SPANNING
A Kaseya COMPANY

THE COMPLETE SaaS BACKUP BUYER'S GUIDE

TABLE OF CONTENTS

INTRODUCTION

Adoption of Software-as-a-Service (SaaS) solutions like Google Workspace, Microsoft 365 and Salesforce continues to increase rapidly as more businesses look to integrate them into their workflows to enhance productivity and collaboration.

ACCORDING TO GARTNER, END-USER SPENDING ON PUBLIC CLOUD SERVICES IS EXPECTED TO REACH $482 BILLION IN 2022 AND WILL EXCEED 45% OF ALL ENTERPRISE IT SPENDING BY 2026. CYBERSECURITY VENTURES FORECASTS TOTAL DATA STORED IN THE CLOUD TO REACH 100 ZETTABYTES BY 2025, OR 50% OF THE WORLD'S DATA TO BE STORED IN THE CLOUD.

SaaS solutions have become a critical part of modern business. The volume of mission-critical data stored in them is growing by the second. However, many organizations still do not back up their SaaS data. This is because they operate with a false belief that backing up SaaS data is not necessary, and that solution providers back up and protect their data. Although SaaS providers are responsible for fixing issues that arise due to inadequacies on their end, they are not responsible for data loss or downtime that occurs due to human mistakes, programmatic errors, insider activities or cyberattacks. The bottom line is that the protection of your data is your responsibility. That's why a more reliable and efficient approach to backup and recovery of your invaluable SaaS data is vital to maximizing uptime and working with confidence in the cloud.

This buyer's guide aims to inform IT decision-makers and professionals like you about the realities of SaaS data protection, what your responsibilities are with respect to SaaS data, why having a dedicated SaaS backup solution is essential for data protection and business continuity, and the key things to consider when evaluating a backup solution.

THE SHARED RESPONSIBILITY MODEL

YOUR ORGANIZATION'S DATA IS THE FUEL THAT DRIVES YOUR BUSINESS, WHICH IS WHY ITS PROTECTION IS PARAMOUNT. HOWEVER, WHEN YOU ADOPT CLOUD SERVICES AND MOVE DATA TO THE CLOUD, WHO IS RESPONSIBLE FOR PROTECTING YOUR SAAS DATA?

Is it you or your cloud service provider?

As you consider migrating to a cloud environment, it is critical to understand that cloud service providers like Google, Microsoft and Salesforce follow the shared responsibility model. In simple terms, the workload responsibilities are shared between the service provider and the customer. It is important that you understand which aspects of data protection are applicable to your organization and which operational burdens are handled by your service provider.

In a shared responsibility model, the customer is the "data controller" while the vendor is considered the "processor" of that data. As a controller, you retain control over your data, including the users within the environment. That means you determine how data is managed, accessed and utilized. The processor, on the other hand, processes such data as instructed by the controller — adding, deleting or modifying data upon any request submitted by authorized credentials. Even if a request is the result of malicious activity or an accident, if that request is authenticated by valid credentials, the processor will consider the request legitimate and execute it. As a result, accidental, malicious or fraudulent deletions, in all cases, are the responsibility of the customer/controller.

Cost of non-compliance

Today, organizations hold large volumes of sensitive business and customer information. With industry regulations like the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA) and the California Consumer Privacy Act (CCPA) getting tighter and more complex, businesses can no longer afford to ignore data protection. In fact, compliance standards, such as HIPAA and GDPR, place 100% of the fault of a SaaS-based compliance violation on the "controller" (customer). Failure to meet regulatory requirements can be detrimental to your business. For example, non-compliance with GDPR can attract administrative fines of up to 20 million EUR, or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Apart from regulatory fines, your company may also incur legal fees and recertification costs.

While most headlines about GDPR fines involve major corporate entities, GDPR applies to small businesses as well.

Here are some real-world examples of GDPR fines and penalties issued by various European Union regulators to small and midsize businesses.

ELDON INSURANCE SERVICES LIMITED

The Information Commissioner's Office (ICO) imposed a fine of £60,000 on Eldon Insurance Services Limited for sending unsolicited direct marketing emails without consent.

LIFESTYLE MARKETING, MOTHER & BABY LTD.

The ICO issued a monetary penalty of £140,000 to Lifestyle Marketing, Mother & Baby Ltd. for selling the personal data of more than one million subscribers without their consent.

TUSLA

The Ireland-based child and family agency was fined £75,000 for wrongly disclosing information about children to unauthorized parties.

RISKS TO YOUR SAAS DATA

SaaS solutions provide numerous benefits that make them a viable option for businesses large and small. However, data security is not one of them. As per the shared responsibility model, the vendor is responsible for application uptime and availability, including the integrity of the data center — security, infrastructure and operations — to ensure the performance of its service. As such, most major cloud service vendors provide a financially guaranteed SLA for 99.9% application uptime. However, customers are responsible for application data, account, administration and user management. They are operationally and contractually responsible for the security of their user credentials and the protection of their data.

