Why Your SaaS Data Needs Backup Protection

Software-as-a-service (SaaS) applications are more in use than ever before. Almost every company uses either one or the other SaaS application on a daily basis. The global SaaS market size is expected to reach $185.8 billion by 2024 as businesses move online and adapt to the cloud for an agile and lean growth model.

However, most companies operate under the misconception that SaaS providers are responsible for the protection of their data. In the 2020 IT Operations Survey Report, about 60% of the participants — IT leaders, IT managers and technicians from small and midsize businesses (SMBs) — believed that their data remains private and secure in the cloud, which is true but only to a certain extent. And only one-third of the SMBs backed up their SaaS application data.

There are significant limitations to SaaS data protection provided by cloud vendors. While cloud service providers do manage the network, OS and application side of things, the companies themselves are responsible for the data housed in the cloud and on cloud applications.

Let's take a look at the top factors that lead to SaaS data loss for businesses:

1. **Human Error** – Many users find themselves in a situation where they have unintentionally deleted emails or tons of data permanently. This data often cannot be restored—not even by the SaaS providers.

2. **Malicious Intent** – Disgruntled employees who want to harm their employers can delete important information, which is often difficult to recover.

3. **Cyberattacks** – Social engineering attacks, such as phishing emails, trick employees into clicking on a link or opening an attachment that allows hackers to gain access to the company network and data. This can prove disastrous since it not only leads to a data breach but also damages the reputation of the company.

SaaS Data Backup Is the Ultimate Protection

Many SaaS providers cannot protect your SaaS data against the threat actors mentioned above. In fact, cloud providers like Salesforce and Microsoft 365® recommend third-party backup services and many compliance regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), General Data Protection Regulation (GDPR) and more, direct companies to adopt the "shared responsibility" model for data protection in the cloud.

According to the "shared responsibility" approach, the cloud provider bears the responsibility of the infrastructure while the customer is responsible for the control and access of the data in the cloud.

To protect your SaaS data, you need a backup solution that allows you to:

- **Automate your backup –** Automating your backup procedure ensures that your technicians do not miss backups. Also, data can be backed up daily in the background without disrupting other applications.

- **Scale as required –** Your backup solution must be able to scale immediately so you do not have to worry about running out of space.

- **Restore immediately –** You must be able to restore data quickly in case of an incident, with 100% accuracy and without any data loss.

What's Your SaaS Backup Strategy?

Every business must have its own backup and recovery strategy in place that can help them prepare for the unexpected. Using the right SaaS data backup and recovery solution can make the process easier for you. Can your backup solution fully recover your business-critical SaaS data?

Schedule a consultation with us today to learn how effective your backup solution can be in case of a disaster.