rubrik

5 Things You Don't Know About Your **Cloud Vendor's Native Data Protection Tools**

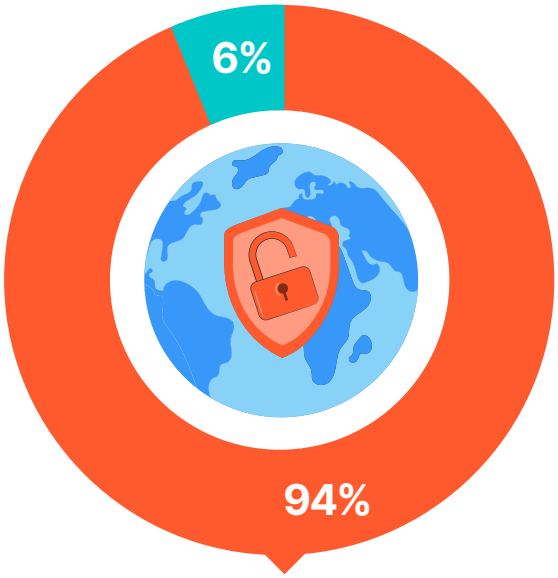
Protecting your cloud data isn't safe—or cheap—if you're using your cloud vendor's data protection tools

Table of Contents

Cyberattacks threaten your cloud backup data

You opened this ebook to learn five things you didn't know about your cloud vendor's native backup and cyber resilience tools. Don't worry. We'll get there soon enough. But first, let's get on the same page with a couple of facts.

1. Your data is under attack. Last year, ***94% of IT and security leaders*** indicated their organizations were hit by a major cyberattack.
2. Your cloud data is especially at risk. The cloud makes it super easy to spin up resources, something not possible with on-premises environments. But that convenience comes at a cost. The easier it is to access resources, the easier it is for folks to spread your data across different accounts, regions, services, and even clouds. And with that sprawl comes a bigger attack surface.



Organisations hit by major cyberattack

For almost as long as humans have created data, we've also created ways to protect it. One of the most tried and true ways of protecting data is creating another copy of it, or backing it up. For all our innovation, that premise still holds true in the cloud. The idea is that if your production data is compromised in some way, you can use a recent backup to continue operations with minimal disruption.

Many organizations utilizing cloud services, such as AWS, Azure, and GCP, are inclined to use the native backup resources offered by those cloud services. The thinking goes something like this, "I'm already getting all this great flexibility and scalability with my cloud vendor. Why not use their built-in backup services to protect our cloud data?"

And they'd be right … with a few notable exceptions.

Many organizations think that once they hand their data over to their cloud vendor, they're also handing over the responsibility to protect that data. That idea is reinforced by many cloud vendors' claims that they offer some version of **99.9%** availability. High availability might keep your systems running, but it doesn't shield your data from threats.

In fact, every public cloud vendor operates under the shared responsibility model, meaning that the vendor and the customer each hold some responsibility for availability and security. The details of who owns what are different from provider to provider and service to service, but they all have one thing in common: The customer is always responsible for who has access to their data and who can edit it.

Bearing the responsibility of protecting your data in the cloud is a bigger job than most organizations expect. Here are just a few reasons why:

01 Attackers know that you have critical data in the cloud, and they're going after it. Of the **94%** of IT and security leaders that indicated their organizations were hit by a major cyberattack, ***66% said the attack affected their cloud environments.***

02 Attackers know that backup data is your last line of defense, and they're going after that, too. Of that same ***94%, 96% of IT and security leaders said that the attackers tried to affect their backups.***

03 Attackers know that all they have to do is get the right credentials, and they can likely hop, skip, and jump their way across your cloud environment.

What's more: Cost efficient doesn't mean free. While true, on-demand scalable resources beat big on-premises investments, many organizations are starting to pay more attention to—and reel in—their cloud costs.

With all that in mind, it makes sense to question whether your cloud vendor's native backup and cyber resilience tools are really the right fit for your data and your business.

Your cloud vendor's built-in backup tools aren't equipped to protect your data

The backup tools your cloud vendor offers, like Azure Backup and AWS Backup, could be a good option if you're just getting started with the cloud and only have a small data footprint and a few non-critical apps running on the service.

However, for enterprises, they're just not ready for prime time. Cloud vendors are pouring their energy into services that require computing power, networking, and artificial intelligence (AI). Native backup services aren't their main focus. That means they won't have the features your business needs to protect critical data and keep your business resilient in the face of cyberthreats, malicious insiders, and operational disruptions.

