YOUR CLOUD-BASED DATA YOUR RESPONSIBILITY

Cloud-based Software-as-a-Service (SaaS) applications are an increasingly popular choice for companies looking for flexibility and cost savings. While SaaS can offer new opportunities and more advanced security, these cloud providers fall short in preventing data loss triggered by user errors, data corruption or malicious attacks.

3 REASONS WHY SaaS BACKUP IS CRUCIAL

JUST BECAUSE DATA IS STORED ON THE CLOUD, DOESN'T MEAN IT'S PROTECTED.

1 SaaS Vendors Do Not Protect Against Data Loss

Leading SaaS platforms may have enterprise-grade security, but they protect your data only from infrastructure threats, such as hardware or software failure, power outages or natural disasters.

Your SaaS Data Still Needs Protection From These Common Data Loss Risks.

HUMAN ERROR

Employee negligence, failure to back up regularly and accidental file deletion are just a few ways your data can be compromised by your workforce.

HARDWARE ISSUES

Server and hardware malfunctions happen regularly, causing downtime costs to increase every minute data is not restored.

CYBERATTACKS

Ransomware, data breaches and phishing scams can result in blocked access to servers and compromised business information.

MALICIOUS INSIDER ACTIVITY

Although SaaS providers have implemented security measures to protect data, malicious insiders can still gain access to sensitive information. They could do this using social engineering techniques or stolen credentials.

PROGRAMMATIC ERRORS

Your SaaS provider may not always be able to protect your data from programmatic errors. A programmatic error is an error that occurs during the execution of a program. This can happen for a number of reasons, such as an incorrect setting in the code or unexpected input.

SaaS RETENTION POLICIES

Most SaaS applications have some sort of retention policy in place that dictates how long data is stored and how it is purged. For example, a SaaS application may have a 30-day retention policy, which means that data is only stored for 30 days and then it is automatically deleted.

2 The Shared Responsibility Model

SaaS providers are NOT responsible for the protection and total security of your data.

Data protection regulations worldwide, such as GDPR or HIPAA, assign personal data protection as a shared responsibility.

Accountability for data protection and privacy involve both the controller (your business) and the processor (third-party service providers/ vendor).

PROCESSOR'S RESPONSIBILITY

- Hardware failure
- Software failure
- Natural disaster
- Power outage
- Delete requests

CONTROLLER'S RESPONSIBILITY

- Human error and user mistakes
- Programmatic errors
- Malicious insider activity
- Hackers or other external actors
- Malware, ransomware and virus

3 Data Backups Are Not Included or Standard

Be sure to read your Contract and Service Level Agreements (SLAs). SaaS solutions offer built-in solutions, such as Recycle Bins and Vaults, which can store deleted data for a limited period.

These solutions should NOT be confused with backup and recovery. They are temporary archival solutions with no guarantee of data recovery.

Most SaaS SLAs address availability, not recoverability, of your data.

INVEST IN THE RIGHT BACKUP SOLUTION TODAY

It's ultimately your responsibility to protect your data against inevitable loss or threats. Invest in a robust and reliable backup solution for your crucial SaaS data.

CONTACT US AND ENSURE YOUR SaaS DATA IS PROTECTED FROM LOSS NO MATTER THE THREAT!

ACS Advanced Computer Solutions

Contact: Mike Buchanan
mike@acsapp.com
www.acsapp.com