rubrik

With Great Cloud Comes Great Responsibility

How to Fully Protect Your Data in AWS

People today like to say

that “data is the new oil.” But data, unlike oil, is multiplying at a truly astounding rate. Organizations are rightly capitalizing on their data, using it to better understand their audiences and create new revenue streams. As a result, organizations are facing unprecedented data proliferation.

By 2025, the amount of data generated, consumed, copied, and stored will reach over 180 zettabytes. How much is that? Well, one zettabyte has the capacity to hold 36 million years of HD video.[1]

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.

Organizations have turned to the cloud to harness the power of their data because of the cloud’s well-documented ability to help companies dynamically scale up and down without having to shell out large amounts of money in infrastructure investments.

The move to the cloud increased exponentially during the COVID-19 pandemic. A 2022 Statista survey found that 68 percent of enterprise decision-makers said the pandemic greatly accelerated their digital transformation plans.[2]

Today, AWS is the clear global leader in cloud infrastructure, owning 46 percent of the market.[3] Since its launch in 2006, AWS has 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. And because AWS has the largest customer base in its category with 1.45 million businesses, AWS has better insights than other cloud providers into how their customers use the cloud, allowing AWS to innovate new infrastructures that deliver exactly what customers are looking for.[4]

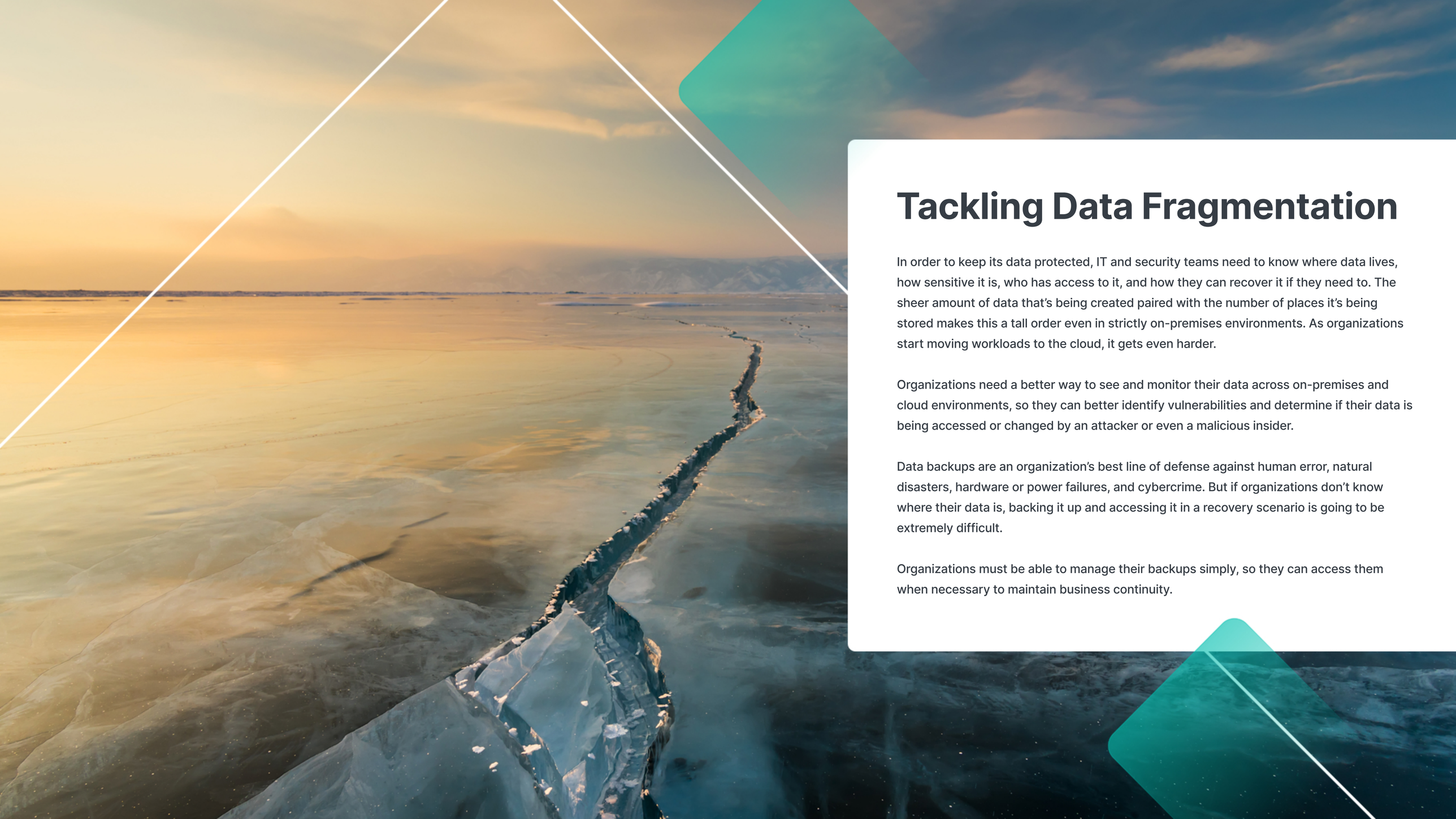
As more organizations capitalize on the enormous benefits of the cloud, best practices are also evolving on how to secure data across on-premises and cloud environments.[5] A 2022 Thales Security Study found that 51 percent of the organizations surveyed agreed that managing data protection in a hybrid or multicloud environment is more complex than a solely on-premises environment. And ultimately, more complexity makes it easier for users to make mistakes that can leave an organization vulnerable to 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, often preying on the psychological needs of their human victims to get access to an organization’s network.

