10 Steps to Cloud Resilience

Contents

Introduction

Cloud adoption has transformed how organizations operate, driving innovation and delivering unparalleled scalability, flexibility, and efficiency. But with these advantages come real risks. Cyberattacks, ransomware, and misconfigurations are perpetual threats that can disrupt operations, erode trust, and harm reputations. In an increasingly complex landscape — where over 85% of organizations rely on cloud-powered protection — even minor vulnerabilities can have significant consequences.

For IT and business leaders, resilience in the cloud is not about eliminating risk. Instead, it's about building the capacity to anticipate, withstand, recover from, and adapt to challenges while ensuring critical operations continue seamlessly. A resilient cloud strategy isn't just a safeguard — it's a competitive advantage that secures the future of your business.

Each strategy is actionable, designed to mitigate risks, safeguard sensitive data, and ensure regulatory compliance. This guide simplifies complex concepts into practical steps and advice, making it a valuable resource for both seasoned professionals and those new to cloud security.

Whether you're starting your cloud journey or strengthening an existing infrastructure, these principles provide the tools and insights to protect your digital assets and achieve sustained success. In a world where threats evolve as rapidly as technology, every step taken toward cyber resilience is one taken toward growth, innovation, and trust.

Let this guide be your blueprint for building resilience — and securing success — in the cloud.

85%

of organizations rely on cloud-powered protection

This e-book is your roadmap to cloud resilience. This guide will outline 10 foundational strategies tailored to the complexities of modern cloud environments. Topics will include:

- Aligning security policies with business objectives to create a solid foundation
- Protecting data integrity and ensuring recoverability in the face of cyberthreats
- Minimizing attack surfaces and restricting unauthorized access
- Achieving real-time threat detection and swift responses

1. Governance, Risk, and Compliance

Governance, Risk, and Compliance (GRC) policies have quickly become a cornerstone of resilient cybersecurity and operational strategies. As seen discussed in the 2024 Cloud Protection Trends Report, regulatory compliance was among the top reasons organizations shifted to more strategic DRaaS offerings. With an emphasis on aligning technology initiatives with organizational goals, GRC frameworks have proven capable of both bolstering cloud security and guaranteeing adherence to regulatory requirements.

Governance establishes the strategic framework for managing, utilizing, and securing cloud resources effectively. Aligning cloud operations with business objectives through clear policies, procedures, and controls can be achieved in a few ways:

- By establishing baseline security and performance criteria for third-party services.
- By documenting acceptable use policies that guide internal users while minimizing risks.
- By assigning roles and permissions that enhance oversight and reduce the likelihood of misconfiguration (which account for more than 80% of cloud security incidents, according to a recent Gartner study).

Risk management is the detection, evaluation, and mitigation of inherent vulnerabilities of cloud environments — such as data breaches, unauthorized access, and service disruptions. It begins with documenting all cloud services, applications, and data assets to maintain a comprehensive inventory. Anticipating potential attack vectors and conducting regular audits help uncover and remediate weaknesses. Proactive measures, such as leveraging immutable backups (see page 7), significantly reduce the impact of threats like ransomware, protecting operational integrity and financial stability. Risk assessments can help you gauge where your organization stands with respect to common fortifications.

Compliance involves meeting regulations like GDPR, HIPAA, and PCI-DSS, which are especially complex in decentralized cloud ecosystems. Organizations must balance strict regulatory requirements with operational flexibility by encrypting data, adhering to diverse policies, and demonstrating accountability to stakeholders. Beyond legal obligations, compliance builds trust with customers and partners, strengthening the organization's reputation as a responsible steward of sensitive data.

Integrating GRC into cloud strategies involves a few things. It requires alignment with business goals, standardized controls across diverse platforms, and automation tools for real-time monitoring and vulnerability detection. Far from being a mere risk management tool, a well-implemented GRC framework transforms security and compliance into catalysts for innovation. Even if you are required to do so, embedding GRC into an organization's operational DNA, organizations can thrive in the cloud — navigating its complexities with clarity, agility, and purpose.

