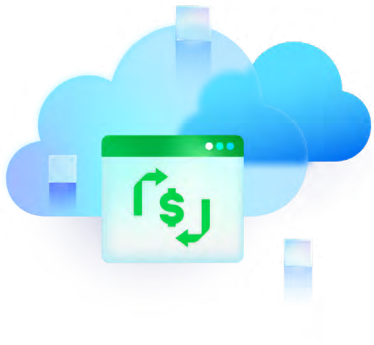
Mastering Hybrid Cloud Backup Costs, Security and Management

Key insights and best practices to hybrid cloud backup success

Contents

Introduction

This e-book is designed as a dynamic resource, offering a comprehensive overview and actionable insights for making informed, strategic decisions so that your organization will have a cost-optimized and secure environment. Whether you are an IT professional, a business leader, or a member of your company's cloud team, this e-book aims to polish your understanding of the intricacies of managing cloud costs, security, and backup so you can traverse the ever-changing hybrid and multi-cloud landscape with confidence.



Control cloud costs

Secure backups

Unify management

Chapter 1: Controlling Cloud Costs

In both hybrid and multi-cloud environments, cost control is crucial — which may explain why 82% of organizations consider managing cloud spending as their top business challenge.[1] Resources spread across both on-premises infrastructure and multiple cloud services lead to increased management complexity and the potential for bill shock. Without cost-control measures, organizations run the risk of incurring unnecessary expenses due to duplicated efforts, underutilized assets, and misaligned resources.

Put simply, you must plan, implement, and optimize for an effective yet cost-efficient cloud strategy.[2] Through comprehensive understanding and adherence to the guidelines provided below, organizations will be able to maximize the financial efficiency of their cloud storage solutions.

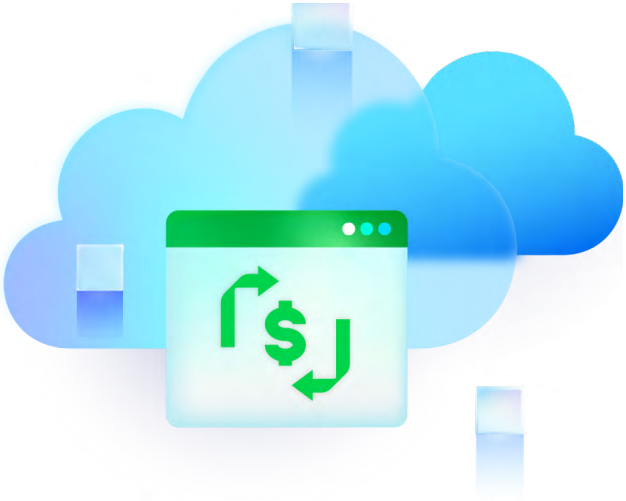
Plan

Snapshots vs. Backups

As we begin, it's essential to understand the difference between snapshots and backups when tasked with the management of hybrid or multi-cloud environments.

Snapshots are a point-in-time copy of a data set, usually taken for quick recovery purposes. However, like storage snapshots, snapshots of cloud services are often stored on the same volume(s) they're supposed to protect. As such, they fail to protect against all data loss scenarios, such as accidental deletion of the primary data store, corruption, security events, and more.

Backups, on the other hand, are a separate copy of that data set stored in a different location. They offer an additional layer of protection and point of recovery, and thus give you the flexibility to recover data in the event of human error or security event. With backups, organizations can ensure comprehensive cyber resilience and recovery options, making them the preferred choice in ensuring data resiliency and business continuity.



[1-2] Considerations for Cutting Cloud Costs

Cost Calculators

Utilizing the cloud can be costly. Without proper care and research, it can render organizations with bill shock and overspend. This is why it is important for organizations to properly plan, monitor, and optimize their usage to create a cost-optimized environment. There are many tools available from hyperscale cloud providers and third-party vendors that help organizations forecast their spend. Proactive forecasting, as well as ongoing monitoring and alerts, can help curb bill shock through right-sizing instances, auto-scaling, unused resource termination, data lifecycle management, and much more.