More specifically, they don't offer:

- Simple and centralized backup management
- Fast recovery
- Truly cost-effective storage
- Data security built on zero-trust principles
- Robust cloud security features

If you rely solely on your cloud vendor's backup tools, you could be opening the door to higher cloud costs, operational complexity, and worst of all, not having your data when you need it the most. You need a cyber-resilient backup solution that covers all these bases. Unfortunately, these built-in backup tools don't. So, let's take an in-depth look at five things you might not know about your cloud vendor's built-in backup tools.

Five things you don't know about your cloud vendor's built-in backup tools

01 Your cloud vendor's built-in backup and data protection tools can get complicated—fast

In a perfect world, protecting your data across all your cloud platforms would be simple—same security policies, same UI, same recovery process, no matter the data source. With your cloud vendor's built-in backup and data protection tools, you get the opposite.

Not only do they not allow you to manage backup and data protection across different cloud vendors (AWS, Azure, GCP), oftentimes there isn't an easy way to manage them across services on *the same* cloud vendor.

Different types of data across different workloads on the same cloud require organizations to independently manage different backup schedules. Managing these multiple backup processes introduces complexity, adds significant work to your IT teams' plates, and increases the risk of errors like missed backups or incomplete data.

And if you're using multiple cloud providers—which most organizations are—things get even more complicated. Backing up all your data across different services, across different clouds is a tall order that requires tons of manual configuration and policy setting, and your cloud vendor won't offer you an easy way to do it all at once, especially across different clouds.

PRO TIP

Use a single system to manage backup and data protection across all your cloud and on-premises workloads. This cuts down on complexity, reduces IT headaches, and guarantees all your important data gets backed up properly, helping to make your organization cyber resilient in the face of cyberattacks, malicious insiders, operational disruptions.

02 Your cloud vendor's backup tools aren't built on zero-trust principles

Remember when we talked about how once a cybercriminal has access to your credentials, they likely have the power to hop, skip, and jump their way across your cloud environment—all the way to your backups? Zero-trust principles are what keep them from doing that.

Core zero-trust security controls should include:

Air gap: Backup data should be physically or logically isolated from your primary network. If malicious actors can't get at your backup data, they can't mess with it, keeping your backups safe and sound.

Immutability: Once created, backups should be uneditable and undeletable. So, even if your systems are infected, your backup data can't be encrypted, and its integrity is preserved.

RBAC (Role-based access control): Permissions on who gets to access and edit data should be assigned based on what's needed for each person's role. To minimize data exposure, only backup administrators should be able to manage backup configurations and have write permissions for backups.

Encryption: Data should be encrypted at rest and in transit to make it worthless to cyberattackers if they do exfiltrate it.

Least privilege access: Overprivileged users can threaten your backups and other parts of your environment, increasing the risk of unauthorized changes, accidental deletions, and insider threats. So, people with access to data should be granted only the minimum level of access needed to complete necessary tasks.

But here's the kicker: These five features aren't consistently available across all clouds or even all services offered from a single cloud provider. Instead, you're left to figure out which features apply where, adding more headaches to your data security efforts.

