covenco
DATA MANAGEMENT & INFRASTRUCTURE 365

COVENCO GUIDE

Ransomware Attack Recovery Service

How the Covenco Ransomware Recovery Service helps organisations avoid and recover from an attack.

Version 1.1 September 2023

RECOVERING FROM A RANSOMWARE ATTACK WITH HELP FROM COVENCO.

Covenco understands how devastating a successful ransomware attack can be. An impacted customer will likely be dealing with sprawling business and logistics issues as a result of the attack.

Covenco handles ransomware attacks as a top priority to facilitate recovery efforts and mitigate further risk. When a customer invokes the Covenco Ransomware Recovery Service, our team responds with immediate round-the-clock virtual and physical assistance.

Unlike other competitor programs, Covenco deploys physical assets and ‘boots on the ground’ to quickly stop and contain any attacks affecting your data.

The Covenco core recovery virtual team comprises incident leaders, senior engineers, and data management specialists.

Covenco has helped many customers successfully recover from ransomware attacks.

As a result, Covenco has developed a set of best practices to help other customers plan for, identify, and re-mediate ransomware attacks.

THE NEED FOR CYBER RESILIENCE

While ransomware attacks are escalating daily, Covenco customers can quickly and effectively recover their data to minimise damage to their business.

Covenco's Data Security Solution Powered by Veeam.

Our Data Security Solution leverages Veeam Technology. The core architecture of the Covenco platform is based on Solutions that include Veeam Backup & Replication and Veeam ONE, designed to keep your data accessible and secure.

Veeam Backup & Replication is a single backup recovery and data solution for all workloads, both on-premises and in the cloud.

By applying Veeam Backup & Replication, Covenco can deliver a single platform and a powerful aid to secure and protect your data, keeping you closer to business continuity if disaster strikes.

Covenco also implements Veeam ONE alongside Veeam Backup & Replication to enhance our real-time monitoring capabilities while giving you robust business documentation and management reporting. These solutions keep you GDPR compliant by constantly tracking and monitoring your data.

Remediation Services

Once your data is written to the Covenco Cloud Backup Platform with an air-gapped and immutable architecture, it cannot be modified or encrypted by an attack, ensuring that a clean copy is readily available for recovery. It is also possible to lock the data to prevent bad actors from expiring backups early. Multiple recovery options are built-in to every Covenco Recovery Solution, so we can quickly recover your files and workloads if an attack impacts them.

Immutable data backups

Covenco has made your security a key tenant of our backup and recovery solutions since 2017. Our Veeam-based architecture also used solutions from partners such as Zadara to deliver immutability for those customers who request complete recoverability. We also offer a logical air gap to protect customer data from external threats and internal attackers.

Our Veeam-enabled solutions allow users to offload a backup copy to Object Storage as soon as it is created in the Performance Tier or with Veeam Data Platform V12 for backups to go straight to Object Storage.

Combining this with Object Lock on Zadara enables a protection mechanism that reduces the window of opportunity for ransomware while providing a long-term or off-site backup copy. This simplifies the means for providing a comprehensive 3-2-1-1-0 backup rule policy while increasing security against malware.

Leveraging Zadara's Object Storage allows our customers to take advantage of the multi-tenant isolation of both Zadara and Veeam.

Covenco and Veeam deliver:

- Rapid recovery and long-term data retention on-premises and in the cloud, allowing you to meet regulatory compliance requirements with optional local and remote snapshot capabilities.
- Virtual Network Interfaces, providing isolated tenant access to storage resources.
- Air-gapped architecture, reducing the attack footprint.
- Object Lock data immutability to protect against deletion and overwriting, providing an 'air gap' architecture.
- ISO 27001 compliance
- SLA driven service
- On-demand 24/7/365 expert support

Backup data is the last line of defence and the key to recovering from a ransomware attack.

Covenco's approach makes it easy for customers to implement a rigid security posture for data management while freeing up your data, administration, and IT staff to concentrate on mission-critical tasks.

Our comprehensive data backup and recovery platform gives customers guaranteed confidence that they can quickly and reliably recover from an attack.

This guide outlines Covenco's Ransomware recovery Services, including how our built-in capabilities make secured data almost immune to ransomware.

