7 Reasons
Every Business Needs SaaS Backup

Plus, how to maximize its ROI

zix® | appriver®

REASON #1

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

Human error, malicious intent, hackers, malware, sync errors, and natural disasters collectively add up.

SaaS platforms like Microsoft 365, Google Workspace, Salesforce, Box, and Dropbox offer flexibility, scalability, and collaboration. But while they themselves are very secure solutions, your data isn't protected in the same way their infrastructure is. As each of them will tell you if asked (see Reason #3), all of their customers should invest in third-party backup.

One in three companies experiences SaaS data loss

Source: Aberdeen Group

- **Human Error:** If an account is mistakenly deleted, a critical email is erased, or an org-wide shared document is overwritten, it often can't be fixed without a backup and recovery solution.
- **Malicious Intent:** Your SaaS data is also prone to intentional overwrites and deletion by bad actors, disgruntled contractors, or malicious employees.
- **Synchronization Errors:** Syncing or updating multiple SaaS applications—a common scenario in most 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 methods and actors. The damages due to such data breaches are devastating, not only in terms of financial loss, but also reputational damage and a loss of customers.
- **Outages:** Office 365, Google Workforce, Salesforce, Box and Dropbox have high availability, but downtimes and outages are a reality. To prevent work from stopping every time services go down, real-time backup is the only answer.

REASON #2

Data breaches are expensive

They can be a business-killer, especially for medium and small organizations.

The average cost of a data breach is $4.24 million. What is more worrisome, IBM and Ponemon Institute's Cost of a Data Breach 2021 report found that it is a herculean undertaking to recover after such a breach. The time between detection and remediation (known as the breach life cycle) is, on average, 287 days. Which is to say, breaches can cause nearly a year's worth of damage. Half of all mid-sized companies close after a breach, and the latest numbers show the costs are only rising.

The global average cost of a data breach is $4.24 million

Source: IBM and Ponemon Institute's Cost of a DataBreach 2019 Report

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 that the in-application recovery of deleted data is possible—but only within a few weeks or months. Beyond that, it is deleted, and there's often no function for restoring corrupted files. Once the Recycle Bin or Trash folder is emptied, your data is permanently gone and irretrievable. Cloud providers explain this in terms of a "shared responsibility" between you and them for preserving your data, which largely means if the data is sensitive, you are responsible.

Microsoft

> “*We recommend that you regularly backup your content and data that you store on the services or store using third-party apps and services.*”

Google

> “*An administrator can restore a user's Drive or Gmail data for up to 25 days after the data is removed from the user's trash . . . after 25 days, the data cannot be restored, even if you contact technical support.*”

salesforce

> “*We recommend that you use a partner backup solution that can be found on the AppExchange.*”

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

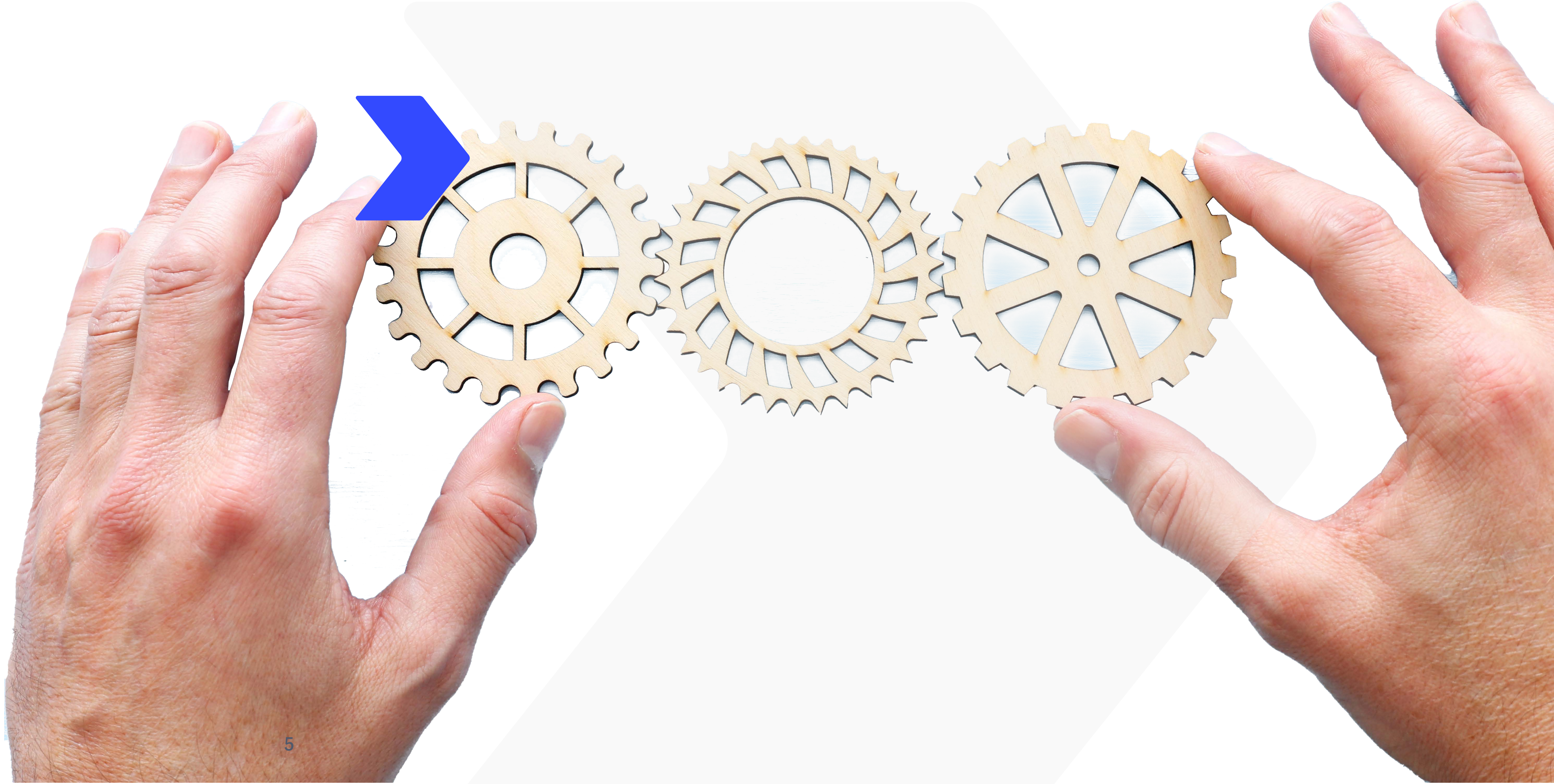
Reliable SaaS backup is a necessary component of compliance

