7 REAL-WORLD STORIES OF CYBER RESILIENCE

How organizations across healthcare, financial services, government, and more recovered quickly and securely after ransomware.

COHESITY

CONTENTS

INTRODUCTION

Since its formation in 2021, Cohesity CERT (Cyber Event Response Team) has helped numerous customers respond to and quickly recover from high-stakes security events. CERT has also helped organizations like yours align with incident response best practices throughout the response and recovery stages following ransomware attacks.

Working with CERT yields several notable benefits, including faster and more comprehensive response, safer recovery, and reduced disruption and financial risk.

In early 2025, those benefits increased further when Cohesity CERT expanded to include partnerships with leading incident response (IR) vendors, including Palo Alto Networks Unit 42, Arctic Wolf, Sophos, Fenix24, Semperis, and Mandiant.

UNIT 42 BY PALO ALTO NETWORKS
ARCTIC WOLF
FENIX24
SOPHOS
semperis
Mandiant

Organizations can now recover clean data even more quickly as Cohesity CERT shares its data security and recovery expertise and customer-approved operational data from the Cohesity Data Cloud with these IR vendors. This allows effective and efficient analysis of the incident to help speed investigations.

Read on to see how 7 organizations across various industries detected, responded to, and recovered from ransomware with CERT's active involvement.

“

With ransomware, data breaches, and other cyber threats becoming an unavoidable reality, organizations need the assurance that they can bounce back **FASTER, STRONGER, AND SMARTER.**

Cohesity CERT is a natural extension of our mission to empower organizations with resilient, secure data management. We’re doubling our commitment to our customers by ensuring they have the expertise and tools to navigate and recover from cyber crises effectively. Cyber resilience is the cornerstone of modern cybersecurity, and we are committed to helping our customers achieve it.”

– **Sanjay Poonen,** *CEO and President, Cohesity*

International nonprofit restores encrypted VMs

CERT Cyber Event Response Team

Industry:
Nonprofit

Target: VMware virtual machines

Initial Attack Vector:
Software vulnerability in firewall

Overview

This global nonprofit runs programs and camps for children and college students in 100+ countries. Data security is critical to protect logins and personally identifiable information (PII) for young people and hundreds of thousands of donors, and for resilient operations. Day-to-day operations such as fundraising and program management depend on VMware virtual machines (VMs).

Adversary tactics, techniques, and procedures (TTPs)

This ransomware has variants that target Windows systems and VMware ESXi virtual machines. Attackers typically gain access through VPNs not configured for multifactor authentication (MFA), RDP, spear phishing, and the abuse of valid credentials.

> “After determining techniques used for initial access and evicting the threat, it’s a straightforward process to help our customers recover their data.”

Greg Tucker, Cyber Incident Handler, Cohesity

1: Detect

As a 2024 summer weekend begins, the IT manager discovers that VMs are encrypted, as is the organization’s compute environment. A ransom note from the Akira ransomware group is found. The organization contacts Cohesity Cyber Event Response Team (CERT) on day 2.

2: Respond

Fortunately, the firewall has already automatically disabled ports in response to the attack. To prevent further damage, the IT manager unplugs the network. As the organization’s IT team begins rebuilding its servers, CERT takes the following actions to contain and investigate the threat:

- Freezes the cluster to preserve potential evidence and assess the scope of the attack
- Gathers logs for forensics analysis by Cohesity security engineers, who confirm the Cohesity backups are clean with no alteration
- Collaborates with the incident response partner to scan for indicators of compromise (IOC)

3: Recover

The IT team rebuilds the production servers over three days. During this time CERT advises the organization on the optimum method to restore VMs from the Cohesity backups, balancing speed against risk of reattack using the same tactics and techniques. When the target server has been prepared, CERT guides the organization through the process of restoring VMs. At CERT’s recommendation, approximately 40% of critical VMs are restored with instant volume mounts, another 40% with file-level recovery, and 20% with VM recovery. With VMs restored, the organization resumes normal operations.

CERT’s recommendations to strengthen data security and cyber resilience

- Immediately change passwords based on information from the investigation
- Validate that phishing-resistant MFA is enabled, especially on externally accessible systems like VPN
- Ensure that role-based access control (RBAC) is used, with minimum required privileges
- Enable multi-person controls (Quorum) on critical systems
- Regularly audit domain user creation, setting up alerts when accounts are created with elevated privileges

Leading lender restores data after attack, expedites recovery of time-sensitive files

CERT Cyber Event Response Team

Industry:
Financial services

Target: Unknown

Initial Attack Vector:
Unconfirmed access through phishing, moving to out-of-band management on critical server

Overview

Data security and cyber resilience are crucial for this consumer lending company, which has a fiduciary responsibility to protect customers' personally identifiable information (PII) and private financial data. Data loss or prolonged recovery times can delay loan closing, prevent customers from making payments, and cause reputational damage.