We also explore our Data Protection Solutions, which will help your organisation regain critical business data quickly and safely should a successful attack occur.

PLAN FOR, IDENTIFY & REMEDIATE RANSOMWARE ATTACKS

The Covenco ransomware Recovery Service pro actively supports customers with additional support to help reduce the likelihood and impact of a cyber attack:

Incident Response Plan and Policy Writing

Covenco will work with your organisation to create an Incident Response policy and plan tailored to your organisational needs and aligned to industry best practices. The program will outline your security team's tools and procedures to identify, eliminate, and recover from cybersecurity threats. By having a well-planned and documented policy and response plan, you can ensure an expedient response when it is needed most.

Tabletop Exercises

Regular practice of your organisation's response to a cyber incident means teams are likely to respond more effectively under the pressure of an actual cyber incident. This engagement has been designed to test your organisation's incident response plan. Covenco carefully crafts bespoke scenarios based on the biggest threats to the organisation. Multiple strategies are used during the engagement to test your team's thought process and decision-making skills. At the end of the engagement, our report identifies any areas that may require improvement or present risk.

Incident Response Maturity Assessment

Covenco's Incident Response Maturity Assessment delivers valuable insight into your incident response capabilities, covering people, processes, and technology. The assessment includes benchmarking your current capability against a robust incident response capability framework. Analysis of the results will provide recommendations that can be used as a roadmap toward improvement. The assessment will also include a review of your existing logging capabilities and suggestions on how to enhance them to maximise the capability of any SIEM or SOC solutions you have in place.

Playbook Review

Response to Cyber incidents requires a well-planned and repeatable process. Using playbooks, we ensure your security team knows what to do in a particular event. This engagement has been designed to support maturing security teams by reviewing in-use playbooks and providing guidance on best practices and how to optimise processes to reduce incident volumes.

Cybersecurity First Responder Training

This one-day training course prepares your cybersecurity team to act effectively and efficiently against a cyber-attack. Ensuring that your team has the correct knowledge to be able to react to a cyber incident can help minimise and ensure an expedient response.

Ransomware Resilience Assessment

The threat from ransomware has increased significantly over the past years, with different techniques adopted by threat actors and ransomware as service operators.

Covenco has designed this service to assess an organisation's current preparation, security technologies and backup strategy to ensure that it can recover from a ransomware attack. This also sets an organisation's security posture to prevent and detect attackers' intent on widely distributing ransomware across the organisation's endpoints.

A successful ransomware attack can cause an organisation critical impacts and lengthy recoveries across its business services and operations.

Threat Hunting

This proactive service complements a penetration test to assure the organisation that they have not been compromised.

A penetration test is used to identify weaknesses in the organisation's infrastructure. A threat hunt can use the findings of this report to complete targeted bunting' to see if any of these weaknesses have been exploited and if an attacker is hiding in the infrastructure.