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.

A new 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.[7]



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.

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.

During a recent event, Michael Mestrovich, former CISO for the CIA, noted just how lucrative cybercrime is: "The cybercrime business is on track to be a $10T business by 2025, and that will make it the third largest economy on the planet."[8]

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]

Like all cloud providers, AWS operates on a shared responsibility model, meaning that AWS and its customers own different portions of security. AWS operates, manages, and controls the cloud operating system, the virtualization layer, and the physical security of the facilities in which the services operate. The customer manages 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.

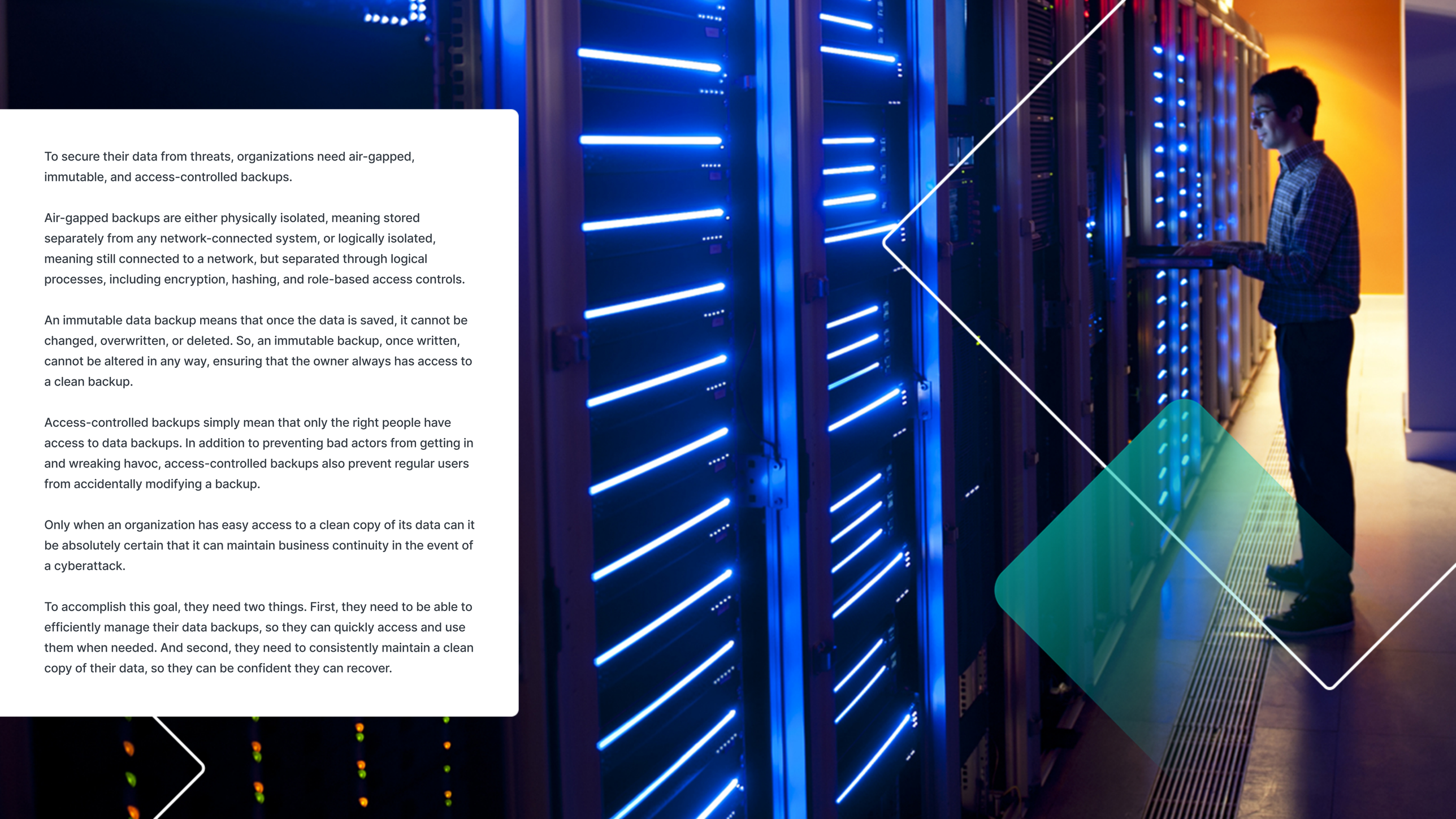
According to the World Economic Forum, human error is responsible for 95% of all breaches.[12]

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?

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



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

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.

How Rubrik Can Help

Rubrik is a cybersecurity company on a mission to secure the world's data. Rubrik pioneered Zero Trust Data Security™ to help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions.

Rubrik Security Cloud, powered by machine learning, delivers data protection and cyber resilience in a single platform across enterprise, cloud, and SaaS applications.