Data loss is not uncommon in the SaaS world. About 40% of users reported losing their data stored in SaaS applications in 2021.

Listed below are some top causes of SaaS data loss.

01

HUMAN ERROR

It goes without saying that humans make mistakes. Accidental deletion of files, configuration errors due to inexperience and overwriting information are some common mistakes made by users. Deletion is the leading cause of SaaS data loss, whether accidental (20%), external and malicious (19%), or internal and malicious (6%). Unfortunately, human error has been a major contributing factor behind many data breaches as well. According to Verizon's 2022 Data Breach Investigations Report, more than 80% of breaches involved the human element.

02

SECURITY MISCONFIGURATIONS

Misconfigured or inappropriately configured security controls can put your systems and data at risk, leading to data breaches. Threat actors can exploit misconfigurations in servers, applications, network devices and so on, to gain access to sensitive information or launch cyberattacks.

03

MALICIOUS INSIDER ACTIVITY

The Verizon 2021 Data Breach Investigations Report revealed that more than 20% of security incidents involved insiders. Insider threats are far more dangerous than external threats since they are well aware of your organization's security check gates, defense mechanisms and vulnerabilities, and have legitimate access to your business' critical data and systems.

04

MALICIOUS OUTSIDER ACTIVITY

Businesses witnessed 50% more attacks per week in 2021 compared to 2020. CISCO's 2021 Cybersecurity Threat Trends report revealed about 90% of data breaches occur due to phishing. Phishing is also the gateway to many types of destructive cyberattacks including ransomware, malware, business email compromise (BEC) and credential compromise.

05

VIRUSES, MALWARE AND RANSOMWARE

New variants of viruses and malware appear every day that increase the risk of data loss. Around 300,000 new pieces of malware are created daily to target individuals and organizations. Viruses and malware can cause serious trouble since an infection on a single machine can quickly spread to other systems, ultimately taking down the entire IT system.

BEST PRACTICES FOR PROTECTING DATA IN ANY SAAS APPLICATION

Data loss and downtime do not have a place in today's 24/7/365 business environment. They could result in business disruption, customer outrage, financial losses, non-compliance, lawsuits and more. That is why SaaS backup should be a cornerstone of your data protection plan. A SaaS backup solution is vital to ensure your organization generates, manages and protects your valuable data responsibly and reliably.

Here are the top six best practices for SaaS data backup:

01

DETERMINE YOUR RECOVERY OBJECTIVES

To better protect your SaaS data, you must evaluate the risk of data loss and create a business continuity plan that aligns with your company's Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs).

- **Recovery Point Objective:** RPO can be thought of as the time between the time of data loss and the last useful backup of a known good state.
- **Recovery Time Objective:** RTO is the maximum acceptable length of time required for an organization to recover lost data and get back up and running.

02

KEEP MULTIPLE COPIES OF DATA IN THE CLOUD

Keep copies of your SaaS data in a separate, secure cloud structure that ensures the integrity of data even if something happens in the original cloud server. Most cloud vendors like Google, Microsoft or Salesforce, have extremely high standards for security and redundancy. However, data loss is inevitable and can happen to anyone. Therefore, it is a good practice to copy your information into another cloud infrastructure to ensure the safety and availability of your data.

04

OPTIMIZE BACKUP SCHEDULE AND FREQUENCY

They say your business is only as good as your last saved backup. It is critical for your backups to be up to date to quickly resume business operations after a disruption. Taking backups regularly will help reduce the risk of losing your critical data and maintain business continuity even in the face of a disaster.

03

BACK UP METADATA TOO

Metadata contains vital information about sharing settings, labels, tags and ownership that enables seamless collaboration and greater control. This information allows end users and IT administrators to easily find and use data.

05

ENSURE BACKUPS ARE ENCRYPTED

Add an additional layer of security to your backups by encrypting them. SaaS backup solution providers like Spanning protect your Google Workspace, Microsoft 365 and Salesforce data with 256-bit AES object-level encryption, with unique, randomly generated encryption keys for every single object and a rotating master key protecting the unique keys. Additionally, Transport Layer Security (TLS) encryption is used to protect all data in transit.

06

TEST BACKUP AND RECOVERY PROCESSES REGULARLY

The best way to know if your backups are occurring properly and can be restored if the need arises is by regularly testing your backup and recovery processes. Testing data backup and recovery systems is critical to having a good understanding of their accuracy, efficiency and effectiveness. By having proper testing mechanisms and procedures in place, your company can rest easy knowing that your data recovery strategies will work as planned in times of need.

BUSINESS CONTINUITY BEST PRACTICES FOR SAAS APPLICATIONS

Disasters in SaaS applications can occur when you least expect them. From accidental, malicious or fraudulent deletions to other threat vectors, a data loss or a security incident could disrupt business operations and bring your company to a standstill.

Listed below are a few business continuity best practices that will help improve your organization's preparedness in the event the unexpected does occur.

