the GORILLA GUIDE® to...

Cloud Cyber Resilience

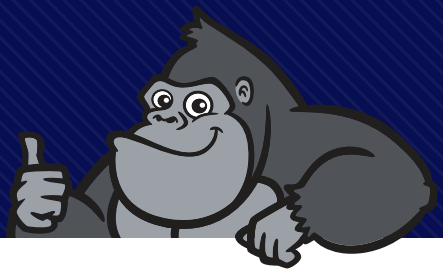
How To Protect Your Organization's Data in Multicloud and Hybrid Environments

LAWRENCE MILLER

rubrik

POWERED BY ActualTech MEDIA

the GORILLA GUIDE® to...



Cloud Cyber Resilience

How To Protect Your Organization's Data in Multicloud and Hybrid Environments

By Lawrence Miller

POWERED BY ActualTech MEDIA

www.actualtechmedia.com

PUBLISHER'S ACKNOWLEDGEMENTS

DIRECTOR OF CONTENT DELIVERY

Wendy Hernandez

GRAPHIC DESIGNER

Olivia Thomson

HEAD OF SMARTSTUDIO

Katie Mohr

WITH SPECIAL CONTRIBUTIONS FROM RUBRIK

Daniel Lu
PRODUCT MARKETING FOR CLOUD

Amanda O'Callaghan
DIRECTOR OF CONTENT MARKETING

ABOUT THE AUTHOR

Lawrence Miller, CISSP, is an information security professional with more than 20 years of professional experience in various industries. He has written more than 200 books on a variety of information technology and security topics.

ENTERING THE JUNGLE

CALLOUTS USED IN THIS BOOK

SCHOOL HOUSE

In this callout, you'll gain insight into topics that may be outside the main subject but are still important.

FOOD FOR THOUGHT

This is a special place where you can learn a bit more about ancillary topics presented in the book.

BRIGHT IDEA

When we have a great thought, we express them through a series of grunts in the Bright Idea section.

DEEP DIVE

Takes you into the deep, dark depths of a particular topic.

EXECUTIVE CORNER

Discusses items of strategic interest to business leaders.

DEFINITION

Defines a word, phrase, or concept.

GPS

We'll help you navigate your knowledge to the right place.

KNOWLEDGE CHECK

Tests your knowledge of what you've read.

WATCH OUT!

Make sure you read this so you don't make a critical error!

PAY ATTENTION

We want to make sure you see this!

TIP

A helpful piece of advice based on what you've read.

INTRODUCTION

Welcome to The Gorilla Guide To…® Cloud Cyber Resilience! In this guide, you'll learn about the rapidly evolving threat landscape and why a cyber resilience strategy built on prevention alone is not enough to protect your organization's data in the cloud.

We'll explain some common approaches to cloud cyber resilience today and introduce a better solution to help your organization protect its data in the cloud and achieve true cloud cyber resilience.

So, without further ado, turn the page and let's get started!

CHAPTER 1

Why Prevention Is Not Enough

As more organizations move critical applications and data to the cloud, cybercriminals are shifting tactics and focusing on the "target-rich environment" in the cloud. Given this dynamic threat environment, organizations must adopt an "assume breach" mindset. Thus, a cybersecurity strategy that focuses exclusively on prevention is no longer enough to ensure the security of your data and the viability of your business. Instead, a more holistic approach to cybersecurity and cloud cyber resilience is needed.

Cyberattacks Are Here To Stay

Threat actors are becoming increasingly persistent and sophisticated in trying to steal valuable company data. A recent Rubrik Zero Labs report highlights the scale of this problem: 94% of organizations have been targeted by cyberattacks. These attacks are not limited to a single point of vulnerability. The report found that many organizations were attacked across multiple environments, including SaaS (67%), cloud (66%), and on-premises (51%).

The complexity of modern cloud infrastructures has exacerbated this issue. Cloud sprawl—the uncontrolled proliferation of an organization's cloud environment— has significantly expanded the attack surface. This expansion makes it more challenging to protect data and requires specialized security expertise that many organizations currently lack.

