# Public vs Private vs Hybrid Cloud: Security Risks Compared

## Key Takeaways

- Public, private, and hybrid cloud models each present different security risks, control levels, and operational challenges.
- Public cloud security relies on a shared responsibility model, making configuration management and identity controls critical.
- Private cloud environments provide greater control but require organizations to handle all security, monitoring, and infrastructure management.
- Hybrid cloud offers flexibility but increases complexity due to multiple environments, tools, and data movement risks.
- Unified security platforms like Fidelis CloudPassage Halo® help organizations maintain consistent protection across public, private, and hybrid cloud infrastructures.

Modern businesses cannot do without cloud computing because it allows them to be innovative at a faster rate, scale, and cost-effectively. Nonetheless, due to the growing migration of workloads to the cloud by organizations, the debate on the issue of public vs private vs hybrid cloud security is becoming more of a concern.

All three cloud models have their advantages but also raise special security threats. These differences are essential to understanding how to create a resilient cloud security strategy and the option of the appropriate deployment model. Public vs private vs hybrid cloud security compares risks, control, and protection across cloud models.

## Understanding Cloud Deployment Models

A public cloud is managed by third parties, and it is provided using the internet. A single organization has a private cloud, and it has more control over infrastructure and data. Hybrid cloud integrates the two models whereby an organization can utilize workloads between the two environments depending on business requirements. Such variations in ownership and control have direct implications on the manner of security is handled.

## Public Cloud Security: Scalability with Shared Responsibility

The popularity of the public cloud environment is that it is flexible and cost-effective. Security work, however, is based on a shared responsibility model where the provider oversees securing the infrastructure and the organization in charge of securing its data, applications and access controls. It is because this common model can result in areas of insecurity through confusion.

Misconfiguration is one of the greatest security threats of the cloud. Sensitive data can be disclosed by improperly set up storage devices, open access privileges, or a weak identity control. Such mistakes have resulted in many high-profile breaches of public clouds instead of failure by the provider.

The other challenge is visibility. When organizations grow in various cloud services, it becomes hard to keep track of assets and threats. Such invisibility is another major contributor to larger

societal challenges to cloud security.

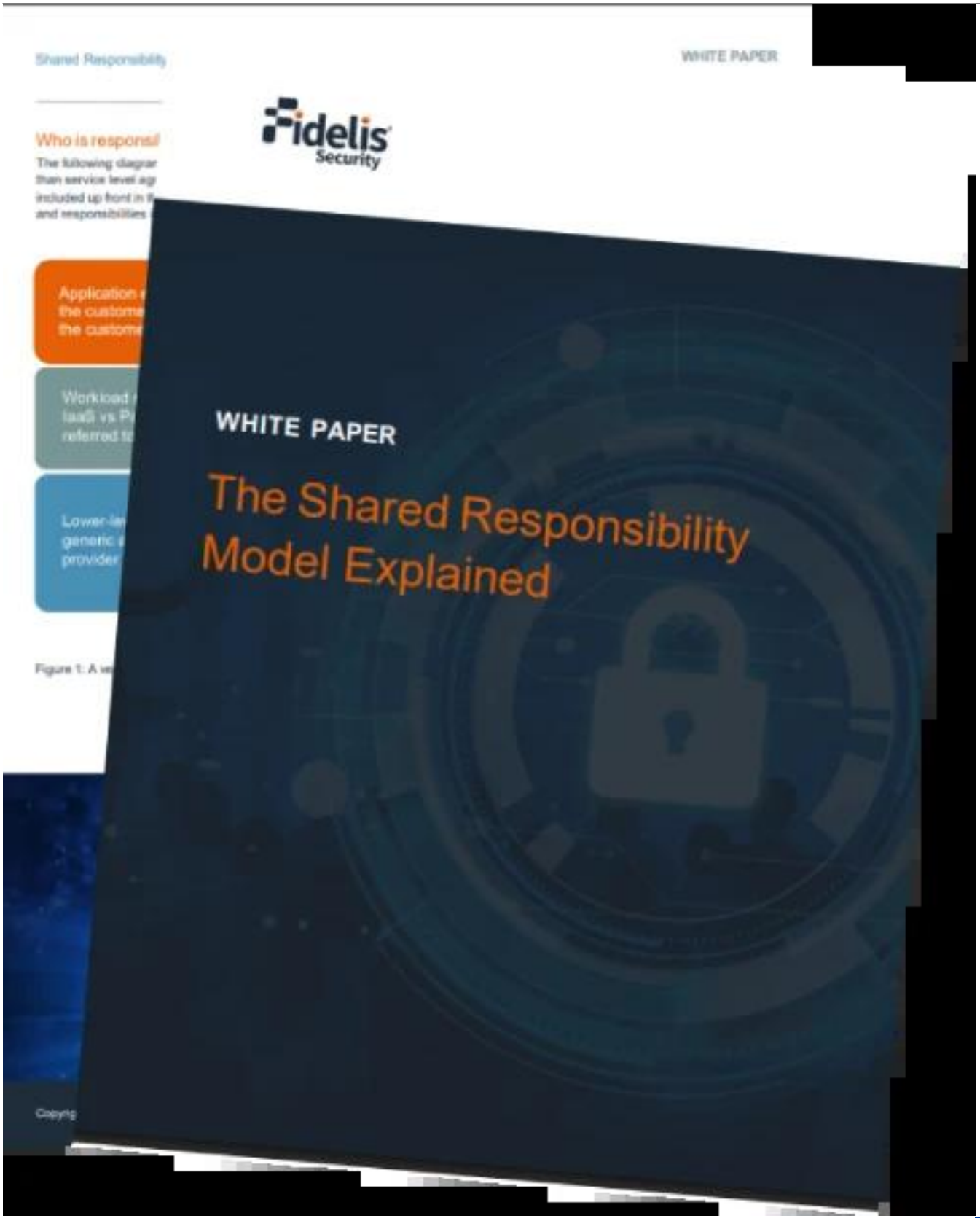
Moreover, multi-tenancy is applied in public cloud environments. Although the providers are doing an excellent job with isolation, some organizations still feel insecure when it comes to a shared nature of infrastructure.

