Your SaaS Data. Your Responsibility.

Cloud-based software-as-a-service (SaaS) applications are an increasingly popular choice for companies looking for flexibility and cost savings. However, 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.

77%

Businesses experience an average of **12** compromised account threats per month.

33%

60% mistakenly believe their SaaS provider is responsible for data protection.

77% of companies that use SaaS applications suffered a data loss incident in the last 12 months.

Alarmingly, **33%** of IT professionals believe SaaS-based applications do not need to be backed up.

3 REASONS WHY SaaS BACKUP IS CRUCIAL

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

REASON 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.

USER ERROR

Be it falling for a phishing scam or mistakenly deleting crucial data, user error have accounted for **23% of security breaches in 2020.**

MISCONFIGURATIONS

19% of breaches can be traced to a misconfigured cloud server as the initial threat vector. Programming errors are not covered by your SaaS provider.

INSIDER THREATS

Malicious employees are responsible for **30%** of data breaches in 2020 so far. It only takes a single individual with ill-intent to cause significant data loss.

ILLEGITIMATE DELETION REQUESTS

Your SaaS provider cannot determine if a deletion request is hasty or malicious and will honor your request no matter what.

SYNC ERRORS

While introducing third-party tools into your IT environment helps streamline your business, it leads to the possibility of your valuable SaaS data being ruined with no way to undo the damage.

MALICIOUS EXTERNAL THREATS

No business is entirely immune to cyberattacks which make up **52%** of all data breaches in 2020 to date.

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

REASON 3

Data Backups Are Not Included or Standard

Be sure to read your Contract and Service Level Agreements (SLA). 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.

CONCLUSION

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 THAT YOUR MICROSOFT 365, GOOGLE WORKSPACE AND SALESFORCE DATA IS PROTECTED FROM LOSS NO MATTER THE THREAT

SOURCES

Trends in SaaS Data Protection Report | Cloud Adoption and Risk Report 2019 by McAfee | ESG Research Report 2020 Kaseya IT Ops Benchmark Survey 2020 | IBM Cost of a Data Breach Report 2020 | Verizon Data Breach Investigations Report