Ransomware attacks have become increasingly devastating in recent years. The global cost of ransomware was predicted to reach $20 billion in 2021, and experts project this figure to skyrocket to $265 billion by 2031.

DORA—No, Not the Explorer

The Digital Operational Resilience Act (DORA) is a European Union (EU) regulation designed to accelerate cyber resilience capabilities among financial services institutions. The law requires financial services organizations in EU member states, and financial services organizations doing business with the EU, to improve their response to operational disruptions, such as cyberattacks, by placing much more emphasis on resilience and recovery as opposed to traditional detect-and-protect approaches.

Organizations that provide critical services to these institutions will also need to align with DORA regulations. Failure to comply may result in fines of up to 2% of their total annual worldwide turnover (revenue from sales of goods or services).

Beyond the cost of the ransom itself, successful attacks inevitably result in downtime, lost revenue, recovery costs, reputational harm, regulatory compliance penalties, and more. It's important to note that there is no honor among cybercriminals. Even if your attacker does provide a working decryptor to restore your data, there's no guarantee that your sensitive data won't still be sold on the dark web.

All in all, the total cost of a cyberattack is often in the millions of dollars. Full recovery, if achievable, can take weeks to months, leaving lasting impacts on the affected organization.

The world is on track to spend over $200 billion on cybersecurity this year, and some enterprise security teams use more than 75 tools in their prevention efforts. Despite these significant investments, attackers are still getting in and wreaking havoc, threatening businesses, reputations, and careers.

- The February 2024 UnitedHealth Group (UHG) ransomware attack reportedly cost more than $872 million and is expected to total more than $1 billion in direct costs.
- The September 2023 MGM Resorts International data breach caused 10 days of downtime and resulted in a $100 million hit to its third-quarter results.
- The Clorox cyberattack, disclosed in August 2023, resulted in nearly $500 million in lost revenues, more than $3 billion in loss of valuation, supply chain shortages, and the departure of their chief information security officer (CISO).

These examples illustrate how the cost of a cyberattack grows exponentially when businesses are unable to quickly resume normal operations, emphasizing the growing importance of cyber resilience in an "always-on" digital world.

What Is Cyber Resilience and Why Does It Matter?

Cyber resilience is an organization's ability to prepare for, respond to, and recover from cyberattacks and data breaches while continuing to operate effectively. The U.S. National Institute of Standards and Technology (NIST) defines cyber resiliency as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."

Developing a robust cyber resilience capability is a must for businesses and organizations in today's threat environment. When prevention fails to stop a cyberattack, the ability to quickly respond and recover is critical to the viability of the business.

The Information Technology Intelligence Consulting (ITIC) *2024 Hourly Cost of Downtime Survey* found that the average cost of a single hour of downtime now exceeds $300,000 for over 90% of medium and large enterprises.

Beyond the damage caused by an attack itself, costly downtime is inevitable—whether as a direct consequence of the attack (such as a ransomware or denial-of-service attack), the organization's incident response efforts (that is, containment and eradication), or both. Case in point, during the May 2021 Colonial Pipeline ransomware attack, the CEO quickly and correctly made the decision to shut down critical systems impacted by the attack to contain the spread of the ransomware. Despite their quick and effective incident response—and their decision to pay the $4.4 million ransom—it took several

days to resume normal operations, disrupting fuel supplies along the U.S. eastern seaboard and leading four U.S. states—Virginia, North Carolina, Georgia, and Florida—to declare a state of emergency.

