rubrik | aws

HOW TO FULLY PROTECT YOUR DATA IN AWS

IN THE AGE OF AI

Your data is growing faster than your ability to protect it.

That's not a prediction. It's already happening. And as AI accelerates both data creation and the sophistication of attacks, most organizations don't know how wide that gap already is.

An estimated 173.4 zettabytes of data were created in 2025, with projections of 230-240 zettabytes in 2026[1]. How much is that? To put it in perspective, a single zettabyte is equivalent to 38 million years of high-definition video streaming non-stop.

As a result, today's organizations have more data stored in more places than ever before. They also have a tough time knowing what data they have, where it lives, and who has access to it.

The primary engine of this growth has shifted. While the pandemic initially accelerated the move to the cloud, the current surge is driven by artificial intelligence. The AI revolution is a key driver of data growth, with systems continuously generating and processing vast datasets to train machine learning models and power generative AI tools. According to IDC, global spending on AI technologies is expected to surpass $337 billion by 2025[2]. This investment is pushing the boundaries of the global datasphere, which is estimated to reach a staggering 394 zettabytes by 2028.

1. How Much Data Is Created Every Day: 40 Key Figures and Insights
2. Unlock the Future of AI: Key Predictions for 2025 and Beyond

Organizations have turned to the cloud—specifically AWS—to harness this power. AWS' ability to dynamically scale allows companies to fuel AI innovation without massive upfront infrastructure investments. However, this rapid adoption can create security blindspots. As the network perimeter expands and the attack surface widens, the risk of data sprawl increases, making robust data governance and Zero Trust security more critical than ever.

Today, AWS is a global leader in cloud infrastructure, owning 28 percent of the market[3]. Since its launch in 2006, AWS has largely retained its leading position due in part to smart investments that have enabled it to expand its network. A greater network means greater scale, allowing AWS to provide customers lower prices and enterprise-grade features.

As more organizations capitalize on the enormous benefits of the cloud—with 94% of enterprises now using some form of cloud service—best practices for securing data across on-premises and cloud environments are evolving. The average organization now manages data across 2.26 cloud providers and 89 SaaS applications[4]. This sprawling infrastructure is a major driver of risk, as human error and misconfiguration remain the leading cause of data breaches, cited by 28% of organizations. Ultimately, as IT environments become more fragmented, it becomes easier for users to make the small mistakes that leave an organization vulnerable to cybercrime.

A REPORT BY RUBRIK ZERO LABS FOUND THAT IN THE PAST YEAR, 52% OF IT AND SECURITY LEADERS' ORGANIZATIONS SUFFERED A DATA BREACH, AND 51% DEALT WITH RANSOMWARE IN THE SAME TIMEFRAME.[5]

3. Big Three Hold Dominant Lead in Accelerating Cloud Market
4. 2026 Edition - Thales Data Threat Report
5. The State of Data Security: The Human Impact of Cybercrime

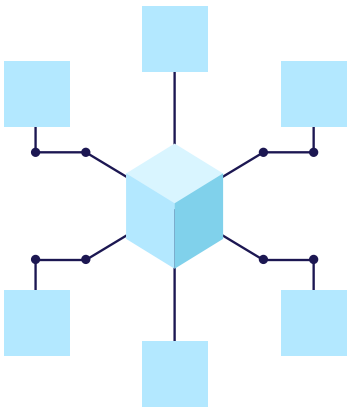
AWS offers robust solutions for security and compliance[6]. In addition to a secure architecture that allows users to build a secure infrastructure for their applications, AWS also houses a broad selection of security services users can employ to meet their security and regulatory requirements.

However, cybercriminals are continuing to find new, more advanced ways to infiltrate even the most secure infrastructures. Threat actors are increasingly using AI-fueled attacks—such as deepfakes and automated misinformation—to exploit human victims and bypass traditional security perimeters. Furthermore, credential theft has emerged as the most widely cited attack technique against cloud infrastructure, emphasizing that identity is the new frontline of the data struggle[7].

To manage data fragmentation and tackle cybercrime in the cloud, organizations must be able to protect and recover all of their data, gain visibility into their data through a single pane of glass, and manage cloud protection in a unified way.

Tackling Data Fragmentation

In order to keep its data protected, IT and security teams need to know where data lives, how sensitive it is, who has access to it, and how they can recover it if they need to. The sheer amount of data that's being created paired with the number of places it's being stored makes this a tall order even in strictly on-premises environments. As organizations start moving workloads to the cloud, it gets even harder.



Organizations need a better way to see and monitor their data across on-premises and cloud environments, so they can better identify vulnerabilities and determine if their data is being accessed or changed by an attacker or even a malicious insider.

Data backups are an organization's best line of defense against human error, natural disasters, hardware or power failures, and cybercrime. But if organizations don't know where their data is, backing it up and accessing it in a recovery scenario is going to be extremely difficult.

Organizations must be able to manage their backups simply, so they can access them when necessary to maintain business continuity.

