COHESITY ATS GROUP

WHITE PAPER

Your roadmap to ransomware resilience



TABLE OF CONTENTS

Your Roadmap to Ransomware Resilience

Recovery from ransomware requires more than having backup copies available. Organizations need a plan for investigation, containment, clean recovery, validation, and safely returning critical systems to production.

Cohesity's *Your Roadmap to Ransomware Resilience* provides a detailed framework for building that capability.

ATS Group works with organizations to translate these principles into data protection and recovery strategies designed around their infrastructure, operational requirements, and recovery objectives.



Cyber resilience vs. data resilience 3

Creating a cyber resilience program 4

Cyber resilience from planning to execution 7

- Be prepared 7
- Be proactive 8
- Reduce the attack surface 10
- Protect your backups 10
- Bolster your ransomware protection 11
- Bolster your ransomware detection 13
- Respond to the incident 13
- Communicate 15

Recover from the incident 16

Establish key takeaways and follow-up actions 17

About Cohesity 18

Cyber resilience vs. data resilience

Most enterprises have a data resilience strategy in the form of Business Continuity and Disaster Recovery (BC/DR), but the technology and processes designed for **data** resilience don't always lead to true **cyber** resilience in the age of ransomware.

Creating a cyber resilient company requires communication, collaboration, security tooling, authentication systems, backup platforms, and a host of other systems to:

- Investigate how the attack happened
- Communicate with impacted data subjects, regulators, and law enforcement
- Mitigate the threat of reoccurrence
- Recover back to production

Destructive cyberattacks, also referred to as wiper attacks, change the traditional detect-respond-recover flow to be more iterative, with a need to recover the response and communications capabilities before investigatory workflows can even begin. In these cases, the backup and recovery platform becomes critical to serve as an authoritative source of forensics for incident responders.

To achieve cyber resilience and withstand modern cyberattacks, companies must consider two areas that are foundational for success:

1. The ability to recover must be put beyond the reach of adversaries
2. Response planning must have provisions for the rapid recovery of not just production systems but also the security, authentication, and communications platforms needed to effectively and efficiently respond to the incident

The iterative nature of recovery-response-recovery in ransomware and wiper attacks requires the Security and IT Operations teams to work closely together to minimize the impact of such attacks.

Creating a cyber resilience program

In traditional BC/DR scenarios such as flood, fire, and natural disasters, the event's root cause can be determined quickly. In the case of a ransomware attack, an adversary is actively working to stop any recovery to ensure the victim's only option is to pay a ransom.

These attackers continually adapt to the target's defenses, making a prescriptive investigation and response program invaluable in establishing the nature of the attack and understanding the correct process to recover. The investigation also allows organizations to get visibility into the vulnerabilities that allowed the attack to be successful—and bolster the defenses to prevent future incidents. This contrasts with a traditional disaster where the response can be nearly instantaneous.

To be resilient against—or to survive—a cyberattack requires more than just a plan to use technology. IT and security teams must understand the attackers and the types of attacks they're launching. This type of intelligence allows them to create targeted defenses, giving them a better chance to block attacks or detect them earlier. Frameworks such as MITRE ATT&CK enable organizations to quantify threats and communicate remediations in a standardized way.

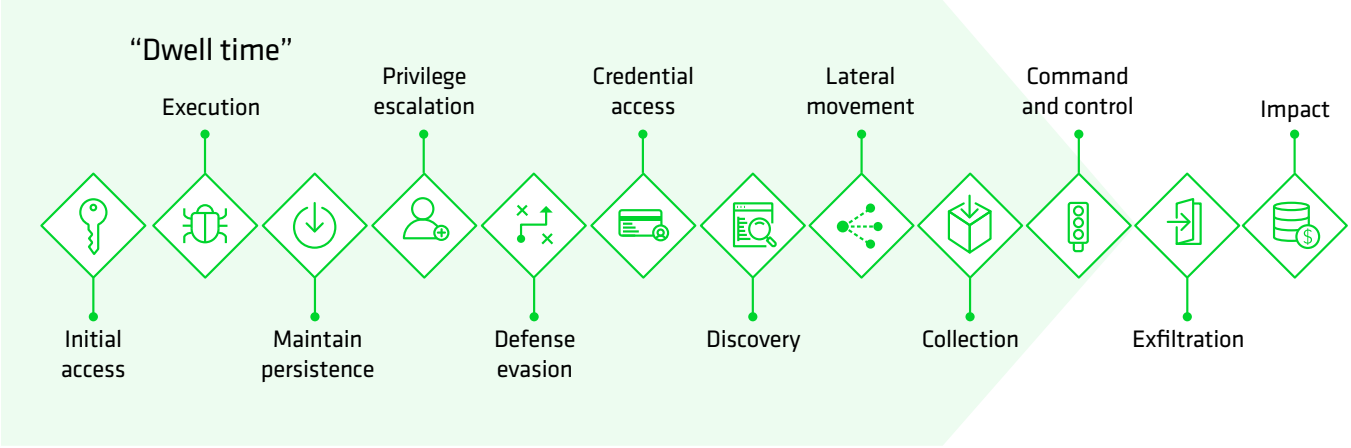
For example, the diagram below shows what attackers may do as they dwell in the environment before the ransomware is activated. In some cases, these could be actions required for the ransomware payload to be successful, while in others, it could help the attacker remain persistent in the network and to launch future attacks. "Dwell time" can be anywhere from days to months. Knowing how an adversary operates in the environment allows security teams to hunt for indicators of an attack proactively.

