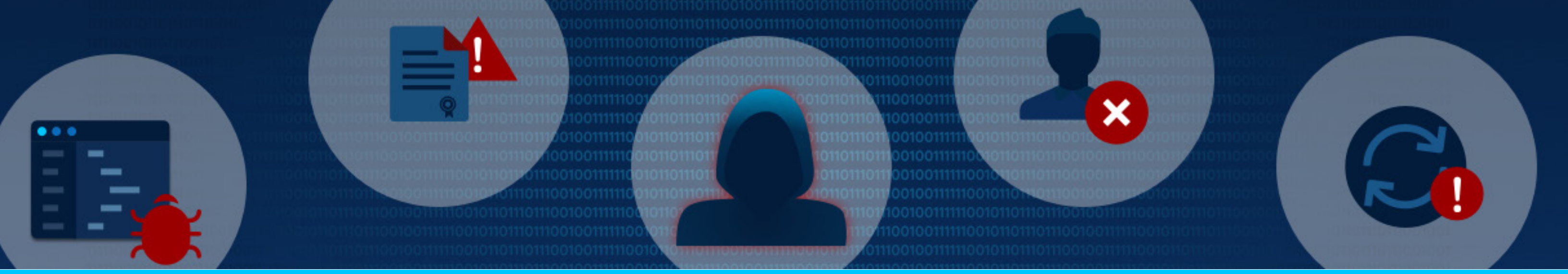
CLOUDALLY
Secure Cloud Backup

7

eBook

7 Reasons Why Organizations Need Box Backup

And Pointers to Maximize Its ROI



#1 Your business-critical Box SaaS data is vulnerable to data loss

due to human error, malicious intent, hackers, malware, sync errors...

One in three companies experiences SaaS data loss

(Source: Aberdeen Group)

Your organization adopted the Box SaaS platform. It is reaping the benefits of its flexibility, scalability and collaboration mechanisms. While it is an extremely secure solution, Box cannot protect you from data loss at your end - from some of the most prevalent causes, such as:

Human error: An account mistakenly deleted, a critical email erased or an org-wide shared document overwritten? Nightmarish scenarios that cannot be fixed without a backup and recovery solution.

Malicious intent: Your SaaS data is also prone to intentional overwrites, and deletes by bad actors like disgruntled or malicious employees.

Synchronization errors: Syncing or updating multiple SaaS applications - a common software scenario in organizations - is prone to errors and can cause loss of SaaS data.

Hackers, Malware, Ransomware, Cryptomining, Phishing: There is an ever-growing list of malware types and scams. The damages due to such data breaches are devastating not only in terms of financial loss, but also damage the business' reputation and cause loss of customers.

Outages: Box has high availability, but downtimes and outages are a reality. Wouldn't it be great to access documents and files from an accurate, real-time backup if your SaaS platform was down?

