Protect your critical data, maximize efficiency and optimize strategy.

An agile, flexible approach to navigating multicloud security challenges.

White Paper by

OVHcloud®

Multicloud is the future, now.

The multicloud strategy does exactly what it says — it enables companies to pick and choose multiple cloud services from various providers and optimize their strategy as far as possible. This might mean using one cloud for certain tasks and another cloud for others, depending on the providers' specialties. Today, the majority of enterprise users employ a multicloud strategy, at least to some degree. The benefits of a multicloud approach include:

Cost savings — By taking advantage of fluctuating pricing models and policies, businesses can increase their return on investment (ROI).

Flexibility and agility — With infinite services to choose from, it might be possible to run your applications more efficiently, including projects without centralized management.

Improved reliability — Not putting all your eggs in one basket makes your set-up less vulnerable to disaster.

Performance optimization — By using best-of-breed solutions for their different advantages, it's possible to improve performance outcomes significantly.

Avoidance of vendor lock-in — With the autonomy to mix and match, you can diversify your risk factors and improve your negotiating power.

But all this comes at a cost, of course. Increased options require a more in-depth approach to data and workload security. The security challenges include:

- Lack of visibility across hosts and services.
- Overall complexity of identity and outlook.
- Network management.
- Loss of control over data.
- Increased attack surface — the greater the number of providers, the larger the attack surface and the more ways to infiltrate.

While many of the security controls have some similarities with a legacy IT response, their delivery needs to be adapted to fit into agile cloud deployments.

An agile approach to security.

With the door to multiple clouds now wide open, the approach to security needs to adapt. Perimeter security is no longer valid for distributed cloud infrastructures where at least part of the communication takes place over the internet. Once data and workloads could be guarded within a simple framework, as if inside a castle complete with battlements, arrow slits and moats. Now sensitive data needs to be understood within and between multiple frameworks. This means taking a more agile approach to security and challenging legacy beliefs.

A simple, perimetric security approach is no longer valid for multiple reasons. The shared responsibility model, for example, is much more pronounced in a multicloud environment because the attack surface is larger. The user, therefore, has to be responsible for a larger variety of management and configuration tasks. There also is much greater exposure to the internet, which demands new ways of protecting assets and systems and a safer, more secure interconnection between internal and external systems. With multicloud, you're no longer safe inside the castle. You need armored cars protected by intelligence agencies with a detailed understanding of the various locations of your data, workloads and applications.

Protect the data, not the perimeter.

The advances in technology have necessitated a change from protecting the perimeter to protecting the data. IT teams need to reposition their target, placing emphasis on securing data and workloads as they are distributed and processed across a large variety of cloud assets. The CISO team needs to develop its own framework for risk analysis, as there is no one-size-fits-all solution. With the criteria relevant to the company's business case, they would be able to map business needs with cloud capabilities, assessing at the same time the risks of each cloud solution. For example, for insurance companies, the security of sensitive data will be a primary objective. On the other hand, the company may not need to have all the data constantly accessible. In this way, your multicloud security priorities and criteria should match the specificities of your business case.

Moving to the cloud improves productivity and helps companies meet the demands of a fast-paced business climate. However, cloud environments present a range of security challenges. With businesses increasingly using multiple clouds to maximize efficiency and optimize strategy, these challenges are now more numerous and complex.

Fortunately, there are secure and reliable methods that help mitigate the potential security fallouts. Following are some of those methods to help you, whether you are migrating to the cloud or already operating within a multicloud environment.

Zero trust means just that.

The widespread adoption of cloud services and the remote work model has created a situation where organizations' data and applications exist both inside and outside of the corporate network. The security teams are no longer able to assume that users and their devices on the corporate network are any safer than devices on the outside. This zero trust security approach operates on the assumption that there is no safe perimeter anymore and access should be granted dynamically based on the risk associated with each request.

The fundamental of this approach is identity management. A modern user may have multiple devices and access resources from different networks and applications. Their identity can serve as a control plane for access requests across all platforms. In a multicloud environment, identity-based access control has many benefits, such as:

- Broad support for identity-based access control in many cloud apps.
- Easier behavior monitoring and conditional access control.
- Richer telemetry for better access control decisions.

Multicloud security risks.

With the increased flexibility offered by multicloud comes increased exposure to threats. It's possible to mitigate potential issues if teams implement changes and avoid common pitfalls, including:

Lack of cloud security skills — The rush to the cloud often comes at the cost of expertise. Companies introduce new solutions without fully understanding the risks or lacking the knowledge to secure them.

