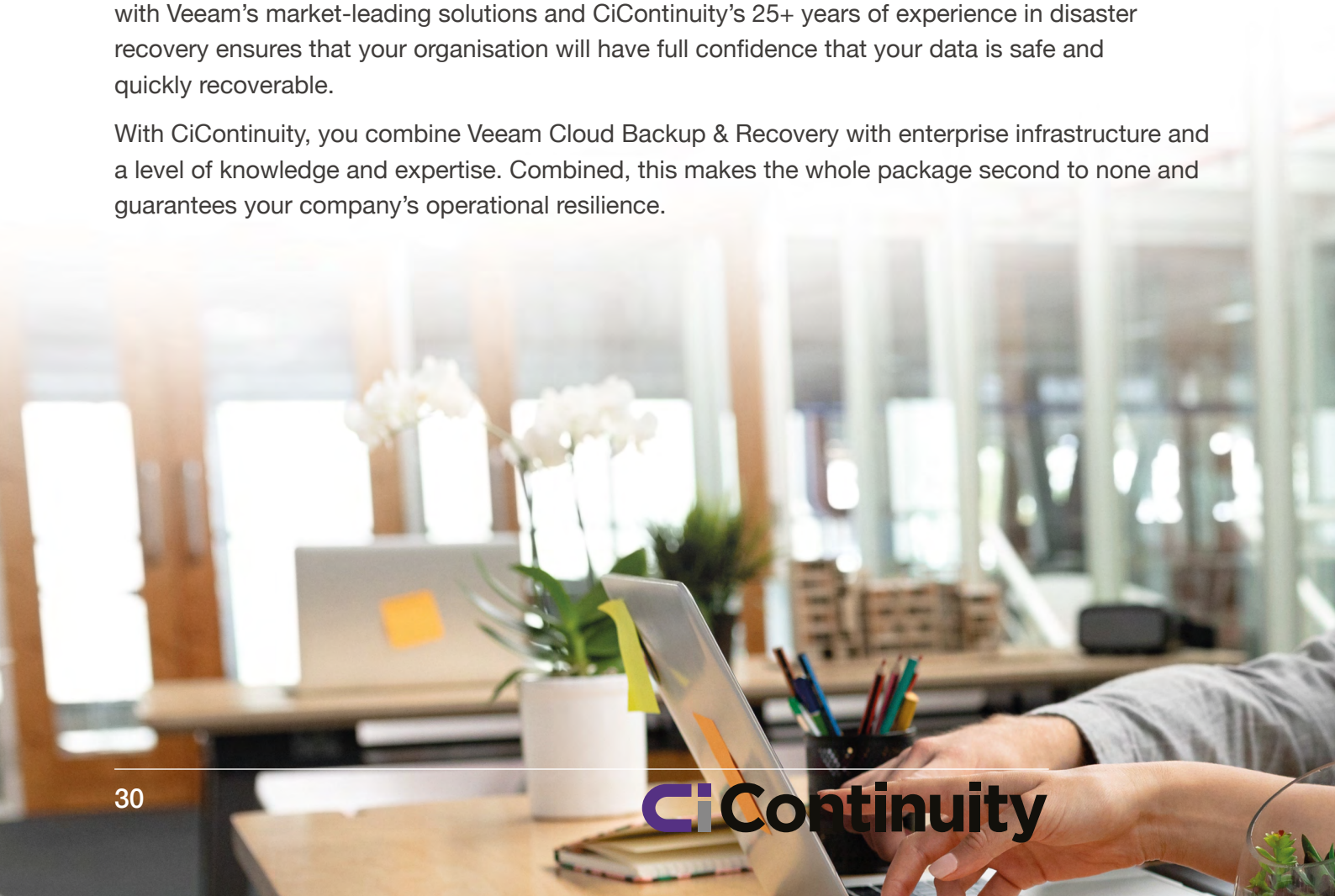
At CiContinuity, we are an official Veeam Cloud Service Provider (VCSP). Veeam is a global leader in backup solutions, and together, we deliver seamless cloud management for virtual, physical, and multi-cloud infrastructures through our Veeam Cloud Backup & Recovery solutions.

Through this relationship, we provide our customers with Veeam licensing, solution design and implementation, and managed services.

Suppose you are already using Veeam for your disaster recovery. In that case, our Veeam-Cloud environment can be used as a second or third target for your data for added security and to provide functionalities such as off-site air-gapped and immutable data copies.

CiContinuity's Veeam environment is located in our CiCloud. Combining this enterprise infrastructure with Veeam's market-leading solutions and CiContinuity's 25+ years of experience in disaster recovery ensures that your organisation will have full confidence that your data is safe and quickly recoverable.

With CiContinuity, you combine Veeam Cloud Backup & Recovery with enterprise infrastructure and a level of knowledge and expertise. Combined, this makes the whole package second to none and guarantees your company's operational resilience.