> Dwell time refers to the amount of time a malicious actor has access to a compromised system before the attack is detected. Longer dwell time creates more opportunity for an attacker to cause damage or steal sensitive information.

Consider each action in the diagram to be a stage of the attack. It may be surprising that 10 of the 12 stages are executed before the payload is even activated. In the case of a ransomware attack, the systems are fully compromised before any encryption or data exfiltration begins. Having this foothold in the network lets attackers thwart recovery efforts and launch new attacks to extort multiple ransoms. This is called "double-bubble" or "double-tap" ransomware and is an increasingly popular way for attackers to create a consistent revenue stream.

For the victim, a single attack can be devastating as it may prevent them from delivering goods and services. But being subject to multiple attacks increases the likelihood of secondary losses, including:

- Reputational damage
- Litigation from data subjects and partners
- Regulatory fines for not protecting the data subject's information appropriately



Further complicating matters, the longer an attacker is allowed to dwell in the network, the likelier it will be that artifacts from the attack will be stored in backups. If these artifacts are recovered without being identified and removed, the attack may restart. Scenarios like this play out often when organizations that have recovered from ransomware attacks don't ensure they're recovering clean data.

Organizations should follow Digital Forensics & Incident Response (DFIR) processes to ensure clean data is recovered within the Security Operations Centers. Historically, DFIR has relied on:

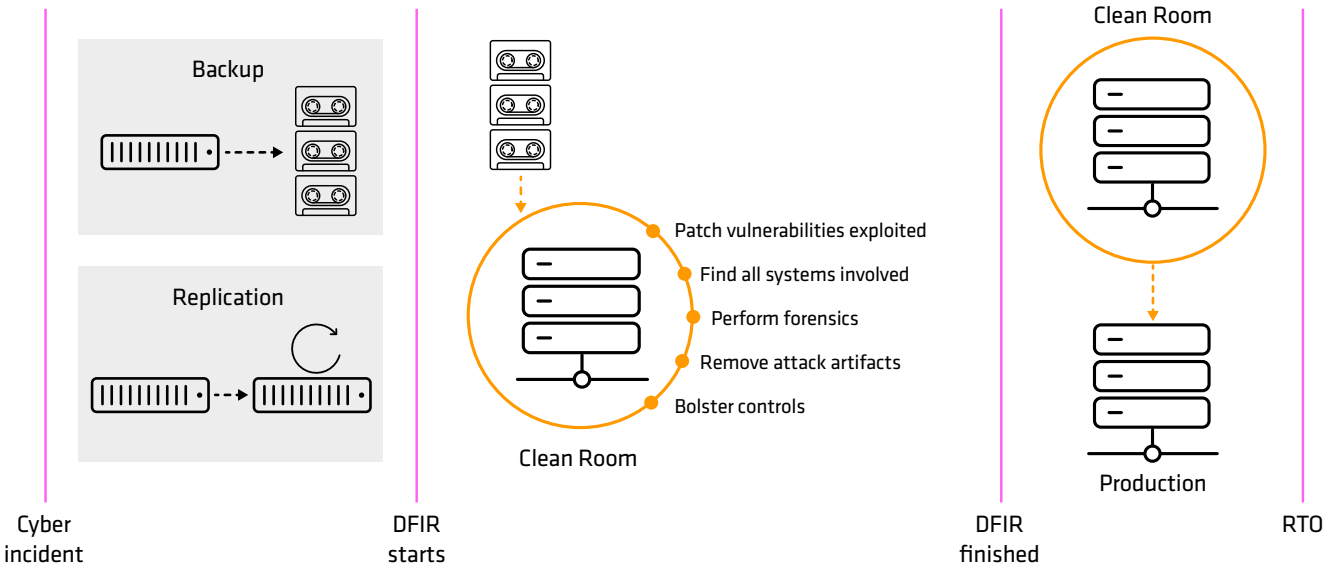
- Forensically imaging a compromised host
- Applying investigatory processes and tooling to identify the incident timeline
- Finding and analyzing the binary artifacts used in the attack
- Uncovering the methods of privilege escalation and persistence used
- Hunting for other compromised systems to extend the scope of the incident
- Scanning for vulnerabilities to be remediated before a platform is put back into production
- Finding out why preventative and detective controls didn't stop or detect the attack

Typically, these tasks are undertaken in an Isolated Recovery Environment (IRE) or "clean room" environment.