Adversary tactics, techniques, and procedures (TTPs)

Affiliates using this ransomware as a service tend to exploit vulnerabilities in public-facing systems or to use valid credentials for initial access. Once inside, attackers use a number of living-off-the-land techniques to further the attack, resulting in exfiltrated data and encrypted systems.

> "After standing up a new server and firewall, the customer engaged us to guide them through restoring data in the most efficient and secure way."

Greg Tucker, Global Escalation Leader, Cohesity CERT

1: Detect

It's 1:00 a.m., and the lender's IT team receives an alert of suspicious activity consistent with a ransomware attack. The IT team immediately powers off the Cohesity cluster as a precaution while they determine the scale and scope of the attack. They also disconnect the network to keep the threat from spreading. An incident response firm identifies the ransomware based on the attacker's TTPs.

2: Respond

The IT team begins preparing a new environment to restore files, including a brand-new VMware ESXi host and firewall. Early in the process, they contact Cohesity CERT (Cyber Event Response Team) for expert-led data restoration and operational recovery. Cohesity CERT:

- Freezes the cluster to preserve potential evidence and assess the scope of the attack
- Gathers logs for forensic analysis by Cohesity security engineers, who confirm the Cohesity backups are available and show no signs of unauthorized access

3: Recover

The lender's CIO urgently needs a folder for a time-critical accounting matter. Cohesity CERT delivers by immediately spinning up a new VM and cloning the folder. When the new infrastructure is ready, the lender's IT team successfully restores all data from the Cohesity backups—with Cohesity CERT on standby to resolve any issues.

Cohesity CERT recommendations to strengthen security posture

- Verify that the Cohesity cluster has not drifted from the recommended security configuration, and confirm the use of DataLock and MFA.
- Assign roles with least privilege required, and configure proper audit logging and alerting to an external collector.
- For more sensitive operations, follow the separation-of-duties principle for oversight and human-based authentication.

Hospital emerges successfully from ransomware attack, recovers payroll system by deadline

CERT Cyber Event Response Team

Industry: Healthcare

Target: Unknown

Initial Attack Vector: Active Directory

Overview

This North American hospital provides care for people with chronic diseases. Cyber resilience is critical for patient safety and operations, and data security is vitally important to protect personal health information (PHI) and personally identifiable information (PII) for patients and staff.

Adversary tactics, techniques, and procedures (TTPs)

It appears that the attackers used valid credentials for initial access and privilege escalation, concluding with encrypted VMs. No ransom note was found.

> "The first step in our response is to contain the attack. This helps to manage risk and to minimize some of the noise to help expedite the response process."

William Wells, Tech Lead, Cohesity CERT

1: Detect

In 2024, the hospital IT team discovers that both data centers are down and the VMware environment is compromised. Active Directory fails first, followed by critical core infrastructure. That same day the IT team opens a case with Cohesity CERT (Cyber Event Response Team).

2: Respond

Cohesity CERT takes the following actions to contain and investigate the threat:

- Disconnects all systems connected to the Cohesity cluster to prevent exposure to attack.
- Changes all cluster passwords and freezes the cluster to preserve potential evidence.
- Gathers logs for analysis to confirm there are no signs of unauthorized access to Cohesity backups.

Immediately after freezing the cluster, Cohesity CERT meets with hospital IT staff to determine which VMs to recover first, including the domain controller, health scanning system, and payroll system.

3: Recover

Working into the night, Cohesity CERT guides the hospital IT staff through repairing core infrastructure, using an encrypted messaging service for privacy. Once the environment is prepared, a Cohesity CERT engineer helps the hospital restore its 32 encrypted VMs—beginning with a 400 GB VM needed for tomorrow's payroll run. Within 3.5 hours, all but two VMs have been restored using the Cohesity Instant Volume Mount capability and then validated for release to production. On the advice of Cohesity CERT, the IT team waits to bring each restored VM online until the incident response firm can verify that the attack signature is not present. The hospital resumes normal business operations three days after the attack, meeting the payroll deadline.

Cohesity CERT recommendations to strengthen resilience

- Consider adding another backup copy in Cohesity FortKnox, an administratively isolated cloud vault.
- Regularly check that users have the minimum privileges to do their jobs—the principle of least privilege.

Auto parts manufacturer recovers more than 100,000 encrypted files

CERT Cyber Event Response Team

Industry: Manufacturing

Target: VMware virtual machines

Initial Attack Vector: Vulnerability in VMware

Overview

A division of a global auto parts enterprise operates a manufacturing plant and R&D center. Damaged or encrypted virtual machines (VMs) and databases exact a high cost on the multi-billion dollar business, including revenue interruption, potential compliance violations, and reputational damage. For cyber resilience, the company maintains one immutable Cohesity backup on-premises and another administratively isolated copy in Cohesity FortKnox, a software-as-a-service (SaaS) offering.