2. Snapshots vs. Regular Backups

Understanding the difference between snapshots and backups is key to building a robust data recovery strategy. Both methods aim to safeguard data — and both do it well — but their unique characteristics apply to different situations. Combining their strengths, however, can improve recovery efforts and minimize downtime, ensuring your business remains resilient in the face of unexpected disruptions.

Snapshots capture a system's state at a specific moment, providing a fast and efficient recovery option. They are ideal for addressing issues like misconfigurations, software bugs, or quickly restoring recent changes. However, snapshots depend on the primary storage infrastructure, which poses a significant limitation — if the primary system experiences a hardware failure, ransomware attack, or another disaster, both the original data and its snapshots may be lost. This dependency makes snapshots unsuitable as standalone recovery solutions, particularly in disaster recovery scenarios where complete data availability is critical.

Backups, by contrast, create independent copies of data stored in separate locations, such as off-site facilities, dedicated servers, or cloud. This separation means that backups remain accessible even if the primary system fails, providing organizations with critical advantages. Backups protect data over long periods, helping meet regulatory requirements and ensuring compliance. They enable recovery from large-scale incidents, including ransomware attacks, natural disasters, and many others. Unlike snapshots, backups are not tied to the original infrastructure, allowing recovery even when the primary system is unavailable.

As such, backups require more resources than snapshots and are usually performed less frequently due to their complexity. However, their independence from the primary system and ability to enable comprehensive recovery makes them essential for mitigating significant risks. Fortunately, organizations can have the best of both worlds. Robust recovery strategies leverage the strengths of both snapshots and backups, addressing both short- and long-term needs.

- Rapid recovery and operational continuity in day-to-day scenarios, reducing downtime and service disruption
- Independent and secure recovery options for catastrophic events, safeguarding data integrity and long-term access

This layered approach is especially valuable in hybrid or multi-cloud environments. By combining localized snapshots with cloud-based backups, organizations enhance resilience while maintaining the flexibility needed to scale large amounts of data and resources (a common challenge for enterprises).

3. Logical Air-Gapping

Unlike traditional air-gapping, which relies on physically isolating storage systems, logical air-gapping uses software-driven controls to virtually separate backup data from the primary network. This approach eliminates the need for costly physical infrastructure, making it both efficient and adaptable to evolving security threats. By isolating backups in environments like virtual private clouds (VPCs) that are inaccessible from the primary network, organizations can protect data integrity without compromising agility or scalability.

Logical air-gapping means fewer risks from ransomware, unauthorized access, and other cyberthreats. The isolation provided by logical air-gapping ensures that even if the primary system is compromised, critical data remains secure and recoverable.

- **Cost Efficiency.** Eliminating the need for physical air-gapping infrastructure reduces operational costs while maintaining high levels of security.
- **Scalability.** Logical air-gapping is inherently compatible with modern IT infrastructures, enabling seamless scaling for large enterprises or growing businesses.
- **Operational Flexibility.** Organizations can safeguard backups without disrupting workflows or sacrificing the speed needed to adapt to emerging threats.

Logical air-gapping has become a cornerstone of cloud security and resilience due to its compatibility with hybrid and multi-cloud environments — it integrates easily with automated backup processes, encryption, and role-based access controls, and ensures that backups remain secure and accessible only to authorized users.

4. Least-Privilege Access

The principle of least privilege (PoLP) and Zero Trust Security are fundamental aspects of cloud security, granting users, systems, and applications only the access needed to complete their tasks. By limiting permissions, organizations significantly reduce the risks of breaches caused by human error, misconfigurations, or malicious actions.

Identity Access Management (IAM) is critical for managing digital identities and controlling resource access. Centralized identity management enforces consistent access policies, enhances oversight, and aligns permissions with organizational roles and security needs while reducing administrative overhead. Key IAM practices include single sign-on (SSO) to streamline access and enhance user experience, automated provisioning and deprovisioning to minimize manual errors and adhere to PoLP principles, and regular permission audits to quickly identify and remove unnecessary or excessive privileges.