Cost calculators are particularly useful when it comes to data protection as organizations create and store multiple copies of data, often for lengthy periods of time. Balancing service level objectives (SLOs), retention, and budgets without hindering resilience can be tricky, but is certainly made easier through proper calculation and assessment.

Implement

Lifecycle Policies

Advanced data lifecycle policies are essential for managing data throughout its lifespan in a cost-effective and efficient manner, particularly in cloud environments. These policies are sets of rules and automations that dictate how data is handled from its creation to its deletion. They govern when data should transition to different storage tiers, how long it should be retained, and when it should be archived or purged. By automating the movement of data to the most cost-efficient storage tier based on its age, access patterns, and relevance, organizations can substantially reduce storage costs.

Similarly, a retention policy may delete data that is no longer required for legal or business reasons. Employing such granular control helps ensure that an organization is not overspending on premium storage for data that doesn't necessitate it and aligns operational expenses with actual data usage and value.

Compression

Implementing data compression within cloud storage settings offers multiple benefits. Firstly, reduced file sizes directly translate to lower storage costs. Cloud storage providers typically charge based on the volume of data stored; by compressing data, you store fewer bytes and incur less cost. Compression also has the potential to speed up data transfer times and reduce network bandwidth consumption — which, of course, is crucial when dealing with large-scale data transfers or backups over the network.

When considering data compression as a cost-saving measure, organizations should evaluate the nature of their data, the frequency of access, and the specific capabilities and costs associated with their cloud storage provider.

Optimize

Automate Processes

Adopting automation tools has become a cornerstone of a resilient and scalable data management strategy, acting as defined sets of rules that dictate how and when data backups are initiated, maintained, and retired without manual intervention.

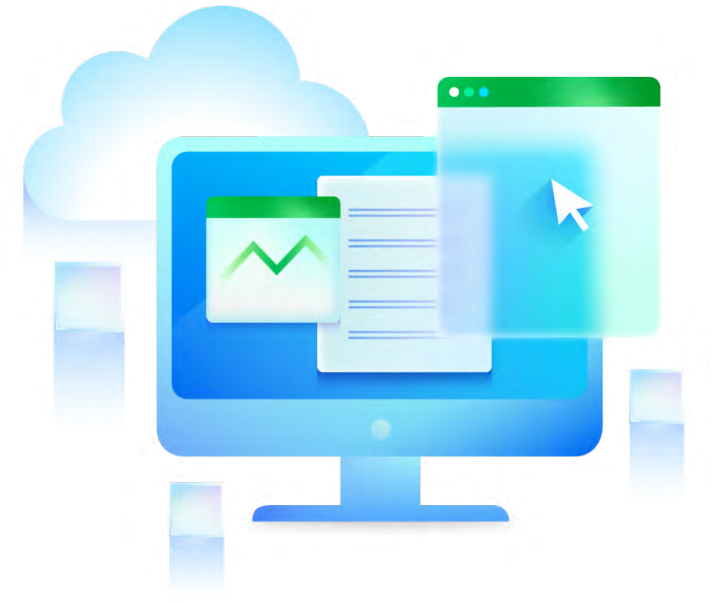
These policies might consider factors like the type of data, its criticality, and how often it changes to determine the frequency and method of backup. Automation tools take the burden off IT teams by handling routine, time-consuming tasks that are sometimes prone to human error; they can be scaled up during peak hours and then scaled back down during quieter periods to ensure consistent performance, conservation of resources, and reduced expenses.

Monitor Backups

Particularly for cloud services, the flexibility and scalability offered can lead to complexities, especially concerning backup policies. As organizations expand, so do their data protection needs. It's not uncommon for an organization's initial backup configuration to become unsuitable as its operational landscape changes.

Reviewing backup policies entails checking not only the frequency and success of backups, but also for data governance, identifying unprotected resources that exposes gaps in resiliency and compliance.

