CrashPlan™

Case Study

Higher Education

Endpoint Data Protection

Industry
Higher Education

Company Size
2,300+ Employees

Location
Mid West

Topic
Endpoint Data Protection

Background

One of the premier research institutions on the planet, **needed to ensure personal and professional data privacy for every user.**

The institution also needed to **strengthen and quicken its recovery and prevention process for data loss incidents**, including ransomware.

While the IT team had existing strategies for protecting endpoint devices, **they recognized that their users' data needed additional protection.** In addition, the University needed to **streamline and automate its existing manual processes** to backup all electronically stored information (ESI) such as critical research data without sacrificing data privacy.

Their previous process relied on user-initiated solutions, including network storage, but users were wary. Researchers didn't trust the idea of their data being stored in a location that was accessible by management out of a desire to preserve academic integrity. Additionally, solutions that required additional steps on behalf of the faculty resulted in inconsistent compliance, out-of-date information and data loss.

The University needed an endpoint backup and recovery solution that people could trust to automatically protect users' data — without hindering their innovation.

Key Challenges

- Data privacy and security
- Ransomware recovery
- Users' aversion to surveillance
- Lack of trust in the cloud

Concern Over Privacy

The institution's culture is renowned for advancing new ideas, and boasts more Nobel Laureates than any other university. **Ensuring user autonomy, research independence, and academic integrity is critical to fuel and protect a culture rooted in discovery.**

With all of these concerns, data privacy was a primary concern when selecting a backup solution. Vendors (and sometimes administrators) having access to unencrypted data was not an option. "As part of our culture, we really respect their privacy," says the Chief Technology Officer of the Major Research University.

Off-device backups for important data were in place, but the global end-user base did not like or trust it. "Sucking all files into a central network-attached storage (NAS) would be a very tough proposition," says the CTO. "We wanted to give people a good experience regardless of how much they want to care about IT or organization."

"If you are concerned about ransomware, CrashPlan is the way to get data back."

Chief Technology Officer of a Major Research University

Research at Risk of Ransom

Educational institutions lose an average of $2.73 million per ransomware incident To avoid that, institutions need to protect their end-users from losing critical research data and the institution from suffering devastating losses from financial fallout, brand damage, and destroyed research.

With 11k+ users on the physical campus, the university knew all critical data had to be protected without additional user action. "Ransomware is a paramount concern, and we didn't want critical research to get ransomed," says the CTO. Pitching CrashPlan to the university, he shared "...if you're concerned about ransomware, [CrashPlan] is the way to get data back."

A centralized system that automatically and continuously **protects unstructured research data — without hindering research or presenting an opportunity for undue surveillance — was necessary.**

By working with CrashPlan, the research institution was able to protect its unstructured research data — while meeting the needs of the institution and the desires of faculty.

Solution

CrashPlan is an automated system that backs up every file on every device every 15 minutes. Instead of using manual processes, the University was able to collect and preserve user-generated data and mitigate the risk from any data loss incident or attack.

CrashPlan's unlimited cloud storage **enables users to retain and store as many versions of their work as they want.** And continuous backup support means **researchers and staff are up and running again quickly** following any issue — **without needing IT support.**

Key Use Cases

- Ransomware protection and detection
- Continuous and incremental backup
- Centralized management
- Delegated access
- Data privacy

Continuous, centralized management and privacy

With CrashPlan, the University has an efficient, secure way to remotely and centrally manage, deploy, and monitor backups.

Before CrashPlan, the higher education institution leveraged data-protection solutions which relied on human compliance. “When I would tell people to use a box or drive, I have no idea what’s going on with someone’s files or machine,” says the Chief Technology Officer. **“With centralized management, we are very glad to be able to see which machines are checking in and which ones aren’t.”**

CrashPlan’s security feature also allows institutes to **provide backup services to users without processing data or impacting academic integrity.** It is possible to configure the system to only allow access to research data by the researcher themself.

Today, the CTO and his team can have peace of mind knowing that essential data is always safe, no matter what. “When users are outside of our ‘perimeter’ we can still help them out,” says the Chief Technology Officer. “I like being able to say ‘if CrashPlan is on the machine, we’ll get you back up and running in just a moment.’”

> **“I like being able to say ‘if CrashPlan is on the machine, we’ll get you back up and running in just a moment.’”**
>
> **A Major University’s Chief Technology Officer**

Ransomware attacks cause significant disruptions to academic and administrative operations that lead to financial losses, reputational damage, and legal consequences. With the heavy use and reliance on digital resources, such as online learning platforms and research data, educational institutions are particularly vulnerable to cyber attacks.

CrashPlan is a simple solution that ensures user privacy and research integrity, helping higher education become and remain prepared with scalable, automated, pain-free protection that puts everyone’s mind at ease.

CrashPlan™

crashplan.com

CrashPlan® enables organizational resilience through secure, scalable, and straightforward endpoint data backup. With automatic backup and customizable file version retention, you can bounce back from any data calamity. What starts as endpoint backup and recovery becomes a solution for ransomware recovery, breaches, migrations, and legal holds. So you can work fearlessly and grow confidently.

For more information, visit **crashplan.com**.