#2 A Data Breach is Expensive

and a Business-Killer

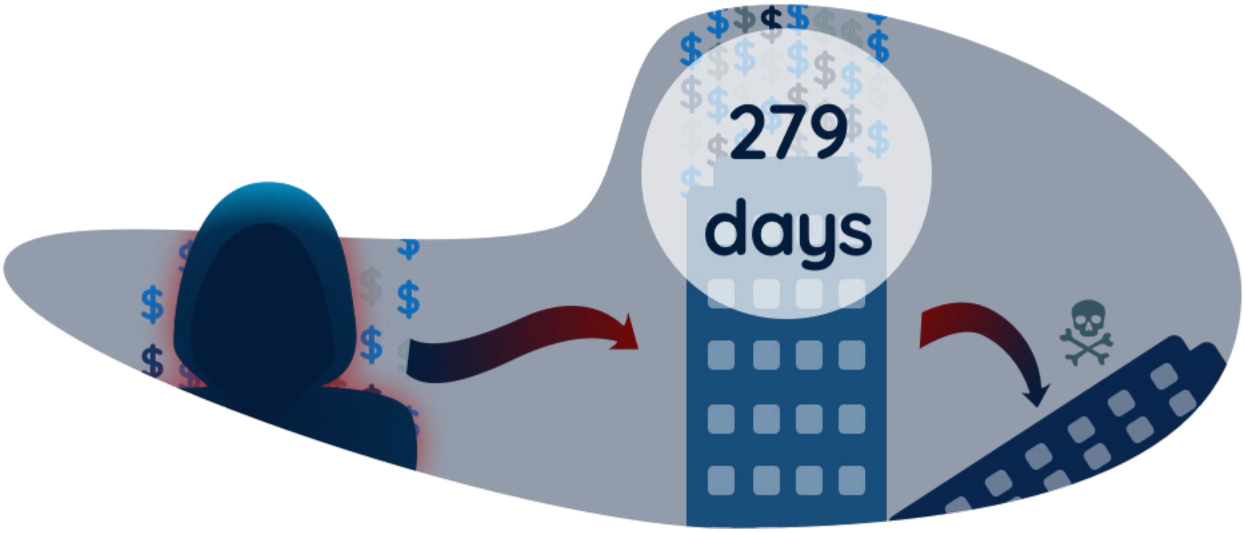
€ $ ¥ £

The global average cost of a data breach is $3.92 million. And the time taken to identify a breach is 279 days.

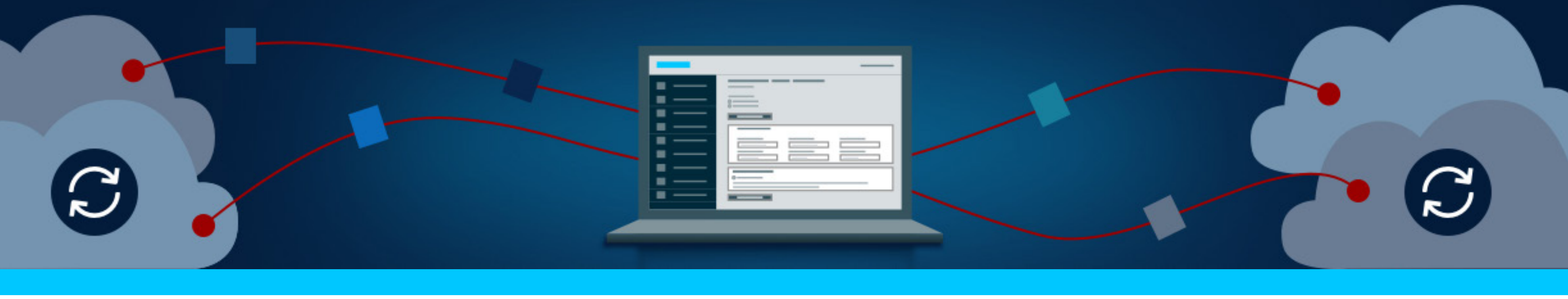
– IBM and Ponemon Institute's Cost of a Data Breach 2019 report

The average cost of a data breach is $3.92 million[1] - expensive in itself. What is more worrisome, is that it is a herculean task for an organization to recover from a breach (*Source: IBM and Ponemon Institute's Cost of a Data Breach 2019 report*).

The time it takes organizations to identify and contain a breach, also called the data breach life cycle is 279 days! This is almost a year's worth of damage. Hence it is no surprise that almost half of mid-sized companies close shop because of a breach. Both the cost and the data breach life cycle have also been reported to be increasing year-on-year.



[1] https://www.ibm.com/security/data-breach



#3 Box Data Protection is a Shared Responsibility

One that You Share with Box

Box makes it amply clear that in-solution recovery of deleted data is possible only within a couple of weeks to months. Restoring corrupted files to their former glory is almost impossible.

Restoring data with native options time-bound and tedious. Once emptied, there’s no hope - your data is permanently gone and irretrievable.

