When Your Cloud Goes Down, Your Business Doesn't

A DR Platform That Backs Up Once and Restores to Any Cloud

Portable backups. Tested switchover. No vendor lock-in.

Rediacc | 2026

The Problem in One Page

Your cloud will go down. Will your business?

On October 20, 2025, Amazon Web Services had its biggest outage in years. One deleted setting took down 141 services for 15 hours.

Snapchat, Robinhood, Uber, and Delta all stopped working. Two weeks later, Microsoft Azure had its own global outage that took Microsoft 365, Xbox, and even Scottish Parliament voting dark for 9 hours.

Cloud outages are getting worse. Critical events were up 18% in 2024 and lasted 19% longer (Parametrix 2024).

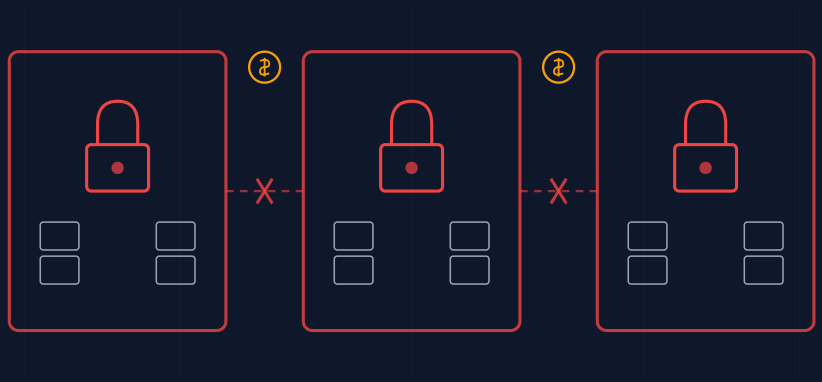
The world's 2,000 biggest companies lost a combined **$400 billion** to downtime that year, or about $200 million each (Splunk and Oxford Economics 2024).

Here is the gap: 89% of companies say they use more than one cloud company (like AWS and Microsoft Azure). Only 13% can actually switch from one to the other when one fails (Flexera 2024, Veeam 2024).

> **13% can actually switch.** That gap is why a single outage can take you down.

The Single-Vendor Failure Reality

One vendor means one point of failure



Three recent outages prove that betting on a single vendor is a single point of failure.

AWS, October 2025. A bot deleted one DNS record, taking **141 AWS services down for 15 hours**.

The list included Snapchat, Venmo, Robinhood, Coinbase, Delta, Uber, Starbucks, McDonald's, and Netflix (NBC News, CNN, AWS Post-Event Summary). Anyone using AWS for backup lost their main systems and their backup at the same moment.

CrowdStrike and Microsoft, July 19, 2024. A bad software update took down 8.5 million Windows PCs in the biggest IT outage on record.

Fortune 500 companies (not counting Microsoft) lost about $5.4 billion, or $44 million each on average (Parametrix). Delta Air Lines alone lost $500 million.

Azure, October 2025. One bad setting change crashed Azure Front Door for 9 hours. The outage took down Microsoft 365, Databricks, Xbox, Costco, Starbucks, Alaska Airlines, and the Scottish Parliament.

> If you run on one cloud, your recovery plan can vanish at the same moment you need it.

The Economics of Downtime

When minutes cost millions

How much does an hour of downtime cost? More than 90% of mid-size and large companies say over **$300,000 per hour** (ITIC 2024).

41% say between $1 million and $5 million per hour. The average is about $23,750 per minute (BigPanda 2024).

The world's 2,000 biggest companies lose roughly $400 billion a year to downtime (Splunk and Oxford Economics 2024). That is about 9% of profits gone.

A single outage drops a public company's stock price by **2.5% on average** and takes 79 days to recover. Outages keep getting worse, with critical events at the big three clouds up 18% in 2024 (Parametrix 2024).

The gap between plan and reality is stark. 82% of companies say their IT is not ready for disaster recovery (Datacore).

60% say their recovery plan did not work when they actually needed it (Alert Find).