Adversary tactics, techniques, and procedures (TTPs)

The ransomware that hit the company encrypts VM images hosted on VMware ESXi servers. Attackers can also gain initial access to victim networks via RDP, drive-by compromise, phishing, abuse of valid credentials, and exploitation of public-facing applications.

> **“Manufacturing is one of the seven industries most vulnerable to cyberattacks.”**

Source: 2024 Cohesity global cyber resilience report

1: Detect

In late 2023 an IT administrator discovers that all VMs have been encrypted.

2: Respond

The manufacturer contacts Cohesity CERT (Cyber Event Response Team) the morning after the attack. Cohesity CERT works in partnership with the company's incident response firm, Fenix24, to contain and investigate the threat. The investigation identifies the threat actor and reveals that more than 100,000 files are locked up, some containing proprietary company information and personally identifiable information (PII). Working with the incident response firm, Cohesity CERT helps to bring data back from FortKnox, working with the IT and incident response teams to validate that the threat has been mitigated and that remediation steps are successful.

3: Recover

Cohesity CERT works alongside the manufacturer's IT team to prepare a target server. When the target is ready, Cohesity CERT begins restoring large VMs (>12 TB) from FortKnox. Normal operations resume weeks sooner than they would have otherwise, and the company avoids significant business disruption.

Cohesity CERT recommendations to strengthen cyber resilience

- Take care that backups do not share hardware with the workloads they are protecting
- Follow the 3-2-1+ backup rule for cyber resiliency: three copies, two different storage media, and one copy geographically separated *plus* administratively isolated
- Make sure that backups do not share infrastructure with production data
- Verify that backups are successful

City government restores services less than 24 hours after ransomware investigation begins

CERT Cyber Event Response Team

Industry: State and local government

Target: VMware

Initial Attack Vector: Compromised credentials

Overview

For this city, data security is critical to protect residents' and employees' personally identifiable information (PII) and to avoid interruption in city services, including online payment of taxes and fees that fund essential city services.

Adversary tactics, techniques, and procedures (TTPs)

The city was attacked by a ransomware-as-a-service group that typically gains initial access by exploiting public-facing vulnerabilities, and has been observed to self-propagate. More recently the group has been observed using valid credentials with VPN accounts. In some cases the attacker exfiltrates data prior to encrypting systems, and has recently targeted VMware ESXi hosts directly.

> "Government facilities were the third largest critical infrastructure sector targeted by ransomware attacks in 2023."

Source: FBI Internet Crime Report 2023

1: Detect

On a Sunday evening, an employee discovers that all applications are offline, quickly realizing that three separate virtual machine (VM) environments have been encrypted. Services are down for residents and the workforce.

2: Respond

While initiating the response, the city's incident response partner, Surefire Cyber, develops reasonable confidence about which ransomware group is behind the attack. As Surefire focuses on the forensic investigation, the Cohesity CERT (Cyber Event Response Team) is called in to focus on the Cohesity environment. Cohesity CERT delivers the following:

- Access to all available backup data
- A posture review report that highlights drift from recommended settings
- Details of all platform login data, compared against the customer digital forensics and incident response (DFIR) analysis
- Assistance with data and system restores to further the investigation and confirm mitigation steps

3: Recover

Cohesity CERT facilitates the transition from response to recovery by providing the servers and objects that Surefire needs for mitigation, validation, and documentation. The Cohesity Instant Volume Mount capability streamlines the process and ensures that each recovered server's operating system remains benign until all checks are completed. At this point the systems are returned to service—less than 24 hours after the investigation begins.

This response highlights the difference between traditional backups and a robust, fortified data management platform for cyber incident response. Trust, visibility, and quick access to data can shave hours, or even days, from the time to recover.

Cohesity CERT recommendations for cyber resilience

- Configure quorum feature for operations typically associated with an administrator role. Quorum adds an additional layer of protection from compromised credentials or insider threats by adding a time-based, multi-user approval flow.
- Assign minimum required user privileges using role-based access control (RBAC).
- For workloads that do not require a very low recovery time objective (RTO), create an administratively isolated backup copy in Cohesity FortKnox, a software-as-a-service (SaaS) offering.
- Expand out-of-band threat hunting and data classification capabilities using Cohesity DataHawk.

Local law enforcement agency confidently restores dispatch system used as a staging area for ransomware attack

CERT Cyber Event Response Team

Industry:
State and local government

Target: VMware

Initial Attack Vector:
Vulnerability in VPN appliance

Overview

This county law enforcement agency has almost 1,000 employees serving half a million residents. Cyber resilience is crucial because personnel rely on law enforcement and public safety applications to protect life and property. The agency is also obligated to protect residents' personally identifiable information (PII), including social security numbers and addresses collected when residents call 911.