You and Box have a “shared responsibility” for protecting your data. Particularly when the causes of data loss are at your end.

Easy, point-in-time recovery is a must for the organization of today. Your distributed remote workforce with all its business-critical data on Box, expects it.

#4 Reliable SaaS Backup ensures compliance

and helps you retain control of your data

Data regulatory laws world over - GDPR, HIPAA, Sarbanes-Oxley Act (SoX), Stop Hacks and Improve Electronic Data Security Act (SHIELD), California Consumer Privacy Act (CCPA) - mandate data encryption, shared responsibility, and demonstrable recovery.

However, note that the backup solution has to be compliant with the laws' requirements such as the choice of data center, data encryption at-rest/in-transit, and 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

#5 Top IT analysts strongly advise SaaS Backup

it's is a must-have safety net

Top analysts like Gartner advise, "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". Gartner adds, "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."

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". They further put it in blunt terms, "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".

Gartner.

"Assuming SaaS Applications Don't Require Backup Is Dangerous"

- Gartner

FORRESTER

"Back Up Your SaaS Data — Because Most SaaS Providers Don't"

- Forrester

#6 Native recovery options are time-bound, and cumbersome

they weren't built for backup and recovery

Native solutions like Box Governance are time bound. Once the time limit is up your data is permanently deleted.

Native solutions such as Box Governance are archival in nature and not built for data recovery. This means that restore is tedious and destructive (changes are overwritten) without unlimited point-in-time, or cross-user recovery. More importantly, data is only stored for a limited time - from 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.

In that stressful moment, it would seem a wasteful and possibly futile use of resources to be cobbling together a way to recover the data using native options. Particularly when there is an elegantly simple way out - SaaS backup and recovery.

#7 Backup blunts the impact of a breach by ensuring business continuity

quick disaster recovery and self-service recovery

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

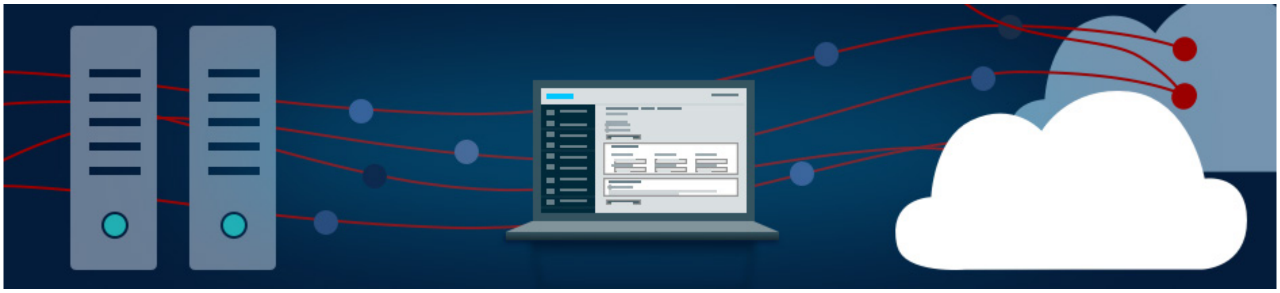
When faced with a security breach, an urgent request to recover an important document, or a system outage - the person facing the heat will be - you - the person responsible for protecting your enterprise's data.

Reducing the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are the holy grail of rapid disaster recovery and business continuity. They hinge on 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 fast data recovery. Moreover, if they offer self-service restore they minimize the time to recover even further, while reducing strain on IT teams.

Pointers to Save on Backup

A holistic SaaS backup solution goes beyond its call of backup and recovery. Enterprise-ready backup can help empower a global workforce, accommodate diverse software/infrastructure stacks, help you comply with stringent data regulatory laws, and increase its ROI.