Of course, forensically imaging a system that has been wiped or encrypted won't provide meaningful evidence, so incident responders have begun to rely on backup repositories for their investigations. Using backup data lets them see changes over time and track the lifecycle of the attack.

Cohesity provides an immutable, forensically sound platform to start the DFIR process. Investigators gain access to historical filesystem snapshots that can be rapidly instantiated and orchestrated via an API, providing not just the context of the impacted systems but also insight into the filesystem during the entire incident timeline. It's like giving the analyst a time travel superpower. Analysts can compare filesystems over time to identify adversary tradecrafts, like changing configuration files to maintain persistence, overwriting legitimate binaries and libraries with malicious copies, or identifying other malicious artifacts used in the attack.

Recovery Time Objective (RTO) is the maximum acceptable amount of time for restoring a network or application and regaining access to data after an unplanned disruption.



Including the backup infrastructure in the DFIR process allows for investigations to be completed before data is put back into production. The challenge here: It can negatively impact the Recovery Time Objective (RTO) set by the organization. After all, most RTOs weren't calculated to account for investigations required during a cyberattack.

Utilizing the backups to create a clean room environment will reduce the overall downtime and ensure the restored data is clean, eliminating the need to go through the process again during a reinfection. Thisl helps organizations meet their RTOs and avoid continued downtime.

Cyber resilience from planning to execution

Be prepared

Establish a cross-functional ransomware resilience team with all stakeholders.

Ransomware incidents are different from other cyberattacks. They impact the whole organization and its ability to deliver products and services to customers. Every second a response and recovery takes is a primary loss. Staff can't communicate or do their jobs. The press will be eager to publish reports on the incident. And customers will be frustrated. Ensuring everyone in an organization knows their role during a cyberattack is critical.

This includes determining:

- How communication will occur if primary methods, like email, are down
- Who will take the lead for each function and stage of the response
- What process to follow if a team member isn't available—and who is the secondary contact will be

Employees who aren't directly involved in the response and recovery should also know what's expected of them. Why? Because in the absence of reliable information, rumors and conjecture can impede the response and slow the recovery.

Perform a realistic tabletop ransomware simulation with all stakeholders.

One of the best ways to bring the organization together is a realistic tabletop ransomware simulation that focuses on the specifics of your organization. You'll get insight into some of the threats and challenges to ransomware response you're likely to face during a real ransomware attack.

Consider all impacts in the ransomware risk calculation. Impacts include:

- Primary Impact:
  - The inability of the organization to deliver its products and services.
- Secondary Impacts:
  - Operational costs of investigating and responding to incidents, including professional services and any payments to the ransomware operator
  - Reputational damage to the organization
  - Regulatory fines related to the ransomware incident or payment to sanctioned entities
  - Loss of intellectual capital
  - Litigation from partners or customers related to data breaches

Integrate ransomware risk into enterprise risk management.

While it seems obvious, many companies don't consider the impact of ransomware as a significant operational risk. Ensuring ransomware risk is integrated into the organization's enterprise risk management helps establish appropriate levels of governance to gain adequate backing for cybersecurity policies—and helps maintain appropriate levels of risk management.

Create an organization-wide ransomware policy. It should do the following:

- **Lay out clear criteria for an incident to be declared a ransomware attack.** Workflows to respond to and recover from ransomware differ from those dealing with traditional malware and data exfiltration. The criteria

that empower a SOC analyst to declare an incident should be established so they can take the appropriate investigation, containment, and eradication actions. Without this clarity, a ransomware attack may spread within an organization while the SOC seeks authorization to take these steps.