In a bid to fix these problems, corporations adhere to the set standards of cloud security like ISO 27001, SOC 2 and NIST to maintain the same and acceptable practice of security.

Shared Responsibility Automation—It’s Not Optional

- Shared Responsibility Basics
- The Shared Responsibility Model in Practice
- Key Attributes of a Security Automation

Download the Whitepaper Now!




## Private Cloud Security: Control with Responsibility

Private cloud environments are often seen as more secure because they provide dedicated infrastructure and full control. However, this also means that the organization is entirely responsible for securing the environment.

This shift introduces a different set of risks.

Many private cloud security issues originate internally. Insider threats, poor access management, and lack of monitoring can create vulnerabilities that are difficult to detect. Unlike public cloud environments, there is no provider sharing the burden of security.

Another concern is limited automation. Private clouds don't have the built-in security tools that many companies are used to in the public cloud, and first-response time detecting threats can be much longer giving attackers more time to act and potentially more time to breach the system.

Infrastructure management is another important step in maintaining a secure private cloud infrastructure. Inadequate patch management, updates, and vulnerability scans can have severe implications on the security of private clouds.

While private clouds deal with similar security issues as traditional data center environments, there are a number of challenges and complexities involved that have to be considered. When considering flexibility of control in a private cloud, one is often reminded of the reasons one went hybrid/virtual in the first place: the ability to custom tailor controls in all three dimensions.

Specifically, when needed, one can enforce highly granular segmentation, highly customized control points to enforce compliance to one's own governance rules, as well as very fine-grained access control (versus a fixed set of policies mandated by a shared infrastructure provider). Most Private Cloud security offerings include some variants of continuous monitoring, endpoint protection, and proactive vulnerability management.

## Hybrid Cloud Security- Flexibility Meets Complexity

Hybrid cloud refers to an IT model, which combines private clouds, managed or on-premises servers, storage and networking with a public cloud -infrastructure, services, platforms and applications offered through the Internet. Hybrid cloud allows workloads to be transferred across private, hosted, public and multi-cloud environments, and vice versa.

As an example, organizations might choose to keep their most business-critical applications and sensitive information in their private cloud environment and move less business-critical applications to a public cloud.

However, this flexibility introduces complexity, which becomes the primary security challenge.

Hybrid cloud security offers a whole host of benefits, but with those there are also a new set of challenges. One of the most difficult to deal with is the fact that in a hybrid cloud model there are different security policies that cannot always be enforced with the same level of control in all locations. Having so many different systems and the way they are configured also means that a hybrid cloud environment has vastly more different security controls and tools. So, with so many more potential openings to which attackers can infiltrate a system, there are obviously far more security gaps and attack surfaces – which is why so many worry about hybrid cloud security.

Data in motion can also be breached. If information is transmitted in an unencrypted format or transmitted over an unsecured media, it will be at risk.

Hybrid environments are much more complex and consequently their attack surface is larger, more dynamic and much harder to manage and secure. With a hybrid environment, there are more endpoints and more APIs and connections to other systems, applications and services which all add to the number of potential points of entry for an attacker and can obscure visibility of the layers of security that need to be managed.

