



# Simplify endpoint backup with Druva

Six customer stories for overcoming  
data protection challenges

# Endpoint backup is **critical**

With the proliferation of remote work, misuse of cloud-syncing services for backup, expansion of eDiscovery and data governance requirements, rise in ransomware, and increasing insider threats, backing up endpoint data is a challenge for any IT organization. To ensure data protection and business continuity, it's critical to deploy an endpoint backup solution.

With Druva's endpoint backup solution, your data is protected anytime, anywhere. Our SaaS application ensures integrated backup, eDiscovery and compliance monitoring, simplified endpoint data protection, regulatory compliance, and improves data visibility for your mobile workforce.

Druva is well prepared to help our customers overcome any data challenges. Learn more about why our customers chose Druva for endpoint backup.

## Device loss, theft, or corruption

- Endpoint backup for all end-user data
- Remotely wipe data on lost or stolen devices
- Rapidly recover entire devices from snapshot

## Administration

- Centrally managed by IT
- Single sign-on support
- Role-based access control

## Security

- Customer-only access
- No key management required
- 256-bit encryption for data at rest

# The Institute **resolves** data compliance and security challenges



The Queensland Brain Institute is an Australian neuroscience research institute located in Brisbane at the St. Lucia campus of The University of Queensland. It is one of eight institutes at The University of Queensland and was established in 2003.

## The challenge

The Queensland Brain Institute's researchers work to understand the development, organization, and function of the brain. Collaboration with clinicians and commercial partners to develop new therapeutic approaches for brain diseases generates terabytes of data in the form of images and video files, much of which becomes paramount to research papers and grant funding.

## The solution

With most researchers having several hundred gigabytes of critical data on their machines and the need to facilitate global collaboration, an increasing issue The Queensland Brain Institute needed to solve was data availability and backup reliability at the endpoint. The team discovered Druva and quickly saw the benefits of cloud-based data protection for endpoints.

## Highlights

- 400 endpoints backed up protecting critical research data
- Data can be accessed 24x7x365
- Higher level of security with end-to-end encryption
- Faster restores for both compliance and recovery purposes

[Read the full customer story here](#)

# NCI **drives** data governance initiatives with Druva + AWS



The National Cancer Institute (NCI) is the federal government's primary agency to address research and training needs for the cause, diagnosis, and treatment of cancer.

## The challenge

NCI's storage systems automatically safeguarded data with RAID, but on the road, staff lacked redundancy, and data was vulnerable until it was eventually backed up. Another issue facing NCI was device refreshes. IT was refreshing more than 3,000 devices a year — a never-ending task. Ensuring that all non-app/OS data was properly uploaded for archiving and re-installed on a new device was time consuming and labor intensive. Lastly, files for Freedom of Information Act (FOIA) requests were hard to locate and required device retrieval.

## The solution

The NCI team chose Druva for data protection and governance and then together worked to establish FedRAMP compliance. Druva's solutions for government help organizations meet stringent federal regulations and compliance requirements. Druva is built on Amazon Web Services (AWS) and leverages the power of its high-performance architecture. In addition, 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.

## Highlights

- Cloud-based data protection of 8,000 NCI employees
- Comprehensive backup and data lifecycle management with full FedRamp compliance
- Reduced infrastructure and IT labor costs

[Read the full customer story here](#)

# Services leader **simplifies** search, eDiscovery, and legal holds



Integreon provides right-sized programs leveraging emerging best practices, technology, and a data-driven approach to re-engineer core processes and transform the way clients approach their businesses.

## The challenge

Data protection is critical to Integreon's business operations and reputation, as it provides services to customers worldwide. To protect data on hundreds of laptops, Integreon implemented the Veritas Desktop and Laptop Option. But Veritas' legacy approach became IT resource-intensive and time-consuming, as it didn't deliver full visibility or provide centralized management of endpoints, which exposed Integreon to vulnerabilities.

## The solution

Integreon implemented Druva to simplify backup, archival, compliance, and device management for hundreds of laptops. Druva also enabled Integreon to mitigate data loss and intellectual property theft. In addition, Integreon relied on Office 365 to house business-critical corporate data, but its native data protection capabilities weren't enough. So, Integreon expanded its Druva deployment to unify Office 365 backups into a single data pool that simplifies search, eDiscovery, and legal holds.

## Highlights

- 25% reduction in labor costs
- 25% in OPEX savings
- One-click legal hold for any user
- Easy connection to modern eDiscovery tools

[Read the full customer story here](#)

# University **improves productivity** by reducing backup times



Angelo State University is a public, doctoral-level, degree-granting university located in San Angelo, Texas. It offers more than 100 majors and concentrations through six colleges.

## The challenge

The challenge at the university is to protect a wide variety of valuable data that includes proprietary research, long-term records, administrative files, and course materials accessed by a diverse group of students, faculty, and staff. The IT department was looking for a solution to provide consistent and dependable data backup and recovery as the university has a four-year device refresh cycle. During the refresh process, the university would back up each device to a network drive, which would then be backed up to tape, a process that took 5 to 6 hours per device.