Reduce SaaS platform license costs and ease workforce management

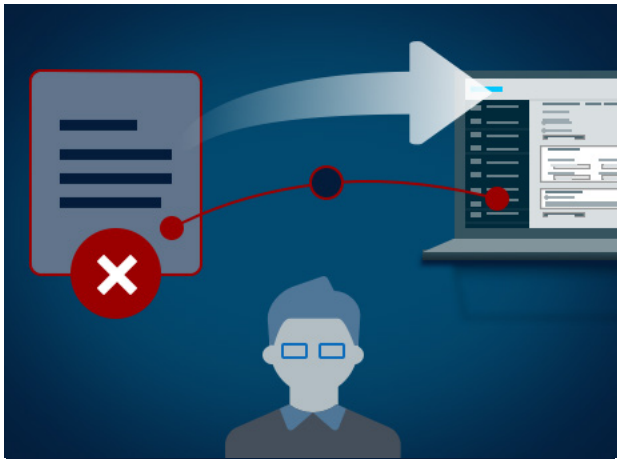
Are you paying for inactive licenses of Box to prevent the account data from being deleted? With CloudAlly you can backup the account data when an employee exits and then use cross-user restore of the data to the new employee's account. Not only does this significantly reduce license costs, but it also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

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. CloudAlly has all your bases covered with comprehensive backup for Microsoft 365, Google Workspace, Salesforce, Dropbox, Box. Moreover, we also offer custom discounts for multi-solution backup.

Minimize effort of IT teams with self-service recovery

A mistakenly deleted critical document or a malware attack could be turned on its head if employees could recover their own data with a few clicks. CloudAlly's self-service recovery[2] further improves the disaster recovery time, while reducing the dependence on over-worked IT Admins, by putting the ability to recover in the hands of the end user. Particularly helpful with a globally distributed team.



Bring down costs with high-volume discounts

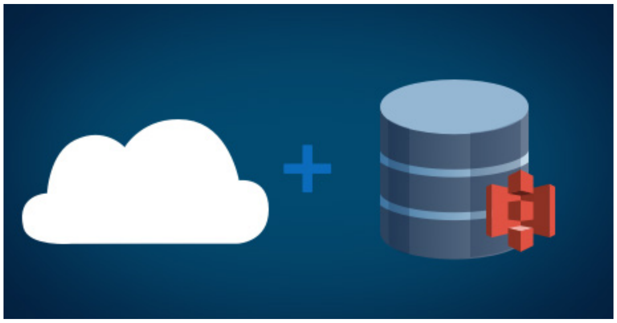
CloudAlly offers high-volume discounts for more than 100 users.

Non-profit or an educational institution? Save even more

We provide a discount for non profit organisations and academic institutions.

Maximize your existing storage with BYOS

CloudAlly's Bring Your Own Storage (BYOS) allows you to use your own Amazon S3 compatible storage to backup your data. Maximize on your existing infrastructure while reducing costs with BYOS. However, if you avail of the BYOS option, you would have to manage the storage limits and protection of your database.



[2] Q2 2020 Release

About CloudAlly

CloudAlly pioneered SaaS Backup for the enterprise in 2011. Consequently, our backup solutions for Microsoft 365, Google Workspace, Salesforce, Dropbox, and Box are tried and tested by organizations with thousands of users. We're top-rated by Gartner Capterra and G2, and were voted as a leading SaaS backup solution by over 10,000 IT Pros in a survey conducted by Newsweek. We're secure, scalable, and built with features tailored to secure for the enterprise. Your enterprise.

Intelligent Workforce Management: Simplified employee on-boarding and off-boarding with bulk activation, automated addition/deletion users, and backup of inactive accounts.

