druva

NIH NATIONAL CANCER INSTITUTE

National Cancer Institute prevents data loss with Druva

About National Cancer Institute (NCI)

NCI is the federal government's primary agency to address research and training needs for the cause, diagnosis, and treatment of cancer. As part of the National Institute of Health, it manages cancer research centers, local cancer control programs, and an international cancer research data bank. A good proportion of its workforce is mobile, supporting healthcare providers, laboratories, and research institutions in every corner of the country. Its IT group of nearly 300 supports over 8,000 NCI staff worldwide working on a variety of endpoints—PC, iOS, and Linux. IT also manages an extraordinary volume of data from genomics and trials to medical records and Freedom of Information Act (FOIA) requests.

The Challenge

There are often double standards between onsite and mobile infrastructure for employees, and NCI's was no exception. In the office, storage systems automatically safeguarded data with RAID, but on the road, staff lacked redundancy, and data was vulnerable until it was eventually backed up. According to Jeff Shilling, CIO and Chief, NCI, "We had intolerable data losses from hardware failure."

Another issue facing NCI was device refreshes. With a three-year refresh cycle and thousands of devices, IT was refreshing more than 3,000 devices a year—a never-ending task. All non-app/OS data was considered critical, and ensuring it was properly uploaded for archiving and re-installed on a new device was time consuming and labor intensive—particularly with unscheduled break/fixes.

> *"Cloud-first is a no-brainer, and the Druva platform aligned with our goals for digital transformation."*
>
> — Jeff Shilling, CIO and Chief, NCI

Challenges

- Lack of unified backup or archived data
- Device refreshes were time-consuming and lacked comprehensive restores
- Files for Freedom of Information Act (FOIA) requests were hard to locate and required device retrieval

Solution

- Druva provides NCI with comprehensive backup and data lifecycle management with full FedRamp compliance

Results with Druva

- Comprehensive cloud-based data protection of 8,000 NCI employees
- Self-service restore capabilities for end users—transformed restore time from hours to minutes
- Reduced infrastructure and IT labor costs
- Increased use of cloud apps and services by NCI and sister agencies in the National Institutes of Health

Also, protecting data for FOIA requests meant that when someone like a tobacco company lawyer asked for all NCI documents related to a particular case, NCI had 21 days to produce possibly thousands of files. This often meant forensic teams physically retrieving complete record sets.

> *"We have a lot of type-A, get-it-done people, they don't want to be without their computers, and this was hugely disruptive. We had to become a more automated, nimble, and agile organization."*
>
> — Jeff Shilling, CIO and Chief, NCI

The Solution

Recognizing the challenges, the NCI team deployed Druva based on its highly-efficient deduplication and the fact that it was a cloud-native solution leveraging AWS. "Cloud-first is a no-brainer, and the Druva platform aligned with our goals for digital transformation," said Jeff. The team chose Druva for data protection and governance and then together worked to establish FedRAMP compliance. Once achieved, NCI quickly deployed it throughout the organization.

Druva enables centrally-managed data protection for NCI—including backup and archiving, remote wipes, and geo-locating. It provides a simple approach to protecting, preserving, and discovering data while reducing costs, risk, and complexity. Patented global deduplication offers class-leading efficiency and decreased bandwidth usage by up to 80%—supercharging transfers. And, Druva harnesses the native efficiencies and global reach of industry-leading cloud provider AWS, offering unmatched storage flexibility, data durability, and security.

Importantly, Druva's solutions for government are built to meet the stringent federal regulations and compliance requirements, including FIPS 140-2, NIST 800-53, FedRAMP, FISMA, HIPAA and SOC2. Druva has a dedicated federal team and fosters strong ecosystem partnerships. As an AWS Government Competency Partner, Druva has consistently provided government agencies with powerful data protection and management—specifically tailored for compliance, security, and governance regulations.

Results

With Druva, data loss was no longer an issue—users could easily restore files on their own or involve IT when needed. And when hardware failed, refreshes included all of a user's recent data. Additionally, forensic teams could quickly access files when needed for FOIA requests regardless of their location. "We've saved untold infrastructure costs by moving data-protection workloads to the cloud that would usually be on-premises," said Jeff.

Druva solved NCI's data-loss issues and lightened their infrastructure load. Yet perhaps more importantly for NCI, it opened the door to a new understanding of the cloud. Deploying Druva, which leverages AWS as an integral part of its architecture, the NCI IT group began to understand AWS and the rich potential of cloud services. They contacted AWS and began setting up their own applications and services that were compliant with the Federal Information Security Modernization Act (FISMA).

According to Jeff, "We now see the cloud as a way to fulfill our strategic plan. By moving our resources away from functions that cloud services can do, we can focus on empowering the NCI staff to do their jobs better and fulfill the mission better."

Next Steps

Learn more about Druva and how cloud strategies help federal agencies meet the deluge of Freedom of Information Act requests in our white paper. Also, visit our government solutions page.

druva

Sales: +1 800-375-0160 | 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. 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 worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital, Viking Global Investors, and Nexus Partners. Visit Druva and follow us @druvainc.