OVHcloud

ovhcloud.com

Protect your critical data

How to choose the right level of cloud security

It doesn't take much research to work out the benefits of moving to the cloud. Scalability, cost, and performance to name but a few. However, evaluating whether or not a transition to the cloud is a secure option, isn't quite so simple. Different IT projects require varying levels of security and different providers have different security offerings. In this article, we discuss the reality of cloud security and offer advice on how to approach an effective security evaluation – helping ensure your journey to the cloud, is a secure one.

Security - a common goal but shared responsibilities

Security should be a common goal for all actors involved in any cloud strategy – from the cloud provider to the hardware vendor, software producers and end consumer. But it's wrong to assume that any of these parties can enforce cloud security alone. Effective security systems require cooperation and transparency. To succeed, all parties must play their part in the security game.

For any chance of success, each party needs to understand where their responsibilities lie. At OVHcloud, we find it useful to split security responsibilities into two separate camps: **security of the cloud** (cloud infrastructure) and **security in the cloud** (customer environment).

Cloud security – a two-faced monster you need to tame

As is the case with some Roman gods (see: Janus) and all double-headed snakes, cloud security is a two-faced opponent. To identify and evaluate cloud security, you must understand both sets of requirements. This is because one set - security of the cloud - relates to the cloud provider, and therefore guides your decision in choosing the most secure cloud vendor. The other set – security in the cloud – speaks to the responsibility of the customer to manage their own cloud setup securely.

Security of the cloud platform

There are no two ways about it, the cloud platform itself plays a large role in cloud security. The cloud provider is responsible for offering security features that keep your data secure. But not all clouds have the same security offering, and some providers are more diligent than others. To evaluate a provider, you need to be able to identify each piece of the security puzzle.

Datacentres: A secure data centre is the one armed to the teeth with maximum security features. This should include a restricted-access physical site, key-card access, video surveillance, motion detection systems, third-party access management, and security guards.

Networks: A provider should offer a private network solution (such as vRack) to limit public network transfer between servers. Data transfer and processing should be encrypted against risks such as malicious intrusions and network vulnerabilities.

APIs: Any API interface needs to be guarded with authentication and identifier systems to be secure. Duel-factor authentication via the control panel should be activated and all activity logged.

Security policies: Look out for an IT system security policy (ISSP), as well as dedicated CSIRT and SOC teams, security systems managers, risk-managers and data protection officers. These units are vital in enforcing security protocol across the board. We also recommend querying the providers ‘employee best practices’ in relation to security.

Architectures: The most secure providers will build, assemble and operate their own security systems. If hardware is built and assembled on-site, providers can optimise systems to suit customer needs and better manage security incidents if they arise.

Operational processes: Processes might include a methodology for risk management which identifies threats and vulnerabilities. Corrective measures and action plans should be formalised, tracked, and then followed up with regular reviews. An incident management system should provide a formal guide for handling security events.

‘Security by design’ principles: Clouds should be built like fortresses, with security by design principles. Strict security measures achieve availability, integrity and confidentiality.

Security in the cloud environment

The ‘Security in the cloud’ environment refers to the security of the customers content, systems, applications and networks. It’s up to the customer to configure and manage their ‘in the cloud’ environment with security top of mind (albeit with guidance from a secure cloud provider).

Depending on the cloud provider, ‘in the cloud’ features - such as security tools, visibility and control - can vary. Here are some elements to consider when evaluating any security in the cloud setup:

Security tools: A basic kit of tools will aid security processes and operations. This includes monitoring tools that allow users to monitor their infrastructure and network, enabling automatic alerts in case of any incident. It should also include ‘security groups’ to protect access to clusters, as well as other types of security management tools.

Visibility: Visibility is where secure cloud providers can really differ. A truly secure cloud is one which you can manage completely. Less visibility means increased complexity, which increases the burden of security management. Teams need to have holistic visibility across all cloud estates. They should also be able to manage change from a single console, and have access to automated processes, so they can manage the cloud while orchestrating security changes.

Control: Having the right amount of control to manage the cloud means being able to access platform and applications management tools, as well as having the power to configure operating systems, firewalls and networks, and even encryption services.

While it is useful to express these sets of security requirements as two separate groups, they are not entirely divorced. There is a thin line between the responsibility of the provider, and that of the customer. Getting it right, means understanding how your cloud strategy relates to a model of shared responsibility.