Role-Based Access Control (RBAC) streamlines access management by assigning permissions to roles rather than individuals, ensuring privileges align with specific job responsibilities and minimizing excessive access. Effective RBAC implementation involves defining clear roles based on job functions to reduce ambiguity, establishing privilege hierarchies for efficient inheritance and scalability, and enabling dynamic role adjustments to adapt to organizational changes or evolving security needs.

Multi-Factor Authentication (MFA) bolsters security by requiring multiple verification methods, such as a password (something you know), a hardware token (something you have), or a biometric identifier (something you are). Integrating MFA into cloud operations strengthens defenses against internal and external threats. Key steps include applying MFA to all access points, particularly for privileged accounts and critical systems, and promoting employee awareness to drive adoption and adherence to MFA protocols.

When IAM, RBAC, and MFA are integrated, organizations can consistently enforce PoLP and Zero Trust practices across their cloud environments. As threats grow more frequent and sophisticated, this streamlined approach provides a proactive defense, enabling organizations to maintain confidence in their cloud security.

5. Encryption

Encryption is key to cloud security, protecting sensitive data and ensuring compliance with regulations. It secures data at rest and in transit, reducing risks of unauthorized access while preserving confidentiality, integrity, and availability.

In the cloud, encryption focuses on two main areas:

- **Data at Rest.** Information stored in databases, storage systems, and backups should be encrypted using strong algorithms like AES-256, the gold standard for preventing unauthorized access.
- **Data in Transit.** To protect data as it moves across networks or between applications, protocols such as Transport Layer Security (TLS) ensure security by preventing interception and tampering.

Centralized key management systems streamline the lifecycle of cryptographic keys, including creation, rotation, and retirement. Look to:

- Restrict access to key management systems to authorized personnel only.
- Reduce key compromise risks and ensure compliance with security policies.
- Automate key-related tasks to enhance both security and operational efficiency.
- Use end-to-end encryption to keep data encrypted throughout its lifecycle.
- Apply application-layer encryption during processing and storage, even in cloud-native applications.

Additionally, automating encryption processes and aligning with compliance standards like GDPR, HIPAA, and PCI-DSS further strengthens data protection and ensures regulatory adherence.

When IAM, RBAC, and MFA are integrated, organizations can consistently enforce PoLP and Zero Trust practices across their cloud environments. As threats grow more frequent and sophisticated, this streamlined approach provides a proactive defense, enabling organizations to maintain confidence in their cloud security.

6. Immutable Backups

An organization's ability to trust and rely on backups is more critical than ever. According to the 2024 Ransomware Trends Report, 93% of ransomware attacks target backup systems, emphasizing both their value and vulnerability. In response, 85% of organizations are now adopting cloud-based immutable backups, which have quickly become a cornerstone of modern data protection strategies. Immutable backups ensure data integrity and provide a reliable foundation for recovery, safeguarding businesses against increasingly sophisticated threats.

Immutable backups follow a write-once, read-many (WORM) model, ensuring data cannot be altered or deleted after it is written. This safeguards backups against ransomware, malicious insiders, and accidental changes that could compromise data integrity. By preserving data in its original state, immutable backups enable recovery to a secure, known point. Additionally, they help organizations meet compliance requirements for non-rewritable and non-erasable storage, as mandated by regulations like SEC Rule 17a-4(f) and GDPR.

To build an effective immutable backup strategy, organizations should focus on these key elements:

- Use technologies with object lock functionality or immutability features.
- Establish policies that specify data types for backup, frequency, and retention periods.
- Keep multiple versions of backups.

Immutable backups are very reliable. Even still, they require effective management. Backup data lifecycle management ensures backups remain secure, accessible, and compliant throughout their lifespan. This process involves four key phases: creation, retention, usage, and retirement.

- **Creation.** Focus on accurate and consistent backups, using automation to minimize errors. Techniques like deduplication and compression optimize storage while maintaining data integrity.
- **Retention.** Define retention periods based on regulatory, business, and operational needs. Regulations like GDPR require that data is not retained longer than necessary. Implement tiered storage solutions to move older backups to cost-effective, long-term systems like archives.