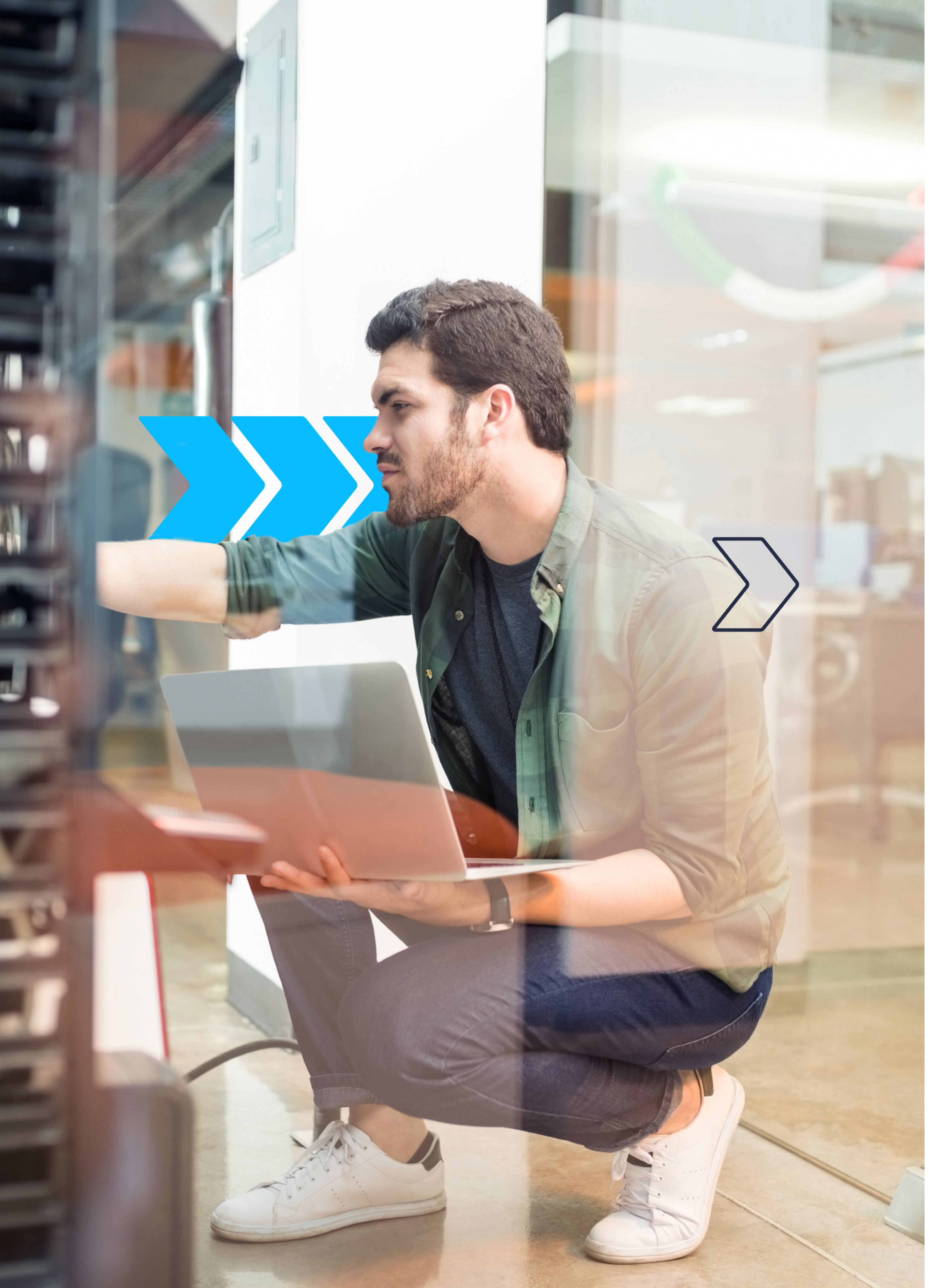
Regulators want you to be in control of your data. Backup is key to satisfying their requirements.