Tools provided by organizations such as Veeam bring additional value through cross-platform support and enhanced features such as predictive analytics, a single platform for centralized management, and advanced cost management capabilities, offering more sophisticated analytics which can be useful in large or complex environments that span multiple cloud providers.



Chapter 2: Architecting Secure Cloud Backup

Securing data is necessary for organizations of all sizes. A staggering 95% of businesses report moderate to extreme concern about their cloud security posture,[3] a source of unease stemming from a simple yet harsh reality: that cyberthreats are evolving, and the frequency of devastating incidents is on the rise. With 85% of organizations experiencing at least one ransomware attack within the past year, the need for a comprehensive cloud backup strategy has proven a certainty.[4]

No matter how thoroughly secure and protected an organization believes they are, the perfect defense is almost unattainable. Each attack averted is a victory, but it only takes a single oversight for an incursion to occur — and with 93% of cyberattacks targeting backups, there will come a day when your organization must shift focus from preventing cyberattacks to limiting damage and restoring normal operations.[5]

So, what can you do to prepare?

[3] Fortinet, Cloud Security Report 2022
[4] 2024 Ransomware Trends Report, Veeam
[5] 93% of Cyber Attacks Target Backup Storage to Force Ransom Payment
[6] What is the 3-2-1 backup rule?

Follow the 3-2-1-1-0 Rule

Incorporating the 3-2-1-1-0 rule into cloud backup strategies provides both depth and breadth in your data defense plan.[6] It's a proven methodology that builds redundancy and resilience into the very fabric of data management, ensuring that organizations can recover from data loss promptly, thereby minimizing operational downtime and mitigating the consequences of data-related disasters.

Air Gapping

Air gapping has been a mainstay in the data protection world, often achieved through backups stored on ejected tapes physically separating backup data from the network. However, in the cloud, where we have no control over physical infrastructure and network connectivity is always on, logical air gapping is a necessity.

Across all three major cloud providers Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, the logical separation of backups from production workloads demands the planning and implementation of dedicated accounts, subscriptions, and/or projects — and even private clouds or other clouds — to isolate protection data from production. This is true whether production is on-premises or also in the cloud. Logical air gapping (and the fine grain access controls needed discussed below) are critical to preventing threat actors traversing your environment(s) and compromising backup data.

Zero Trust & Least Privilege Access

The "principle of least privilege" is a fundamental principle of Zero Trust cybersecurity, advocating for the minimal level of user rights and permissions necessary to perform a job.[7] Within cloud environments, implementing least privilege can be accomplished via a combination of Identity and Access Management (IAM) rules, Role-Based Access Controls (RBAC), and Multi-Factor Authentication (MFA).

IAM systems are integral for controlling user identities and their access to various resources within the cloud. They manage permissions with fine-grained detail, allowing administrators to specify exactly what actions users can perform on which resources. Enabling IAM can dramatically lower the risk of unauthorized access or inadvertent data exposure.

RBAC takes this a step further by assigning permissions to roles rather than to individual users. Users are then assigned roles based on the specific tasks they need to perform. This model simplifies the management of user permissions, making it more straightforward to adjust roles as job functions evolve or as personnel change within an organization. By assigning roles rather than specific permissions to individual users, it's easier to ensure consistent access policy enforcement across the organization.

MFA is an essential security feature that adds an additional layer of protection. By requiring users to provide two or more verification factors to gain access to cloud resources, MFA reduces the risk of compromised credentials leading to a security breach, making unauthorized access significantly more challenging for attackers.

Routine maintenance of access privileges is critical to prevent "privilege creep," wherein users accumulate access rights over time that are no longer necessary for their job function. Organizations need to regularly review and revise user privileges, ensuring that old credentials are revoked, access rights are appropriate for current roles, and any temporary privileges granted for special tasks are removed upon completion. Additionally, regularly rotating credentials, such as passwords and access keys, can stave off potential compromises.