Compromise Assessment

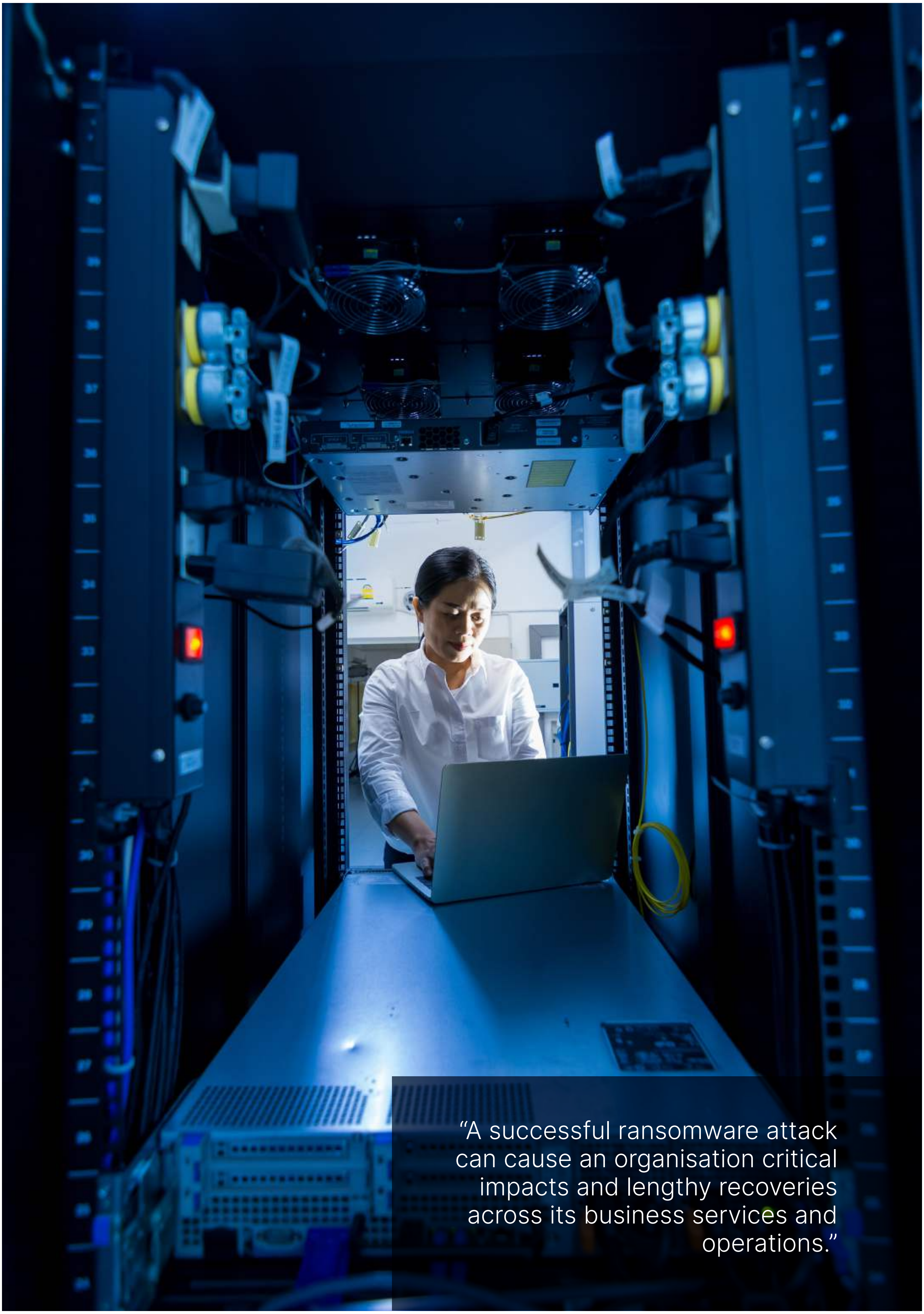
This is a reactive engagement when an organisation suspects its infrastructure could have been compromised.

This service can be called upon to provide confidence that a zero-day or critical vulnerability has not been exploited. This assessment has been designed to discover unknown security breaches, malware, and signs of unauthorised access.

The Covenco Ransomware Recovery Service

The Covenco Ransomware Recovery Service helps customers before, during and after a ransomware attack.

- Certified experts on hand 24/7/365 working with your IT team to support your business in response to any cyber-attack.
- Expert advice and guidance covering technical remediation, incident management, risk and business continuity during any incident.
- Dramatically reduce the time and cost impacts of an incident. Maintaining productivity while our specialists resolve any incidents.
- Complete containment of threats to prevent them from sprawling.
- Early and rapid incident resolution to prevent data loss from any compromised systems.



“A successful ransomware attack can cause an organisation critical impacts and lengthy recoveries across its business services and operations.”

AVOIDING RANSOMWARE

The following steps outline our recommended approach to avoiding ransomware.

There are many additional processes that can be employed, but these are the primary measures to safeguard your systems and data. Covenco helps customers deliver and improve upon these processes:

Preparation

Organisations put themselves in the best position for success when they prepare for a ransomware attack ahead of time. The following steps can be useful in preventing or dealing with a ransomware attack:

Build a Plan

Develop a ransomware response and recovery plan and supporting playbook. A comprehensive plan developed before an attack is critical to a successful outcome. This plan should be updated and reviewed periodically.