- **Define your cyber backup strategy.** The backup strategy for cyber resilience scenarios may differ from the data resilience strategy for traditional disaster recovery and business continuity events. It's driven by the structure and maturity of the response and recovery capability.
  - Backup data only: Bring up servers needed to investigate the incident and rebuild infrastructure from bare metal, then recover data. This policy should establish how the Golden Master images used for recovery are maintained, including scanning for vulnerabilities and misconfigurations.
  - Backup infrastructure: Recover the entire infrastructure, then clean it by restoring different parts to different points driven by the incident response.
- **Define operational resilience categories.** Base these categories on your already established data resilience Business Impact Analysis, and include the ability to bring up our response tooling within a clean room and your cyber resilience backup strategies.
  - **Include the ability to recover the communications and security infrastructure required to respond to and recover from the incident.** Consider:
    - Physical access control
    - Domain Name Services
    - Voice communications
    - Email
    - Collaboration platforms used to coordinate response
    - Case management
    - Forensic and incident response tooling
    - Vulnerability scanning and management
    - Identity and access management
- **Define under what conditions the organization would consider paying the ransom.**
  - How would the organization secure funds to pay the ransom?
  - Does the organization's insurance policy include paying ransom?
  - Does the insurance provider treat actions by partisan ransomware actors as combatants?
  - Does the insurance provider cover payments to sanctioned entities?
  - What is the organization's approach to negotiation with a ransomware operator?
  - What are the reputational, regulatory, and criminal implications—for example, if the group being paid is sanctioned?
  - How would your organization obtain the cryptocurrency to pay the ransom? Factor in the time to confirm with the Know Your Customer timelines.
- **Ensure that the ransomware policy is periodically updated:** Doing so will better reflect the changing nature of ransomware attacks.

Be proactive

- **Understand ransomware operators and their Tools, Techniques, and Procedures** (TTPs).
  - Obtain governmental, commercial, or open-source intelligence on ransomware gangs, campaigns, and techniques.
  - Prioritize intelligence gathering and analysis on ransomware operators and those conducting wiper attacks with operations on your vertical market or geography.
  - Map the Techniques they're using against the MITRE ATT&CK framework.
  - Plan regular phishing tests, incorporating the latest techniques used by ransomware gangs.

  - Ensure that vulnerabilities exploited by ransomware operators are prioritized for patching in your vulnerability management program.
  - Understand how ransomware operators exploit relationships between third parties and Managed Service Providers to target organizations similar to yours. Take this into account in your third-party risk assessments and controls.
- **Document and maintain contact information.** Include all members and backup members of your response team, key personnel, and key stakeholders, ideally through an out-of-band communications channel that a ransomware incident wouldn't impact.
- **Create reporting channels.** Include third parties such as customers, peer organizations, and supply-chain partners to report ransomware incidents.
- **Create a reporting channel for internal users to report ransomware-like behavior.** Capture:
  - Name and role of the reporting person
  - When it happened
  - What they noticed
  - Why they thought it was ransomware
  - What they were doing at the time
  - Where they were physically located and what networks they were attached to
  - What account were they using
  - What system(s) they were using (operating system, hostname, IP address)
  - What account they were logged in to
  - Who they contacted and what they told them
  - What they typically access in their role
- **Create a reporting channel for law enforcement and cybersecurity agencies to report ransomware or wiper incidents involving your organization.**
- **Assemble a cyber crisis response team.** Include:
  - Leaders from the business
  - IT (including recovery and vulnerability management)
  - OT (if relevant)
  - Security operations (including incident response manager, digital forensics, and–if the organization has them–malware reverse engineering, hunt team, and threat intelligence)
  - Legal counsel
  - Public relations
  - Human resources
- **If necessary, retain the services of an incident response organization.**
  - Gain preauthorization to contract the incident response organization.
  - If relying on an insurance provider for incident response, be aware they may also seek evidence of noncompliance to control attestations made when the policy was taken out, as well as dealing with the actual ransomware incident.
- **Draft holding statements and breach announcement templates.** Having the bulk of a statement drafted will make it easier to respond quickly and ward off speculation, even if you need to add details later.
  - Appoint a spokesperson and a backup for the organization who is both media-trained and trained on the breach response narrative.
  - Get a communications channel ready (one that won't be impacted by an incident) for briefings and media interviews.
- **Pre-establish relationships with law enforcement and national Computer Emergency Response Teams.**
- **Have legal counsel review any agreements with law enforcement.**
- **Have legal counsel review proposed response plans and statements, and the potential for civil, regulatory, and criminal liability.**