This security reality demands hybrid cloud security innovations like centralized visibility, unified identity management, and Zero Trust.

## Public vs Private vs Hybrid Cloud Security- Comparison Table

Aspect Public Cloud Private Cloud Hybrid Cloud Infrastructure Ownership Managed by third-party provider Fully owned/managed by organization Shared between provider and organization Security Responsibility Shared responsibility model Full responsibility on organization Shared + internal coordination required Control Level Limited control over infrastructure High control and customization Moderate control with flexibility Scalability Highly scalable Limited by internal resources Scalable with flexibility Visibility Can be limited across services High visibility within environment Complex visibility across environments Common Security Risks Misconfigurations,

data breaches

, multi-tenancy risks Insider threats, mismanagement, outdated systems Integration gaps, inconsistent policies, expanded attack surface Security Challenges Managing IAM, compliance,

shadow IT

Maintaining updates, monitoring, skilled resources Securing data movement, unified policies, tool integration Compliance Management Depends on provider + user configuration Easier to enforce strict compliance Complex across multiple environments Data Protection Requires strong encryption and access control Fully customizable data protection policies Needs consistent encryption across environments Attack Surface Broad due to internet exposure Narrower but internally vulnerable Largest due to multiple environments Cost of Security Lower upfront, ongoing management needed Higher due to infrastructure and tools Variable depending on architecture Best Use Case Rapid scaling, startups, SaaS apps Sensitive data, regulated industries Enterprises needing flexibility and balance

This comparison highlights how private vs public cloud security differs in terms of control, risk exposure, and operational complexity, while hybrid cloud introduces additional integration challenges.

## Security Issues Across Cloud Models

Comparing security concerns of public cloud computing to a private cloud computing to a hybrid model of cloud computing, it is evident that there are risk profiles of each setup.

Public cloud settings are more vulnerable to attack by outsiders and misconfigurations. The internal risks and operational gaps are more exposed to private cloud settings. Hybrid cloud environments have issues of integration, consistency, and data movement.

These distinctions indicate that a single security strategy cannot be applied to different organizations, but a bespoke approach is required.

## Strengthening Cloud Security Across All Models

Regardless of the cloud model, certain practices are essential. Access to sensitive systems and resources should be tightly tied to a user’s identity. Ideally, this should happen in real time so that any potential breaches can be caught before significant damage is done. Protecting information with encryption both at rest and in motion is essential. This, along with compliance

with the appropriate compliance frameworks, helps to ensure that the information is not only secure, but that the business is following regulatory requirements. Automating IT tasks is another way to minimize the opportunity for user error to cause a disruption. Together, these practices form the foundation of effective cloud security.

## The Role of Advanced Security Platforms

With increasing complexity in cloud environments, organizations are turning to unified security platforms to maintain strong levels of protection against threat. Solutions such as Fidelis CloudPassage Halo® help to give organizations strong security measures in place for public, private and hybrid cloud environments.

Provides real-time threat detection, recognizes vulnerabilities and misconfigurations across all assets and provides multi-cloud coverage for hybrid environments. Simplifies the management of multiple Security Information and Event Management (SIEM) products by consolidating point-products into a single platform that helps to minimize complexity and accelerate incident response.

Outpace Adversaries with Limitless Cloud-Scale Security

- Cloud-friendly Deployment
- Hyper-scalable Workload Protection
- Agentless Cloud Posture Management

Download Datasheet


## Choosing the Right Cloud Model for Security

There is no one-size-fits-all approach to cloud security, and there is no such thing as a “most secure” cloud model. Different cloud models are appropriate for different situations, and choices will vary based on the specific needs of the organization.

Whereas public cloud offers scalable and fast infrastructure (provided that the administration of the instances is taken care of), private cloud is suitable for companies who want to have a very

high level of control and compliance. Hybrid cloud is most suitable for companies that need flexibility but can also handle the extra complexity.

## Final Thoughts

The debate concerning public, private, and hybrid cloud security is not about making a winner or loser, but rather about making trade-offs. Shared responsibility and configuration risk are introduced with public cloud. Control is provided in private cloud, yet complete accountability is required. Hybrid cloud offers flexibility at the expense of complexity and a wider attack surface. With the awareness of the security concerns of the public cloud, privacy cloud security threats, and issues of hybrid cloud security, the organizations will be able to formulate more robust security measures. However, at the end of the day, the success of cloud security is not determined by the model you adopt but rather the model itself and how well it is managed and secured.