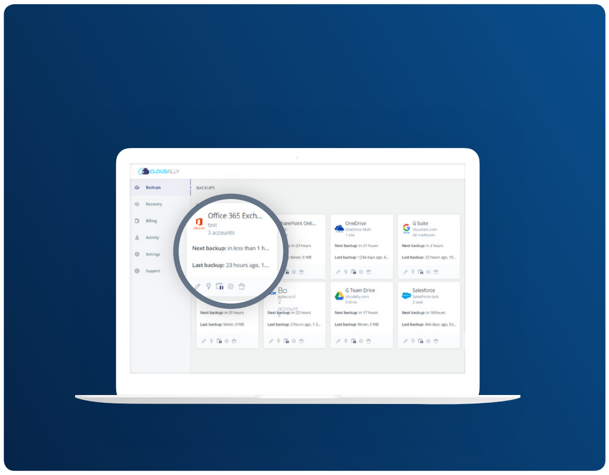
High ROI with Unbeatable Pricing: Custom discounts for bundles, high-volume and multi-year packages. Save on platform license costs with inactive account backup.

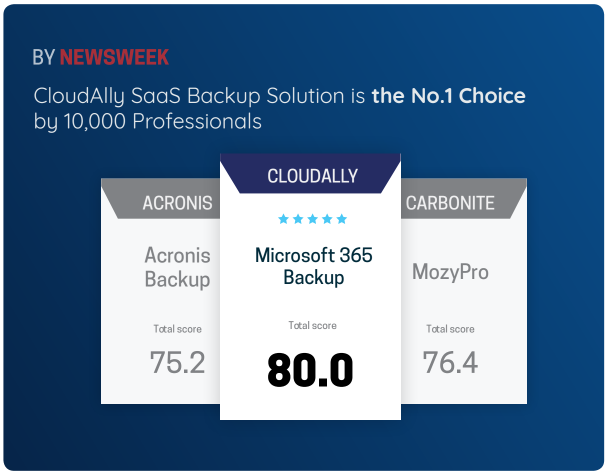
OOTB Setup, Zero Adoption Effort: Seamless integration with all SaaS platforms – Microsoft 365, Google Workspace, Salesforce, Box and Dropbox, intuitive UI with admin-friendly tools.

Flexible Recovery Options to Any Storage with Unlimited Retention: Self-service Point-in-time, granular, and cross-user restore. Non-destructive with unlimited retention. Backup to your own cloud storage.

Secure and Audit-Ready: Global data centers, GDPR, HIPAA and SoX compliant, ISO 27001 certified, MFA/2FA, OAuth and OKTA support, AES-256 data encryption, 99.9% uptime SLA.

Tier 1 – 365x24x7 Real-person Customer Support: Highly-responsive customer service , multi-channel Customer Support Hub.





Conclusion

Monty Sagal
Director of Channel Enablement and Compliance,
CloudAlly

In the 20+ years that I've worked leading cybersecurity and audit teams in various organizations, I have found that increasingly the weakest link is the threat within. The errant employee who clicked on the phishing link, the careless contractor who left the computer unlocked, malware that sneaked in via an infected flash drive, a mistakenly deleted shared file/folder. Reports say that 60% of SaaS breaches are caused by human error[3]. Ponemon Institute noted an increase in the number of insider-caused cybersecurity incidents by a whopping 47% since 2018[4].

But, how do you protect your organization from the threat within? How do you protect your business-critical SaaS data from data loss due to accidental error, malicious intent, outages, and sync errors? By ensuring business continuity and quick disaster recovery. By reducing the Recovery Point Objective (RPO) and Recovery Time Objective (RTO), so your business gets back on its feet ASAP. By blunting the impact of a security breach. All with the safety net of a dependable and secure SaaS backup and recovery solution.

With companies moving to SaaS platforms en masse and with this year witnessing the largest migration to remote work - securing the telecommuting workforce and SaaS data is a top cybersecurity priority. In this ebook we have detailed compelling reasons based on solid data points why SaaS backup is a critical must-have for organizational cybersecurity. And we've also included ways to optimize the ROI from SaaS backup.
We hope you benefit from it...

[3] https://www.infosecurity-magazine.com/news/human-error-linked-to-60-of/
[4] https://www.observeit.com/cost-of-insider-threats/

CLOUDALLY
Secure Cloud Backup

WWW.CLOUDALLY.COM

+1 (424) 304 1959