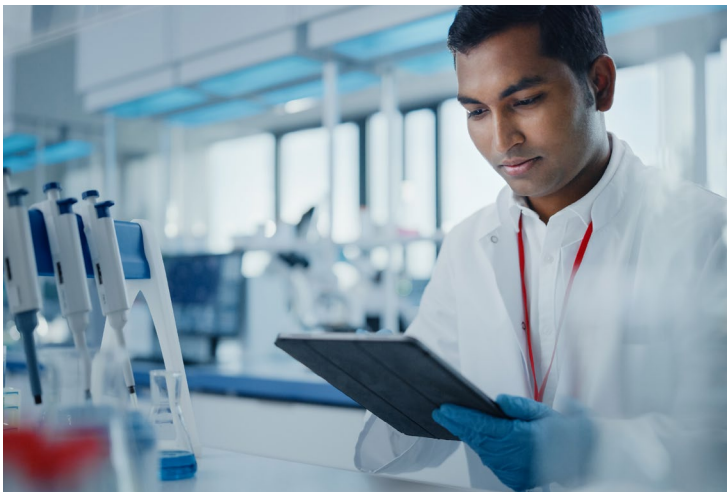
druva

Global Pharmaceutical Company Uses Druva to Back Up Microsoft 365 and AWS Workloads After Ransomware Attack



5x
Faster file recovery with the Druva Data Resiliency Cloud

50%
Less time spent managing backups

The challenge

A leading, independent global pharmaceutical services provider is growing at an enormous rate — increasing headcount by 10 times over the last four years.

Most of that growth has come from acquisitions, leaving the company's small IT team to manage a disparate environment that included seven on-premises Microsoft Exchange servers across the globe. Each server was backed up with a different on-premises solution — including Microsoft Data Protection Manager (DPM), Veeam, Veritas Backup Exec, and Backupify. The lack of consistency made it challenging to recover in 2018 when a ransomware attack took down most of the organization's network infrastructure. Luckily, the team managed to restore 95% of the network within two days.

The attack highlighted the vulnerability of storing data on-premises, as well as the complexity of using so many different backup solutions. So the company increased investment in migrating data to the cloud. The IT team wanted to support the move by choosing one consistent software-as-a-service (SaaS) backup solution to protect the company's data. The busy team needed a solution that could be deployed easily and would simplify the complexities of enterprise data protection. Plus, it needed the ability to restore data at a granular level. Something as simple as restoring a single email, without restoring an entire mailbox, was nearly impossible with the company's existing backup solutions.

Challenges

- A ransomware attack in 2018 highlighted the need for backup protection that was impenetrable to encryption or attacks
- Dependence on a variety of on-premises solutions Veeam and Backupify across IT locations made backups inconsistent and complex
- Needed a cloud-first data resiliency solution to enable centralized management of backups for SaaS applications, hybrid, and AWS workloads

Solution

- Isolated, long-term backups on the AWS platform are protected against ransomware attacks and are fully separate from the primary Microsoft Azure environment
- Multiple restore options to recover data at a granular level (any level, point in time, single file, or an entire site)
- Cloud-native backup and recovery for Microsoft 365 data and AWS workloads means no hardware, minimal administration, and the flexibility to scale infrastructure on demand

Results

- 5x faster email file recovery, compared to restoring from Microsoft's recycle bin
- 50% less time spent managing backups, increasing workforce productivity
- Data for 3,800 Microsoft 365 users is protected, including Exchange, OneDrive, SharePoint, and Teams
- The ability to prove compliance with strict data regulations in multiple countries — including GDPR, HIPAA, and California's CCPA

Finally, since the company's clients were pharmaceutical giants, it was subject to intense scrutiny and regular audits. It needed a better way to demonstrate compliance with multiple regulations for sensitive data and data residency, such as GDPR, HIPAA, and CCPA.

The solution

The team considered several solutions but many of the providers weren't mature enough to meet regional data residency requirements. The IT team uses Microsoft 365 Multi-Geo to store data in specific geographical locations for compliance, and as a result, needed a provider that could back up data in those same locations.

"We reviewed different solutions but were surprised that the Druva Data Resiliency Cloud was the only one that natively supports a multi-geo environment," a senior IT leader said. "That made us eager to evaluate Druva."

And with Druva storing backups in Amazon Web Services (AWS) — fully separate from the company's primary Microsoft Azure environment — the IT leader knew using it would help protect against ransomware. The team then met with Druva for a demo of how the solution would handle different scenarios. Even from the brief demonstration it was clear Druva was the right fit for the company. "It was one of the shortest sales cycles I've ever had," the senior IT leader added. "I could tell straight away that Druva would make it fast and easy for my team to restore data at a granular level. Plus, it would be simple to prove compliance with regulations to clients and governments."

The pharmaceutical services provider now protects its most important customer and business data using Druva — including Microsoft 365 (Exchange, OneDrive, SharePoint, and Teams) for 3,800 users and Oracle databases running in Amazon EC2. The team prioritized deploying Druva to protect those critical databases first, since each stores pharmacovigilance information related to adverse medical events.

Results

Choosing the Druva Data Resiliency Cloud has proved a wise decision, enabling the IT leader's team to recover files five times faster than previously possible with Microsoft's recycle bin. Plus, the team now manages backups in half the time it did before, improving workforce productivity.

Equally important is peace of mind. The senior IT leader is finally confident that the company will recover easily if data is compromised again. "When ransomware hits, we know our data in the Druva Data Resiliency Cloud is completely detached from Microsoft Active Directory," the senior IT leader said. "That allows us to simply log into it using non-Active Directory credentials on a system that's not tied to our domain so we can immediately start restoring data."

He said people often underestimate the importance of restoration capabilities. "I'm an IT consultant, and a lot of people think they have great backup in place," the IT leader said. "But I always ask if they've ever tested it, and they often say no."

"Knowing that with the Druva Data Resiliency Cloud I can literally go in and run a restore on a OneDrive folder, SharePoint document library, or somebody's email, and pull a single email back, really sold it."

And since recovery is simple with Druva, it's straightforward to satisfy auditor requirements. "Clients want to know how the company handles case intake, the speed of data recovery, patch management, and even how we manage end user workstations," the senior IT leader said. "These audits used to be really stressful, but with Druva it's easy to prove where we're storing our backups, how we protect data, and what measures we have in place to restore data in case of accidental deletion, corruption, or ransomware."

Looking forward, the IT team continues its active migration to the cloud. "We're glad we have Druva in place so we can keep retiring on-premises equipment and supporting our company's increasing cloud projects. Plus, we know we can easily scale our backups as we continue to grow."

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 enables cyber, data and operational resilience for every organization with the Data Resiliency Cloud, the industry's first and only at-scale SaaS solution. Customers can radically simplify data protection, streamline data governance, and gain data visibility and insights as they accelerate cloud adoption. Druva pioneered a SaaS-based approach to eliminate complex infrastructure and related management costs, and deliver data resilience via a single platform spanning multiple geographies and clouds. Druva is trusted by thousands of enterprises, including 60 of the Fortune 500 to make data more resilient and accelerate their journey to cloud. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.