[7] Zero Trust cybersecurity

Immutability

Data immutability is a crucial aspect of data protection and integrity in cloud environments. As organizations increasingly rely on cloud storage for their critical data, it becomes essential to implement measures that prevent unauthorized modifications or deletions.

Immutability in the cloud is effectively implemented through features like Amazon S3 Object Lock, immutable storage for Azure Blob storage, and more, placing backup data in a Write-Once, Read-Many (WORM) state. By doing so, data remains unalterable (e.g., encryption, corruption, or deletion), maintaining data integrity and to ensure a clean and successful restore when disaster strikes.

Encryption

With data exfiltration now ranking as one of the major cloud security concerns, encryption ensures that, even in the event of unauthorized access or theft, the data remains unreadable and therefore of little value to an attacker. To facilitate user-friendly yet robust encryption capabilities, cloud providers offer specialized services.

AWS Key Management Service (KMS) presents a scalable and secure way to manage cryptographic keys used to encrypt data.[8] AWS KMS integrates with other AWS services, providing a centralized architecture that allows for the encryption of data across AWS workloads. AWS KMS ensures that encryption keys are used securely without ever being exposed to end-users, and it maintains a stringent set of policies that dictate how and when the keys can be used, audited, and rotated.

Azure Key Vault is a service provided by Microsoft Azure for managing cryptographic keys, secrets, and other sensitive information that applications and services might need to remain secure.[9] With Azure Key Vault, you can simply encrypt your backup data using keys stored and managed in these secure vaults. This not only bolsters your data's security posture but also provides comprehensive control over key lifecycle management, including the creation, storage, authorization, and deletion of keys.

Both AWS KMS and Azure Key Vault offer the means to implement encryption at rest and during transit. They also provide extensive logging capabilities, enabling the tracking of when and where encryption keys are used. This level of auditing is crucial to detect and respond to any unauthorized access attempts. Moreover, using these services assists in meeting regulatory compliance requirements that dictate the protection of sensitive data through encryption.

[8] AWS KMS Encryption
[9] Step 4. Enable Data Encryption

Chapter 3: Managing Hybrid/Multi-Cloud Backup

Driven by the appeal of scalability, flexibility, and cost-efficiency, organizations of all sizes have embraced the cloud. Cloud solutions such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) offer varying levels of control and abstraction, catering to a wide range of needs and allowing businesses to focus on innovation rather than on managing hardware and data centers.

The growing complexity of modern data environments makes it clear that traditional data management practices are no longer sufficient. Organizations must navigate this complexity by adopting advanced cloud management tools, embracing automated and orchestrated workflows, ensuring communication between cloud services, and comprehensive, robust security measures.

Hybrid vs. Multi-Cloud Management

Hybrid and multi-cloud management are two distinct strategies for enterprise cloud adoption, each serving different business needs and technical requirements.

Hybrid cloud models combine on-premises infrastructure, or private clouds, with public clouds, allowing data and applications to be shared between them.[10] This approach provides businesses with greater flexibility and more deployment options, which is particularly beneficial for companies with significant investments in a private data center or those dealing with sensitive data that might not be suited for a public cloud due to regulatory requirements.

Multi-cloud models involve the use of multiple cloud services from different providers.[11] Rather than unifying private and a single public cloud, a multi-cloud approach allows organizations to use best-of-breed services from various cloud providers to meet specific application requirements. Through a multi-cloud strategy, companies can avoid vendor lock-in, choosing different providers for different tasks based on performance, features, or cost-effectiveness.

The choice between a hybrid cloud and a multi-cloud strategy typically depends on a company's specific business needs, technical requirements, and strategic goals.[12] However, mobilizing data across platforms isn't made easy by cloud providers, often rendering organizations with vendor lock-in/out.

[10] Hybrid Cloud
[11] Multi-Cloud
[12] Multi-Cloud vs Hybrid-cloud

Overcoming Challenges in Hybrid and Multi-Cloud Environments

Hybrid and multi-cloud environments offer a heap of benefits that align with an organization's aspirations for flexibility, resilience, and optimized services. Still, these perks come with a suite of challenges that, ifnot addressed, can hinder an organization's ability to capitalize on their full potential.