Reduce the attack surface

- **Prioritize patching systems with vulnerabilities that are often exploited by ransomware gangs.** Identify critical asset vulnerabilities and patch them.
- **Harden systems.** Prioritize the critical systems and attack vectors ransomware gangs use that are discovered through your Threat Intelligence. Correctly configure devices with ports and protocols and disable those not being used for a business purpose. Ransomware operators use legitimate tools in "Living off the Land" attacks, so restricting access to these tools decreases the likelihood of an attack.
- **Follow best practices for using Remote Desktop Protocol and other remote desktop services.** Remote access services are a primary initial access vector for ransomware operators. Enforce account lockouts after a specified number of attempts, multifactor authentication, and logging of all remote desktop login attempts. Ensure a valid business reason for remote desktop services justifies the remote access. Audit your network for unauthorized use of remote desktop services.
- **Disable or block file-sharing protocols.** These include Server Message Block (SMB) protocol outbound and removing or disabling outdated versions of file-sharing protocols. Threat actors use file-sharing protocols to propagate malware across organizations.
- **Ensure that credentials and access rights on all systems are managed along the lines of least privilege—and limit the number of privileged accounts.**
- **Prevent privileged accounts from being used for day-to-day activities.**
- **Implement network segmentation.** Network segmentation remains one of the most effective ways to limit the spread of ransomware and increase the likelihood of detecting lateral movement.
- **Use baseline configurations and implementation change control.** Using baseline configurations and knowledge of changes means backup images can be compared to known-good during investigations.
- **Identify poorly secured data repositories within your organization.** Cohesity DataHawk data classification scans across backups to identify sensitive data without impacting production systems. This comprehensive view of where sensitive data resides lets organizations assess its risks.

Protect your backups

- **Ensure backup systems are sufficiently air gapped.** This should prevent them from being deleted or corrupted by adversaries. Cohesity FortKnox improves cyber resiliency with an immutable copy of data in a Cohesity-managed cloud vault via a virtual air gap.
- **Ensure backup systems use immutable data stores that prevent them from being corrupted or deleted by adversaries.** The Cohesity Data Cloud, for instance, is built on an immutable storage platform with a Data Lock capability to prevent even those with escalated privileges from deleting backups.
- **Use multifactor authentication on backup administrator accounts.** Implement multiple options in case your primary identity and access management server is impacted by ransomware. Cohesity supports both SSO and TOTP multifactor approaches.
- **Use role-based access control (RBAC) to assign least privilege.** Your backup system users should be allocated only the minimum privileges needed to undertake tasks related to their role. Cohesity has granular RBAC to support least privilege.
- **Ensure backup systems have a separation of duties to prevent a compromised administrator account from making malicious changes.** Cohesity's Quorum capability allows organizations to define multiple layers of authorization for tasks related to backup and recovery.
- **Adopt a 3-2-1 backup strategy.** Have three copies of your data on two different media with at least one copy offsite.
- **Test backups regularly.** Backup testing should be regular and automated. Report the results of tests so corrective action can be taken when needed. Cohesity DataProtect supports automated testing.

- **Collect and report metrics on critical systems' completed/failed/tested backup coverage.**
- **Ensure adequate capacity in backup infrastructure for growth.**
- **Ensure the backup system can support the cybersecurity functions needed to respond to a ransomware incident.** During an incident, the security team can't forensically image the victim system as it is encrypted. They'll need to rely on the backup system to enable them to investigate the incident. Cohesity has built response capabilities—such as data classification and threat intelligence feeds and hunting—into its data management platform itself. It also offers pre-integrated solutions with leading security vendors like Splunk, Cisco, Palo Alto, Tenable, Qualys, Crowdstrike, and ServiceNow through the Data Security Alliance.
- **Build and maintain Golden Masters of critical systems to speed rebuilding after an incident.** Maintain image templates that include a preconfigured operating system and associated application software that can be quickly deployed to rebuild a system within the clean room.

Bolster your ransomware protection

- **Identify gaps in your existing preventative and detective control coverage against the ATT&CK Techniques used by ransomware gangs.** Do this on an ongoing basis to maximize your chances of prevention or detection as adversaries adapt their behavior.
  - Typical indicators of compromise (IOCs) that can be used in the prevention, detection, and response stages include:
    - Anomalous file transactions (encryption and deletion volume deviations)
    - Suspicious boot time of services and applications
    - Unknown and unexpected services and applications present
    - Presence of unauthorized remote access/VPN software
    - Decreased system performance (increased CPU/RAM utilization)
    - Degraded/disabled host security instrumentation performance is Security agents disabled
    - Unknown/unexpected domain name and IP address connections
    - Protocol mismatches
    - Known-bad file hashes
    - Suspicious changes to configuration files
    - Anomalous inbound and outward traffic or source/destination
    - Suspicious processes and text in memory dumps
    - Suspicious accounts in logged-on users (historic and current)
    - Suspicious network shares and mounted network shares
    - Suspicious user accounts
    - Suspicious installed certificates
    - Suspicious entries in ARP and DNS caches
    - Anomalies in date/time on systems, or in log files or NTP servers
    - Suspicious entries or leases in DHCP logs
    - Anomalous user agent strings
    - Nonstandard application beacons and updates
    - Binaries inside of full packet capture
- **Test preventative and detective content.** Test any created rules against ransomware IOCs.
- **Implement detection of endpoint filesystem anomalies that correspond to ransomware and wiper attacks, such as encryption or deletion of files.** Cohesity uses machine learning to identify these patterns.
- **Implement email gateway filters to block emails with known malicious indicators.**