Ask your IT team: what is our hourly cost of downtime, and what is our plan when AWS or Azure has its next big outage?

Why Cloud Companies' Own Backup Tools Don't Help

Each one only recovers to its own cloud

Most backup tools sold by cloud companies only recover back to that same cloud. That defeats the whole point if the cloud itself is the thing that failed.

Tool	What it does	What it can't do
AWS Elastic Disaster Recovery	Cheap. Recovers fast.	Only recovers to AWS.
Azure Site Recovery	Built into Microsoft Azure.	Only recovers to Azure.
Google Cloud Backup and DR	Built for Google Cloud.	Only recovers to Google Cloud.
Zerto (HPE)	Recovery in minutes. Works on AWS and Azure.	No Google Cloud support at all.
Druva	Backs up many sources.	Only restores to AWS. The whole platform runs on AWS.

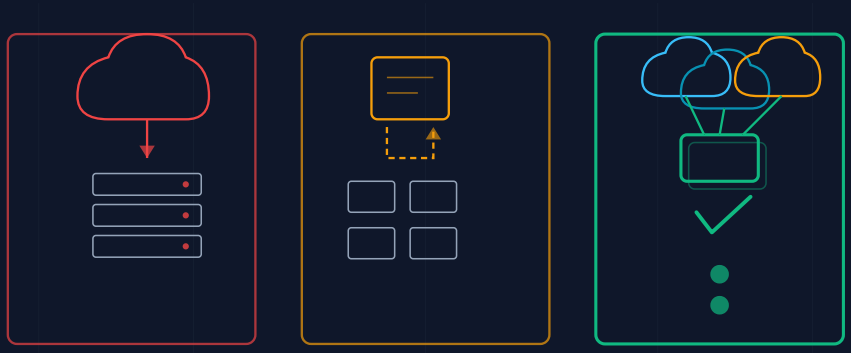
Druva looks like a product that runs on more than one cloud, but every recovery target is an AWS server. The whole platform is built on AWS.

When the cloud you depend on goes dark, a tool that recovers only to that same cloud is useless. You need to recover to a different cloud company entirely.

> Ask your vendor: if AWS is down for 15 hours, can your tool recover our systems on Azure or Google Cloud today, without any extra work?

Backup Vendors: Portability Claims vs. Reality

"Cross-cloud" rarely means what you think



Some backup vendors say they support more than one cloud. Read the fine print.

Veeam is the market leader, used by over 550,000 organizations. It stores backups in **a file only Veeam software can read**.

To restore to AWS, Azure, or Google Cloud, you need Veeam running on both sides. Veeam's newer Data Cloud Vault product runs only on Azure, creating fresh lock-in.

Commvault can move servers between AWS, Azure, and Google Cloud, but customers say it is hard to set up and expensive to run.

The pattern across every backup vendor: cross-cloud recovery is a marketing claim, not a tested process you can prove works.

The Hidden Tax: Exit Fees and File Formats

Why moving your data costs more than storing it

Exit fees are what your cloud company charges you to take your own data out. They run **$0.087 to $0.12 per gigabyte** across AWS, Azure, and Google Cloud.

One company watched its monthly data-export bill grow from $150 to $2,800 in six months. That was 25% of its total cloud spend (CloudOptimo).

Recovering 50 terabytes to a different cloud during an outage could cost **$4,350 to $6,000** in exit fees alone. Cross-cloud recovery inflates your total cost by 30 to 40% just from these fees (Mordor Intelligence).

The waste piles up. 27% of cloud spend is wasted on average (Flexera 2024), and companies overshoot their cloud budgets by 17% (Flexera 2025).