Here are some of the ways Veeam protects against ransomware:

Immutability: Veeam uses storage technology to create immutable backups. This means that once the backup is created, it cannot be changed or deleted, protecting it from ransomware attacks that attempt to encrypt or delete backup data.

Encryption: Veeam allows for the encryption of backups. This ensures that even if data is somehow accessed, it cannot be understood without the encryption key.

Access control: Veeam recommends using different credentials for backup storage and limiting access to backup data. This reduces the risk of ransomware gaining access to backups through compromised credentials.

Verification: Veeam allows for regular verification of backups. This ensures that your backups are not only secure but also reliable and ready to be used in the event of a recovery.

Air-gapped and offline storage: Veeam supports storing backups in an air-gapped or offline environment. This means the backup data is not continuously connected to the network, making it inaccessible to ransomware attacks.

SafeMode snapshots: A built-in feature that enables you to create read-only snapshots of backup data and associated metadata catalogues after you've performed a full backup. You can recover data directly from these snapshots, helping guard against attacks by ransomware and even rogue admins.

Disaster recovery plan: Veeam encourages the implementation of a comprehensive DR plan to ensure business continuity in the event of a ransomware attack.

SOURCES

01,02 **PNJ Technology Partners:** 10 Tips To Guard Against SamSam Ransomware

03 **Heimdal:** SamSam Ransomware 101: How It Works and How to Avoid it

04 **BlackBerry:** Pro Tips on How to Avoid a SamSam Ransomware Infection

05 **Coveware:** What Is SamSam Ransomware and How to Recover and Remove It [Guide]

06 **Naked Security:** How to defend yourself against SamSam ransomware

07 **Comodo Antivirus:** SamSam Ransomware: Definition and Prevention

08 **Cybersecurity & Infrastructure Security Agency:** SamSam Ransomware

09 **Stop Ransomware:** Ransomware 101

10 **Stop Ransomware**

11 **Comparitech:** What is Dharma Ransomware & how to protect Against It?

12 **Heimdal®:** Dharma Ransomware Analysis: Origins, Operation Mode

13 **Microsoft Tech Community's:** Dharma Ransomware: Recovery and Preventative Measures

14 **PCrisk:** What is Dharma ransomware?

15 **Coveware:** How to Protect Your Business From Dharma Ransomware

16 **CrowdStrike:** Under Attack: Protecting Against Conti, DarkSide, REvil and Other Ransomware

17 **CybelAngel:** Identify and Prevent a Ransomware Attack: REvil Soddinokibi Use Case

18 **Heimdal:** Dharma Ransomware Analysis: Origins, Operation Mode

19 **Malewarebytes:** All about ransomware attacks

20 **Mimecast:** How Sodinokibi/REvil Ransomware Takes On The World

21 **Critical insight:** Stop Ransomware like REvil with Managed Detection and Response

22 **Securelist:** REvil ransomware attack against MSPs and its clients around the world

23,24 **Securelist:** Stop Ransonware

25 **Securelist:** NetWalker Ransomware

26 **America's Cyber Defence Agency:** Understanding Ransomware Threat Actors: LockBit

27 **America's Cyber Defence Agency:** CISA and Partners Release Joint Advisory on Understanding Ransomware Threat Actors: LockBit

28 **America's Cyber Defence Agency:** FBI, CISA, and MS-ISAC Release #StopRansomware: LockBit 3.0

29 **America's Cyber Defence Agency:** Understanding Ransomware Threat Actors: LockBit

30 **America's Cyber Defence Agency:** Official Alerts & Statements - FBI

31 **America's Cyber Defence Agency:** Understanding Ransomware Threat Actors: LockBit

32 **America's Cyber Defence Agency:** FBI, CISA, and MS-ISAC Release #StopRansomware: LockBit 3.0

33 **CiCloud & Continuity Services:** Veeam Cloud Backup & Recovery

CiContinuity

advice@cicontinuity.co.uk 01256 378000 centerprise.co.uk centerprise international

Partner with CiContinuity

Choose CiContinuity as your partner for success. With CiCloud Backup and Recovery, your data is protected by the industry's best. Contact us today to learn how we can transform your data protection strategy.

cicontinuity.co.uk

Elevate your data protection strategy with CiContinuity's CiCloud Backup and Recovery – because your organisation deserves nothing less than the best.

* Remember, no single solution can provide 100% security against ransomware or other cyber threats. It's important to follow best practices for cybersecurity, including regular patching, user education, network security measures, secure storage, authenticating backup solution logins, and a robust backup and recovery options. **Always consult with a cybersecurity professional for tailored advice.**

CiCenterprise INTERNATIONAL

info@centerprise.co.uk 01256 378000 centerprise.co.uk centerprise international