Adversary tactics, techniques, and procedures (TTPs)

Affiliates of this ransomware-as-a-service group gain initial access through unpatched vulnerabilities in public-facing systems and compromised accounts, sometimes through an access broker. Attackers then use a variety of tools to rapidly enumerate the network, move laterally, and elevate privileges. The ransomware avoids detection in various ways and can move to the impact stage within hours of initial access.

> **"Ransomware attacks on state and local governments were 51% more prominent during the first eight months of 2023 than they were during the same period a year earlier."**

Center for Internet Security

1: Detect

Late one evening, an agency IT specialist sees a flurry of alerts about unusual activity in the computer-aided dispatch (CAD) system. The alerts come from the virtual security operations center (Arctic Wolf Networks) and the antivirus client.

2: Respond

To contain the attack, the county's IT specialist proactively turns off the CAD system, and the county temporarily reverts to manual dispatch methods. A Cohesity partner, Arctic Wolf, determines that the system had been used as a staging area to deploy the ransomware. The county's quick action stopped the attack in its tracks, before any data could be exfiltrated or encrypted. The cyber response partner's investigation determines that the attackers entered the network by exploiting a vulnerability on the VPN appliance. As the agency begins restoring the network, Cohesity CERT (Cyber Event Response Team) is contacted to recover the CAD server.

3: Recover

Cohesity CERT takes steps to confirm that the backups are accessible, then validates that the security posture of the Cohesity environment aligns with hardening recommendations. For extra assurance, Cohesity CERT reviews audit logs for indicators that credentials may have been compromised. Cohesity CERT finds no evidence that the Cohesity environment was accessed and confirms that the backups are ready for restores. The most time-consuming step is setting up the replacement VPN appliance to restore network functions. When that's done, Cohesity CERT guides the county team through restoring a full copy of the CAD server to another location. At this point the county's automated dispatch operations fully resume.

Cohesity CERT recommendations

The county already followed recommended data security practices from Cohesity CERT:

- ↗ Storing an administratively isolated backup copy in Cohesity FortKnox, a software-as-a-service (SaaS) offering
- ↗ Using multifactor authentication
- ↗ Setting a time-based lock on backup snapshots (DataLock)

Library successfully restores Cohesity-protected services after cyberattack

CERT Cyber Event Response Team

Industry:
Public sector

Target: Unknown

Initial Attack Vector:
Unknown

Overview

A major city's library system depends on more than 100 virtual machines (VMs), used for the library website, online catalog, in-person checkouts, self-checkout lanes, issuing library cards, free Wi-Fi, online homework help, and more.

> "Most companies follow Cohesity's security hardening guidelines when they start out. But as staff come and go, the configuration may drift. We strongly recommend frequently reviewing sensitive accounts and making sure that the DataLock retention period is appropriate."

Jonathon Mayor, Security Solutions Architect, Cohesity CERT

1: Detect

When the IT staff arrives on a weekend morning to perform routine maintenance, they discover that all systems are down. Suspecting a ransomware attack, they immediately disconnect the network switch to limit the attack's impact. They call an incident response firm, which confirms that a ransomware attack is in progress and all virtual machines (VMs) have been encrypted.

2: Respond

The library begins replacing its IT infrastructure. Early in the process they engage Cohesity CERT (Cyber Event Response Team) to advise on data restoration and operational recovery for the 60 VMs protected with Cohesity. (About 40 VMs are protected with other backup solutions.) The same day the case is opened, Cohesity CERT takes the following actions to contain and investigate the threat:

- Freezes the cluster to preserve potential evidence and assess the scope of the attack
- Gathers logs for forensics analysis by Cohesity security engineers, who confirm the Cohesity backups show no signs of unauthorized access

3: Recover

The incident response team collaborates with Cohesity to confirm that recovered VMs are validated and signed off for return to service. Then the IT team begins restoring the VMs, with Cohesity CERT standing by to help with any issues. All 60 VMs are quickly restored. In contrast, many of the 40 VMs protected with other backup solutions are lost. Rebuilding them takes weeks, disrupting normal library operations.

Cohesity CERT recommendations for stronger security and cyber resilience

- Enforce password policy that requires sufficient complexity and length
- Verify that the Cohesity cluster has not drifted from the recommended security configuration, and review the use of DataLock and MFA
- Validate that backups are successful

CONCLUSION

The scope, frequency, and sheer variety of destructive ransomware attacks can stun those who are unprepared for their impact. But these real-world case studies show that organizations like yours never have to handle an attack alone. Whether you're faced with sophisticated ransomware, data breaches, or targeted attacks,

Cohesity CERT will be there in your corner, helping you respond and recover—quickly and securely.

Learn more about Cohesity CERT ↗

COHESITY