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.



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



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





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



Leading SaaS platforms may have enterprise-grade security, but they

SaaS Vendors Do Not Protect Against Data Loss

protect your data only from infrastructure threats, such as hardware or software failure, power outages or natural disasters.

THESE COMMON DATA LOSS RISKS.

YOUR SAAS DATA STILL NEEDS PROTECTION FROM

Be it falling for a phishing

USER ERROR

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.

Malicious employees are

INSIDER THREATS

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



DELETION REQUESTS Your SaaS provider cannot

ILLEGITIMATE

determine if a deletion request is hasty or malicious and will honor your request no matter what.

While introducing third-party

SYNC ERRORS

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



total security of your data.

The Shared Responsibility Model

SaaS providers are NOT responsible for the protection and

responsibility. PROCESSOR'S **RESPONSIBILITY**

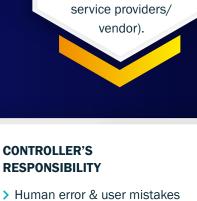
Data protection

regulations worldwide,

such as GDPR or HIPAA

assign personal data

protection as a shared



Accountability for data

protection and privacy

involve both the controller

(your business) and the

processor (third-party

> Delete requests

> Power outage

> Hardware failure

> Software failure

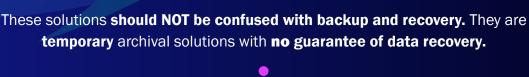
> Natural disaster

- > Hackers or other external actors > Malware, ransomware and virus

> Programmatic errors

> Malicious insider activity

REASON



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.



CONCLUSION

crucial SaaS 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

SALESFORCE DATA IS PROTECTED FROM LOSS NO MATTER THE THREAT

SOURCES

Kaseya IT Ops Benchmark Survey 2020 | IBM Cost of a Data Breach Report 2020 | Verizon Data Breach Investigations Report

Trends in SaaS Data Protection Report | Cloud Adoption and Risk Report 2019 by McAfee | ESG Research Report 2020

CONTACT US AND ENSURE THAT YOUR MICROSOFT 365, GOOGLE WORKSPACE AND