



CASE STUDY



When Ransomware Hit, a Logistics Leader Was Recovery-Ready

Following a breach, the company minimized downtime and kept operations moving with help from Commvault.

INDUSTRY

Logistics

HEADQUARTERS

United States

IN NUMBERS

Locations: 200+

ENVIRONMENT

- Backing up all operational and sensitive employee data
- Protecting data across a hybrid cloud infrastructure, which includes Microsoft 365, SQL, Oracle, Sybase, OneDrive, SharePoint, Active Directory, file servers, virtual machines, and more

CHALLENGES

- Frequent acquisitions left the logistics company with multiple data protection solutions to manage.
- A ransomware attack encrypted some of its production data.
- The IT team needed around-the-clock support to recover data and resume all operations.

SOLUTIONS

- Commvault Support and the 24x7 Incident Response Services team immediately began recovery, aligning with the customer's priorities.
- A backup copy of the CommServe was stored in Commvault® Cloud — a decision that ultimately sped recovery.
- Commvault's fleet of engineers expedited recovery and allowed the customer's team to take much-needed breaks.
- The logistics company is consolidating its cyber resiliency with Commvault globally, reducing management and simplifying recovery.

RESULTS

- The company minimized downtime, avoided ransomware payouts, and kept operations moving.
- Commvault restored the most critical systems within 72 hours.
- Deliveries could resume, minimizing the disruption to retail clients and end customers.
- IT leadership estimates that, without Commvault's response, downtime would have been extended by at least two weeks.



The logistics company recovered business-critical applications at **least two weeks faster**, thanks to Commvault Cloud, Support, and Incident Response Services.

**A BREACH: NOT IF, BUT WHEN**

When ransomware targeted a global logistics company, its IT leaders learned that a recovery strategy is just as critical as prevention and data protection.

"Expect a breach. It's not if, it's when," says the company's Senior Systems Engineer.

The leading logistics company stores and moves goods across locations globally. When the attack came, it took out production and backups, leaving trucks parked and customers waiting. However, prior data protection decisions and subsequent steps enabled the company to restore business-critical systems at least two weeks faster than otherwise.

ONE GLOBAL SOLUTION WITH IMMUTABLE CLOUD STORAGE

In recent years, frequent acquisitions have left the IT team with multiple data protection solutions. Looking to consolidate globally, the company chose Commvault Cloud to reduce management and simplify recovery.

"Most solutions focus on getting backups done faster," said the Director of IT Infrastructure and Operations. "Commvault helps to make sure our data is well-protected and gives us one solution across all operating and storage systems, on-premises and in the cloud. It gives us a single pane of glass to manage all sites."

Commvault Cloud protects data across its hybrid cloud infrastructure, which includes Microsoft 365, SQL, Oracle, Sybase, OneDrive, SharePoint, Active Directory, file servers, virtual machines, and more. Commvault Air Gap Protect provides immutable cloud storage to secure these business-dependent applications.

As they rolled out Commvault, the company chose to host its CommServe® Server, the command and control center of the Commvault solution, on-premises. However, it also uploaded its disaster recovery backup copy to Commvault Cloud — a decision that ultimately sped rebuilding and recovery later on.

COMMVAULT: THE PATH TO QUICKER RECOVERY

When the team noticed anomalies in their systems, they found that ransomware had encrypted all their data, taking out the CommServe and Commvault MediaAgents. At the time, the company had yet to enable ransomware protection with Commvault.

The company quickly evaluated its recovery options and engaged Commvault's Support team. First, Support restored their CommServe database from the cloud, enabling them to rebuild their on-premises server. They also rebuilt three MediaAgents and restored some data from legacy tape.

Commvault's 24x7 Incident Response Services team then took over. Working closely with the logistics company, the team addressed a triaged list of applications based on the impact on the business.

In those grueling first days, the company's IT leadership and team put in the longest days of their careers, but thanks to 24/7 Incident Response services, they could take much-needed breaks.



We got a fleet of Commvault engineers supporting our team day and night in recovering our systems. They were mindful of our priorities and advised us on best practices to restore faster. It was true collaboration..

Senior Systems Engineer

CRITICAL SYSTEMS: RESTORED IN 72 HOURS WITH HELP FROM COMMVAULT

Once the company engaged Commvault's Incident Response, the most critical systems were restored within 72 hours, and the rest of the production systems were back up within a week. That meant deliveries could resume, minimizing the disruption to retail clients and end customers. The only data that wasn't recoverable resided in regions using another backup solution.



If we had not had Commvault Support and Incident Response Services, it would have extended our downtime by at least two weeks. We owe a huge thank you to Commvault engineers.

Director of IT Infrastructure and Operations

The logistics company effectively minimized downtime, avoided ransomware payouts, and kept operations moving.

In the following months, Incident Response continued to provide coverage as needed and offer suggestions to strengthen the company's cyber resilience.

"During this challenging time, we were offered multiple recovery options," the Director of IT Infrastructure and Operations added. "In Commvault, we chose the optimal path for quicker recovery."

LESSONS LEARNED TO FORTIFY THEIR STRATEGY

With business back to normal, the IT team shares their lessons learned. First, they advise having a documented recovery plan before you need it.

They also urge keeping multiple copies of backups across the cloud and various media. In their case, backups on Commvault Cloud expedited recovery time. Also, ensure that backups are completed correctly and thoroughly tested.

"You should know if you're recovery-ready," said the Senior Systems Engineer.

Since the attack, the logistics company has expanded and standardized with Commvault globally. They added Commvault Cloud HyperScale™ X for high-performance backup and recovery, enhanced ransomware protection, greater scalability, and cost-optimized cloud data mobility.

They added Commvault's Remote Managed Services to provide 24/7 remote monitoring and reporting, remediation, administration, and annual Health and Security Analysis. IT leadership has greater peace of mind and is ready for today's threats.



Commvault Cloud is now our cyber resilience solution globally. When a breach came, Commvault came out with flying colors and sealed my confidence in them. They are a true partner, not a vendor.

Director of IT Infrastructure and Operations

To learn more, visit [commvault.com](https://www.commvault.com)