# 6 ways to fail with your enterprise cloud if you don't plan appropriately.

## Private cloud has many benefits but presents its own set of challenges.

White Paper by

OVHcloud®

**Cloud computing has become firmly entrenched in mainstream IT. With digital transformation happening across all industries, organizations are turning to multicloud strategies to better adjust to new market demands. For enterprises, a key element of this approach is private cloud, which is considered inherently more secure than public cloud.[1]**

**Though an enterprise private cloud offers more control over the physical environment and unmatched customization capabilities, building your private cloud presents its own set of challenges.**

## 1. Security Breaches

Data breaches, compromised credentials, broken authentication, hacked interfaces and APIs – the digital world has seen more than its share of massive security problems. And weekly reports of rapidly increasing cyberattacks don't help alleviate security concerns about cloud computing.

This leads many organizations to believe their data is safest in-house in their custom-built cloud environments. The reality is that hosted environments are as secure or even more so than on-premises environments. Cloud environments are designed and maintained by security experts who understand all the many ongoing cloud security challenges and know how to mitigate them.

## 2. DDoS Attacks

Distributed denial of service (DDoS) attacks remain a major concern for all digital companies. Attackers have become increasingly sophisticated in their methods, and with advanced technologies come new threats.

A DDoS attack overloads a web server and can render a website inaccessible for hours and even days. This can cause a major loss of revenue and customer trust. Anti-DDoS protection is no longer just a nice-to-have feature for enterprises. It's a core security system. However, on-prem protection is no match for the industry-leading systems' capacity to mitigate attacks.

[1] An IDC Infobrief, June 2019.

> *Being a cloud service provider, we receive and mitigate over 2,000 DDoS attacks each day. Our anti-DDoS system protects all customers by default. There is a very simple reason behind this — a DDoS attack, if not mitigated, can result in collateral damage. It means that not only does the target experience the attack, but all neighboring servers in the rack also will. The VAC (a combination of technologies developed by OVHcloud to mitigate DDoS attacks) only activates when an attack is detected. However, for customers with specific security needs, we provide constant traffic filtering; in other words, a permanent activation of the VAC."*
>
> **— Jakub Słociński, Network Innovation Manager at OVHcloud**

## 3. Physical Security and Redundancy

Most organizations don't have the same physical security features offered by third-party data centers, which can put critical, valuable data at risk. A reputable data center will be a fortress with strictly monitored access and barbed wire fencing. Video surveillance and motion detection systems will be in continuous operation, as will fire detection and extinguishing systems.

Today, constant accessibility, high availability and resilience are key elements for many IT services. Achieving the same level of redundancy and safety for an in-house private cloud would be an ambitious task. Double electrical power supplies, power generators, UPS devices and redundant network links all add up to high maintenance costs, not to mention requiring a high level of in-house expertise and availability in today's always-on digital world.

## 4. Compliance Concerns

The PCI DSS standard lists hundreds of controls and security features that need to be set up to process payment card data securely. Private cloud grants greater control over security, but that doesn't make regulatory compliance any easier.

Maintaining compliance should always be at the forefront of planning, particularly when multiple types of regulated data are in play, such as payment card data, sensitive business intelligence and customer data. It's a time-consuming and expensive process, often requiring an organization to employ IT experts familiar with these regulations. In addition, the IT team will need to continuously monitor systems, develop clear security incident procedures, and use data encryption to ensure that compliance requirements are constantly met.

## 5. Performance Issues

Performance is a well-known issue in dynamic virtualized environments. It's difficult to predict how changes at the infrastructure level will affect application performance, as even a simple software update can unbalance a closed ecosystem. To make sure you get the most out of your infrastructure, it's crucial to put in place a continuous process to validate your cloud's performance. For every new deployment and core change, you need to have a realistic performance test, preferably an automated one that can expose issues at an early stage. Having such a process in place protects your company from unnecessary costs and allows you to keep close control over the price/performance ratio.

## 6. Capacity Overbuying

Whether you're building your private cloud with OpenStack or VMware, there is always the same major challenge: How to achieve agility and scalability when managing an internal infrastructure. When maintaining your infrastructure, an increase in capacity will require more hardware equipment. When unable to precisely predict the capacity you'll need, IT teams often overbuy to ensure they can deliver the expected resources when needed. As a result, the organization ends up with high investment costs and a feeble promise of scalability.

It's debatable whether an on-prem infrastructure can truly become the cloud, as the definition of the cloud highlights flexibility and scalability without having to invest in additional hardware. However, though many assume that a private cloud just means on-prem, this doesn't have to be the case. A private cloud is an infrastructure used solely by one organization. Its resources are not shared but isolated and dedicated.

A hosted private cloud provides organizations with the necessary means to gain agility and increase operational efficiency while mitigating the common risks that come with enterprise clouds. In a hosted private cloud environment, part of the control and responsibility for security is relinquished to a trusted service provider. That means choosing the right vendor with a proven record for security is essential to overcome all the challenges successfully.

**OVHcloud US is a subsidiary of OVHcloud, a global player and Europe's leading cloud provider operating more than 400,000 servers within 37 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