# Parking your data on the cloud? Here are the security risks you should consider

In 2020, Cybersecurity Insiders published a report on cloud security, and the details took the IT world by storm! The report revealed that 94% of organizations were moderate to highly concerned about cloud security. 68% of the respondents said they were afraid of misconfiguration, 58% admitted they were worried about unauthorized access, while 52% and 50% of respondents said that they feared insecure interfaces and accounts hijacking.

Post covid, most organizations have migrated to cloud infrastructure for improved collaboration, easy accessibility, enhanced storage capacity and hassle-free mobility. However, cloud computing involves its distinct set of risks. Increasing attacks on cloud-based services are evident that organizations need a cyber security tool that can protect their cloud data from different types of attacks.

Here are some of the most common types of cloud security attacks that one should be aware of:

**1. Intellectual property loss**

The Ponemon institute surveyed over 400 IT companies and found that about 21% of the cloud data uploaded by company employees contained sensitive information. The current BYOC (Bring Your Own Cloud) trend poses a significant risk to the Intellectual Property related information uploaded on the cloud.
Unencrypted data storage and weak cloud security measures open gateways for cyber assailants, potentially resulting in the loss of intellectual property.

## 2. Zero-day exploits

Using a cloud is like using someone else's computer. Therefore, data parked in the cloud is vulnerable to zero-day exploits. When assailants target unpatched vulnerabilities in operating systems or software, it is called zero-day exploits. This is a severe cloud security risk because it allows the assailant to penetrate the cloud environment even if the security configurations are top-notch.

## 3. Contract breach and legal actions

Businesses are bound by contracts restricting data sharing and other processes. However, in several cases, the data uploaded on cloud accounts are stolen by the attacker and shared in the public domain, breaching the terms of the contract.
The unknowing contract violation leads to legal suits against the organization. So, data parked on the cloud may land the organization into a legal conflict.

## 4. Misconfiguration

There is limited awareness about protecting cloud infrastructure. As a result, in several cases, mistakenly, the user may misconfigure cloud security settings, exposing the confidential data parked on the cloud. This can happen due to some of the below-mentioned reasons:

- Organizations lack visibility and control over cloud infrastructure.
- They are unfamiliar with cloud infrastructure security.

- They have multi-cloud deployment and juggle between multiple security controls provided by different vendors.

It goes without saying that an organization might have to pay a hefty price for security oversight or misconfiguration if it results in a data breach or data leakage.

Read More: Parking your data on the cloud? Here are the security risks you should consider