CASE STUDY

SOCAL MUNI ACHIEVES TRUSTED SYSTEMS COMPLIANCE IN THE CLOUD, WITH IMPROVED SECURITY AND DISASTER RECOVERY FOR THEIR LASERFICHE ECM SYSTEM.

Serving around 50,000 residents, this Southern California municipality maintains nearly 7 million files of regulatory compliance data in their Enterprise Content Management system. This includes data from various city functions such as the Mayor's office, the city council, city administration, police and finance.

Location: Orange County, California

Application: LaserFiche Enterprise Content Management server with 3 TB local storage

Problems: Primary storage running out, no cloud backup, no ransomware protection

Objectives: Upgrade to Trusted Systems compliant storage, protection from ransomware, provide cloud access and backup options

Solution: restorVault Compliant Cloud Archive, Offload Data Virtualization and Copy Data Virtualization

THE PROBLEM

City administration and IT have operated a Laserfiche Enterprise Content Management (ECM) platform for many years, enabling various municipal departments to store and retain their regulatory data. By mid-2020, almost 7 million data files had been captured and archived in the ECM system, with growth to more than 10 million files projected by 2023.

This growth coupled with long retention terms, presented several challenges. Millions of inactive files with retention dates over 10 years were consuming precious capacity on their Laserfiche server storage, and spare space was fast running out.

The city administration wanted to upgrade their system to California Trusted System compliant storage, and to protect their data from ransomware. Doing these things would save the city from having to retain paper copies of compliance documents. But they did not have the budget to replace existing storage equipment outright. They also wanted to make the data accessible to other departments by putting copies in the cloud.

For these reasons, they reviewed cloud storage options from Amazon Web Services (AWS) and Microsoft Azure in conjunction with ghosting backup solutions such as Veeam, Rubrik or Commvault. Could this let them safely replicate the Laserfiche ECM server in the cloud for different business functions and provide a cloud-based disaster recovery option for their ECM system?

No! It soon became clear that conventional cloud storage solutions fell short of the Trusted Systems requirement that the data files to be stored on immutable, unalterable storage. And, since the Laserfiche ECM server relies on a standard window file system, the cloud instances would still have been vulnerable to ransomware attacks, as well. So, none of these options were viable without additional layers of security and additional expense.

THE SOLUTION

Enter restorVault – a virtual cloud storage solution for compliance data in the cloud. The Laserfiche reseller introduced restorVault Compliant Cloud Archive (CCA) as a solution to all of their requirements for Trusted Systems compliant storage in the cloud, along with protection from ransomware.

Unlike conventional cloud storage, restorVault CCA uses purpose-built object storage specifically designed for long-term compliance data retention. Files are stored on redundant, tamperproof, immutable WORM storage with strict retention policies up to 30 years.

This type of storage provides superior file protection at a hardware level, using fingerprinting, serialization and various other identification and verification techniques. Furthermore, since object storage has no file system to attack, data stored on a restorVault CCA is impervious to ransomware.

When compliance data is ingested into a restorVault CCA, it is hashed for comparison with the original data file and to enable periodic verification to ensure data integrity. Then files are fingerprinted and asset-tagged for auditing, and to track long term retention timeframes for disposition. After that, on-demand access is provided by lightweight Virtual Data Files (VDFs) which point to the protected files. 1 GB of VDFs can represent many terabytes of archived data.

VDFs enable big savings is storage both on-premise and in the cloud. For example, policies may be setup on the production system, to offload inactive files and replace them with VDFs. Thereby reclaiming capacity and delaying upgrade costs.

Also, cloud copies of the ECM server for DR and other uses, can be created using much smaller servers than in production. Since only the OS, the ECM system and VDFs are needed – not the compliance data itself.

THE RESULTS

As a native windows application, the restorVault CCA agent integrated seamlessly with the city's Laserfiche ECM server. Providing the Trusted Systems compliance for their ECM data and immunity from ransomware attacks, they were looking for.

Meeting the city's two compliance assurance goals, led to other important benefits. It allowed the city, for the first time, to safely make the data accessible in the cloud, while at the same time eliminating the need to retain paper archives in their regulatory work flow processes.

In time, the city expects to shred many tons of paper, eliminating additional handling and preservation costs.

"The deployment has been a great success. Our data is safer than ever before, and we have more control over our long-term storage costs." says the city's IT Director.

They hope to save a lot of money by using Copy Data Virtualization, to give other departments access to the data in the cloud, while using almost no additional cloud storage. And they have already extended the life of their existing ECM server, by freeing up nearly 60% of its previously-used capacity through Offload Data Virtualization with VDFs.

Benefits Realized

- Seamless integration with Laserfiche ECM
- Superior file protection on immutable storage
- CA Trusted Systems compliance assured
- Periodic auto-verification for data integrity
- Almost 60% of primary storage capacity saved
- 500x faster file copies and disaster recovery