Multiplication of dedicated tools — Adding another cloud to your portfolio often means yet more complexity, another control panel, another set of credentials and yet another surface for the attackers.

Vendor lock-in — When choosing a multicloud strategy, you definitely want to avoid being locked in with a particular vendor. While many of them now offer standardized solutions, there are services native to each platform, such as encryption key management, which, while making your cloud deployment more secure, may limit or make it impossible for you to move away from the cloud.

Shadow IT — A variety of PaaS and SaaS solutions on the market make it easy for the business units to purchase them directly, bypassing the CIO team. An unsupervised platform poses a threat to the company's overall security.

Zero trust operates on the assumption that there is no safe perimeter and access should be granted dynamically based on the risk associated with each request.

Best practices for multicloud.

Map Your Assets

With multiple cloud solutions, the first step to a successful and secure cloud strategy is to be aware of what's in your cloud portfolio. Gather all information about each cloud asset, such as dependencies and network links. Invest in mapping tools to automate the process.

Define Your Requirements

Each of your cloud solutions has a specific characteristic regarding technical, contractual, localization and regulations. For better security and control, it's necessary to understand why each of these solutions has been chosen. Understanding a business case will help you choose the right security level for each of them.

Diversify Your Risks

Due to their distributed nature, multicloud ecosystems offer an opportunity to diversify the risk. With a variety of offerings and providers, automation allows you to build a resilient multicloud environment suited to meet your most demanding business needs.

- From SaaS to IaaS — you decide how much control over your data and workloads you want to share with providers.
- Automatic deployment and monitoring — to eliminate human mistakes and misconfigurations and monitor and detect unusual behaviors.
- Disaster recovery planning — distribute resources across dispersed data centers and providers.

With a variety of offerings and providers, automation allows you to build a resilient multicloud environment suited to meet your most demanding business needs.

Prepare to Deploy Anywhere

You may be surprised, but APIs and automation are great security tools. The less you do manually, the less you allow for human error. Automated deployment enables you to reverse and deploy in the same way on premises or on cloud.

Categorize Your IT Assets

All your workloads and applications can be put into one of the following baskets. Each of these categories will share a different ratio between required data security and workload availability.

- Highly available services like identity and access controls.
- Active Directory and master databases.
- Architecture assets such as DNS, backup systems and configuration management.
- Disposable assets, such as front ends, temporary services and non-persistent services.

Build Your Security Template

Controls, processes, plans and policies that you implement in your company should be built with organizational needs, risk assessment and known vulnerabilities in mind. The way you collect and analyze logs and manage security alerts and user identity should reflect your security and business priorities. Your template should include:

- Hardening and configuration management.
- Log management and observability.
- SIEM — security information and event management.
- Identity and access management supported by SSO (single sign-on) authentication.
- Data encryption.
- ACL management.
- Asset management.

Stay Agile

Once your security template is in place, it doesn't mean you can rest. As technologies and services evolve, so should your security tools and processes. With every new tool or service your company acquires, there's a risk. Your work is never done.

A flexible approach to security.

While using multiple cloud options can improve productivity and reduce costs, the strategy comes at a price. Achieving the right amount of security for your IT projects will mean adjusting or challenging legacy beliefs. With multicloud, workloads are processed and distributed across multiple cloud assets. For an effective security response, the emphasis should be on protecting the data rather than any perimetric approach.

It also is vital for companies to avoid common security pitfalls in their multicloud strategy, such as vendor lock-in, excessive dedicated tools or building inefficient virtual security perimeters. While there are fundamentals to bear in mind, there also are multicloud best practices essential to any effective multicloud security strategy. With multicloud, it's no longer possible to simply lock your data away from threats. You need a flexible security approach that responds to ever-changing data needs and requirements.

OVHcloud US is a subsidiary of OVHcloud, a global player and Europe's leading cloud provider operating more than 400,000 servers within 43 data centers across four continents. For over 20 years, the company has relied on an integrated model that provides complete control of its value chain, from the design of its servers to the construction and management of its data centers, including the orchestration of its fiber-optic network. This unique approach allows it to independently cover all the uses of its 1.6 million customers in more than 140 countries. OVHcloud now offers latest generation solutions combining performance, price predictability, and total sovereignty over their data to support their growth in complete freedom.


us.sales@us.ovhcloud.com


x.com/OVHcloud_US


us.ovhcloud.com