The bottom line is that the longer you are down, the greater the impact on your bottom line. Downtime negatively impacts your business and your customers, and sometimes—as in the case of Colonial Pipeline—the entire supply chain. **Thus, cyber resilience is business resilience.**

A New Strategy Is Needed That Enables Businesses to Operate, Even When Under Attack

Traditionally, the cybersecurity industry has been busy building taller walls and wider moats across a variety of layers—endpoint, network, application—to prevent successful attacks. Every time there's a new type of attack, there's a new "must-have" prevention tool. But while prevention is necessary, prevention alone is not working. Modern cloud applications are decentralized, distributed across multi-cloud and hybrid environments, making it harder to secure with traditional defenses. To recover from cyberattacks, organizations must prioritize cyber resilience beyond infrastructure security. They must secure data itself because if data is secure and available, the business can continue operating.

CHAPTER 2

Recognizing the Challenges of Protecting Data in the Cloud

Protecting your data in the cloud comes with inherent challenges. One of the benefits of the cloud is that the cloud makes it easy to spin up resources. Because of that flexibility, it's also easy for data to sprawl across multiple accounts, regions, services, and clouds. This dynamic makes it hard to keep track of what's protected and how. More importantly, it's hard to identify what isn't protected. Threat actors know this all too well and, as a result, are increasingly targeting data in the cloud.

Cloud Sprawl Greatly Increases Your Attack Surface

When it comes to the cloud, sometimes you can get "too much of a good thing." While the cloud offers its customers many benefits, cloud sprawl has become a real problem for organizations today. In addition to driving up costs, cloud sprawl greatly increases your attack surface and amplifies the risk of misconfigurations that can easily lead to a data breach.

Cloud sprawl is often the result of shadow data—that is, data that is created, stored, or shared without being formally managed or protected by IT and security. Often, different lines of business or departments within an organization will provision their own cloud services from different cloud providers to suit their unique needs. For example, your developers may prefer Google Cloud Platform (GCP) because of its robust development ecosystem, Amazon Web Services (AWS) may be your marketing team's choice for the ease of use and familiarity of the Amazon Marketplace, and your infrastructure and operations (I&O) team deploys systems to Microsoft Azure to take advantage of a broad array of Windows services.

This situation leads to siloed accounts/tenants/subscriptions, as well as disparate user access controls and security policies. Without a clear and consistent view of your security posture across all cloud services, gaps in protection are inevitable. This lack of visibility and control not only puts data at risk but also makes it tough to meet compliance requirements.

More Attacks Are Targeting the Cloud

The unfortunate reality today is that it is a matter of when, not if, your organization will be the target of a cyberattack. The cloud doesn't make all these problems just magically go away. In fact, 94% of cloud tenants were targeted every month in 2022, and 62% of those tenants were successfully compromised. Ransomware attacks, in particular, have become increasingly common. Gartner Inc. reports that 75% of organizations will face a ransomware attack by 2025.

Threat actors are also increasingly targeting organizations with "double extortion" ransomware attacks in which they threaten to publish an organization's sensitive data unless another payment is

made. "Triple extortion" ransomware attacks go a step further and involve the threat actor launching a denial-of-service attack against the victim organization, or directly extorting a ransom payment from individual victims whose personal data has been compromised in the initial ransomware attack.

The growth of Ransomware-as-a-Service (RaaS) has also made it easier for threat actors with limited technical expertise to conduct ransomware attacks that are built and/or managed by others and licensed to the threat actor for a fee or commission. Many RaaS providers also offer technical support, collection services, and other "value-added" concierge services for the threat actor licensee.

Organizations that decide to pay a ransom to get their data back do so at their own risk. Even if an organization pays the ransom, it still might not get its data back. In fact, according to a 2023 Rubrik Zero Labs report, only 16% of organizations that paid a ransom were able to recover all their data and 46% that paid were only able to recover half or less of their data. Before making the decision to pay a ransom demand, organizations should consult with both law enforcement and legal counsel.

What you do now to prepare for the inevitable will determine whether an attack is successful and what, if any, damage it does to your business. Developing a cyber resilience strategy is one of the best ways to protect your business against the effects of cyberattacks.

CHAPTER 3

How Do Others Do Cyber Resilience Today?