The ‘shared responsibility’ model

The nature of the different responsibility groups depends on your specific cloud service. To make an informed decision, based on security, it is vital that you determine what your responsibilities are in relation to your cloud. Any lack of understanding will sow the seeds of confusion and ultimately expose vulnerabilities that may lead to serious security breaches or data leaks further down the line.

Depending on the cloud model the share of your responsibility will be quite different:

Table 1. Your responsibilities in the cloud

	IaaS	PaaS	SaaS
Data	✓	✓	✓
Application	✓	✓	
Operating system	✓		
Virtualisation	✓*		
Network	✓*		
Physical hardware and DC			

Compliance and security evaluation – two approaches

Digital transformation - while game-changing when it comes to flexibility, control and cost - is seen as a risk for those companies who host sensitive data. Potential security issues often discourage companies from making the transition to the cloud - but this doesn’t have to be the case. Utilising a cloud provider is a good option even for companies who retain sensitive data, as long as the company asks the right questions and matches the providers offering to their unique security requirements. Security should be central to evaluating your cloud provider before committing to any partnership. We recommend utilising one of two strategies during this process:

The compliance-based approach

The compliance-based approach seeks to audit the providers’ security processes and systems. By following a checklist of security requirements, it is possible to evaluate a provider’s security offering in a methodical but comprehensive manner. This helps verify the provider’s level of security.
A key benefit to this method is that it reduces the likelihood of a customer forgetting to ask important questions about security control (providing the checklist is detailed and in-depth). However, the approach does not allow companies to evaluate security measures and processes that respond specifically to their IT project. It is, therefore, an unsuitable method for IT projects with unique data requirements.

* Depends on the type of IaaS offering.

The risk-based approach

The risk-based approach is more flexible to a customer's unique IT project because it involves asking the provider to demonstrate security features that respond specifically to their use cases. If an IT project deals with sensitive healthcare data that needs to be protected, for exa-mple, the customer may want to piece together a providers' security offering on a risk-by-risk basis. Take this example of an OVHcloud customer from the banking sector, who may have specific security requirements:

> *"To meet the security needs of one of our customers in the banking sector, we privatized our public network. We provided them with two separate network accesses, each connected to a different Point of Presence (PoP) with its own switch. This guarantees the connectivity of the service, but also redundancy. In accordance with their specifications, the teams were given direct access to our network equipment (including the switches TOR) so that they could check their configuration. The monitoring is also secured, as the connections go through a dedicated IPMI gateway. And every quarter, we re-evaluate any security indicators – related to accessing their isolated spaces – together."*
>
> **Corinne Renault, Customer Success Manager at OVHcloud**

How well-protected are the physical hardware facilities? What kind of measures are in place to ensure employees manage risks appropriately? Each question is tailored to the legitimate fears of the client and each should be met with a response. Through this process, the customer and provider are able to form a deeper understanding of the key challenges associated with the project. This reduces the potential for security fallout, as well as improving the likelihood of a successful partnership more generally.

By utilising a risk-based approach to security evaluation, the customer brings their own unique IT projects into focus – ensuring that the cloud provider considers the companies security challenges and key requirements. This approach isn't necessarily as full-proof as the compliance-based approach, where a detailed list of security requirements eliminates the likelihood of overlooking important factors.

Summary

Both these approaches are only successful when their drawbacks are considered and a company has a good awareness of their own unique security needs. The best option is to use a combination of both approaches. A compliance-based approach ensures your provider meets a universal set of security requirements, where the risk-based approach accounts for unique requirements, potentially related to sensitive data.

For anyone new to the cloud, the process of security evaluation can seem daunting. However, understanding that cloud security is achieved through first defining responsibilities will help you avoid security issues further down the line. As we have discussed, there are two sides to security – 'security in the cloud' and 'security of the cloud' – one which relates to the cloud itself and the other being the responsibility of the customer. Crucially, before partnering up with any cloud provider, we recommend digging deeper into their security offering by utilising a compliance 'checklist' based approach, combined with a risk-based approach, which questions the provider on security fears unique to your IT projects. Cloud security is not a single feature, bit of software or hardware; it is a combination of various systems, processes and architectures. Customers must ensure their criteria are met before committing any IT project.