Additionally, you should store this plan in a secure location that ransomware cannot compromise. A printed copy is suitable for this. Following an established procedure during an attack will limit confusion as everyone will know what to do. Also, a plan will help expedite the identification and clean-up of the ransomware by reacting efficiently and effectively.

The plan should identify key stakeholders across management, public relations, IT, system/application teams, etc., who will execute and manage the incident response. Ensure those people know their responsibilities and how to complete their portion of the recovery plan. A key success factor is timely and thorough internal communication within the affected organisation.

The aftermath of a cyber-attack is stressful, and all concerned parties must know their role in recovery. The recovery plan should be tested regularly to identify potential gaps or improvement opportunities. A well-rehearsed team is in the best position to recover confidently when the attack occurs.

Covenco can help you engage with a reputable, experienced digital forensics and incident response service provider if an attack or suspected attack occurs. These vendors can provide critical assistance with determining the blast radius and neutralising the attack. Subsequently, they can help with data validation to help orchestrate a safe time to recover. Your cyber insurance provider may provide this service or recommend a third party for the role.

Finally, the plan should include methods of communication that will be available during a ransomware event. An attack may cause an impact on corporate email and phone systems, so plan for alternate means of communicating both internally and with outside vendors such as Covenco.

Prioritise Critical Data and Systems

Identify the criticality of each system to the business and any dependencies. Knowing which systems need attention first and how they interact with other business systems will allow a smooth and orderly recovery. For example, foundational infrastructure services must be operational before applications and lines of business can be restored.

Services in this category typically include Active Directory, DNS, DHCP, NTP, and certificate servers. Based on each system's criticality level, document a recovery plan of which systems would be recovered and in which order. As crucial as those fundamental services is knowing what sensitive data you have and where this resides.

Covenco Sensitive Data Monitoring & Management can provide visibility into this and is vital to the ongoing risk management process and incident response in a ransomware attack.

Monitoring and investigation tools

A Ransomware Monitoring and investigation tool can help identify what data has been impacted by ransomware at a file or object level. Having this information during an attack

“Covenco put ‘boots on the ground’ to deliver an entirely clean set of hardware for your recovery and configure the systems ready for the recovery process..”

will be invaluable to speeding up recovery and preserving uninfected data. If engaged, determine a safe recovery point with a digital forensics and incident response service provider.

Ransomware’s impact is felt when the payload is triggered. The data is encrypted; however, the hackers may have been in the system for quite some time beforehand, gathering intelligence, installing malware, establishing command and control, and planning the attack.

Furthermore, classifying this data with a Sensitive Data Monitoring & Management tool will help determine if any compromised data is sensitive and who has access to it.

Know your data retention policies

Make sure that you protect all critical systems and data with the required levels of data retention. Here, it is better to include all data and exclude as needed rather than only including targeted systems and data. In this manner, all data required for recovery will be in the data protection system.

Assigning Covenco SLA Domains at the top level of a hierarchy (e.g., vCenter Server, SQL Server) is an excellent way to ensure that existing objects and any objects created in the future are protected.

Know Your Recovery Strategy

Determine the best recovery methods for each workload. For example, Covenco Instant Recovery instantiates the recovered workload from backup, running live on the Covenco cluster storage. Because of this, the workload can be recovered much quicker than it would be if recovery of a full backup to production storage would be required. This method, however, rolls entire systems back to a safe point in time. With this approach to recovery, you may lose data that was not infected or encrypted. File-level and database-level restores for infected data may be more desirable.

For more widespread attacks, Mass Recovery might be the best choice. For some workloads, leveraging Live Mount to stand up a VM based on a point-in-time backup for recovery of transaction logs or forensics purposes would be the best approach.

In addition to recovering production, there is a need to recover systems in an isolated environment. This allows for deeper inspection of systems for compromises. For this, there is Covenco Cyber Recovery, a tool that allows instantiation of point-in-time images of systems for forensic analysis. For each situation, evaluate the appropriate method ahead of time to select the proper course of action during an attack quickly.

A key factor during the Recovery phase is automation, as it minimises the risk of human error. It also speeds up recovery and aids in progress tracking. With our Orchestrated Application Recovery solution, you can predefine application-level blueprints that include all the resources associated with that application to allow for unified automated recovery.