## The solution

Angelo State University implemented Druva inSync to simplify backup and recovery during the refresh process, drastically reducing initial backup time to 90 minutes per machine. This dramatic reduction in time required has freed up IT staff, enabling them to be more efficient and focus on other assignments.

## Highlights

- 75% reduction in backup times and restores
- Simplified OS and device refresh process
- Accelerated IT efficiency and productivity

[Read the full customer story here](#)

# ACS **minimizes** costs, risks, and complexity



The American Cancer Society is a nationwide, community-based voluntary health organization dedicated to eliminating cancer as a major health problem. It's mission is to save lives, celebrate lives, and lead the fight for a world without cancer.

## The challenge

With thousands of employees and volunteers spread across the United States, the American Cancer Society's IT team must constantly monitor and manage an enormous amount of data from primarily mobile endpoints to keep their organization running smoothly every day. Because most of its workforce consists of mobile volunteers, the American Cancer Society needed a way to rapidly and easily provision, deprovision, back up, and restore endpoint systems for their new users and existing users.

## The solution

Druva inSync provides a single pane of glass for the American Cancer Society to automatically protect, preserve, and discover information across their endpoints, wherever they may be – dramatically increasing the availability and visibility of business-critical data, while reducing costs, risk, and complexity.

## Highlights

- **Deduplication benefits to over 4,500 users**
- **IT saved an average of 20 hours during hardware refresh periods**
- **Achieved critical alignment with regional data residency policies**

[Read the full customer story here](#)

# Pharmaceutical company **streamlines** data retention processes



Allergan, PLC is a specialty pharmaceutical company producing branded and generic drugs as well as driving product innovation through research and development.

## The challenge

In the pharmaceutical space, there is the substantial level of regulation and government oversight to which all pharmaceutical companies in the U.S. are subject. Legal holds and demands for eDiscovery are common, and data retention requirements are often measured in years. While Allergan's acquisition of new companies has led to an exponential rise in the amount of data under its control, it was the divestiture of a portion of the company that brought its acute need for a more effective data retention strategy to light.

## The solution

To cope with the rapid expansion of the company, and the corresponding volumes of data being introduced, as well as the need to retain data from divested subsidiaries, Allergan made the decision to implement Druva inSync across all endpoints in the company. Druva inSync was installed on each workstation and laptop, allowing data to be automatically and unobtrusively collected in the cloud.

## Highlights

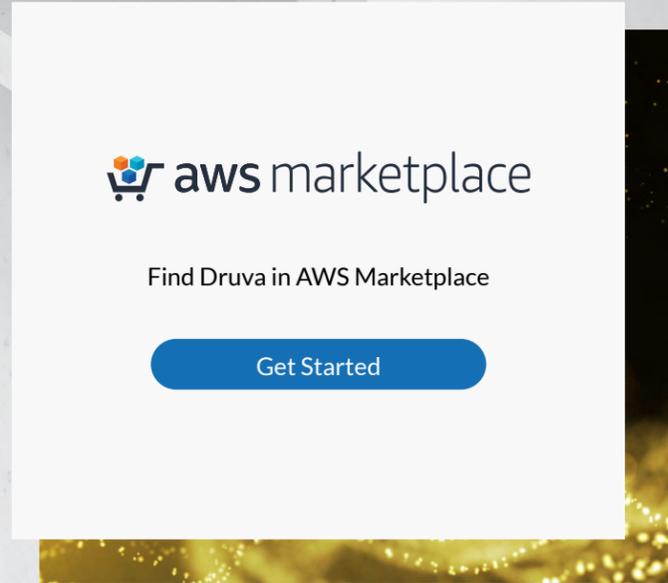
- Performed efficient data collection, visibility, and control during M&A
- Streamlined eDiscovery and legal hold process
- Provided endpoint backup without impacting end-user productivity

[Read the full customer story here](#)

# Next steps

Overcoming the challenges of ransomware, geographically-dispersed endpoints, cloud-syncing services limitations for backups – and eDiscovery and data governance – requires a more strategic endpoint backup plan. An industry leader like Druva provides an all-in-one endpoint backup solution to ensure your organization has complete control over all of its data.

**Learn more about how Druva provides seamless protection for your endpoints.**



The screenshot shows the AWS Marketplace interface. At the top is the AWS Marketplace logo. Below it, the text 'Find Druva in AWS Marketplace' is displayed. A prominent blue button with the text 'Get Started' is centered on the page. The background of the screenshot is a white box with a gold bokeh effect at the bottom.

 **aws marketplace**

Find Druva in AWS Marketplace

[Get Started](#)



The Druva logo consists of the word 'druva' in a lowercase, sans-serif font, followed by a stylized orange icon of a person or a shape.

**druva**

**Sales: +1 888-248-4976 | [sales@druva.com](mailto: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](#).