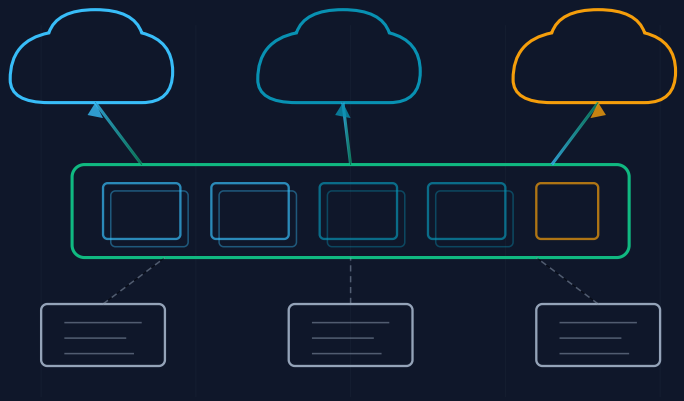
Lock-in is part of why. You pay to keep duplicate setups across clouds, you pay to move data, and you have no easy way out.

Then there are the file formats. Each backup vendor and each cloud uses its own format, so reading the data means buying that vendor's software.

> Like a phone plan where it's free to download but $5 per gigabyte to upload. Moving costs more than storing.

How Rediacc Changes This

A backup that does not belong to any cloud



Think of a Rediacc backup as a Polaroid of your filing cabinet that can't be edited. The picture is just the data, and it does not belong to any cloud.

Other vendors store backups in a file only their own tool can read. Rediacc takes the picture at the part of the disk that holds the data, before any cloud tool touches it.

A Rediacc backup from AWS can restore to Azure, Google Cloud, or your own servers. No file to convert, and no vendor tool needed at the other end.

This gives you three wins:

- No file format to convert when you switch clouds.
- The backup is locked the moment it is made.
- Only the changes get sent between clouds, so your exit fees stay low.

> At $23,750 per minute of downtime, a one-hour faster switch pays for the platform for a year.

Backups That Survive a Cyber Attack

Cross-cloud copies are physically separated by design

More than half of all downtime is now caused by cyber attacks (56%, Splunk 2024). Ransomware recovery costs the average victim **$2.73 million per incident**, up from $1.82 million the year before (Sophos 2024).

When backups are spread across more than one cloud, they are physically separated so a hacker can't reach them all. If AWS is hit, restore from Azure; if Azure is hit, restore from Google Cloud.

No single attack can wipe out every copy.

This is built into how the storage layer works, not added on top. The backups are locked the moment they're made, and they sit in clouds the attacker doesn't have access to.

> Ask your IT team: if a ransomware crew got our top admin password tomorrow, could they delete every copy of our backups? If yes, you have a problem.

Tested Switchover: Plan vs. Proof

Most plans for running on two clouds have never been tested

Here is the hard truth. Most companies that say they have a plan for running on two clouds have never actually tested it.

Only 13% of companies test recovery across clouds (Veeam 2024). When they do test, only 58% of servers come back on time.

50% of businesses test recovery once a year or less, and 7% never test at all (Security Magazine). 77% of companies that tested their backups found something broken (Storage Magazine).

It is like test-driving your backup generator every Sunday. Most companies find out on the morning of the storm that theirs has been broken for six months.

Rediacc tests the switch from one cloud to another for you. You get a date, a recovery time, and proof it worked.

Show your board the last successful switch instead of just a slide that says "we have a plan."

Ask your IT team: when did we last test a cloud switch, and how long did it take?

Backups in the Right Country

Region rules without losing recovery options

Europe's GDPR rule keeps data in Europe. US HIPAA does the same for health records. Banking rules add more. This sounds simple until you need to recover.

Many tools force a choice. Either you keep backups in one country (and one cloud), or you keep recovery options open.

Rediacc puts backups in set countries and on more than one cloud at once. Your European data stays in Europe, but you still have backups in two cloud companies inside that region.

If one cloud goes down, you switch to the other. If a regulator asks where your backup data lives, you can point to a specific country.

> Like keeping two house keys with two trusted neighbors on the same street: both nearby, neither one a single point of failure.

When Your Cloud Goes Down, Your Business Doesn't.

Rediacc backs up once and restores to any cloud, with tested switchover you can prove to your board.

Survive any cloud outage. Stop being stuck with one cloud company. Prove your recovery actually works.

Request a Demo | Schedule a Switchover Test | Calculate Your Savings

rediacc.com

One backup. Any cloud. Tested and proven.