> *"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*

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

Be careful, however: Not just any backup service will do. To comply, 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.





REASON #5

Top IT analysts strongly advise SaaS backup

Backup is a must-have safety net, at a cost every business, large and small, can afford.

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, adding, "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."

> *"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, where available, are often time-bound, cumbersome, and ineffective

‘Recycle Bins’ were not built for true backup and recovery, much less to comply with regulation.

Native solutions are archival in nature and not built for data recovery. This means restoring deleted data is tedious, destructive (changes are overwritten) and incomplete without unlimited backup or cross-user recovery. More importantly, data is only 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 be doing is trying to scrape together what data was preserved by native features like a Recycle Bin or Trash. It can be particularly frustrating when there is an elegant and simple alternative—SaaS backup and recovery.

Native solutions like Litigation Hold, Recycle Bin, and Trash are time-bound, meaning once the time limit is reached, your data is permanently deleted.

REASON #7

Backup blunts the impact of a breach by ensuring business continuity

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

> *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 blame often falls on you—the person responsible for protecting your enterprise's data. Having a solution to reduce the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are, together, the holy grail of 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 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

The best SaaS backup solutions go beyond simple backup and recovery. Enterprise-ready backup can help empower your global workforce, accommodate diverse software or infrastructure, help you comply with stringent data regulatory laws, and offer a better return on investment.

✓ Reduce SaaS platform license costs and ease workforce management

Are you paying for inactive licenses of Office 365 to prevent the account data from being deleted? With Zix you can back up the account data when an employee exits and then perform a 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.

✓ Get comprehensive protection for multi-solution backup

Modern enterprises have complex stacks which could include multiple SaaS solutions. Zix has all your bases covered with comprehensive backup for Office 365, Google Workspace, Salesforce, Box, and Dropbox.

✓ 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. Zix's self-service recovery 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. It's particularly helpful for globally distributed teams.

✓ Maximize your existing storage with BYOS

Zix's 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.

About Zix Cloud-to-Cloud Backup

Zix Cloud-to-Cloud Backup is an important part of Secure Cloud – a full suite of solutions inside a scalable platform to keep your organization's business communications secure and resilient.

In 2020, Zix acquired CloudAlly, and its robust suite of award-winning solutions. This solution has been around since 2011 and was a pioneer in SaaS backup. Consequently, our backup solutions for Microsoft 365, Google Workspace, Salesforce, Dropbox, and Box are tried and tested by organizations with thousands of users. It was also top-rated by Gartner, Capterra, and G2, and was voted as a leading SaaS backup solution by over 10,000 IT professionals in a survey conducted by Newsweek.

✓ **Unlimited Retention and Flexible Recovery Options to Any Storage:**

It's self-service, point-in-time, granular, and allows cross-user restore. The storage is non-destructive with unlimited retention.

✓ **Out-Of-The-Box Setup, Zero Adoption Effort:**

Seamless integration with all SaaS platforms—Microsoft 365, Google Workspace, Salesforce, Box and Dropbox, plus an intuitive UI with administrator-friendly tools.

✓ **Intelligent Workforce Management:**

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

✓ **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.

✓ **24/7/365 Real-Person Customer Support:**

Highly-responsive customer service , multi-channel Customer Support.

Conclusion

Monty Sagal
Director of Channel Enablement and Compliance

In the 20+ years I've worked leading cybersecurity and audit teams in various organizations, I have found that the weakest link is the threat within. The errant employee who clicked on the phishing link, the careless contractor who left the computer unlocked, the flash drive user who didn't know it carried malware, and the end user who mistakenly deleted a shared folder, are collectively, the most destructive. Reports say that 60% of SaaS breaches are caused by human error. Ponemon Institute noted an increase in the number of insider-caused cybersecurity incidents by a whopping 47% since 2018.

But, how do you protect your organization from the threat within? How do you protect your business-critical SaaS data from 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 quickly.

With companies moving to SaaS platforms en masse, and with the sudden migration to hybrid and remote work, securing the telecommuting workforce and SaaS data is a top cybersecurity priority. The question is, will you recognize the need for backup and recovery now, while it can still be helpful, or after it's too late?