druva

AWH

AWH Replaces Legacy Solutions With Druva for Ransomware Protection

3x
Increase in speed of data center backup restores compared to Veeam

100%
Business critical data protected — SaaS applications and hybrid workloads

3x
Global deduplication storage savings

About AWH

Originating in Geelong, with a heritage tracing back over many years, the business has been known as Australian Wool Handlers (AWH) since 1998. AWH has grown to become the largest independent logistics services provider to the Australian wool and cotton industries. AWH owns and operates the country's three national wool selling centers and handles over one million bales of wool annually, comprising more than 80% of Australia's national market share. With operations across the country and more than 220 employees, AWH is the world's largest wool logistics company by a considerable margin.

The challenge

For many years, AWH has managed a data center at its Lara, Victoria location. The data center contains a mix of infrastructure, including VMware virtual machines (VMs) and Windows file servers, which run business critical applications including data analytics, accounting, and budgeting. According to AWH CIO Darryl Drake, the company was using Veeam to protect data on VMware VMs and Windows file servers, but the backup data was both on-premises and on its network.

The latter became a critical concern when a ransomware attack struck Talman Software, a major wool-management IT solution, which shut down wool sales in Australia in early 2020. As Drake explained, "At three of our major sites, wool is sold in what is called an open-cry auction. It's important to note that AWH actually sells over 80% of all wool sold in

Challenges

- Dependent on an aging Veeam infrastructure to protect business critical data on VMware VMs and Windows file servers. Backup data was on-site and connected to the business network, making it vulnerable to ransomware
- A ransomware attack at Talman Software, a key technology partner, completely shut down wool sales and impeded its ability to sell wool for nearly three weeks
- After migration to Microsoft 365 and away from Barracuda, AWH had no way of restoring data that was older than 90 days, as Microsoft maintains a shared responsibility model

Solution

- The Druva Data Resiliency Cloud protects AWH's VMware VMs, Windows file servers, and Microsoft 365 data without any hardware, software, or associated complexity
- Backups are stored in the Druva cloud, powered by Amazon Web Services (AWS), which meets the company's goals of off-site and off-network backups
- Purpose-built orchestration and automation through their use of Druva solutions

Results

- Multi-layer defense against ransomware for data center workload and Microsoft 365 backup data delivers confidence to recover quickly if hit by ransomware
- 3x increase in the speed of data center backup restores compared to Veeam
- 3x global deduplication storage savings, which exceeded the CIO's expectations

Australia. The ransomware attack crippled the auctions business for nearly three weeks, completely preventing AWH from selling wool on the open-cry auction."

The ransomware attack encrypted Talman Software's data and backups, all of which were onsite and online. This was a clear signal to Drake and his team that they needed to move backups to the cloud so it would be offsite and off the company's network. They also felt it was critical to identify a resilient solution that would deliver multi-layer defense against ransomware.

The solution

In addition to the ransomware attack, another factor in the team's decision to migrate data protection to the cloud was its aging on-site Veeam backup infrastructure. "Veeam backups were all still online. We needed to move our backups to the cloud so they would be off site and off our network," said Drake.

The team discovered the Druva Data Resiliency Cloud in its search for cloud-native data protection and was impressed by its at-scale software-as-a-service (SaaS) platform. It was immediately clear the ways in which Druva could advance their organization's cyber, data, and operational resilience without any hardware, software, or associated complexity.

By the end of 2020, AWH had migrated its backups for hybrid workloads like VMware and Windows file servers from Veeam to Druva, leveraging air-gapped, cloud backups. The platform's built-in orchestration and automation for accelerated ransomware recovery brought added confidence of security and recovery, should an attack ever occur.

During this time, the CIO and team also initiated the company's two-year cloud strategy, which will eventually result in the closing of the Lara data center and the migration of all infrastructure to the cloud. As part of this initiative, the team has also migrated to Microsoft 365 for 430 active users, deploying Exchange Online, SharePoint, OneDrive, and Teams for collaboration. While it had previously used Barracuda for email backup, it now relies on the Druva Data Resiliency Cloud to also deliver comprehensive Microsoft 365 backup and long-term retention.

Results

With the Druva Data Resiliency Cloud successfully deployed, AWH now has the multi-layer defense against ransomware it was searching for. Drake's team is confident its data center workload and Microsoft 365 backup data are protected from encryption and deletion should a ransomware attack hit their organization. Unlike the on-premises Veeam solution previously used, Druva's cloud-native architecture provides multi-layer cyber defense for data and accelerates the recovery process.

"The driving force for us to select the Druva Data Resiliency Cloud was that when we tested it, it did what it said it would do, and was extremely easy to use. Regarding the latter, I'm referring to the backups — timing of them — and recoveries. What impressed us was how quickly it backed up to the cloud, and, more importantly, it was 3x faster and much easier to restore," said Drake.

Another benefit from the team's perspective is Druva's global, source-side deduplication. "We needed solid encryption and deduplication to reduce the amount of data that gets transferred to the cloud. The 3.14 deduplication ratio we get with the Druva Data Resiliency Cloud was a significant factor in our deciding to go with Druva," said Drake. "Since we began using Druva, the backup windows are always met or exceeded."

Ultimately, AWH has a solution that is empowering its cloud journey while protecting backups of VMware VMs, Windows file servers, and Microsoft 365 data through an air-gapped, secure architecture. The organization was able to eliminate aging hardware, and can now simplify management of backups and disaster recovery through an automated, cloud-based solution, reducing security risks and allowing AWH to focus on its data, not infrastructure.

druva

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

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

Druva® delivers Data Protection and Management for the cloud era. The Druva Data Resiliency Cloud 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.