Recognizing that prevention alone is not enough and that protecting your data in the cloud is increasingly challenging, you may be wondering how other organizations are doing cyber resilience today. In this chapter, we'll cover the four most common approaches to cyber resilience today.

Do Nothing

Your first option for backup and recovery isn't really an option, but many organizations mistakenly believe that moving their data to the cloud will also address their data protection and cyber resilience needs. As a result, they essentially do nothing. This dangerous assumption is rooted in several common misconceptions:

- **Shared responsibility model.** Every public cloud provider has a shared responsibility model (see the example in **FIGURE 1**) that shows which components of the technology stack (that is, physical infrastructure, network, virtualization, operating systems, applications, data, and so on) are the responsibility of the cloud

provider, and which components are the responsibility of the customer. The shared responsibility model differs slightly across cloud providers and for different service models—such as, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). But they all have one thing in common: The customer is always responsible for their own data.

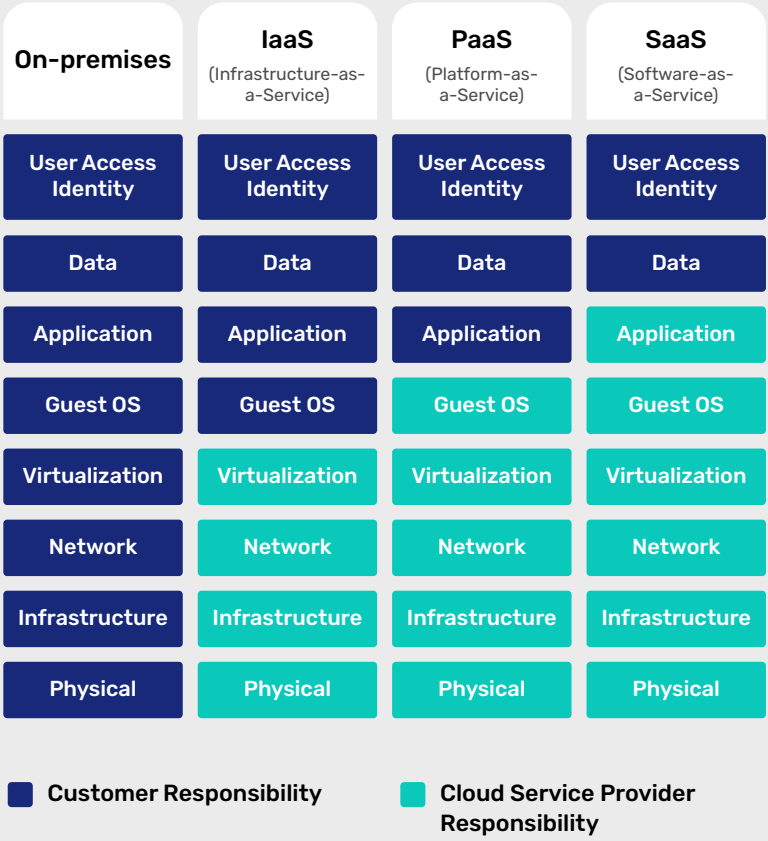


FIGURE 1: An example of the shared responsibility model

- **High reliability.** All the major cloud providers offer robust infrastructure and services with iron-clad "five-nines" (or better) availability (uptime) and "eleven-nines" durability (data integrity). Surely, there's no way you'll lose your data with that level of reliability. But high reliability is not the same as cyber resilience. High reliability minimizes downtime in critical systems due to hardware failures (such as a hard drive or server), whereas cyber resilience ensures your business can quickly detect, respond to, and recover from a cybersecurity incident.
- **Poor planning on your part does not constitute an emergency on the cloud provider's part.** Cloud providers do backup data and replicate it to other data centers and regions, but they do this to meet their service-level agreements (SLAs) and to ensure their cyber resilience, not yours. Also, cloud providers don't do anything to ensure that data is valid; if your original data has already been encrypted in a cyberattack, then the replicated backup copy is also encrypted. A cloud provider will not restore your data for you if a malicious insider deletes critical files or a privileged account is compromised and used to encrypt your data in a ransomware attack.