PRO TIP

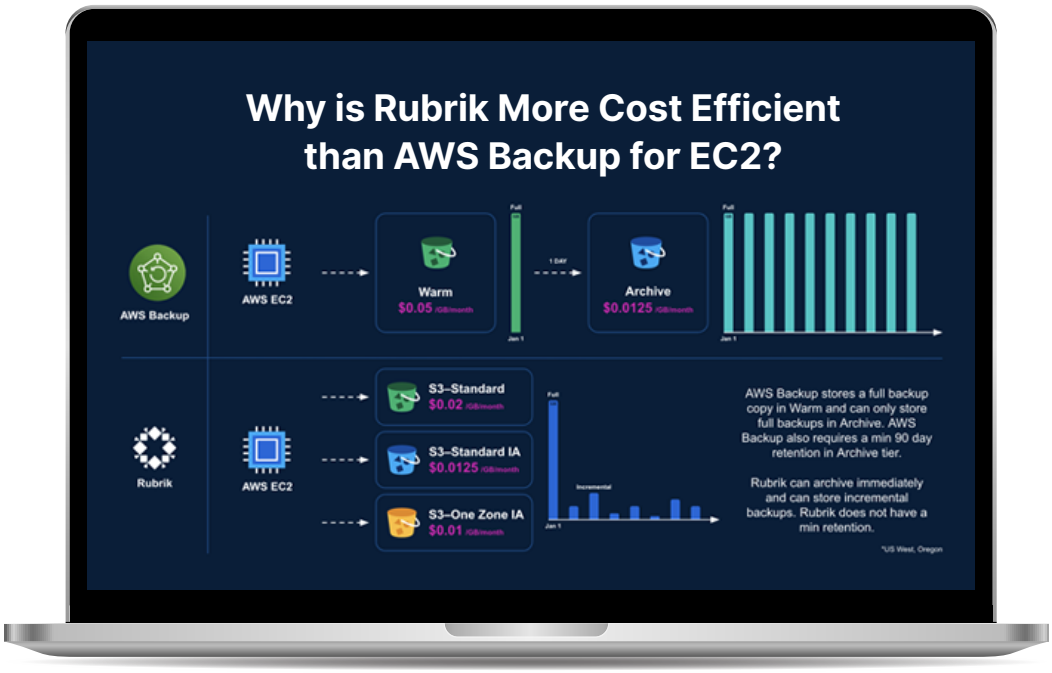
Adopt a zero-trust model for your backups that implements security controls (such as air gapping, immutability, RBAC, encryption, and least privilege access) consistently across all your data. These measures lock down your data and boost operational security.

03 Your backup data may cost more than your production data

Cloud vendors' built-in backup tools often miss the mark on cost efficiency. Despite having access to a range of cheaper storage tiers, cloud vendors typically store backups in warmer, more expensive tiers.

Backups can be shifted to colder, more cost-effective storage—and sometimes they are—but there's no guarantee that option will be available for your workloads.

For instance, with AWS, you initially have to back up EC2 data into Warm storage at **$0.05/GB/month**. Granted, that data only has to stay in Warm storage for a day before you can move it to AWS's Archive tier at **0.0125/GB/month.** But the Archive tier can only store full backups. So, every time you back up your EC2 data, you have to save a full backup to Warm storage, wait a day for it to be moved to Archive storage, and keep that backup for a full 90 days whether you planned to or not.



You would think that the same terms apply for AWS S3, but they don't. With S3, you have to back up your data to Warm storage at **$0.05/GB/month**. It doesn't automatically move to a colder and less-expensive tier—period.

Ideally, you'd want to optimize these costs by having the option to back up your data to a tier that's right for both your needs and your pocketbook, but that option isn't available with cloud vendors' built-in backup tools.

Wait ... but what if I need my data ASAP?

Some folks might argue that it takes longer to retrieve your data from Cold storage, so it's worth the added cost to have quick access to your data. This is a fair point. Still, you likely won't need access to 100% of your data immediately. Let's say there's 10% of your data that you would need access to immediately if something were to happen. Great. You should have the option to put that 10% in Warm storage and the other 90% in a colder tier. Plus, for many of these colder tiers, customers still have access to their data within roughly two hours, which very well may be an acceptable amount of time to justify the cost savings.

PRO TIP

Before you go with your cloud provider's backup service, explore other options that allow you to use cost-effective storage tiers from the start, by bypassing expensive warm tiers and moving data directly to cold storage. This approach saves money and helps allocate resources efficiently, keeping your cyber defenses financially sustainable.

04 Your cloud security controls aren't robust enough

Think your cloud vendor has the security controls that can protect your data? Think again. Data protection is more than just copying your data to another location.

Your cloud data isn't truly protected until you can:

See and control all your cloud data—especially sensitive data

Protect your data with immutable, air-gapped, access-controlled, and encrypted backups

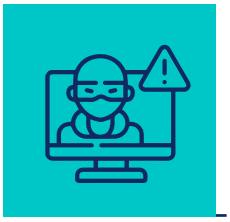
Automatically identify data risks, such as overexposed or unprotected data

See who has access to what data

Flag anomalies, monitor for threats, and identify out-of-the-ordinary user activity

The truth is: Most cloud providers don't offer these capabilities, so you're responsible for making sure you can protect your data. At a minimum, choose a backup and recovery option that allows you to:

Detect anomalies: You should have the ability to analyze your backup data for unusual behavior and changes that could be caused by a cyberattack. This analysis should also give you a clearer picture of which files and applications may be affected during an incident, so you know where to concentrate your recovery efforts.



