COHESITY | Florida

Municipality comes through ransomware attack unscathed, with zero data loss and no ransom paid

Industry: State and Local Government

Use Case: Backup and Recovery Ransomware Recovery Data Security

Cohesity Solutions: DataProtect, FortKnox

Solution Partner: AWS

When the county was hit by a ransomware attack in 2024, the IT team was halfway through a migration from the existing Veeam backup solution to Cohesity Data Cloud. Fortunately, the most critical data had already been moved to the Cohesity solution when the attackers struck. The county's IT team was able to quickly restore virtual machines (VMs), databases, and documents from the Cohesity backups in a fraction of the time needed with the previous solution. Many critical services were back up just 72 hours after the forensics team gave the go-ahead. Zero data loss, 3-day recovery, and no ransom paid: it's a formula for resilient government.

Challenges

Ransomware attacks were up by 73% from 2022 to 2023, prompting municipal governments to revisit their approach to data security. "When ransomware hits, government services stop in their tracks," says a Florida county IT executive. "Staff scramble to get work done when they can't access data and have no way to enter new data. Meanwhile, residents and local businesses can't apply for building permits or driver's licenses, pay water bills, request public records, or use other government services they count on."

Cybercriminals usually go after backups as well as production systems, so the county IT team is diligent about securing its backups. Until early 2024, the county backed up more than 350 VMs and an ever-growing collection of documents in a local data center and colocation facility. Approximately 1,600 Microsoft 365 mailboxes were backed up with a separate cloud service. But when it came time to add capacity, the county experienced sticker shock. "Our data footprint is constantly expanding because of long document retention requirements–75 years for certain documents–and the fact that nobody wants to get rid of email," the county executive said. Concerned that only a couple

Key Benefits

- 72 hours to restore mission-critical VMs after forensics analysis
- $0 ransom paid
- 66%-75% faster restores
- >30% lower TCO
- 10 hours management time saved each week

of IT team members had the institutional knowledge to manage the county's complicated backup architecture, the executive began looking for a more modern solution. Top criteria: fast data recovery after a ransomware attack or system failure, immutable backups, and an easy-to-use management interface that new IT team members could learn quickly.

Solution

After trying a M365 backup solution that proved to be error-prone and cumbersome to manage, the county found its solution in Cohesity. "Cohesity makes our data security posture stronger with immutable backups, an option to lock backups so nobody can delete them until a specified time, and a requirement for multiple approvals (a quorum) to change settings or administrative functions," the executive says. "Plus, Cohesity's recovery speed is the best we've seen, allowing us to stand up a new VM almost instantly after an attack or system failure." The county opted for Cohesity's capacity-based pricing over per-user pricing because of the flexibility to use available capacity for any kind of data, including VMs, mailboxes, and unstructured data like court documents and maps.

The county currently maintains three Cohesity immutable backup copies—one locally, another in a colocation data center about 200 miles away, and the third in Cohesity FortKnox, an isolated, Cohesity-managed vault on AWS. Storing an immutable backup copy meets a requirement to obtain cyber insurance. Coming plans include using Cohesity DataHawk, the cloud service for artificial intelligence (AI)-based threat detection and threat hunting. DataHawk will help the county comply with regulations to notify people whose personally identifiable information (PII) is exposed by flagging sensitive data in databases and documents.

Staff quickly came up the learning curve by taking self-paced courses through Cohesity Academy. "Cohesity Academy has been very valuable for getting our team up to speed on Cohesity," the executive says. "We've been able to find answers to almost every question, which in my experience is almost unheard of in vendor training. My entire networking team has taken courses, and for new hires it's part of their onboarding."

> ***With Cohesity we had zero data loss after the ransomware attack, which is very rare even for organizations that pay ransom, which we did not. I attribute the positive outcome to the fact that we had already moved our most critical data to Cohesity."***
>
> **- Florida County Government Official**

Results

Cohesity's value was put to the test in 2024, when the county was hit with a ransomware attack affecting 350+ servers. At the time, the county was midway through migrating from its previous solution to Cohesity Data Cloud, creating a real-world opportunity to compare the two solutions head to head. The executive recalls the day of the attack: "Our service desk manager woke me up at 1:00 a.m. because he got an alert that someone was trying to log into one of our security systems—and we don't have people working at that time. When we saw that administrative accounts had been deleted, I immediately drove to the emergency operations center and started unplugging the internet to stop command and control."

As soon as the forensics team allowed it, the IT team began restoring data from Cohesity backups, starting with the mission-critical financial and court management systems. "Thankfully, when ransomware struck we were already backing up our most critical systems with Cohesity," the executive says. "Restoring from a Cohesity backup is as simple as connecting to vCenter and clicking Restore. In contrast, to restore backups from our previous solution we first had to recover the data to another server, which took an agonizing three or four times longer." Restoring a 150 GB server backed up on Cohesity took 30 minutes, compared to 90-120 minutes for the same size server backed up with the previous solution.

For guidance throughout the ransomware response, the county engaged Cohesity's cyber emergency response team (CERT). "During the tense days following the attack it was reassuring to have CERT's expertise," the executive

says. "Having been through this before, they knew just what to do, starting with locking down the Cohesity backups so that files wouldn't be deleted at the end of their retention period–just in case we hadn't restored them yet. CERT also walked me through changing Cohesity settings to pause memory recycling, aka garbage collecting, which can better preserve our forensic options. Our experience with CERT was excellent in all respects."

The county's critical applications were back up just 72 hours after the forensics team gave the go-ahead to start restoring data. "We had zero data loss after the ransomware attack, which is very rare even for organizations that pay ransom, which we did not," the executive says. "I attribute the positive outcome to the fact that we had already moved our most critical data to Cohesity."

Along with strengthening data security posture, Cohesity Data Cloud is helping the county cut costs. "Cohesity's 3-year total cost of ownership–hardware, software, and licensing–is 30% less than our previous hardware alone," the executive says. "The savings are actually even greater because Cohesity's simpler management saves us 10 hours a week, and restoring from backups no longer requires highly paid network and systems engineers."

All told, the switch to Cohesity is helping the county achieve its goals to provide reliable services to the workforce and residents, be resilient, and keep costs down. The executive sums it up: "Though the ransomware attack was one of the most stressful events in my career, it's comforting to know that with Cohesity we came through it with zero data loss–and could do it again if we had to."

Learn more at Cohesity

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

5000156-001-EN 4-2025