



WHITE PAPER

SECURING YOUR DATA IN THE CLOUD: BEST PRACTICES & STRATEGIES

- How Cloud makes data security easier



IT revolution has allowed companies focused on data and processes to bring their businesses to a whole new level, however, with increasing concerns around data security. Let's discuss how cloud sets up businesses for success by solving their data security challenges.

Just a decade ago, if you were a scientist, financial organization, or a company that handles calculations for oil & gas (one of the most resource-demanding task in the industry), you would need to go through the full process of ordering hardware for your datacenter: that included procurement, deployment and maintenance. After going through these long steps, you would end up with the hardware that is difficult to scale. Many companies sacrificed a lot of time for something that is easily solved by the cloud today.

If you are working with data or critical business processes, you need to ensure that security aspects are fixed. It is more or less clear what the on-premises approach is, however, the question of how to secure workloads in the cloud became the main issue that continues to delay many companies from migrating to the cloud, even today, and ultimately doing more with less effort.

Although, doing more with less is the key to scalability and focus, security is a highly sensitive and complex topic. While it's critical to understand the security landscape, it's incredibly difficult to maintain a security perimeter and be secure enough to face new challenges. That was one of the reasons for developing cloud platforms - many of the processes and technologies are incorporated into cloud Native tools that are available as a service or built-in into your infrastructure. cloud platforms host many critical infrastructures that power a major part of the Web so the security needs to be high. Any type of breach or security issue connected to the customer data will compromise the cloud platform brand, so cloud vendors invest a lot into providing their users with the highest possible level of security.

During the years of evolution of cloud platforms, security became a process - and you can apply Gcore's learnings to your project by delegating some security questions to us, whilst keeping your focus on the business. In this article, we will demonstrate a few cases of cloud deployment that show how cloud actually makes your life with data security easier.

Let's start from reviewing a list of must-have considerations that a business needs to keep in mind when working with any type of data.

Security and privacy:

Sensitive data should be protected from cyber-attacks and unauthorized access.

Compliance:

Industry and government regulations for data storage and protection should be met. These regulations are defined by the physical data's location.

Data loss:

A data recovery should be created for system failures or natural disasters.

Cost:

Hosting data on-site can be expensive. In large projects, data is generated quickly, and often local infrastructure can become a bottleneck due to lack of capacity. Moving data to the cloud means that the company can switch from a CAPEX to an OPEX model, giving them a more flexible approach to cost management.

Integration:

It is common that a company wants to have a part of data in the cloud and part on-premises. If Cloud has a toolset to implement this, it allows to connect cloud and datacenter on-premises in a secure way.

Performance and reliability:

Having the system working in a reliable way means that customers are being offered the data as it was intended by the developer, in a consistent way. Outages lead to serving inconsistent data.

The list is not intended to be exhaustive and any data project manager will have more to say. We want to stay on a higher level and focus on where cloud can be applied. Let's go through the applicability of Cloud in a few common scenarios.

I Case I. Launching workstations in the cloud

One of the situations where cloud really excels is in delivering flexible and secure workstations to the users. A virtual workstation is a cloud-based workstation that is accessible from anywhere.

In Gcore's cloud, you can order a virtual machine or a cluster of VMs and use it until the project is done, and then stop paying. During this period, your entire deployment resides in the secure Gcore perimeter which is protected by a set of compliance certificates and many layers of security. When using VMs in the cloud, you receive built-in security functionality straight out of the box - logging, SSH keys, secrets manager.

However, there are additional scenarios with virtual workstations that sometimes slip under the radar. Let's imagine that you are a financial institution – if you hire a development team from outside, you would need to provide them with access to your perimeter. Very often, companies do this using very manual and error-prone processes, like opening the firewall IP or maintaining a demilitarized zone (DMZ). But this approach makes these ports vulnerable and require continuous monitoring by the system administrator because the ports often remain open even after the external teams have left. To fix this, companies can pre-create (using golden image) the dev and test infrastructure in the cloud, set up a VPN, and close it whenever needed without opening extra ports or allowing extra IPs to access their system.

You might think that this problem is artificial: unfortunately not. Even if your staff consists of highly professional specialists and you have established processes in place, there is always a chance that something will go wrong because of the human factor, or even worse, misconfiguration, or a floating bug. If we can eliminate this problem via a cost-effective solution, it should be done.

Adding to that, while using Gcore Cloud, you have access to a variety of different virtual machines and options, and additional services that are called IaaS Protection. So if you need a customized and advanced level of security, do check it out.

This approach to allocating workstations to temporary external contractors (of course, the same is valid for internal staff) allows to not just secure the process overall, but also prevent the appearance of shadow IT and settings in the future, and save businesses from spending extra resources to solve this.

I Case II. Scaling data processing system

The cloud is the ideal place for hosting a data processing system. By combining cloud capabilities that are available as IaaS and PaaS services, you can set up an infrastructure that will be available all the time, will use different rules for scalability, and which could be used in a hybrid mode (for example, by using the cloud to add computing resources to your on-prem processing system when needed).

Following the same model on-premises limits the scale of the business because it is hard to allocate needed computing resources in a fast manner. In the case of cloud, you have virtually unlimited resources and options to scale your deployment.

This depends on the specific security requirements and constraints, and model of using cloud for the data (will it be in the cloud or in a hybrid mode, in which case we need us to transfer data and secure it in transit). Nowadays, it is possible to find the best combination by securing it beforehand, during the transit, and when the data is at rest in the cloud.

There are several options for securing data in the cloud, including:

Encryption:

Encrypting data at rest and in transit to protect from unauthorized access and theft. Basic instruments include SSL channels that are de-facto standards of securing data in transit, and these are fully supported at Gcore.

Access control:

Implementing access controls to restrict access based on user roles and permissions.

Network security:

Securing the network connection between the user and the cloud server using firewalls, Virtual Private Networks, and other security tools. In Gcore Cloud, data at rest is secured by many layers of physical (the data-center layer) and service level (instantly evolving algorithms to prevent DDoS attacks, unauthorized access, and other attack). Security threats are actively prevented on many levels by using sophisticated heuristics and cutting edge technologies like eBPF.

Adding to this toolset, it is always critical to implement a data backup and recovery plan against data loss in case of system failures. Gcore has these plans in place for datacenters and your data is fully secured even in case of major disasters, however it is always a good idea to have processes in the company.

What about regulations? This is one of the biggest questions that often prevent companies from using the cloud, and we have it covered. The question is covered. Gcore Cloud has industry certificates - ISO/IEC 27001, PCI DSS, and GDPR - that allow you to put sensitive data and delegate compliance to the platform. The platform complies with industry and government regulations for data storage and protection, and regularly conducts third-party security assessments to identify and address potential security risks.



Data security is the foundation of a secure and resilient cloud infrastructure and new emerging technologies are further enhancing cloud data security. It's easier now to safeguard the confidentiality, integrity, and availability of your data in the cloud.

