



Are you confident in your hybrid cloud security?

Getting hybrid cloud security right doesn't have to be insurmountable. Here's how to overcome five key challenges.

While organizations are demonstrating their commitment to the strategic and operational value provided by hybrid cloud—91% now use a hybrid model in some form¹—their confidence in hybrid cloud security is not as strong. When asked which enterprise architecture is most secure, 75% of respondents in a recent HPE hybrid cloud survey rated private cloud as having the “right level of security,” with on-premises architecture second at 63%. Just 60% of organizations ranked the three-pronged hybrid cloud approach of on-premises, private cloud, and public cloud as the most secure.

This shouldn't be too surprising. It's logical to assume the more environments you manage, the more complex the task of securing them will be, especially as AI initiatives proliferate. While it's true that securing local and cloud-based data requires slightly different security approaches, much of hybrid cloud security hinges on following some foundational practices. Let's look at five of the most common hybrid cloud security challenges and how you can mitigate them.

¹ [“From hybrid cloud by accident to hybrid cloud by design,”](#) Hewlett Packard Enterprise, May 2023.



1. Preventing unauthorized data access

One of the biggest benefits of hybrid cloud is that it gives organizations greater flexibility over how they host and use their data. You can keep sensitive data in an on-premises data center or a private cloud while simultaneously taking advantage of public cloud's greater computational power for AI training and other high-performance computing needs. However, you must carefully balance the security of your data with the ability of users—both employees and customers—to access it.

Identity and access management functions as the key gatekeeper to an organization's most valuable assets, says Jan De Clercq, distinguished technologist for HPE Services. It manages user identities and controls access to the organization's critical information and resources. As its name suggests, identity and access management is a two-part process. When someone logs into a service, an identity management database checks their identity, which contains up-to-date records of all the organization's users. Once the identity is verified, the access management system makes sure the person has the appropriate privileges for the resource they are attempting to access.

You can implement identity and access management in different ways, but it should always have the following objectives:

- Ensure authorized users have the appropriate level of access to the right resources in the right context for their role.
- Prevent unauthorized users from accessing data and resources by limiting access to specific groups and roles, such as employees, customers, vendors, and so on.
- Protect the organization's systems by monitoring user activities for unauthorized access and hacking attempts.
- Prevent fraud committed by users who abuse their access privileges.
- Ensure the organization meets relevant regulatory criteria for customer identification, suspicious activity detection, and identity theft prevention.

"Identity and access management is the cornerstone of securing the hybrid cloud," De Clercq says. "Most public cloud platforms provide identity and access management tools for customers to use. The key is making sure you can align your identity and access management solution with both your internal and your public cloud components."





2. Understanding your security responsibilities

A common challenge organizations face is integrating their security operations with the hybrid cloud. “To do that, you first need to have a very clear understanding of what you will manage in the public cloud and what’s the responsibility of the cloud provider,” De Clercq says. “Based on that, you need to consider what security operations resources you currently have and how you can extend them into the hybrid cloud environment.”

While organizations are responsible for the security of their private data centers, they share the security responsibility of the public cloud with the cloud service provider. This arrangement is codified in the shared responsibility model, which outlines who is responsible for each security element in the cloud environment.

In most implementations, the model stipulates the cloud service provider is responsible for safeguarding the cloud environment and its underlying infrastructure, such as physical facilities, servers, and so on. The customer is responsible for protecting the apps, data, AI models, and other assets they run and store in the cloud environment.

A simple way to understand the shared responsibility model is to consider what you have direct control over. In addition to the data you store in the cloud, you’re also typically responsible for the security of your network, any devices that connect to the public cloud, your users’ credentials, and any regulatory compliance controls you have in place. It’s your responsibility because the cloud service provider lacks visibility into them.

The shared responsibility model provides a high-level view of which security areas each party is accountable for. But in practice, security responsibilities may differ depending on the cloud model, service provider, and other factors. You must review the service-level agreement (SLA) with your cloud provider to ensure you understand your security responsibilities. If you operate in a multicloud environment, you must review your vendors’ SLAs individually because terms are not standardized across vendors. Any differences should be factored into your organization’s overarching hybrid cloud security strategy.

“There are subtle details in each vendor’s responsibility model,” De Clercq says. “You always must look in the details to see what you need to do and what you don’t need to do.”





3. Meeting compliance requirements

New and increasingly complex data protection regulations have presented organizations with another challenge to overcome. Many organizations are unclear about their compliance obligations and how to be compliant in a public cloud.

In most cases, compliance requirements are the same whether you're hosting data in an on-premises data center or a private or public cloud. The difference is in how to meet those requirements.

