MICRO FOCUS

Customer Success Story

IT Operations Management (ITOM)

International Logistics Company

Micro Focus® Data Protector helps an international logistics company recover quickly from a potentially crippling ransomware attack.

Overview

The international shipping provider specializes in customs brokerage, international freight forwarding, and door-to-door cargo logistics. With offices around the U.S. and a network of agents throughout the world, the company provides comprehensive import and export shipping services, from a single-carton airfreight shipment to complete supply chain management.

Challenge

Running a global logistics and shipping network requires a very reliable IT infrastructure backed by a disaster recovery solution—and that's what this organization has.

The company's U.S. head office has a fully virtualized VMware environment running on a Hewlett Packard Enterprise 3PAR storage array. Its environment supports critical applications and data, including the user profiles and files of the company's staff members, IBM Notes email servers, and virtualized Windows-based desktop systems running on Citrix.

"We were 80 percent recovered by the next business day, and fully restored by the day after that."

SYSTEM ANALYST

However, even the most robust IT environments can be tested by ransomware, which is what recently happened to this organization. From a single infected file, a ransomware attack spread across 90 percent of the company's servers within 24 hours.

"Users started calling in, saying they couldn't access their apps or find their data," said a systems analyst at the company. "So, when we looked into it, sure enough data was missing or not accessible. There were errors coming up left, right, and center."

The team soon identified the issue—but not before the email servers had gone down, affecting staff productivity and, more crucially, communications between the company and its clients.

The ransomware was able to self-replicate rapidly by creating a new administrator-level user. "We later found that numerous other attacks occurred the same time as ours," said the systems analyst.

Solution

The organization had the foresight to implement an enterprise-grade backup and disaster recovery solution in the form of Micro Focus Data Protector more than a decade ago.

At a Glance

- **Industry**
  Transportation
- **Location**
  Los Angeles
- **Challenge**
  To recover from a ransomware attack that had infected 90 percent of the company's systems within 24 hours.
- **Products and Services**
  Data Protector
- **Results**
  + Recovered 80 percent of the company's servers by the next business day after ransomware detection, with all servers fully restored the day after that
  + Prevented the loss of the business's valuable data
  + Saved money by restoring data without having to pay the ransom
  + Protected the company's reputation, preventing loss of customers and revenue

Contact us at:
www.microfocus.com

The company's backup strategy included a full backup of all data every weekend, followed by another full backup to tape, and then incremental daily backups on weekdays. The strategy leveraged Data Protector's integration with VMware to perform agent-less backups to protect both the virtual machines and their data.

Thankfully, the ransomware only affected the virtual machines, not the VMware hosts. So, the systems analyst and his team were able to minimize the recovery time.

"Using the Data Protector interface, we were able to get started on the restoration process quickly and seamlessly," he said. "Within three or four hours, we'd restored several servers."

The team hit a snag when restoring larger files, with not enough disk space on the allocated destination servers. This caused some delay in the restore process, but once that was resolved, they used Data Protector's advanced recovery features to restore the affected virtual machines very quickly.

Results

The ransomware attack was a significant disruption to the business, but that disruption was kept to a minimum due to the company's backup strategy and Micro Focus' disaster recovery solution.

The IT team was able to restore a recent backup that wasn't compromised by the ransomware, ensuring the company's data was recovered without having to pay the ransom.

"We were 80 percent recovered by the next business day, and fully restored by the day after that," said the systems analyst.

The quick recovery time ensured the attack did not affect the company's core delivery services—a crucial outcome considering the company specializes in time-sensitive deliveries.

Asked if the company had made any IT changes since the ransomware attack, the systems analyst commented: "We've tightened security, we're scanning emails more thoroughly, and policies are set tighter, but we've made no changes to our backup strategy."

That strategy, and Data Protector, had delivered when it mattered.