93%

of ransomware attacks target backup systems

85%

of organizations are now adopting cloud-based immutable backups

- **Usage.** Regularly test recovery procedures to validate backup integrity and ensure efficient restoration. Enforce strict access controls to limit access to authorized personnel only.
- **Retirement.** Safely and permanently delete expired data at the end of its retention period using. Maintain detailed documentation to ensure compliance and accountability during audits.

Integrating lifecycle management into an immutable backup strategy maximizes backup value while maintaining strong security and compliance. This structured approach helps organizations optimize costs, reduce risks, and ensure operational continuity, enhancing resilience against evolving threats.

7. Incident Response Plan

An effective incident response plan (IRP) is critical for minimizing the impact of security breaches and ensuring rapid recovery of operations. Cyberattacks increasingly target cloud environments, which store a substantial portion of the world's most valuable data — with more than half of all backup data (61%) now stored in the cloud. These attacks threaten sensitive information, disrupt business continuity, and damage reputations.

In May 2024, UniSuper, an Australian superannuation fund, experienced an outage of their primary cloud provider (hosting 1,900 of their virtual machines). Due to an unexpected and unprecedented user error, this outage resulted in the deletion of their entire cloud. Sensibly, UniSuper anticipated the possibility of an outage and maintained two distinct backups across two cloud geographies. But the unique nature of the outage, a simple misconfiguration, meant **both backups were entirely deleted.**

It was only by the grace of their third backup, managed by a separate third-party provider, that UniSuper was able to restore operations weeks later. In essence, UniSuper's IRP — in adherence with the 3-2-1-1-0 Backup Rule — saved the company $125 billion and restored service to over 600,000 customers.

While this is an extreme case, the principle applies to organizations of all sizes. A well-structured and managed IRP is essential for managing risks, providing them with the necessary steps and failsafe solutions to recover data and restore operations even in the worst-case scenario.

- Analyze and assess the nature, scope, and impact of a security incident.
- Once an incident is identified, immediate containment is essential to limit damage and prevent further spread.
- Effective response formulation is crucial for recovery, stakeholder communication, and regulatory adherence.

But a robust IRP is never static, especially in the cloud. It evolves alongside emerging threats and technological advancements. Regular testing through simulated breach scenarios, periodic updates to address new vulnerabilities, and comprehensive employee training ensure that the organization is prepared for future incidents.

8. Recovery to an Alternate Location

Recovering to an off-site, alternate, or cloud location ensures that systems can be swiftly restored when the primary site is compromised. This strategy can leverage a secondary region within the same cloud provider, a different cloud provider, or on-premises infrastructure, depending on an organization's risk tolerance, compliance needs, and operational goals.

With 81% of organizations now operating in a multi-cloud environment, leveraging the cloud for data recovery is increasingly recognized for its efficiency and dependability. Utilizing a cloud provider's global infrastructure provides geographical redundancy, safeguarding against localized disasters like regional outages or natural catastrophes. Staying within the same cloud ecosystem simplifies integration and reduces complexity, making it an attractive option for organizations seeking streamlined operations.

Many businesses adopt a hybrid approach, combining cloud-based recovery with on-premises solutions to balance resilience, cost-efficiency, and scalability. For instance, an organization might configure rapid failovers to another location for immediate recovery needs while maintaining on-premises systems for sensitive workloads requiring strict oversight. 71% of enterprises already use hybrid strategies, leveraging the flexibility of the cloud while ensuring robust data protection.

In industries like finance, healthcare, or government, where strict control over physical and network security is essential, on-premises recovery remains a practical solution. This approach keeps sensitive data under direct oversight and ensures compliance with stringent regulations but comes with the added costs of infrastructure and maintenance.

81%

of organizations now operating in a multi-cloud environment

71%

of enterprises already use hybrid strategies

Recovery plans must address emerging risks and align with evolving business needs. Multi-cloud strategies, hybrid models, and proven cloud providers offer organizations unmatched flexibility, ensuring that critical systems and data remain secure, recoverable, and resilient in an ever-changing threat landscape.

9. Monitoring and Logging

With 76% of businesses identifying protection gaps, effective monitoring and logging practices have become indispensable. In response, industry advancements have outfitted organizations with the ability to detect threats early, respond quickly to anomalies, and maintain adherence to compliance requirements. In every sense, organizations can achieve real-time visibility, protect assets proactively, and maintain seamless operations more effectively — and through backup providers, more accessibly — than ever before.