- **Implement a mechanism to remove emails identified as carrying ransomware-related content from users' mailboxes.**
- **Implement Domain-based Message Authentication Reporting and Conformance (DMARC) policy and verification.** You'll be less likely to receive spoofed or modified emails from valid domains.
- **Disable macros for Microsoft Office files transmitted via email unless there's a specific business requirement.**
- **Use applications that allow listing/whitelisting on critical assets to ensure only authorized software can run.** On Windows platforms, use Microsoft Software Restriction Policy or AppLocker. Use directory allow listings rather than attempting to list every possible application. A default to restrict the running of many ransomware attack vectors allows applications to run from PROGRAMFILES, PROGRAMFILES(X86), and SYSTEM32, though this won't stop "living of the land" attacks. Disallow all other locations unless an exception is granted for a specific application.
- **Understand the supply chain's risk management and cyber hygiene practices, third-party partners, and Managed Service Providers (MSPs).** Many ransomware attacks are facilitated through third parties.
  - Understand the company's and partner's role in cyber risk management and controls. Ensure roles and responsibilities are clearly defined and measured and mechanisms for corrective action are included in contractual agreements.
- **Employ multifactor authentication for as many services as possible, particularly for remote access and privileged accounts.**
- **Implement logical or physical network segmentation to separate business units or categories of IT resources, any any Operational Technology (OT) environments.** This will limit the spread of ransomware in the event of an attack.
- **Reduce the opportunity for PowerShell to be used in Living off the Land attacks.**
  - Restrict usage of PowerShell to specific users on a case-by-case basis
  - Update PowerShell to version 5.0 or later, uninstall all prior PowerShell versions
  - Ensure module, script block, and transcription logging is enabled
  - Ensure the "PowerShell" Windows Event Log and the "PowerShell Operational" Log have a retention period of at least 180 days on systems with PowerShell enabled
- **Analyze historical network traffic for anomalous East-West and North-South traffic patterns.** Use network traffic metadata (NetFlow/sFlow) or, if available, full packet capture or a Network Intrusion Detection/Prevention System.
- **Secure domain controllers.**
  - **Ensure no additional software is installed on domain controllers other than data management and security agents.** Access to domain controllers should be restricted to the administrators group. Any users within this group should use a separate restricted account for day-to-day activities.
  - **Configure host firewall on domain controllers to prevent access to the internet.**
  - **Enable Kerberos for authentication and enable NTLM auditing to ensure that only NTLM v2 responses are sent across the network, if possible.**
  - **Audit LSASS.EXE to understand what applications would be affected if Local Security Authentication protections were enabled.** This will prevent code injection from acquiring credentials and enable these protections if impact is acceptable.
  - **Ensure that SMB signing is required between the hosts and the Domain Controllers.** This prevents the use of replay attacks on the network.

Bolster your ransomware detection

- **Proactively hunt using historical data to find compromises.** Use new threat intelligence and IOCs related to ransomware gangs for which there's no preventative or detective rule. Cohesity includes an integrated threat intelligence feed that provides over 110,000 IOCs used by ransomware gangs and provides the ability to hunt for their presence against the backups. By passively hunting against backups rather than live systems, attackers can't detect this activity—so it's not subject to the defense evasion techniques adversaries use against end-point solutions. In addition, retention periods on backups tend to be longer than those of security solutions allowing for an extended horizon of detection.
- **Implement a mechanism for unusual changes in CPU and disk utilization.** These metrics are typically collected by IT Operations platforms, but they can be additionally channeled to the security team as additional signals to improve detection.
- **Identify unusual network protocols.** These include I2P or TOR, which are known to be used by ransomware gangs.
- **Identify network connections using known ports or destinations used in ransomware and wiper Command & Control.**

Respond to the incident

- **Identify and group similar alerts related to impacted assets.**
- **Create an initial loss expectation (blast radius) of the incident, including:**
  - Estimated number of end-points encrypted/wiped
  - Business value chains impacted by encrypted/wiped systems
  - Regulatory obligations of the data impacted (number of records, types of data)
  - Any evidence of exfiltration

> Cohesity automatically searches the backup of impacted systems to identify the potential regulatory impact of ransomware incidents. Systems that are being backed up can also be classified on-demand, both prior to an incident or in response.

