SPANNING

THE RIGHT WAY TO SECURE YOUR SAAS BACKUP

Data stored in G Suite and Office 365 is the lifeblood of your business.

77% of companies that use SaaS applications suffered a data loss incident over a 12 month period.

CAUSES OF SAAS DATA LOSS

1

HUMAN ERROR

64% of data loss incidents are due to human error

2

DELETION REQUEST

SaaS providers are blind to bad deletion requests

3

SYNC ERROR

Sync issues with third-party apps puts your critical data at risk – with no undo

4

HACKERS

Bad people driven with one idea: steal your precious data

5

INSIDER THREAT

27% of all electronic crime events are caused by malicious employee action

6

MALWARE

Rogue software intentionally designed to attack your applications

7

RANSOMWARE

Failure to meet industry-scale extortions results in data loss

KEEP YOUR SAAS DATA SAFE

RIGHT QUESTIONS
RIGHT ANSWERS
RIGHT SAAS BACKUP

THE ONLY THING WORSE THAN NO BACKUP SOLUTION — A SLOPPY BACKUP SOLUTION

WHAT

format is my data transferred and stored in?

WHERE

is my data stored?

HOW

does my backup provider connect with my email and collaboration systems?

WHO

has access to my backup system?

WHAT

UNDERSTAND THE POWER OF ENCRYPTION

- Secure data at rest with 256-bit AES object-level encryption
- Generate unique encryption keys
- Consistently rotate master key protecting the unique keys
- Provide autonomy to manage keys on your own

WHERE

DATA CENTERS MUST MEET COMPLIANCE STANDARDS

- Compliance with government regulations for data retention
- SOC 2 compliant
- Third-party certifications

HOW

ENSURE YOUR APPLICATION ACCESS IS SECURED

60% of IT professionals shared privileged account access credentials with co-workers

OAUTH 2.0	Protects privileged credentials with multi-factor authentication (MFA)	Google and Microsoft recommend MFA	Security guaranteed
VS			
SERVICE ACCOUNTS	The risky practice of storing passwords does not allow for MFA	Many SaaS backup providers use service accounts, knowing the dangers all too well	Provider convenience at the cost of your data

WHO

AVOID MISUSE OF PRIVILEGED ACCESS

- Robust intrusion detection system
- Audit logs
- Password management
- Dark web monitoring of lost credentials

‘123456’ and ‘Password’ — rated as the worst passwords account for almost 10% of all passwords.

FIND ALL THE ANSWERS

SAAS BACKUP WHITE PAPER

SECURING YOUR SAAS BACKUP - THE WHAT, WHERE, HOW, AND WHO

SPANNING

DOWNLOAD WHITEPAPER

SOURCES

SaaS data loss · *Data breaches by human error* · *Insider threat* · *Shared privileged account access* · *Weak passwords*