The first step to achieving cloud compliance is understanding which regulations and industry standards your organization is subject to. Some common ones include:

- **General Data Protection Regulation (GDPR):** This is the primary legislation governing the protection and privacy of European Economic Area (EEA) citizens. It applies to any organization that stores or processes personal data about EEA residents, regardless of where the organization is located.
- **ISO/IEC 27001:** This is an international information security standard for businesses of any size, which provides a best practice framework for implementing, maintaining, and continuously improving an effective information security management system.
- **Systems and Organization Controls 2 (SOC 2):** This is a reporting framework developed by the American Institute of Certified Public Accountants (AICPA). It's used worldwide to define and evaluate customer data management around five Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy.
- **Payment Card Industry Data Security Standard (PCI DSS):** Applies to any organization that accepts and processes payment cards worldwide. It includes 12 primary requirements to protect cardholder data and achieve compliance.
- **Health Insurance Portability and Accountability Act (HIPAA):** Standardizes how healthcare providers must handle the patient data they collect in the U.S.
- **Children's Online Privacy Protection Act (COPPA):** Regulates the collection of personal information from children under 13.

Just as you share responsibility for cloud security with your provider, you also share responsibility for compliance. The same guidelines apply. The cloud vendor is responsible for the compliance of infrastructure and services it provides, and you are responsible for the compliance of apps, data, devices, AI models, and any other assets in your direct control.

Major cloud providers deliver tools to help their customers achieve compliance. These include offerings tailored to your specific industry's key security standards and compliance certifications as well as monitoring and auditing services. Again, it's essential to review your vendor's SLAs to ensure everything is consistent with the regulations governing your organization.





4. Ensuring data remains secure

In a hybrid cloud environment, data is often transferred among on-premises data centers and private and public clouds. This has become especially prevalent with AI training operations, as the necessary data often lives in multiple locations. Many organizations believe their cloud service provider is responsible for the security of their data once it enters the cloud environment. However, this isn't the case.

“No matter what cloud platform you're using, you're always responsible for the security of your data,” De Clercq says. “You can never outsource that responsibility to a cloud provider. Regardless of where your data lives, you always need to implement the right levels of protection.”

Ultimately, you can protect your cloud data by following the same best practices that guide the security of the data in your on-premises data center. Those include:

- **Encrypt your data**

It's important to encrypt your data across your hybrid cloud environment. Most major cloud providers encrypt your data while it's being stored in the cloud and when it's in transit between private and public clouds. It's also recommended you encrypt your data files before they are moved into cloud storage.

- **Secure your end-user devices**

It's equally important to secure any smartphones, computers, and other devices connected to your network with an endpoint protection solution. This is especially true if you have a bring your own device policy, as your security team may not be able to implement security measures on employees' personal devices as easily as on company-owned devices. Endpoint protection software can mitigate this by allowing you to manage how data enters and exits the cloud via these devices.

- **Control access with strict credentials and permissions**

An easy way to protect your data is to make sure your users can access only the data they need. Use a zero trust architecture that permits users to access the data they need to perform their role. It's also important to implement strong credential management policies, so unauthorized users can't abuse the permissions granted to legitimate ones.



5. Filling the skills gap

The cybersecurity workforce shortage has been well documented. There just aren't enough people with the necessary cybersecurity skills to meet the increasing demand. Exacerbating the challenge is that on-premises security operations knowledge and skills don't necessarily transfer to public cloud environments. Skill requirements can even differ between one cloud platform and another.

In this scenario, it's understandable that most organizations can't handle hybrid cloud security independently. Enlisting help from a managed service provider enables you to augment your security team with hybrid cloud security specialists. These providers can help you acquire the right people, processes, and tools to maximize your hybrid cloud capabilities while minimizing security risk.

"Most companies' cybersecurity teams are already overwhelmed with their current workloads," De Clercq says. "They don't have time to learn something new. If you don't have trained and tailored resources for securing your cloud platform, then it's best to partner with a service provider who can provide the necessary skills."



Bringing unified protection to the hybrid cloud environment

The goal of hybrid cloud security should be to protect your data, applications, and resources across your environments. While this can present challenges, it can ultimately enable greater security and compliance than any singular operating model. With an appropriate level of security up and running, your organization can be well-positioned to focus on its business needs and new market opportunities.

Learn more at

[HPE.com/security](https://hpe.com/security)

Visit [HPE GreenLake](#)



Chat now (sales)

 **Hewlett Packard
Enterprise**

© Copyright 2024 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a50008530ENW, Rev. 1