6. AWS Cloud Security
7. Cloud Adoption Statistics 2026: Growth, Migration Drivers & ROI Highlight

Combating Cybercrime

Data in the cloud can be compromised as a result of accidental human error, outages, and everything in between, but cybercrime is its own beast—and one that's only getting bigger. Cybersecurity risk in 2026 is fueled by advances in AI, deepening geopolitical fragmentation, and the increasing complexity of global supply chains.

The scale of this threat remains unprecedented. Michael Mestrovich, Rubrik CISO and former CISO for the CIA, has noted that cybercrime is on track to be a $10 trillion business, positioning it as the third-largest economy on the planet[8].

Put simply, AWS is responsible for the security of the cloud, and customers are responsible for security in the cloud.

More specifically, ransomware is among the most profitable of cybercrimes. The average ransom demand grew 144 percent more in just the last year, according to the Unit 42 Ransomware Report[9]. And by 2031, Cybersecurity Ventures predicts that ransomware will attack a business, consumer, or device every 2 seconds[10]. As AI becomes more deeply integrated into attack methods, these threats are expected to become even more effective and difficult to defend against.

AWS operates on a shared responsibility model, meaning that AWS and its customers own different portions of security. AWS is responsible for security "of" the cloud—it operates, manages, and controls the hardware/global infrastructure and software, the virtualization layer, and the physical security of the facilities in which the services operate. The customer, on the other hand, is responsible for security "in" the cloud and manages their data, the guest operating system and associated application software and is responsible for configuring their security firewall[11].

Unfortunately, mistakes made by an organization's users are the most common way cybercriminals get access to data in the cloud.

8. Data Security Talks
9. Unit 42 Ransomware Report
10. Cybersecurity Ventures
11. Shared Responsibility Model

All it takes is one person to click on an especially convincing phishing email, and the network can be compromised.

These breaches are incredibly common. Organizations need a way to continuously monitor their data for threats. And should an attack happen, they need to be able to rapidly recover exactly the apps, files, and objects that were compromised—all while avoiding malware reinfection.

In these situations, backups are an organization's go-to resource. However, what happens when attackers target the backups themselves?

To secure their data from threats, organizations need air-gapped, immutable, and access-controlled backups.

ACCORDING TO THE WORLD ECONOMIC FORUM, HUMAN ERROR IS RESPONSIBLE FOR 95% OF ALL BREACHES[12]

Air-gapped backups are either physically isolated, meaning stored separately from any network-connected system, or logically isolated, meaning still connected to a network, but separated through logical processes, including encryption, hashing, and role-based access controls.

An immutable data backup means that once the data is saved, it cannot be changed, overwritten, or deleted. So, an immutable backup, once written, cannot be altered in any way, ensuring that the owner always has access to a clean backup.

Access-controlled backups simply mean that only the right people have access to data backups. In addition to preventing bad actors from getting in and wreaking havoc, access-controlled backups also prevent regular users from accidentally modifying a backup.

Only when an organization has easy access to a clean copy of its data can it be absolutely certain that it can maintain business continuity in the event of a cyberattack.

To accomplish this goal, they need two things. First, they need to be able to efficiently manage their data backups, so they can quickly access and use them when needed. And second, they need to consistently maintain a clean copy of their data, so they can be confident they can recover.

12. The Global Risks Report 2022: 17th Edition

How Rubrik Can Help

Filling the customer side of the shared responsibility model requires more than good intentions. It takes visibility across all your data, backups that can't be tampered with, and the ability to recover fast without reintroducing malware.

Rubrik Security Cloud was built for exactly this. It works alongside AWS to cover the data protection and cyber resilience responsibilities that sit on your side of the shared model — across your cloud workloads, SaaS data, and on-premises environments.

The goal isn't to replace what AWS does well. It's to make sure nothing falls through the gap.

Rubrik Security Cloud can help AWS customers with:

Data Security

Preserve data integrity, keep data readily accessible, and reduce data risks.

Rapid Recovery

Maximize uptime and ensure business continuity by reducing recovery times.

Unified Management

Use a single control plane via either the built-in UI or scripting to automate and unify data management across on-prem, edge, and the cloud.

Many infrastructure and operations leaders have turned to Rubrik to protect their organizations' cloud data. And Rubrik was positioned in the "Leader" quadrant in the 2025 Gartner® Magic Quadrant™ for Enterprise Backup and Recovery Software Solutions[13].

Rubrik can give you the peace of mind that you're doing everything you can to secure your data in AWS.

Available in
AWS Marketplace

Journey to AWS

For those organizations who are still evaluating their decision to move to AWS, Rubrik provides the opportunity to gradually enter the cloud. By archiving backups in AWS, users can retire costly storage solutions and move to a more affordable one.

Once data backups are in AWS, Rubrik can turn these backups into cloud instances, allowing organizations to run workloads in AWS. In other words, Rubrik gives organizations the option to take a slow-and-steady approach to their AWS journey.

Contact a representative to discuss in detail how you can cyber-proof your AWS cloud data.

13. 2025 Gartner® Magic Quadrant™ for Enterprise Backup and Recovery Software Solutions

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

How-to-fully-protect-your-data-in-aws / 20260612