Rubrik Security Cloud can help AWS customers:

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 2022 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.

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

Journey to the Cloud

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

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

Rubrik Cloud Cluster

Rubrik Cloud Cluster, available in AWS Marketplace, is a simple way to enable what Rubrik does on premises in AWS.

Rubrik Cloud Cluster runs as a virtual appliance in AWS that leverages AWS services such as Amazon EBS snapshots and Amazon Machine Images to protect cloud-native workloads running on Amazon EC2 instances.

Cloud Cluster users enjoy access to features such as ransomware investigation and sensitive data discovery. Cloud Cluster also allows users to back up additional services.

rubrik

Available in
AWS Marketplace

References

1 What's a zettabyte? By 2015, the internet will know, says Cisco
2 Has the COVID-19 pandemic sped up digital transformation in your organization?
3 Gartner, Vendor Rating: Amazon, May 2022
4 https://hginsights.com/data-report/hg-insights-intricately-aws-ecosystem-report-in-2022
5 2022 Thales Cloud Security Study: The Challenges of Data Protection in a Multicloud World
6 AWS Cloud Security
7 The State of Data Security: The Human Impact of Cybercrime
8 Data Security Talks
9 Unit 42 Ransomware Report
10 Cybersecurity Ventures
11 Shared Responsibility Model
12 The Global Risks Report 2022: 17th Edition
13 2022 Gartner® Magic Quadrant™ for Enterprise Backup and Recovery Software Solutions