Monitor for threats: You should be able to detect security threats early by using an up-to-date feed of threat intelligence to automatically identify indicators of compromise within backups.

Discover sensitive data: You should be able to see what types of sensitive data you have and where they live, so you can take steps to reduce sensitive data exposure and exfiltration risk.

Utilize data security posture management: You should have the ability to proactively reduce your data exposure risk by hardening your data security posture.

PRO TIP

Protecting your cloud data means having mechanisms in place to easily see and control it (including who has access to it), automatically identify risks within it, and flag suspicious activity. If your cloud vendor isn't helping you take these proactive measures across cloud environments, you need to find a better way to protect your cloud data.

05 Your backup is slow to recover

In situations where rapid recovery is essential for business continuity, your cloud vendor's rigid recovery options can slow you down at a time where every minute counts.

Here are four ways your cloud vendor's backup tools might slow you down:

1. Your cloud vendor's backup tools likely lack a search option that you can use to find the specific files you need to recover quickly, instead of hunting for those files manually.

2. Similarly, your cloud vendor's built-in backup tools probably don't offer a selective recovery option, so you can recover just the files you need. Instead, they often force you to restore entire backups.

3. Your cloud provider's built-in backup tools don't help you avoid infected backups. So, you run the risk of doing a recovery that ends up reinfecting your data and putting you back at square one.

4. Again, your cloud provider's built-in backup tools will only work for their cloud platform. So, if you need to do a restore across multiple clouds, you're left to do each recovery separately, which is an enormous time investment at a moment when you really can't afford it.

PRO TIP

Choose a backup solution that arms you with powerful recovery capabilities and helps you shrink your recovery time objectives (RTOs). At a minimum, this should include:

- Efficient, global search capabilities
- Selective, granular recovery
- Safe-backup validation
- A single interface with a unified recovery workflow

Don’t leave your data to chance. Choose RUBRIK SECURITY CLOUD

Your cloud provider may leave quite a few boxes unchecked when it comes to data protection and cyber resilience. But, of course, you don’t have to be limited by your cloud vendor’s built-in tools.

Rubrik Security Cloud can protect all your data, no matter its location, and keep your business resilient against cyberattacks, malicious insiders, and operational disruptions.

Here’s how:

01

Simpler backup management

Managing your cloud data protection with Rubrik is easy. The interface is intuitive and easy to pick up. With Rubrik, you can say goodbye to juggling a long list of policies and backup schedules across different cloud services and vendors. Rubrik gives you a single pane of glass to handle all of that, no matter the workload type or cloud provider. This centralization cuts down on complexity for a more comprehensive and resilient data protection strategy.

02

Built using zero-trust security principles

Rubrik Security Cloud has all the key zero-trust security controls your organization needs to keep your cloud data safe, including: air gapping, immutability, RBAC, encryption, and least privilege access. These controls keep cybercriminals from affecting your backups if they should happen to compromise someone’s credentials. Plus, unlike your standard cloud provider, Rubrik offers these controls across cloud, on-premises, and SaaS environments, so you don’t have to worry about which features apply where.

03

Optimizes cloud storage costs

Cloud vendors' built-in backup services, like AWS Backup, don't give you a lot of flexibility when it comes to optimizing backup storage costs. But with Rubrik, cost-effective storage tiers are used right from the start with no retention requirements. No more shuffling data through pricey, warm tiers first or storing more of your data for longer than you want to. Rubrik keeps your storage costs low and your backups affordable.

04

Lightning-fast recovery

Rubrik's recovery tools empower you to quickly locate the exact data you need, restore only what you want, and ensure backup fidelity, all from a single, unified interface.

05

Robust cloud security features

Not only does Rubrik offer anomaly detection, threat monitoring, and sensitive data discovery, Rubrik also helps you find unprotected or sensitive data, manage it well, and keep it safe. Rubrik DSPM gives you the control needed to lower the risk of data breaches and soften the blow of cyberattacks.

Act Now to Protect Your Data

Don’t wait for a cyberattack to expose the flaws in your cloud vendor’s native backup tools. Turn to Rubrik Security Cloud, the ultimate solution for cyber resilience. Rubrik’s proven approach protects your data, detects threats early, and helps you recover quickly, even in the worst-case scenarios.

Find out how you can achieve complete cyber resilience in the cloud.