Do-It-Yourself (DIY)

Some organizations choose to go the DIY route to address their backup and recovery needs. Homegrown backup tools typically include custom-developed software and script-based solutions that are tailored to address an organization's specific or unique requirements. But these tools can vary significantly in terms of

complexity and functionality. While these homegrown tools provide granular customization and control, they also present several significant challenges:

- **Cost (actual and opportunity).** These tools are resource-intensive to develop, maintain, and update throughout the data lifecycle. They pull scarce and expensive resources (that is, your application developers) away from more strategic, value-added projects that support your core business.
- **Scalability.** Homegrown solutions are often purpose-built to solve a specific problem, such as backing up a specific type of data in a specific environment. As the application architecture evolves, and perhaps moves to a different cloud, these tools and scripts must be tailored to each and every cloud account, tenant, and subscription. This makes it difficult to scale as data volumes grow and infrastructure becomes increasingly complex. Finally, it's important to remember that backing up your data is relatively easy—ensuring those backups expire and that you aren't paying to store them indefinitely is the hard part.
- **Security and compliance.** They often lack the advanced security features essential for minimizing risks and ensuring regulatory compliance.

Lift-and-Shift Legacy On-Premises Tools

Some organizations may attempt to simply lift-and-shift their existing on-premises backup and recovery tooling (whether homegrown or off-the-shelf) into the cloud. Unfortunately, this approach often

hampers the agility and elasticity that organizations seek when adopting a cloud strategy because these legacy tools weren't designed or optimized for the cloud. These tools are inefficient because they are not able to take advantage of cloud native services, which hampers performance and can drive up costs. This lift-and-shift also results in a fragmented environment requiring different tools to protect data in different applications and clouds, making it challenging for IT to provide consistent protection for all the organization's data wherever it is located. Other challenges associated with legacy on-premises backup tools that are retrofitted to the cloud include:

- **Legacy backups are vulnerable to cyberattacks.** Legacy backups often do not have proper authentication and access controls based on a zero trust architecture with immutability, allowing threat actors to exploit vulnerabilities and gain unauthorized access to sensitive data, which compromises an organization's security posture. Additionally, these systems frequently use open storage protocols, exposing data to unauthorized access and manipulation by malicious actors.

- **Legacy backups do not provide critical insights or visibility into what data is at risk or what has been compromised during a cyberattack.** With legacy backup and recovery tools, it can be incredibly challenging to determine what to restore, when the attack occurred, how far the threat actor went, and the extent of the damage they caused. This piecing together of information is very time-consuming and can significantly delay the recovery process. And without the ability to identify clean point-in-time backups, organizations run the risk of reinfection from a compromised backup.

- **Legacy backup tools are not built for the cloud.** On-premises environments are relatively static compared to the highly dynamic nature of the cloud.

> Legacy backup tools typically provide little or no support for API-driven operations and Infrastructure-as-Code (IaC) principles, are unable to capture cloud-native configurations, metadata, and stateless components, and are not optimized for cloud network latency and bandwidth constraints. As a result, legacy backup tools are ill-suited for the cloud.

Native Backup Tools from Cloud Vendors

Finally, many organizations rely upon their cloud provider's native tools to address their backup and recovery needs. Cloud-native backup tools are services designed and optimized specifically for backing up data in the cloud providers' respective cloud environments. These tools integrate seamlessly with other services offered by the cloud provider and offer basic (sometimes advanced) backup and recovery features, making them a popular choice among customers who need foundational backup capabilities in the cloud. A big reason organizations use a cloud provider's native tools is because it's "easy" and they want to save time; but "easy" does not necessarily mean "right."

Some organizations think that native backup and recovery tools are "good enough," but a "good enough" approach to cloud cyber resilience won't protect your critical data and your business from modern threats.

