COHESITY

Emerge IT Solutions restored critical files in just three days with Cohesity DataProtect

emerge

Industry
Service Provider

Use Case
Backup and Recovery, Ransomware Recovery

Cohesity Solutions
Cohesity DataProtect, offered by a Cohesity-Powered Service Provider

Environments
VMware vSphere virtual machines, VMware Horizon

A full-service IT provider serving companies in the Midwest, Emerge IT Solutions had just deployed a Cohesity-Powered backup as a service. Less than a month later, a manufacturing customer that used the service was targeted by a ransomware attack. Based on past experience the manufacturer's cyber insurance provider expected partial recovery to take two to three weeks. Emerge blew past the expectation, using Cohesity DataProtect to restore the majority of operations in just three days. No ransom was paid. With a downtime cost of $35,000/hour, accelerating recovery by 11 to 18 days saved the customer approximately $12 million in potential lost revenue.

Challenges

Emerge IT Solutions has been helping customers in the Midwest with their IT needs since the early 2000s. "In addition to designing and implementing IT solutions, we also act as a managed services provider," says Jesse Kegley, Chief Revenue Officer. "We either extend the company's internal IT team or manage the entire IT function for them."

For several years Emerge has seen surging interest in its managed cybersecurity services. "Executives recognize that cyberattacks have become a significant business risk," Kegley says. "Everyone knows someone who has experienced an attack, and qualifying for cybersecurity insurance has become much more difficult." Some companies that Emerge works with face pressure from supply chain partners to meet more stringent cybersecurity policies, making compliance important for revenue attainment and retention.

Key Benefits

- 3 days to restore 80% of files encrypted in attack
- 11 - 18 days faster recovery than typical for this type of attack
- $12M saved in downtime costs
- No ransom paid

> "Just three days after the ransomware attack we had restored the majority of our manufacturing customer's operations, enough to resume production. The customer's cyber insurance provider said that other companies hit by the same targeted attack needed two to three weeks for even partial recovery. We give credit to our team – and to Cohesity."
>
> – **Jesse Kegley,** Chief Revenue Officer, Emerge IT Solutions

Emerge offers managed data protection as part of its OmniWATCH suite of security offerings, which also include penetration testing, security auditing, and threat detection. Until 2022, Emerge used several popular backup technologies. But backing up several petabytes took 24 hours, and restoring large data sets sometimes took days. "A company that experiences a cyberattack can't afford to be down for weeks," says Andrew Miller, Backup and Disaster Recovery Specialist. "We wanted to offer faster file recovery to help our customers get back to business quickly after attacks or server failures."

Solution

Emerge found its answer in Cohesity DataProtect, which it offers as a managed service. Running on Emerge's private cloud, DataProtect reduces risk with immutable copies that can't be altered easily, multifactor authentication, and role-based access controls. And it's fast. "When the Cohesity solution restored a 1.5 TB server in just two minutes in our tests, we thought it was a mistake!" Miller says. "Our previous solution could have taken several hours or days."

Today Emerge uses Cohesity DataProtect to back up several petabytes of customer files, including VMs, virtual desktops, applications, and data. "Companies that use our Cohesity-Powered service meet a common requirement for cyber insurance, which is to maintain immutable backup copies offsite," Kegley says. For extra protection, Emerge uses Cohesity's DataLock feature to create a backup snapshot that nobody can alter—not even an administrator—until the lock expires.

For a large manufacturer with multiple locations, Emerge's Cohesity-Powered backup and recovery service paid for itself many times over in the first month. Weeks after Emerge implemented Cohesity DataProtect for backup and recovery, the manufacturer was hit by a targeted ransomware attack that encrypted nearly all of its 65 VMs and 500 virtual desktops.

Kegley vividly remembers how the attack unfolded: "While we don't manage the customers' cybersecurity, we do manage their helpdesk, and the morning of the event we received a few calls from employees who couldn't access systems," he says. Emerge quickly confirmed that certain production servers were encrypted—and that the problem was spreading. The manufacturer's security partner soon determined that the event was a large-scale attack by a nation-state threat actor. "At that point the manufacturer's incident-response team, including Emerge and a 'breach coach' from the cybersecurity insurer, made the decision to shut down all servers and start the recovery process," Kegley says.

Emerge sprang into action to restore clean files from the Cohesity backups, forming a team that worked around the clock for three days. "Every minute counted because each hour of downtime costs our customer $35,000—each 24 hours costs $840,000," Kegley says.

The first step in recovery was identifying the most current backup copy that wasn't infected. "The forensics team didn't know yet when the breach had happened," Miller recalls. "Fortunately Cohesity gives us two ways to identify a clean copy of our data." The Emerge team used a third-party tool to identify the most recent backup without the attack signature. The other method, which Miller learned about later, was to view Cohesity's report of data-ingest anomalies, which signal when a ransomware attack has started.

Working from the clean copy, Miller began restoring VMs and virtual desktops in the order the customer requested—most critical first. "Cohesity has awesome enterprise search capabilities," he says. "With other backup software I've used, just finding the file you want to restore takes multiple steps. With Cohesity it was as simple as entering the file name, selecting the most recent copy from the list, and clicking Restore Now. Then boom!—a few minutes later the VM came up and started migrating over to production. Even large VMs were back in production in two minutes." Emerge's engineers logged into each VM to confirm it behaved normally before they connected it to the network. "Saving a couple of minutes finding each VM might sound trivial, but two minutes times 60 VMs equals two hours faster recovery, worth $70,000 to our manufacturing customer," says Miller.

The recovery process was so straightforward that Emerge needed no help from Cohesity support despite having deployed DataProtect only one month earlier.

Results

Speedy restoration of files slashed the business impact of the attack. "Just three days after the ransomware attack we had restored the majority of our manufacturing customer's operations, enough to resume production," Kegley says. "The customer's cyber insurance provider said that other companies targeted by the same attack needed two to three weeks for even partial recovery. We give credit to our team—and to Cohesity."

Fast recovery had a significant impact on the bottom line. Recovering in three days instead of the 14 to 21 days typical of this type of attack saved approximately $12 million in downtime costs. No ransom was paid.

Now Emerge is putting Cohesity DataProtect to work for disaster recovery, using it as part of a hybrid cloud. "We'll use Cohesity DataProtect on our private cloud for recent backups, and Microsoft Azure for archiving, reducing customer costs," Kegley says. If a customer's production environment goes down, Emerge can spin up their VMs right on its private cloud or in Azure.

COHESITY

Kegley sums it up, "Effective cybersecurity depends on people, process, and technology. Cohesity DataProtect is the technology that helps our people put in place the processes to help customers manage risk, and recover quickly after an attack or unplanned outage."

Highlights of the ransomware attack recovery for Emerge's manufacturing customer:

- 3 days to restore 80% of operational data encrypted in attack
- 11 to 18 days faster recovery than typical for this type of attack
- ~$12M saved in downtime costs
- No ransom paid

About Emerge IT Solutions

Founded in 2004, Emerge is committed to be the most trusted technology adviser in the Ohio Valley. The company accomplishes this with best-in-class technical knowledge and competency, leading technology, superior customer service, and a commitment to long-term relationships. Emerge's team includes dozens of highly skilled engineers providing a full range of IT solutions.

Learn more at www.cohesity.com

COHESITY.com | 1-855-926-4374 | 300 Park Ave., Suite 1700, San Jose, CA 95110 5000137-001-EN 1-2024