Hybrid Cloud, Multi-Cloud, Every Cloud, Secured.

10 Best Practices for Protecting Every Environment

Table of contents

Introduction

In a world where agility matters more than ever, cloud computing has emerged as the unsung hero of business transformation. At the forefront of this transformation is the growing adoption of hybrid and multi-cloud architectures, with 57% of organizations now using multi-cloud as their primary model and 73% embracing hybrid cloud strategies that blend public and private cloud platforms.

Adopting multi-cloud is no longer optional - it's a critical component for modern organizations where agility and flexibility are key drivers of success. Businesses are gravitating toward these architectures due to the unparalleled flexibility, cost optimization, and freedom from vendor lock-in. These setups enable organizations to meet dynamic business needs while leveraging the unique strengths of different cloud providers and architectures.

However, these benefits come with significant challenges. The distributed nature of hybrid and multi-cloud environments introduces an exponential increase in complexity. Applications and data span diverse platforms, each with unique configurations, security protocols, and compliance requirements. This can result in security gaps and inefficiencies, often hindering organizations from fully capitalizing on the economic benefits of multi-cloud.

This e-book explores the essential considerations and strategies for securing hybrid and multi-cloud deployments. Whether you're safeguarding sensitive data in a private data center, managing workloads across multiple public clouds, or navigating the intricate web of compliance requirements, this guide provides actionable insights to help you address the unique challenges of hybrid and multi-cloud deployments and ensure robust protection of your applications and data.

86%

of organizations have already adopted a multi-cloud approach thanks to its benefits including increased agility, flexibility, and choice.

SANS 2023 Multicloud Survey:
Navigating the Complexities of Multiple Clouds," SANS Institute.

Businesses today are embracing IT environments that combine the best of private data centers and public clouds, making hybrid and multi-cloud setups the standard. Public clouds provide scalable, cost-efficient, and easily accessible infrastructure that accelerates innovation and enables businesses to focus on growth rather than managing IT resources. Hybrid clouds offer flexible deployment options, allowing workloads to move seamlessly between private and public clouds as computing needs and costs change.

While these architectures offer flexibility and scalability, they also introduce new challenges, especially when it comes to security. Developing robust strategies to protect these complex systems has become essential for organizations to address diverse platform requirements and regulatory frameworks.

What is
Hybrid Cloud Security?

Hybrid cloud security allows comprehensive protection across multiple cloud platforms, including both private clouds and public clouds like AWS, Azure, Google Cloud Platform (GCP), and Oracle Cloud Infrastructure (OCI). Enforcing uniform security practices, avoiding configuration errors, maintaining consistent monitoring, and ensuring comprehensive protection across public and private cloud components can be difficult. By orchestrating consistent security policies and controls across these environments, organizations can ensure that data integrity, confidentiality, and compliance are maintained, no matter where applications are deployed.

What is
Multi-Cloud Security?

Multi-cloud security takes this a step further, focusing on protecting assets distributed across multiple public cloud platforms from different providers. Enterprises adopt multi-cloud strategies to avoid vendor lock-in, optimize costs, and leverage specialized features of various cloud services. However, managing security across multiple providers adds another layer of complexity. Each platform operates with distinct tools, policies, and compliance standards, making it essential to implement a unified security approach that ensures visibility, control, and protection across all environments.

Both hybrid and multi-cloud security involve safeguarding data, applications, business processes, and infrastructure distributed across these interconnected ecosystems. Effective security strategies must account for:

Data security
Ensuring that sensitive information remains protected both in transit and at rest, regardless of the cloud or data-center location.

Workload protection
Securing applications and services operating across diverse platforms with consistent security configurations.

Compliance management
Navigating the intricate regulatory requirements that vary between deployments and cloud providers.

The ultimate goal is to provide seamless protection that doesn't compromise the flexibility and scalability benefits of hybrid and multi-cloud architectures. A well-executed security strategy not only protects critical assets but also empowers organizations to innovate confidently in today's digital world.

Top Challenges in Hybrid and Multi-Cloud Environments

Harmonizing the security posture across the entire hybrid cloud builds a fabric of protection that helps keep "bad guys" from entering through the weakest link.

IBM

Increased Complexity

Managing diverse environments spanning private data centers and multiple cloud providers adds significant complexity to IT operations. Each environment comes with its own set of tools, configurations, and security protocols, making it difficult to enforce consistent security policies. This complexity demands specialized expertise and advanced solutions capable of handling the intricate dynamics of hybrid and multi-cloud ecosystems.