Covenco also provides a complete set of APIs and SDKs to help automate recovery. These can be integrated with automation tools such as Ansible, Terraform, Puppet, Chef, PowerShell, and Python. Once a recovery plan and prioritisation have been established, automation is the next step in building a more robust recovery capability.

Test Your Plan

Periodically test data recovery to be prepared for an actual incident. Without testing the recovery plan, there can be no assurance that it will work when an attack happens. Testing also provides the experience and confidence to staff members that an attack can be successfully and quickly remediated.

Tests should be made as realistic as possible without disrupting business operations and performed at planned and unplanned intervals. These tests are known as tabletop exercises.

THE COVENCO FIVE STEP RECOVERY SEQUENCE

This section describes the sequence of events a customer should take when dealing with a ransomware attack.

1. Determine the scale of an attack.

Ransomware continues to evolve at breakneck speeds. It is reasonable to suggest that no organisation is entirely immune. Assuming you have already been breached is an advisable position.

An "assumed breach" mindset requires a "Zero Trust" or "never assume trust, always verify" approach. Even with the best prevention tools, humans are undoubtedly the weakest link, making detecting an attack crucial. Once an attack is detected, determining its blast radius is vital so that you can mitigate damage and recovery can begin.

Covenco deploys Ransomware Monitoring and investigation tools from our partners that help to detect ransomware. These tools use unsupervised machine learning to analyse your backup data. The model is designed to analyse multiple recent snapshots and identify outliers without requiring human input.

The analysis is primarily based on file system behaviour and content analysis. The file system analysis performs behavioural reviews on the metadata, looking at the number of files added and deleted and file system entropy.

Once outlier behaviour is detected, these tools can perform file content analysis on the backup to identify if encryption has occurred. A list of the impacted files and their associated probability of being infected is then presented to the user.

Covenco can work with partners to integrate with your preferred security orchestration, automation & and response (SOAR) platforms, such as Palo Alto Networks Cortex XSOAR and Microsoft Sentinel, to assist investigations from a Security Operations perspective.

2. Isolate infected systems

Systems suspected or confirmed to be infected with ransomware must be isolated as a first step. This can be a physical isolation by crudely disconnecting the hardware from the network to prevent the ransomware from spreading to other systems across your environments.

For the affected systems we isolate, we also carefully review snapshot expiration to ensure no valid snapshots expire, involving data recovery. We then note the original retention periods to reset after the ransomware event.

Covenco can also help you plan for a scenario where you may need to heavily restrict internet access to prevent an attacker from maintaining control of their ransomware. We can work with you to identify an allowed list of trusted URLs, including Covenco Services, any EDR/XDR providers and essential third parties.