While it might seem convenient to adopt a native cloud backup solution if a company has already invested in a specific cloud platform, native backup tools typically lack the flexibility, scalability, capabilities, and features that are needed to achieve cyber resilience for an organization's critical data in the cloud. Native tools can also be complex and cumbersome to use. And of course, native tools focus on protecting only data in the cloud provider's environment, not data in other clouds or in on-premises data centers. Other challenges associated with native backup tools include:

- **Lack of multicloud and hybrid support.** Often, cloud-native tools are built and optimized for a single cloud environment, such as AWS, GCP, or Microsoft Azure. This limitation makes it difficult to manage backup and recovery across multiple clouds, SaaS applications, and on-premises infrastructure. Even when these essentially proprietary tools do support other cloud environments, their functionality is limited, and the customer may incur additional data egress costs.
- **Fragmented management.** Even within the same cloud environment, these tools can have fragmented management approaches for different workloads, making it difficult to ensure comprehensive data protection and requiring individual management and configuration in each cloud account. Additionally, these tools may employ different approaches for different workloads—some look more like snapshots, some like basic backups; some can be made immutable, some cannot; some can be stored long term, some cannot. It can get complicated to say the least.
- **Limited security insights.** Cloud-native backup tools often lack data threat analytics and security posture management capabilities, making it difficult to monitor the environment for suspicious activities, detect potential cyberattacks, or identify sensitive data risks.

- **Backup storage costs.** Cloud-native tools are generally not cost optimized for storing backup data. As a result, the cost of storing backup data is sometimes more than the cost of storing the original data itself. For example, AWS Backup costs $0.05/GB/month to store S3 backup data, which is more expensive than storing the original data ($0.022/GB/month).

CHAPTER 4

A Better Solution for Cloud Cyber Resilience

Traditional approaches to data protection—whether it's doing nothing, going the DIY route, lifting-and-shifting your legacy on-premises tools, or using your cloud provider's native tools—often lack enterprise-grade features, like search and file-level recovery, logically air-gapped backups, and advanced security capabilities, like sensitive data discovery, necessary for true cloud cyber resilience. Clearly, a better approach to cloud cyber resilience is needed. But what exactly should you look for in a cloud cyber resilience solution? Ideally, a cloud cyber resilience solution should be built with the following capabilities and features in mind:

- Simple unified protection
- Holistic cyber resilience
- Rapid recovery
- Low total cost of ownership (TCO)

Simple Unified Protection

As companies continue to adopt public cloud services, it's becoming more difficult to get a baseline backup across dozens or hundreds of cloud accounts and subscriptions to ensure cyber resiliency and prove compliance. Implementing consistent policies at scale requires manual job scheduling or painful scripting, draining IT productivity. Multicloud and hybrid environments have become increasingly common as organizations choose best-of-breed solutions to address their unique business requirements. However, a multicloud and/or hybrid strategy requires specialized skills across different environments to configure and manage disparate cloud resources and tools, often leading to risky misconfigurations, operational inefficiencies, and inconsistent data protection.

Look for a cloud cyber resilience solution that provides a single platform covering multicloud and hybrid cloud environments, including SaaS applications and on-premises data centers. It should support all major public cloud providers, such as AWS, GCP, Microsoft Azure, and others. It should automatically discover and secure cloud workloads, as well as SaaS and on-premises applications, making it the central control point to set data protection policies, enable visibility of backups, restore data, and ensure compliance and auditability. Finally, look for a solution that provides out-of-band management, ensuring your data protection stack runs independently from your production stack.

According to a 2023 Rubrik Zero Labs report, nine out of 10 organizations reported malicious actors attempted to access data backups during a cyberattack, and 73% were partially successful.