Integration and Interoperability

Hybrid and multi-cloud strategies rely on seamless data exchange and operational compatibility between various platforms. Ensuring interoperability can be challenging, as each cloud provider has unique APIs, services, and infrastructure designs. Organizations must overcome these differences to maintain operational efficiency and reduce the risks associated with misaligned systems.

Security Concerns

Security remains one of the top priorities and challenges for organizations operating in hybrid and multi-cloud environments. Distributed infrastructures increase the attack surface, while varying security models across providers can create gaps in protection. A unified security strategy is essential to safeguard sensitive data, applications, and workloads against potential threats, ensuring end-to-end visibility and control.

Cost Management

While hybrid and multi-cloud deployments offer opportunities to optimize costs by leveraging the most suitable services from various providers, they also pose the risk of cost sprawl. Unmonitored usage, duplicate services, and unforeseen expenses can quickly escalate budgets. Effective cost management requires granular monitoring, budgeting tools, and cost-control measures across all environments.

Data Governance and Compliance

Navigating regulatory frameworks and ensuring data governance in hybrid and multi-cloud environments can be daunting. Compliance requirements often vary between regions, industries, and cloud providers. By implementing robust data-management practices and maintaining thorough documentation, organizations can meet these obligations and avoid potential fines.

Siloed Security Tools

The use of disparate security tools tailored to individual cloud platforms often results in silos that hinder visibility and collaboration. These silos can lead to inconsistent protection measures, leaving gaps and entry points for attackers. A unified approach to security tools and practices is critical to eliminate redundancies and ensure a cohesive security posture.

Successfully addressing these challenges empowers organizations to fully leverage the benefits of hybrid and multi-cloud architectures. By implementing integrated strategies and investing in advanced solutions, businesses can overcome these obstacles and unlock the potential of their cloud investments.

10 Best Practices for Hybrid and Multi-Cloud Security

Being multi-cloud increases management and governance challenges, increases the complexity and cost of IT, and demands greater skills.

Gartner

Standardize Access Controls

Implement standardized access control mechanisms across all cloud and on-premises environments. Use role-based access control (RBAC) and enforce least-privilege principles to ensure that users and systems access only the resources they need. Centralized identity and access management (IAM) solutions can streamline these efforts, reducing the risk of unauthorized access.

Implement Data Security Measures

Protect sensitive data by encrypting it both at rest and in transit, using strong encryption protocols. Enable encryption features on all cloud platforms, as some may not apply these protections by default. Additionally, implement robust data loss prevention (DLP) strategies to prevent accidental exposure or unauthorized transfers of critical information.

Standardize Tools and Configurations Across Clouds

Use the same infrastructure-as-code (IaC) platform to provision and manage all cloud environments. This standardization ensures consistency in configurations, policies, and security baselines. Additionally, employing consistent IaC templates can help automate security checks and reduce the risk of misconfigurations.

Strengthen Network Protections

Segment your networks to isolate sensitive workloads and restrict lateral movement in case of a breach. Use firewalls, intrusion detection systems (IDS), and secure VPNs to safeguard data traffic across hybrid and multi-cloud environments. Incorporating zero-trust network architecture ensures that all traffic is continuously authenticated and monitored.

Adopt a Zero-Trust Architecture

Implement a zero-trust security model in which no user or device is inherently trusted, regardless of its location. Continuously verify all access requests, enforce least-privilege access, and ensure that all communication is encrypted.

Automate Threat Detection

Leverage AI-driven tools to automate the detection and mitigation of threats across your hybrid and multi-cloud landscape. Automation is particularly effective when integrated into CI/CD pipelines, enabling security scans to be performed at every stage of development and deployment.

By identifying vulnerabilities early in the pipeline, teams can address issues before they reach production. This approach not only minimizes human error but also enhances efficiency and consistency, which is especially critical in complex, distributed architectures.

Use Threat Intelligence to Stay Proactive

Integrate real-time threat intelligence into your multi-cloud security framework to stay ahead of emerging threats. This enables you to update policies and configurations to address new vulnerabilities proactively.

Conduct Regular Compliance Checks

Hybrid and multi-cloud environments span different regulatory jurisdictions, making compliance a moving target. Conduct routine compliance checks to identify gaps and ensure adherence to relevant regulations and industry standards. Tools that automate compliance audits can save time and reduce the risk of non-compliance.