3. Notify Stakeholders

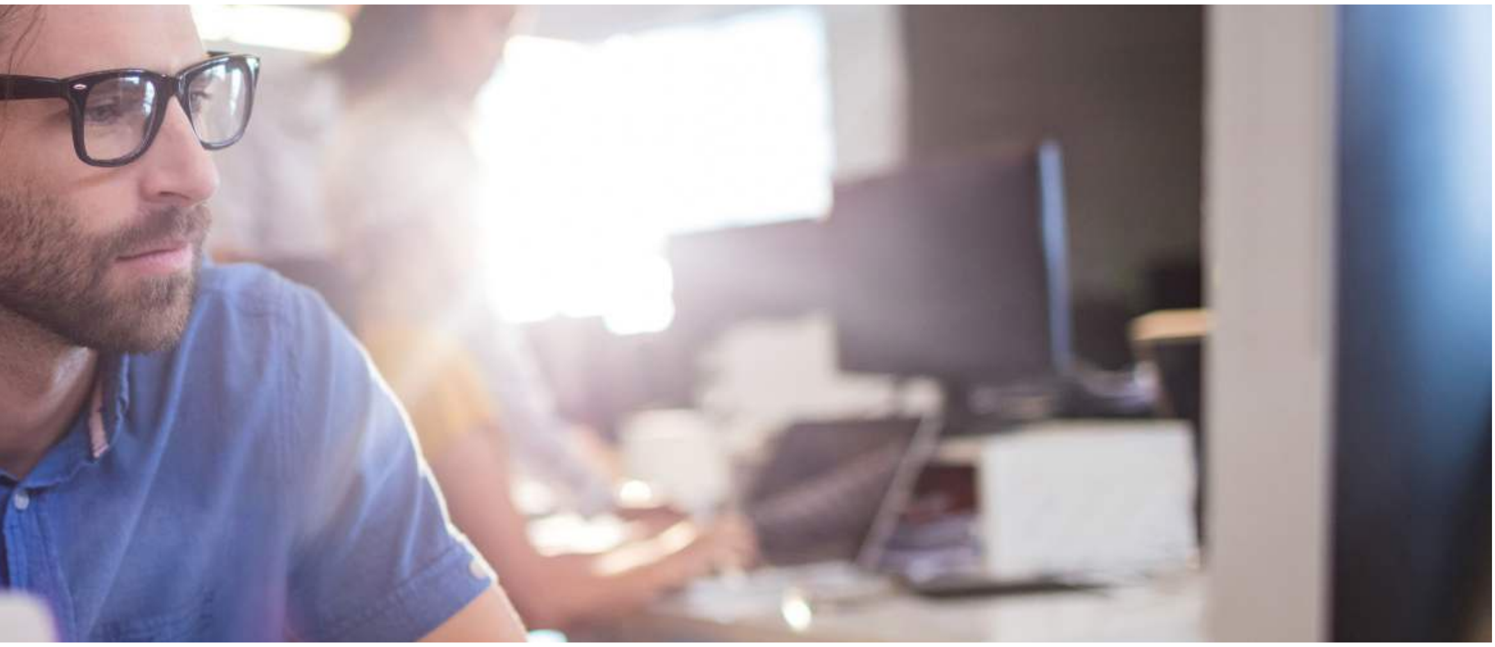
All stakeholders should be notified of the ransomware attack to start executing their parts of the recovery plan. Early notification of those responsible, Covenco, and other partners will allow us to all respond even while the attack is still being investigated. Covenco will partner with your cybersecurity and technology vendors in assessing and recovering data.

4. Assessment and Containment

Covenco will work to confirm the attack's status, impact, and scale. We then mobilise our ship-to-site hardware to establish a quarantine environment at your location or within our data centre in Banbury, UK.

Covenco also deploys engineers and technicians with the equipment to help recover host(s) into this quarantined environment. Our approach allows the restoration data to be thoroughly scanned for malware and validated as clean before releasing it into your production environment.

Scoping the attack involves understanding which business functions, systems, and data were compromised. Our monitoring and investigation tools can help determine



the scale of the attack to be contained, meaning only the affected systems need to be recovered and leaving other critical systems to continue their operations.

Otherwise, the safest approach would be to recover all systems and data, leading to more data loss than is necessary. Doing so would also restore systems unaffected by the attack from a previous point in time. Covenco's insight allows for more surgical recovery, avoiding unnecessary data loss and restoring service more quickly.

Covenco can also indicate the most recent snapshot without anomalous activity to make it easier to identify potential recovery points.

Taking assessment one step further, Covenco can help determine which sensitive data and assets have been exposed or compromised. This information can help prioritise recovery efforts and determine if additional procedures must be followed and if customers or regulatory authorities need to be notified.

As the scope of the ransomware attack is understood, you must take the appropriate action to stop the spread or reintroduction of the ransomware. If it is necessary to pause protection of affected systems, pause protection on only the compromised infrastructure vs. a blanket pause. Taking this approach will limit the impact to only the parts of the business that the ransomware has affected.

Once it is clear which systems and data have been affected, prioritise recovery based on the established plan. Doing this will allow those systems and data to be recovered quickly and per the business needs.

Finally, determine if local copies of the backups are available or if they will need to be recovered from archives. The recovery point determined for each system based on when the ransomware payload was activated will help dictate this. Also, determine if the archival or cloud data has been compromised. If so, recovering from an alternate copy will be necessary.

5. Containment, eradication, and recovery

Before starting the recovery process, knowing what type of recovery is required is essential.

You can use a file-based recovery method if the ransomware only affects files on servers or user shares on a NAS. If, however, the ransomware attacks the virtual disk images for a hypervisor or the master boot records (MBRs) of a physical system, you may need a complete system recovery.