Visibility: With various services deployed across diverse platforms, maintaining comprehensive oversight of costs, performance metrics, and security becomes a complex task. Achieving a bird's eye view seems almost unattainable through traditional methods, mandating the need for unified dashboards that serve as integrated control panels and can amalgamate data from multiple cloud services into a singular, coherent interface. By providing real-time insights and analytics, IT managers can make informed decisions quickly and keep the a pulse on the entire cloud ecosystem, including identifying potential risks or inefficiencies.

Cost management: Without vigilant governance, it's easy for costs to spiral as instances proliferate and services extend beyond their initial scope — often referred to as "cloud sprawl." Effective cost management strategies usually involve cloud management software that provides sophisticated tools to track and optimize resource usage. Additionally, adhering to standard cloud best practices, such as setting budget alerts and using cost management solutions offered by cloud providers, can help prevent unexpected expenses and maintain financial control.

Compliance: While cloud providers often furnish specialized services designed to meet stringent compliance standards — such as government, healthcare, or finance — these services can be siloed or vary considerably between providers. This reality requires meticulous planning and deployment strategies to ensure that workloads are positioned on the appropriate clouds. Compliance involves not just the physical location of data but the processes surrounding access, audits, interactions, and data management — all needing careful orchestration to avoid non-compliance and the ensuing repercussions.

Data Protection and Backups: The diversity of environments can necessitate multiple tools and management approaches to secure and safeguard data. This adds layers of operational overhead and demands significant expertise from the personnel tasked with managing these systems. Furthermore, the portability of data — moving backups or undertaking disaster recovery operations across cloud boundaries — is a crucial consideration. Organizations need to ensure interoperability and compatibility between different clouds and the ability to handle different data formats, service models, and APIs with dexterity.

Addressing these challenges requires a thoughtful and strategic approach, leveraging the right mix of tools, practices, and expertise. From the administrative ease of unified dashboards to the proactive cost-controls of management software, and from rigorous compliance alignment to comprehensive data protection mechanisms, hybrid and multi-cloud environments demand attention to detail and an unyielding commitment to operational excellence.

Summary

When you're faced with new cloud services being rolled into your tech stack, existing legacy tools and point products fail to deliver the data resilience and freedom you need. But it doesn't have to be that way...

Veeam empowers your teams with comprehensive, industry-leading data resilience and recovery capabilities across hybrid and multi-cloud environments. Natively protect, secure, and recover mixed environments, consolidated under one, seamless platform that eliminates the headaches and inefficiencies of multiple point products and legacy tooling. Better yet, Veeam delivers the unmatched data freedom required to backup, recover, migrate and modernize applications and data across any platform — no questions asked.

Whether you are bolstering security protocols, streamlining data protection, or pivoting towards modern cloud infrastructure and platforms, take a look at Veeam. We will strip away the complexity of ensuring resilience in a hybrid or multi-cloud setting so you can focus resources toward innovation and growth while being confident your data is protected, secure, and recoverable.

About Veeam Software

Veeam®, the #1 global market leader in data resilience, believes every business should be able to bounce forward after a disruption with the confidence and control of all their data whenever and wherever they need it. Veeam calls this radical resilience, and we're obsessed with creating innovative ways to help our customers achieve it. Veeam solutions are purpose-built for powering data resilience by providing data backup, data recovery, data portability, data security, and data intelligence. With Veeam, IT and security leaders rest easy knowing that their apps and data are protected and always available across their cloud, virtual, physical, SaaS, and Kubernetes environments. Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 67% of the Global 2000, that trust Veeam to keep their businesses running. Radical resilience starts with Veeam. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.

- Watch our Cloud Cost Management webinar for a live, hands-on cost-savings demo
- Learn more about Veeam hybrid cloud solutions