

Billion dollar construction firm fully recovers from ransomware with Druva, where Veeam backups fail



66%

Cost savings after replacing competitors with Druva

2.5x

Global deduplication storage savings

40

File servers fully restored after ransomware attack

The challenge

A billion dollar construction firm with thousands of employees was experiencing rapid growth across North America as it continued winning new contracts, meaning it needed to set up remote locations quickly.

It had 50+ remote office locations – at least 40 of which stored data in on-premises file servers. To protect its business-critical data, the firm used Veeam for its virtualized environment, and Mozy to protect the physical machines in remote sites, but the costs to manage data were escalating.

“The nature of our business is that we spin up a site sometimes for a year or two and on very short notice. So we have 40+ offices with servers today, but three months from now we could have 45 sites. The fluctuation means we have more data to protect. The previous data protection solution was getting too expensive and unpredictable,” said a senior leader at the firm. “We had to get costs under control.”

In addition to reducing costs, the firm needed to have centralized visibility of its backups, streamlined access to data across all locations, and the ability to protect other workloads, such as software-as-a-service (SaaS) applications.

“We wanted backups to be securely stored offsite, and the only logical answer was moving to a cloud-first

Challenges

- Business growth resulted in remote sites being added quickly for an indeterminate period of time, impacting its data protection needs
- The cost of its previous backup solution was rising and unpredictable
- Needed a cloud-first data protection solution that would enable centralized management of all backups, including SaaS data as it expanded
- Needed to have ransomware protection that is impenetrable to encryption or attacks

Solution

- Ransomware protection for the backup and long-term retention of 40+ remote file servers in the cloud with data isolation (“air-gapped”)
- Centralized management and visibility for physical workloads across 40+ remote locations, and flexibility to protect data quickly as new sites are added
- A single pane of glass through which IT can easily manage backups and restores of file servers, and SaaS application data

Results

- Druva and AWS Snowball Edge solution facilitated restoration of data on 40+ file servers within a matter of days following a ransomware attack
- Reduced data protection costs by two-thirds leveraging a flexible cloud-native platform which can start protecting SaaS data from day one
- Achieved 2.5x global deduplication storage savings within hours of launching the POC

approach. As a customer, we were familiar with Veeam, but were not comfortable using it for backing up remote sites to the cloud,” the senior leader said.

The solution

The firm conducted a proof of concept (POC) with Druva, and saw significant global deduplication within the first few hours, before deciding to roll it out across all 40+ locations. Druva gave the firm the visibility, flexibility, and cloud-native data protection it needed for about one-third the price of its previous solution.

When the firm was hit by a ransomware attack in early 2020, their choice of Druva became even more serendipitous. Bad actors exploited a Citrix vulnerability to gain access to the firm’s network. “At 6:00 a.m. hackers unleashed the ransomware, and by 7:00 a.m. our entire network had been compromised,” said the senior leader.

The ransomware spread quickly and the hackers were on the firm’s system for about one week. The Veeam data catalogue was corrupted by the ransomware and the firm was unable to restore from the Veeam backups they had been investing in for years. It lost years of backup data that could have significant compliance complications down the road.

“This was our first time getting attacked like this and we needed outside help,” the leader said. Some of the remote sites had very small network links, and the bandwidth necessary to do a complete restore was not there. The firm had all affected servers shipped from the remote locations to the home office to facilitate data recovery.

Druva restored many servers over the network, but also leveraged its integration capabilities with [Amazon Web Services \(AWS\) Snowball Edge](#), a data migration and edge computing device with 100 terabytes (TB) of capacity to handle low bandwidth servers.

The results

With standard restores from the cloud and the new AWS Snowball Edge-dependent feature, the firm was able to quickly rebuild its affected machines, restore the data equally fast, and move on to the next machine.

“Our strategy was to let the restoration run on a number of servers overnight and ship the servers back to our remote sites the next day,” said the senior leader.

The firm’s cloud-first backup strategy with Druva enabled it to recover 100% of the compromised data quickly, as the servers were wiped, rebuilt, restored, and shipped back to the 40+ sites in a matter of days.

The ransomware attack was stressful, but the firm was confident it could recover with the data protected safely in the cloud. That confidence was evident when it wasn’t tempted to pay criminals the ransom – an eye-watering seven-figure sum.

The Federal Bureau of Investigation’s (FBI) [Internet Crime Complaint Center](#) (IC3) reported a record number of ransomware complaints in 2020, with losses exceeding \$29.1 million. Not only did the firm gain ransomware protection with air-gapped, long-term backup of its 40+ file servers in the cloud, but it did so at one third the cost of its previous backup solution, while achieving 2.5x global deduplication storage savings.

“With Druva, we are already saving money on year one,” he added. And equally important, the firm now has the centralized visibility it needs across all remote sites, with the ability to scale storage capacity easily as it wins new contracts.



Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976	Japan: +81-3-6890-8667
Europe: +44 (0) 20-3750-9440	Singapore: +65 3158-4985
India: +91 (0) 20 6726-3300	Australia: +61 1300-312-729

Druva® delivers Data Protection and Management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted by thousands of companies worldwide, including over 50 of the Fortune 500. Druva is a privately held company headquartered in Sunnyvale, California, and is funded by Sequoia Capital, Viking Global Investors, CDPQ, Neuberger Berman, Tenaya Capital, Riverwood Capital, and Nexus Partners. Visit druva.com and follow us on [LinkedIn](#), [Twitter](#), and [Facebook](#).