CASE STUDY

Rescuing a French company from a costly ransom

When a French construction equipment retail and rental company was hit by a ransomware attack, they turned to HYCU to help free their data taken hostage.

> **“Using HYCU proved a real advantage, because it is very secure and it offers a really powerful and simple process to restore in case of damage or a ransomware attack.”**
>
> – *IT Manager, French Construction Equipment Company*

System Environment

The company was in the process of transitioning from its legacy three-tier VMware environment to a new Nutanix hyperconverged infrastructure (HCI) using AHV and HYCU for backup and restore. This left the company with two separate computing and backup infrastructures.

Challenge

On a Sunday morning, the company’s IT manager started receiving alerts indicating strange activity in the system infrastructure. Logging in remotely, he found that the servers were all encrypted with a cryptolocker.

“We were the victim of a ransomware attack,” he says, noting that the cyber thief demanded a ransom of several hundred bitcoins, equal to hundreds of thousands of Euros. “While we use several types of security software, the virus apparently entered via a computer under configuration and not ready for production and it was able to propagate throughout the environment from there.”

Solution

After shutting down all the company’s servers to limit propagation of the ransomware virus, the IT manager called HYCU support. Despite the fact that the call came on a Sunday, the System Engineer in charge of the customer and the support team was on the case within 30 minutes and elevated the ticket to highest priority.

“HYCU’s Fast Restore feature keeps local snapshots on the Nutanix cluster, enabling rapid restore of VMs. This snapshot was not compromised by the cryptolocker, so it offered a simple restore point for our Nutanix environment,” the IT manager says, noting that the HYCU team then helped him rebuild the environment up to the last virtual machines.

“The HYCU team has extensive knowledge of the Nutanix REST API, so they were able to recreate our VMs with Nutanix snapshots using API request,” he explains, noting that they had the company’s Nutanix infrastructure up and running normally with in five hours.

Impact

With help from HYCU, the IT manager was able to have operations restored in time for the work week, avoiding business disruption—and avoiding a costly ransom.

Simple, reliable restores

“Using HYCU proved a real advantage, because it is very secure and it offers a really powerful and simple process to restore in case of damage or an attack,” he says, noting that he has since replaced the protocol of the backup target with a more secure one, per HYCU best practices, and reinforced all security parameters for the company’s network.

Superlative support

“The HYCU support team was with me from start to finish. They waited until we had the last VM restored before ending the call,” he says. “They also contacted me on Monday morning to be sure everything was back to normal. And they waited several days before closing my case.”

Once disaster was averted, the IT manager shared the following insight from his experience: “Be sure about your backup software—and about the quality of support behind it.”

LEARN MORE

To learn how HYCU can help your Nutanix-based business and support you in the event of a ransomware attack, visit www.hycu.com or email info@hycu.com.

The information, solutions and opinions contained herein are of informative nature only and they are not intended to be a comprehensive study, nor should they be relied on or treated as a means to provide a complete solution or advice for specific case. We try to provide quality information, but we make no claims, promises or guarantees about the accuracy, completeness or adequacy of the information contained herein.

www.hycu.com

HYCU