Monitoring serves several essential purposes, whether it's identifying unauthorized access, collecting forensic insights, and optimizing cloud service performance. Many available services use machine learning to recognize patterns, enabling operational intelligence and a unified view of complex ecosystems.

Centralized log management tools simultaneously store and correlate data from diverse sources, making it easier to comply with regulations and respond to incidents. These tools streamline log collection and analysis, while Security Information and Event Management (SIEM) platforms enhance these capabilities through anomaly detection, automated responses, and seamless integration and coordination with the organization's IRP.

Compliance with frameworks such as GDPR and HIPAA, as always, continue to shape monitoring and logging requirements. These mandates dictate how data must be collected, stored, and protected, making regular audits and continuous evaluation of monitoring systems critical for verifying adherence.

10. Regular Audits and Penetration Testing

In traditional on-premises environments, audits and penetration testing focus on systems and infrastructure under the organization's complete control. These practices include checking server configurations, network settings, and access permissions to ensure compliance with regulatory and internal standards. Audits help identify vulnerabilities such as open ports or excessive permissions, which could lead to unauthorized access or data breaches. Penetration tests simulate real-world attacks to uncover weaknesses before adversaries can exploit them, providing actionable insights to strengthen defenses.

When working with SaaS applications, direct penetration testing isn't possible since the cloud provider manages the underlying infrastructure. However, organizations can and should test elements they control, such as IAM instances, file shares, and virtual private clouds (VPCs). Regular audits of these components ensure configurations align with security best practices and mitigate risks.

In the cloud, audits and penetration testing require different tools and methods. Cloud-native solutions like continuous compliance monitoring, automated vulnerability scans, and activity tracking replace traditional on-premises tools. These cloud-specific approaches make it easier to identify misconfigurations and ensure compliance without disrupting operations.

Without full visibility into your cloud environment, you risk leaving vulnerabilities undetected. Regular audits are essential for mapping your cloud footprint and ensuring every asset is monitored and secured. Understanding what resources are active and identifying dormant or misconfigured systems are critical steps in maintaining a robust security posture.

Cloud environments are highly dynamic and can grow rapidly. To prevent security gaps, organizations should leverage tools that provide real-time alerts for inactive assets or newly exposed threat vectors. This ensures proactive risk management and minimizes opportunities for attackers. Often, cloud providers offer advanced tools, best practices, and real-time threat detection capabilities to enhance audits and penetration testing. Leveraging these resources helps streamline security efforts and gain deeper insight into cloud environments.

To summarize, organizations pursuing a more resilient place in the cloud should:

- **Embed Regular Audits and Penetration Testing.** Incorporate audits and penetration testing into workflows to maintain visibility and address vulnerabilities like misconfigurations or excessive permissions. Use automated tools and real-time monitoring to adapt traditional practices for the cloud, ensuring proactive and continuous security.
- **Partner with Capable Providers.** Collaborate with providers to access advanced tools like compliance monitoring, threat detection, and vulnerability scanning. Choose providers with strong security expertise to align with shared responsibility models and address provider-specific requirements effectively.
- **Focus on Cloud-Specific Practices.** Adopt tailored strategies for cloud security, such as monitoring IAM roles, managing VPCs, and tracking data flows. Leverage real-time alerts and scalable solutions to detect risks, manage resources, and ensure security evolves with the environment.

By adopting the right technologies and practices, organizations can strengthen resilience, safeguard sensitive data, and maintain operational continuity. These approaches are crucial for managing the complexities of multi-cloud environments and staying ahead of evolving security challenges.

Building a Resilient Future in the Cloud

Cyber resilience in the cloud is more than a response to threats — it's a decision to fortify your cloud environment, to remain secure, compliant, and ready for anything. Every element of this approach reinforces a layered defense that safeguards your business.