- **Find staging environments used for data exfiltration.** Identify systems on your network that have unexpectedly large increases in data—or other types of data you wouldn't expect to find on that host. Cohesity automatically searches the backup of impacted systems to identify the potential regulatory impact of ransomware incidents.
- **Isolate infected hosts from both wired and wireless networks.**
- **If the variant of ransomware is known and it spreads itself, block known communications and infection channels (host or network firewalls, email gateways, network access control).**
- **Activate the clean room.** If security tooling, communication, collaboration, or access control systems have been impacted, rapidly instantiate known good instances to allow the response activities to begin.
- **Restore the last backup of impacted systems into a clean room environment.** This acts as a forensic image to start your investigation. The system's state at other points in time can help establish historical trends and identify filesystem changes over time.
- **Redeploy trusted detection/response/forensic tools onto systems inside the clean room.** Attackers will target endpoint tools to ensure they can evade detection. This reduces confidence that endpoint tools are functioning correctly. Reinstalling endpoint tools ensures proper function and can build trust that the tools are reporting correctly.

- **If the ransomware variant isn't known, determine it by doing the following:**
  - Gather ransom messages (graphical popups, text, or html files, which may open automatically after encryption; image files such as wallpaper on infected systems that contain contact emails; sound files with ransom demands)
  - Analyze the ransom messages to identify the ransomware gang and variant (ransomware name, language used, syntax, structure, phrases, artwork, contact email address, user names, ransom demand payment type [i.e. cryptocurrency type, gift cards], payment address in case of cryptocurrency; support chat address or support URL)
  - Analyze encrypted files and other created artifacts (encrypted file renaming scheme and extension; targeted file types; targeted file locations; file ownership and group of affected files; changes to file metadata such as mass changes to file creation/modification times; entropy and byte plot visualization; icon used for encrypted files; file flags; file containing manifest of encrypted files or key material; other data files)
  - Investigate the infection vector more deeply, if necessary
  - Extract suspicious binaries from instantiated filesystems to perform reverse engineering if not a known variant
  - Check collected artifacts to identify ransomware gang and variants against sites such as:
    - Ransomware Census (**https://goo.gl/b9R8DE**)
    - CryptoSheriff (**https://www.nomoreransom.org/crypto-sheriff.php**)
    - ID Ransomware (
    -)
- **Look for evidence of persistence.** Historical snapshots taken by Cohesity can be instantiated to allow analysts to examine file systems and look for evidence of persistence. These include:
  - "Outside-in" persistence mechanisms, which may include authenticated access to external systems via rogue accounts; backdoors on perimeter systems; and exploitation of vulnerabilities on perimeter systems
  - "Inside-out" persistence, which may include malware implants on the internal systems or a variety of living-off-the-land style modifications (including deployment of commercial penetration testing frameworks like Cobalt Strike; use of PsTools especially PsExec to remotely install and control malware and gather information; and use of PowerShell scripts)
- **Capture an image of memory contents to detect suspicious processes or text artifacts.**
- **Identify changed Registry Keys.**
- **Identify recently created compressed files.**
- **Examine scheduled processes and jobs.**
- **Audit active/running network services against what should be operating.**
- **Execute Data Loss playbook if faced with evidence of staging or exfiltration.** Cohesity DataHawk can identify what data was on those systems at the time of the attack, allowing Incident Responders to identify compliance obligations and notify data subjects and regulators.
- **Identify vulnerabilities in systems exploited in the attack.** Cohesity CyberScan allows Incident Responders to run the Tenable Nessus vulnerability scanner against the snapshot near the point of the attack, so you can create a manifest of patches to be applied before the system is brought back into production and any vulnerabilities the attackers may have exploited since the last scheduled vulnerability scan.
- **Identify assets used for staging by scanning for**

intellectual property, financial information, or personally identifiable information on unauthorized assets. Sensitive data can be identified in staging environments using Cohesity DataHawk data classification.

- **Extract suspicious binaries from historical instantiated filesystems.** Analyze, reverse engineer, or upload these to services like VirusTotal. The instantiation of historical filesystems can be orchestrated in Cohesity by Security Orchestration & Automated Response (SOAR) tools such as ServiceNow Security Incident Response, Splunk Phantom, and Palo Alto XSOAR.
- **Extract suspicious binaries from instantiated filesystems and detonate in a malware analysis sandbox.**
- **Check similar systems within the organization for infection.** Investigate hosts with similar users and groups. If systems aren't encrypted, compare the instances of these hosts to the infected system to identify potential impact. Cohesity has indexing and search capabilities that can quickly query an organization's backup infrastructure.
- **Check local accounts, identity and access management tools, and directory services for new accounts or permissions/access rights changes.**
- **Identify other systems attempting to connect to ransomware command and control.**
- **Continue to follow the investigative chain using the MITRE ATT&CK to find patient zero, the initial infection vector, and each infected endpoint.**
- **Identify any preventative or detective controls that were circumvented and the mechanism used.** Add these to your mitigation plan to bolster controls before you recover into production.