Centralize Visibility and Monitoring

Deploy unified monitoring solutions to gain end-to-end visibility across on-premises and cloud environments. Centralized tools enable security teams to detect anomalies, identify threats, and respond swiftly, ensuring consistent protection across diverse infrastructures.

Standardize Security Policies

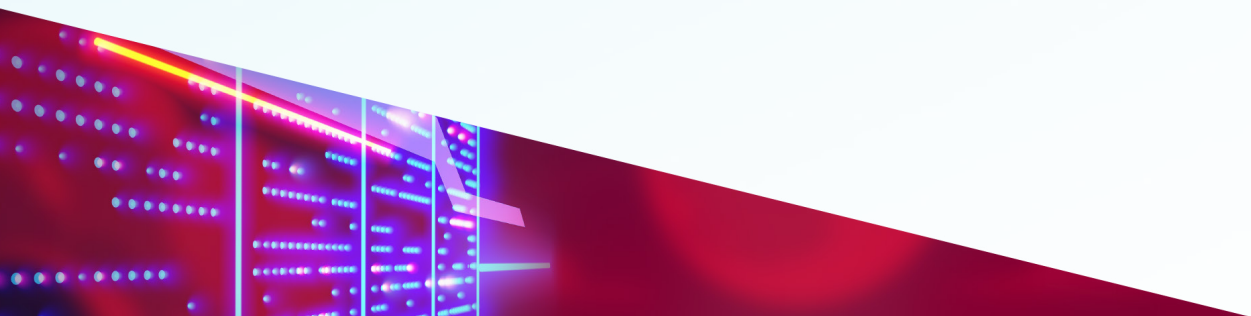
Ensure that security policies are standardized across all cloud providers and on-premises systems to prevent configuration drift. Consistent policies reduce the likelihood of security gaps and streamline management, enabling a cohesive defense strategy.

Adopting these best practices allows you to mitigate risks, ensure compliance, and create a resilient security posture in hybrid and multi-cloud environments.

Mastering Hybrid and Multi-Cloud Security with Aqua

As hybrid and multi-cloud strategies become increasingly essential for meeting evolving business needs and enabling flexible deployments, security challenges are growing more complex. In the face of escalating cyber threats and complex architectures, organizations must implement a comprehensive security strategy to protect their multi-cloud journey.

The Aqua Cloud Native Application Protection Platform (CNAPP) provides end-to-end protection for cloud native applications everywhere they run – whether in the public cloud, on-premises, or across hybrid and multi-cloud environments, such as AWS, Azure, GCP, IBM Cloud, Oracle Cloud, and VMware. By leveraging a single unified platform, you can enhance your security posture, mitigating risks across the full life cycle and fortifying workloads against attacks in runtime.



With the Aqua Platform, you can:

Secure applications everywhere
Protect every application across hybrid environments and platforms such as Red Hat OpenShift and VMware Tanzu Application Service (TAS), ensuring comprehensive coverage.

Streamline operations
Reduce operational overhead by defining security policies once and seamlessly deploying them across diverse environments.

Maintain flexibility
Support diverse cloud native stacks and platforms, from serverless containers like AWS Fargate to specialized deployment options like IBM Z-Series mainframes, empowering teams to innovate without limitations.

Defend against advanced threats
Detect and block even the most sophisticated cloud native attacks with a best-in-class runtime security solution that leverages behavioral threat detection and customizable runtime policies.

Ensure consistent visibility and control
Achieve consistent yet granular policy enforcement with a single, centralized console for visibility and management.

Protect air-gapped environments
Safeguard your isolated systems, detect vulnerabilities, enforce compliance, and block risks, all without external connectivity. Aqua enables secure offline updates and threat intelligence, ensuring that your air-gapped environments remain resilient and always protected.

Are you pursuing hybrid and multi-cloud strategy in 2025?

Discover how Aqua can elevate your security posture, ensuring robust protection across all hybrid and multi-cloud environments.

Start Now >

Aqua Security is the pioneer in securing containerized cloud native applications. The Aqua Platform, a Cloud Native Application Protection Platform (CNAPP), enables organizations to secure every cloud native application everywhere, from code commit to runtime. With enterprise scale that doesn't slow development pipelines, Aqua secures your future in the cloud. Founded in 2015, Aqua is headquartered in Boston, MA and Ramat Gan, IL protecting over 500 of the world's largest enterprises. For more information, visit https://www.aquasec.com