7 Reasons Every Business Needs SaaS Backup

› Plus, how to maximize its ROI

CARBONITE®
opentext™ Security Solutions

Reason
1

Your critical business SaaS data is **more vulnerable** to data loss than commonly **advertised**

1 in 3 **Companies experiences SaaS data loss.**

SaaS platforms like Microsoft 365, Google Workspace, Salesforce, Box and Dropbox, offer flexibility, scalability and collaboration. Even though these platforms are secure, your data isn't protected in the same way their infrastructure is. That's why you should invest in third-party backup.

There are many factors that can lead to **SaaS data vulnerability and loss.**

- **Human Error** and accidental deletion by employees
- **Malicious Intent** and removing data by bad actors or disgruntled employees
- **Synchronization Errors** or updating multiple applications can result in errors
- **From Hackers to Malware** cyber threats can leave businesses suffering reputational and financial loss
- **Outages or Natural Disasters** can jeopardize your critical business data

Source: Aberdeen Group

Reason
2

Data breaches are **expensive**

They can be a business-killer, especially for small to medium-sized organizations

The average cost of a data breach is

$4.24M

On average, it takes 287 days for a breach to be identified and contained. Which is to say, breaches can cause nearly a year's worth of damage.

Source: IBM Cost of a Data Breach Report, 2021

Reason
3

Your CSP recommends **third-party backup**

All of your cloud services (Microsoft, Google, Salesforce, Box and Dropbox) have clauses in their terms of service documents recommending you use a third-party service

Each and every SaaS platform makes it clear to users the recovery of deleted data is possible, but only within a few weeks or months. Once the recycle bin or trash folder are emptied, your data is permanently irretrievable. Cloud providers explain this in their terms of shared responsibility.

Microsoft

"We recommend that you are regularly backup your content and data that you store on the services or store using third-party apps and services."

salesforce

"Effective July 31, 2020, Data Recovery as a paid feature will be deprecated and no longer available as a service."

Google

"You have a limited time from when the data was permanently deleted to restore files and messages. After that, the data is gone forever."

Dropbox

"Deleted files are marked for deletion in our system and are purged from our storage servers. They can no longer be recovered."

Reason
4

Reliable SaaS backup is a **necessary component** of compliance

Regulators want you to be in control of your data. Backup is key to satisfying their requirements

The abundance of information privacy laws around the world demand that businesses encrypt their information, share in the responsibility for its abuse and loss and prove they can recover it if needed. In particular, GDPR, HIPAA, Sarbanes-Oxley Act (SOX), New York's SHIELD and California's CCPA all mention backup services specifically.

However, a backup solution must address the unique needs of each of those laws, such as choice of data center, data encryption, at-rest and in-transit rules and the ability to purge backups.

Organizations should have the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident."

- GDPR, Article 32

Reason
5

All the top IT analysts **strongly advise** SaaS backup

Backup is a necessary safety net

Top analysts like Gartner advise using backup. “Organizations that assume SaaS applications don’t require backup, or that the SaaS vendor’s data protection is good enough, may place critical data at risk,” says the analyst agency. “Organizations cannot assume that SaaS providers will offer backup as part of the service or provide interfaces that backup vendors can use to access data,” adds the analyst agency.

“Assuming SaaS applications don’t require backup is dangerous.”

- Gartner

Forrester concurs. “While almost all SaaS vendors explicitly state that protecting data is the customer’s responsibility, infrastructure and operations (I&O) leaders usually send critical data to those providers without any plan for ensuring data resiliency.” In other words, “Back up SaaS data or risk losing customers and partners. Stop leaving the door open to data loss and start proactively protecting cloud data before it’s too late.”

“Back up your SaaS data—because most SaaS providers don’t.”