Communicate

- **Communicate to the press.** Keep the press updated to help prevent damaging speculation.
- **Communicate to impacted data subjects.** Ensure any notifications comply with regulatory and legal obligations.
- **Communicate to internal stakeholders.** Keep your internal staff apprised of the situation and your expectations of them, especially as the press may use platforms like LinkedIn to identify employees and reach out to them directly.
- **Communicate to regulators to meet regulatory compliance obligations for reporting.**
- **Inform your insurance company.**
- **Inform law enforcement and national/industry CERT.**

Recover from the incident

The best-case scenario would be to find and remove the infection and restore the systems to production using tools like instant mass restore (IMR). In reality, you'll likely have a combination of systems that are restored and those that are rebuilt from bare metal. To undertake bare-metal restores, you'll need access to "gold images" of critical systems, which are secure and maintained with the latest tested patches. These templates can be rapidly deployed to rebuild systems that are beyond recovery. They can also be secured using tools found in the Cohesity Data Cloud, so they're not corrupted during a cyberattack. You can then restore the base operating system and applications—as well as the associated data from other backups. This optimizes the RTO while also creating historical backups of the impacted systems for forensics.

As data and applications are being recovered, you'll need to document the incident and take steps to prevent a recurrence.

Organizations should:

- Use knowledge of the initial infection vector, vulnerabilities exploited, and persistence mechanisms to update your recovery plans to protect against future attacks and ensure each component can be brought back into a safe and stable state.
- Recover the remaining systems back to the clean room and repeat the above steps, quarantining any indicators of compromise
- Patch vulnerabilities you've found
- Issue password resets for all affected systems and accounts
- Remove historical emails containing any exploitation artifacts from removed email inboxes
- Increase focused monitoring of previously infected systems

Establish key takeaways and follow-up actions

After experiencing a ransomware attack, ask the following questions to gather lessons learned:

- What products and services were impacted?
- What were the impacts on the business?
- Which stakeholders were impacted?
- Who were the threat actors involved?
- What went wrong in the process of the response?
- What went right in the process of the response?
- When did we detect the attack?
  - What was the lag between initial infection and detection?
  - Why wasn't it detected sooner?
  - Which controls failed to detect/ prevent it?
- Which controls were circumvented and how?
- What needs to be adjusted within business operations to prevent future incidents?
- How can this be avoided in the future?
- Were we able to recover to production within the required RTO / RPO?

Send newly discovered IOCs to any authorized partners and vendors.

- Update documentation and playbooks.
- Communicate the final incident report and lessons learned to stakeholders and regulators.

Put the Roadmap into Practice

How confident are you in your current cyber recovery strategy?
ATS can help evaluate:

✓ Backup architecture and protection
✓ Immutability and access controls
✓ Recovery readiness and testing
✓ Recovery objectives and priorities
✓ Cohesity architecture and implementation

Talk with ATS about cyber resilience >>>

About Cohesity

Cohesity is the leader in AI-powered data security. Over 13,600 enterprise customers, including over 85 of the Fortune 100 and nearly 70% of the Global 500, rely on Cohesity to strengthen their resilience while providing Gen AI insights into their vast amounts of data. Formed from the combination of Cohesity with Veritas' enterprise data protection business, the company's solutions secure and protect data on-premises, in the cloud, and at the edge. Backed by NVIDIA, IBM, HPE, Cisco, AWS, Google Cloud, and others, Cohesity is headquarted in Santa Clara, CA, with offices around the globe. To learn more, follow Cohesity on **LinkedIn**, **X**, and **Facebook**.

About ATS Group

The ATS Group solves the problems others can't. For more than 25 years, we've helped enterprise IT teams solve complex infrastructure challenges through deep technical expertise, custom solutions, and relentless support. Our IT solutions and services help organizations modernize infrastructure, automate operations, strengthen resilience, and make smarter technology decisions that improve performance, reduce risk, and control costs. Trusted by nearly 500 enterprises across North America, ATS partners with organizations across healthcare, government, finance, retail, and manufacturing to deliver practical solutions that create measurable business value. To learn more, visit https://theatsgroup.com/cohesity-data-protection/.

Learn more at Cohesity.com

© 2025 Cohesity, Inc. All rights reserved.
Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000048-002 EN 4-2025