Covenco will initiate a deployment of our engineers and technicians to help customers recover from an attack. We put 'boots on the ground' to deliver an entirely clean set of hardware for your recovery and configure the systems ready for the recovery process.

Our technicians will work alongside your team to ensure the playbook is followed and all recoverable data is extracted, validated and restored in quarantine.

> "Taking assessment one step further, Covenco can help determine which sensitive data and assets have been exposed or compromised."

GENERAL BEST PRACTICE

The following best practices can be applied to any recovery scenario.

Recover safely:

Only begin recovery operations after you have isolated and neutralised the ransomware virus. Data may need to be recovered in isolation or in our quarantined systems. Covenco can also provide new replacement hardware. Restoring systems or data before fully isolating and neutralising the virus may result in repeat infection. If the ransomware cannot be isolated and neutralised promptly, the alternative is to recover from the quarantined environment and run your production operations.

Decrypt data:

Recovery may not be necessary if a decryptor for the identified ransomware strain exists. When possible, decrypt existing data to prevent data loss. Decryption should occur in a safe environment, which Covenco can supply. If you cannot thoroughly neutralise the ransomware, you may require decryption in quarantine.

Recover to an isolated quarantine environment:

Often, ransomware attacks are so pervasive that recovering back to their original locations will only result in secondary attacks. Recovering in an isolated environment where the ransomware did not have access is the best prevention for a secondary attack.

Covenco will provision and test an isolated environment during the preparation phase. During the Recovery phase, this isolated location is used to recover data if needed.

Prioritising recovery:

As planned for in the Prevention phase, recovery will occur based on prioritising applications and lines of business. Covenco will ensure that foundational services required for basic functionality, such as Active Directory, DNS, DHCP, NTP, and Authentication, are recovered first. These are necessary for the other recovered systems to function correctly.

File-only Recovery

These best practices apply to scenarios where only files and directories need recovery. Consider that malware may lay dormant for some time before executing its payload, and unless you can be 100% confident that this is not the case, a clean OS followed by a file-level recovery is the only safe option.

Verify the operating system:

Verify that the ransomware attack did not compromise the underlying operating system and is trusted.

As more organisations begin to leverage build automation, redeployment of the OS from a known clean template may become the easiest route to take.

Using automation:

Automated recovery via automation tools and our partner system APIs and SDKs will speed up recovery times. Proven and tested automation will also add to the accuracy of the recoveries. Automation might only be necessary for some types of recoveries.

Some examples of where automation can be beneficial are:

- Recovering NAS systems with tens or hundreds of shares.
- Recovering complete virtual environments with hundreds or thousands of VMs.
- Recovering database servers with many databases.
- Recovering filesets across multiple servers to or near the same point in time.

Recover to clean systems:

If you cannot trust the original system, recover files to a known good system. Covenco will build this system on new hardware in isolation or freshly deploy an OS pushed from a known clean template. Covenco provides ship-to-site hardware so you can build an entirely clean system for your recovery.

Identify files for recovery:

Covenco's toolset can help you identify and recover which files the ransomware attacked.

Identify sensitive information:

Sensitive Data Monitoring and Management tools can help identify which files contain sensitive information. We can help you ensure these files are adequately secured no matter where they are restored. A further forensic examination can be carried out to validate if this data has also been taken. If so, the relevant authorities may need to be notified.

Virtual Machine and Database Recovery

These best practices apply when you cannot use the VM itself, which may occur when the NAS that the VM is running on is compromised or the ransomware renders the VM unbootable.

Consider the steps you would take for file-level recovery: can you trust that the guest Operating System does not have a dormant infection? Malware typically lies dormant for some time before the payload is deployed (in the case of ransomware, encryption, or theft of data). If you cannot be confident, deploy a clean operating system and recover at a file or application level.

When to use Instant Recovery:

Recovery efforts can be sped up by employing Instant Recovery tools. Instant recovery can allow VMs and databases to be mounted directly from our replacement storage systems, saving time to copy backups back to primary storage before making resources available. Once mounted, VMs can be moved back to primary storage in the background while providing their regular services. Databases can run in this way until the business can take a planned outage to move the database from our temporary systems to your primary storage.

