COHESITY

CASE STUDY

California Department of Finance paid no ransom, restored Microsoft 365 data in 12 hours with Cohesity

INDUSTRY
Public Sector

USE CASE
Backup and Recovery, Backup as a service, Ransomware Recovery

COHESITY SOLUTIONS
DataProtect delivered as a service on Microsoft Azure

SOLUTION PARTNER
Microsoft Azure

DATA SOURCES
Microsoft 365, VMware vSphere

Key Benefits

- 12 hours for automated restore of M365 data after cyberattack
- 24+ hours/month reclaimed by eliminating software maintenance
- 97% faster file restores: < 1 minute
- 68.7%. savings in TCO
- 18-month ROI

When California's Department of Finance started using Microsoft 365 (M365), they wanted cloud backup. Their existing, on-premises backup solution required costly infrastructure and software maintenance, and didn't provide ransomware protection. The solution: Cohesity DataProtect delivered as a service, hosted on Microsoft Azure. An unexpected payoff came just months later, when the Department was hit with a ransomware attack. Thanks to Cohesity's immutable backups, the Department restored M365 data for nearly all 500 users in 12 hours—a fraction of the time it took to restore data still backed up by another vendor's solution. No ransom was paid. Today the Department also backs up its virtual servers in the cloud with Cohesity, providing peace of mind that data can be quickly restored in the event of cyber attacks or other disasters.

Challenges

January 10 holds special significance for the California State government, as that's the day the governor submits a budget to the legislature. The vote is held on June 15, and the weeks before both dates see a flurry of activity for the Department of Finance. "If data goes AWOL in the busy weeks leading up to those deadlines, the budgeting process grinds to a halt," says Chris Dove, enterprise architect for the State of California Department of Finance.

> "After the ransomware attack we restored all 2.5 TB of Microsoft 365 data—protected by Cohesity DataProtect on Azure—in 12 hours. We paid no ransom."
>
> – **Chris Dove,** Enterprise Architect, California Department of Finance

As part of its data availability strategy, the Department's IT team needs secure backup and recovery of M365 data—Exchange, OneDrive, and Teams—for its nearly 500-person workforce. "M365 doesn't have SLAs for data restores," Dove says. "Your only backup is your recycle bin. So if the recycle bin gets corrupted or you need a deleted file past the retention period, you're out of luck."

Until 2020, the Department backed up M365 data on-prem, using the server vendor's proprietary software. But backups and restores required multiple interfaces, finding lost files took too long, and software maintenance consumed several days a month. "We spent more time on software updates than on backups," Dove says. "We knew we'd move backups to the cloud at some point." That point arrived sooner than expected when the Covid pandemic sent staff home to work. Accidental cuts to fiber lines by construction crews kept staff from connecting to the data and applications they needed to get work done. Moving operations out of the data center and into the cloud suddenly became urgent.

Solution

Comparing the leading data protection solutions in the Gartner Magic Quadrant, Dove chose Cohesity DataProtect delivered as a service, managed by Cohesity. "Cohesity had the only cloud-first solution—the other vendors just had plans," Dove says. He liked the service-level agreements (SLAs) for file recovery, and Cohesity's robust security protections sealed the deal. "Though we hadn't experienced a major cyberattack, we liked knowing that Cohesity's backups can't be altered by attackers, and that data is continually scanned to detect suspicious changes from one backup to the next," Dove says.

The Department started by using Cohesity to back up M365 data in Microsoft Azure. At first, they continued using their legacy software to back up virtual servers on-prem. All was well until December 2022, when the Department was hit with a ransomware attack—in the middle of a budget cycle. "I woke up to an early-morning call from my system analyst, who was alarmed about unusual activity on the network," Dove remembers. "We took what action we could, but soon our laptops were encrypted and mountains of ransom notices started spewing out of every network-connected printer. I'll never forget having to call our CIO to say, 'We've been ransomed.'"

In the frantic hours that followed, a bright spot: "After the ransomware attack we restored all 2.5 TB of M365 data—protected by Cohesity DataProtect on Azure—in 12 hours," Dove says. "We paid no ransom."

The Department also ultimately recovered its virtual servers, which had been backed up on-prem with another solution. But restoring that data took a herculean, 72-hour effort. "Seeing how much faster we recovered data with Cohesity backup as a service, we started also using Cohesity to back up virtual servers, initially on-prem and later in the Azure cloud," Dove says. Today the IT team backs up all data—7.5 TB of M365 data and 85 TB of virtual servers—to Azure with Cohesity DataProtect delivered as a service. No more on-prem servers. "We are one of the first California State government agencies to be 100% in the cloud," says Dove.

Results

With the ransomware attack in the rearview mirror, the IT team has peace of mind, knowing they can recover data quickly when the next security event happens.

Staff appreciate that their lost or corrupted files and virtual servers can be recovered quickly. "Finding emails and documents is practically instantaneous with Cohesity, and we generally restore them in less than a minute," says Dove. "With our old solution, file restores could take 30 minutes."

The IT team saves time. "Maintaining our old on-prem data protection solution took more than 24 hours a month," Dove says. "It was an ordeal: downloading updates, pausing backups, and getting on calls with the vendor. By providing backup as a service, Cohesity has freed up time to work on other projects that support our mission."

All that, and total cost of ownership (TCO) dropped. "Eliminating on-prem storage infrastructure and software maintenance, and shifting from capacity-based to user-based licensing will pay back the upfront investment in Cohesity within 18 months," says Dove.

Now the Department is looking at other Cohesity cloud solutions to support the mission. Plans include using Cohesity SiteContinuity for disaster recovery and Cohesity FortKnox, which stores backups in a Cohesity-managed cloud vault, adding another layer of protection.

Summing up, highlights of Cohesity DataProtect as a service for the State of California Department of Finance include:

- 12 hours for automated restore of M365 data after a cyberattack
- 24+ hours/month reclaimed by eliminating software maintenance
- 97% faster file restores: < 1 minute
- 68.7%. savings in TCO
- 18-month ROI

About the State of California Department of Finance

The Department's mission is to serve as the Governor's chief fiscal policy advisor and to promote long-term economic sustainability and responsible resource allocation. Part of its goal is to leverage emerging technologies to make data and information easily accessible to policymakers and the public.

Learn more at Cohesity.com

COHESITY

Cohesity.com | 1-855-926-4374 | 300 Park Ave., Suite 1700, San Jose, CA 95110

5000132-001-EN 9-2023