Holistic Cyber Resilience

Look for a cloud cyber resilience solution that ensures data integrity and availability of cloud data with automated, air-gapped, immutable, and access-controlled backups designed to withstand cyberattacks, malicious insiders, and operational disruptions for all data sources. The solution should be able to accurately identify sensitive data, continuously monitor your data for anomalies and threats (including ransomware, data destruction, and indicators of compromise), and provide intelligent insights into exposed and at-risk data to maximize data security posture. Determining the scope of an attack and potential sensitive data exposure is particularly crucial for organizations that are subject to regulations, such as the EU General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), which require prompt notification when sensitive personally identifiable information (PII) is compromised.

Built for the Cloud

Your cloud cyber resilience solution should be cloud native and built on well-architected design principles that include:

- **Software-defined:** Consolidate disparate hardware and software components into a single software fabric with deployment flexibility, including on-premises plug-and-play appliances, software on third-party hardware, or software in the cloud.
- **Simplicity at scale:** Easily handle rapidly increasing volumes of information with a linear-scale architecture that eliminates management complexity.
- **Cloud mobility:** Enable cloud and application mobility whether deployed on premises or in the public cloud

to protect cloud-native applications, search across applications and files, and quickly spin up instances for test/dev or disaster recovery.

- **Application programming interface (API)-first:** Look for an easily extensible data management solution that helps users leverage APIs with industry-standard OpenAPI documentation, sample code, and pre-built integrations with various automation tools.
- **End-to-end security:** Protect data across the entire lifecycle with a comprehensive multi-faceted approach to security that includes data encryption in-flight and at-rest, unlimited immutable snapshots, granular access controls, and more.

Rapid Recovery

Restoring a single workload instance in the cloud is often a manual, multi-step process that varies by cloud service and provider. The more manual steps the organization must perform, the more opportunities there are for human error and the longer it takes to restore your data and resume normal business operations.

Look for a cloud cyber resilience solution that provides global search and file-level recovery capabilities across cloud backup data to confidently achieve a near-zero recovery time objective (RTO) by granularly recovering apps, files, and objects with just a few mouse clicks. Incident responders should be able to quickly identify a good backup without having to manually validate each workload, so individual workloads can be confidently restored without the risk of reinfecting your production environment.

Lower TCO

Cloud sprawl has become a major challenge for organizations as they rapidly adopt public cloud services, causing costs associated with cloud storage to escalate. Against the backdrop of rising cloud costs, companies are looking for ways to control costs by optimizing their cloud usage, including hard backup costs, such as compute resources needed for data backup, indexing, archiving, and recovery. Look for a cloud cyber resilience solution that provides the ability to store backups to lower cost object stores AWS S3 Glacier and Azure Blob Archive Tier, perform incremental backups instead of full backups, and leverage data reduction capabilities, such as compression and deduplication.

By streamlining security policy setup, data recovery management, threat monitoring, and compliance reporting, organizations can reduce their soft backup costs, saving time and resources that can be redirected to focus on other critical business priorities.

Wrapping Up

This guide has provided a look at the need for cloud cyber resilience to protect your organization's data in multicloud and hybrid environments. The modern threat landscape is rapidly evolving, and the enterprise attack surface has greatly expanded, creating a perfect storm for threat actors. Achieving true cloud cyber resilience requires a better approach to data protection that's built on a simple, unified cloud-native platform with capabilities that include holistic cyber resilience and rapid recovery while helping organizations reduce their cloud spend.

Learn more about Rubrik's perspective on cloud cyber resilience via content, webinars, demos, and other offers at https://www.rubrik.com/solutions/cloud-solutions.

ABOUT RUBRIK

Rubrik helps enterprises achieve data control to drive business resiliency, cloud mobility, and regulatory compliance. Rubrik bridges the gap between owned, on-premises infrastructure and the cloud by decoupling data from the data center through a software-defined fabric and offering a single management plane for all data, whether on-prem or in the cloud. Comprehensive data management is delivered through instant access, automated orchestration, and enterprise-class data protection and resiliency.

ABOUT ACTUALTECH MEDIA

ActualTech Media, a Future B2B company, is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.

If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit actualtechmedia.com.