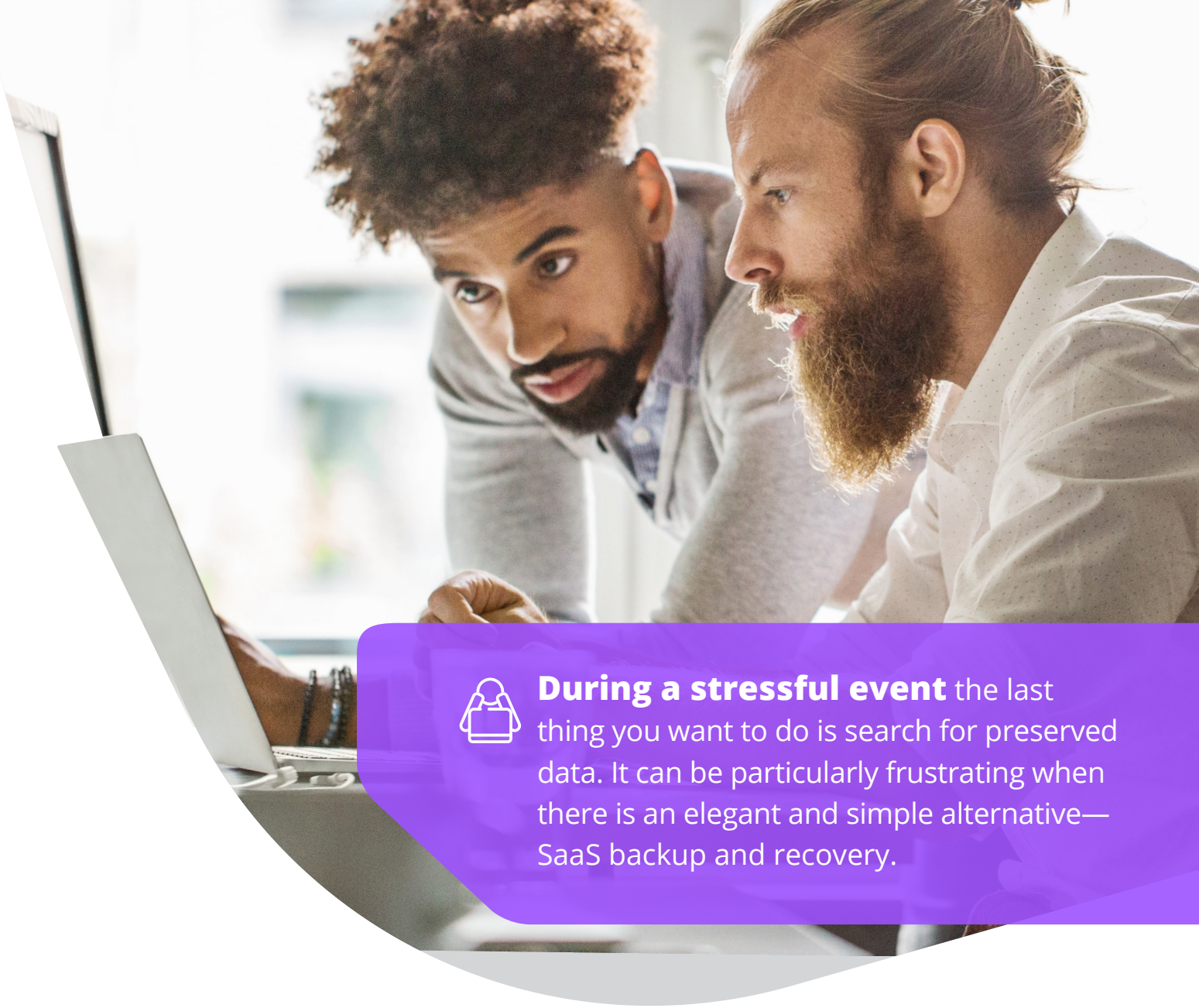
- Forrester

Reason
6

Native recovery options are **often time-bound**, cumbersome and **ineffective**

Recycle bins do not provide true backup and recovery

Native solutions are archival in nature and not built for data recovery. This means restoring deleted data is tedious, destructive and incomplete without unlimited backup or cross-user recovery. More importantly, data is stored for a limited time—just a few weeks to a couple of months. When the average time to detect a breach could span ten months, you need to be able to go back to any point in time to recover critical documents and assets.



During a stressful event the last thing you want to do is search for preserved data. It can be particularly frustrating when there is an elegant and simple alternative—SaaS backup and recovery.

Reason
7

Backup conceals the impact of a breach by **ensuring business continuity**

The key to bouncing back is quick disaster recovery with self-service options

When faced with a security breach, an urgent request to recover an important document or a system outage, the blame often falls to the person responsible for protecting the organization's data. Having a solution to reduce the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are imperative for rapid disaster recovery and business continuity. To achieve them, you need seamless data recovery from an accurate, real-time backup.

SaaS backup solutions that offer non-destructive point-in-time or granular restore with unlimited data retention can reduce your RPO and RTO and ensure rapid data recovery. Moreover, if they offer self-service restore, they minimize the time to recover even further while reducing strain on IT teams.

Backup and recovery are a central part of any business continuity or disaster recovery plan.

How to save **with backup**

Reduce SaaS platform license costs and ease workforce management

Are you paying for inactive licenses of Microsoft 365 to prevent the loss of data from an account? With our solution you can back up the account data when an employee exits and then use cross-user to restore the data to the new employee's account. Not only does this significantly reduce license costs, but it also facilitates easy workforce management with seamless on-boarding and off-boarding.

Maximize your existing storage with BYOS

Our "Bring Your Own Storage (BYOS)" allows you to use your own Amazon S3 compatible storage to back up your data. Maximize on your existing infrastructure while reducing costs with BYOS. However, if you elect to use BYOS, you will have to manage the storage limits and protection of your database.

Get comprehensive protection and discounts for multi-solution backup

Modern enterprises have complex stacks which could include multiple SaaS solutions or migrations from one to another. We have all your bases covered with comprehensive backup for Microsoft 365, G Suite, Salesforce, Box and Dropbox. Moreover, we also offer custom discounts for multi-solution backup.

Reduce costs with volume discounts

We offer high volume discounts for more than 100 users. Not-for-profits and educational institutions can save even more.

Minimize effort of IT teams with self-service recovery

The loss of data as a result from a mistakenly deleted critical document or a malware attack can be avoided if employees can recover their own data with a few clicks. Our self-service recovery further improves the disaster recovery time, while reducing the dependence on over-worked IT admins. It's particularly helpful for globally distributed teams.

Learn more about cyber resilience at

carbonite.com and webroot.com

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia.

CARBONITE® + WEBROOT®

opentext™ Security Solutions