Active Directory Recovery

Microsoft's Active Directory is a widely used, distributed directory service that forms the fundamental platform underlying many enterprise environments.

As well as authentication services, it usually provides DNS and NTP and may also provide the underlying Public Key Infrastructure (PKI) and DHCP in many environments. It is also one of the infrastructure components most commonly hit by ransomware. Due to these factors, it is typically one of the first pieces of infrastructure that should be recovered.

Active Directory relies on multi-master data replication (not only for the Active Directory Domain Services database but also Distributed File Services). Because of this, you must ensure that you do not just add a recovered Domain Controller back to an environment where the infection is still active.

If malware is still present, you may find yourself in a vicious cycle of recovering only to have your recovered server re-infected.

Recovering in a clean-room environment such as the replacement hardware that Covenco can provide during an attack, and scanning each workload for infection before connecting to the network is an excellent way to avoid this. Once confirmed to be clean, you can rebuild your corporate network in a known good state.

Hypervisor Manager Recovery

Coordinate the recovery of vCenter(s) with the appropriate support team to ensure a smooth recovery.

vCenter Server Recovery:

Exercise care if the vCenter Server has to be recovered or when recovering VMs into a new vCenter Server. If the vCenter Server has been compromised, restoring it from backup is better than creating a new empty vCenter Server and then recovering the VMs.

Recovering all VMs to a newly deployed vCenter Server instance on clean hardware provided by Covenco will minimise the risk of re-infection by recovering this to a standalone host.

ORCHESTRATED RECOVERY

In the event of a multi-system or application-based recovery, these best practices apply to scenarios where the impact is to an entire application.

Coordinate and evaluate:

Before any orchestrated recovery of an application or group of systems:

- Ensure that all infected systems are isolated from the production environment.
- Validate your target recovery location for compute and storage resources required for the recovery.
- Take note and understand both the scope of the recovery and the system dependencies needed for the application.
- If applicable, leverage existing DR plans and run books to facilitate these efforts and coordinate with application owners to prepare for recovery.

An Orchestrated Application Recovery solution will be helpful during this process, guiding you to the safest point to recover from while minimising data loss from the event Your target resources and application dependencies can be configured within a blueprint, providing details for orchestrated recovery.

Execute recovery:

Once application recovery is complete, notify application owners and stakeholders to test and validate the application. Validation is critical to the disaster recovery plan and procedures and must occur before sign-off.

ARE YOU UNDER ATTACK RIGHT NOW?

If you think your data may have been infected or received a ransomware demand, contact Covenco immediately. The worst thing you can do is ignore it. Many ransomware demands appear unrelated to your live data systems, yet they can be a precursor to an imminent attack.

Even if you are not an existing Covenco customer, we may be able to assist you with clean hardware, engineering and technical expertise and a recovery process that gets your business back up and running as quickly and safely as possible.

We can also forensically recover data from individual hard drives, identifying encryption patterns and areas of infection before recovering unaffected data to clean, quarantined hardware. This approach can quickly and safely deliver critical business data to your production systems, resulting in business operations resuming faster.

EXPLORE YOUR OPTIONS

Covenco can tailor a complete ransomware protection and recovery solution for your business. Veeam, Nettitude and Zadara power our solutions to ensure a class-leading service with guaranteed performance.

Take the risk out of your data by contacting Covenco today:

Email: helpdesk@covenco.com

Call: **0845 2070 999**

About Covenco

Covenco connects data management services with IT hardware supply and support. With over 34 years of experience in the IT industry, our team offers a reliable source of expertise for data centre administrators.

Covenco supports businesses with world-class data protection, backup, and disaster recovery services. Our UK data centres have over two Petabytes of customer data under management at any time, and we are fully ISO27001 accredited for data security.

Contact Covenco

Covenco UK Ltd Head Office
Unit 3, MXL Centre, Lombard Way,
Banbury, Oxfordshire. OX16 4TJ
United Kingdom

Telephone: 01753 732000
Email: sales@covenco.com

https://covenco.com

covenco
DATA MANAGEMENT & INFRASTRUCTURE 365