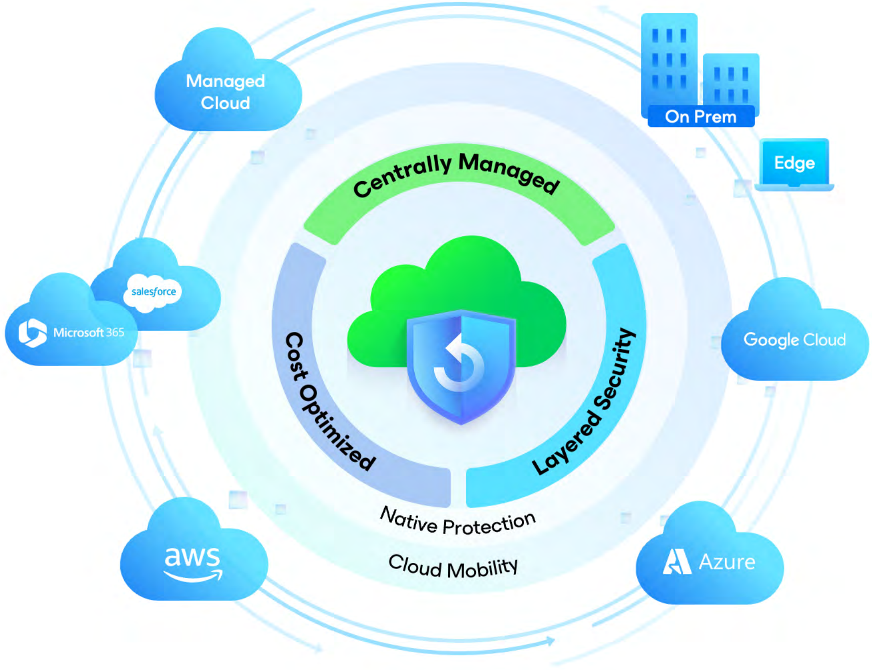
- Governance lays the foundation for strategic alignment, ensuring policies and practices drive resilience across hybrid and multi-cloud environments.
- Advanced encryption protects sensitive data in transit and at rest, while immutable backups guarantee recoverability against ransomware and malicious threats.
- Automated monitoring delivers real-time insights, enabling rapid responses to anomalies and threats.
- And a culture of continuous improvement ensures your defenses evolve as the cyber landscape shifts.

We Protect Everything

AWS	Azure	Google Cloud	VMware	Microsoft Hyper-V
Microsoft	Proxmox	Red Hat	KVM	Nutanix
Linux	Oracle	PostgreSQL	MongoDB	MySQL
Oracle Solaris	IBM AIX	MacOS	SAP Hana	NAS
Object Storage	Microsoft 365	Salesforce	Microsoft Entra ID	Kubernetes

Resilience doesn't stop at defense. With a unified solution like Veeam Data Platform, you can centralize governance, enhance observability, and streamline recovery — turning cloud complexities into a competitive advantage. Features like cost-optimized backup to cloud object storage, seamless workload mobility, and logically air-gapped, encrypted backups strive to turn safeguards into innovations.

Hybrid Cloud Resilience with Veeam



When faced with cloud-first approaches, organizations often find their existing tools fail to integrate with the cloud, landing them with bill shock, cyberthreats, and other surprises. Some just deal with it, while others reluctantly turn to multiple-point products (and the management nightmare that comes with them). But it doesn't have to be that way.

Veeam empowers you with the best of both worlds — native data protection that's built for specific environments, all wrapped up under a single, easy-to-manage platform and license that never boxes you in.

Own Your Data. Any Cloud.

#1 Hybrid Cloud Backup

Protect Cloud Data	Leverage Cloud for Data Protection
Cloud-Native Backup	Backup and Archive
SaaS Backup	Ransomware Protection
Cloud Mobility	Disaster Recovery
Kubernetes Backup	Migrate and Modernize

AWS · Azure · Google · Microsoft 365 · Salesforce · Kubernetes · On-premises

About Veeam Software

Veeam, the #1 global market leader in data resilience, believes businesses should control all their data whenever and wherever they need it. Veeam provides data resilience through data backup, data recovery, data portability, data security, and data intelligence. Based in Seattle, Veeam protects over 550,000 customers worldwide who trust Veeam to keep their businesses running. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.