IMPLEMENT MULTIFACTOR AUTHENTICATION

Implementing multifactor authentication is the single most important action you can take to protect the integrity of your data. Security experts across the board recommend multifactor authentication (MFA) or two-factor authentication (2FA) to prevent unauthorized access to user accounts. It provides two layers of authentication – a password and an additional verifiable factor, like a one-time password (OTP) sent via SMS, or a biometric check like a scan of the fingerprint or retina. The best part is its dual advantage. On one hand, it prevents account takeover (ATO) attacks, and on the other, it keeps the user experience intact by not being too intrusive or demanding too much from users.

PROTECT ACCOUNTS AND CREDENTIALS AGAINST PHISHING

Phishing represents the most effective way for threat actors to compromise login credentials and accounts. We live in a world of single sign-on where email credentials are often used to access multiple accounts. When you consider that more than 50% of people use the use the same password for work and personal accounts, you need to be mindful of sophisticated phishing attacks like spear-phishing. Hackers target a specific individual in an organization to steal data or install malware. They then use the compromised account as a springboard into other email accounts and applications. Since more than 90% of cyberattacks infiltrate an organization via email, using an email phishing prevention solution should be a top consideration.

DEVELOP A DLP POLICY

Data loss prevention (DLP) uses rules and policies to determine which files and data are considered confidential, critical or sensitive, and are protected from being shared or transmitted inadvertently. The goal of applying these rules, policies and protective measures is to prevent data loss and misuse.

CREATE AND MANAGE DATA RETENTION POLICIES

Managing retention enables you to comply proactively with industry regulations and internal policies. This reduces risk in the event of litigation or a security breach and improves knowledge sharing by ensuring you are only maintaining current and relevant information.

CONTINUAL COMMUNICATION, EDUCATION AND TRAINING

Often, data protection tools and technologies are implemented with no communication of why they are needed or how to use them, leading to poor user adoption or Shadow IT. Business continuity and disaster recovery (BCDR) plans are developed, documented and tested once by IT folks and then filed away forever. After all, out of sight is out of mind. The best defense against data loss is user enablement. A data loss prevention strategy is only truly effective when users are aware, educated and know exactly what to do in case of a data loss event.

IMPLEMENT A DARK WEB MONITORING SOLUTION

MFA is a must, but it isn't perfect. Sophisticated hackers have developed methods to bypass second and third-layer security protections like MFA if users are not careful. For instance, Pioneer Kitten targeted Iranian dissidents by deploying malware in the victim's Telegram messaging app, whose MFA was bypassed using previously intercepted SMS codes. Implement a dark web monitoring solution along with MFA to identify potentially compromised accounts before malicious action takes place.

USE A BACKUP SOLUTION

The harsh truth is, SaaS data loss is virtually inevitable. You need a reliable SaaS backup solution with fast, easy, granular and point-in-time data restoration functionality that can help you seamlessly recover your precious data if the need arises. Look for a backup solution that provides easy installation, automated backups and end-user enablement.

BEST PRACTICES FOR MICROSOFT 365

Although Microsoft may have one of the best security infrastructures in place, a major disaster can still occur due to human error, illegitimate deletion, programmatic errors, malicious insiders, hackers, malware or ransomware.

Listed below are some best practices to better protect your Microsoft 365 data.

MANAGE CONSENT TO APPLICATIONS

Allow user consent only for applications that have been published by a verified publisher. This protects you from consent phishing wherein sensitive data is accessed, not by stealing your password but by tricking you into giving malicious apps the necessary permission to access your Microsoft 365 data.

LEVERAGE MICROSOFT'S NATIVE TOOLS

Microsoft provides several tools for organizations to monitor Microsoft 365 activity. Your business can utilize these tools to examine potential security risks, track user behavior, understand how users create and share content and more.

MANAGE ACCESS

Use Microsoft Cloud Access Security to improve access management, revoke access to those who no longer need it, or if their roles have changed. People who should not have access to sensitive data, but do, greatly increase the attack surface. If your organization uses more cloud applications than just Microsoft 365, you may want to invest in a third-party cloud access security broker (CASB) to extend control to third-party apps and API connections.

USE A MICROSOFT 365 BACKUP SOLUTION

The state-of-the-art security infrastructure and processes make Microsoft data centers virtually impossible to breach directly. However, the architectural and functional aspects of Microsoft 365 make your tenant vulnerable to compromise and data loss due to human mistakes, programmatic errors, malicious insider activity, phishing and malware attacks. You need a robust Microsoft 365 backup solution to improve the security of your tenant and quickly recover your precious business data stored in Exchange Online, SharePoint Online, OneDrive and Teams, in case of an emergency.

HERE IS A MICROSOFT 365 EVALUATION CRITERIA CHECKLIST THAT WILL HELP YOU FIND THE BEST BACKUP SOLUTION FOR YOUR BUSINESS.

BEST PRACTICES FOR GOOGLE WORKSPACE

Google's data centers are designed to protect data from infrastructure threats. However, even Google cannot protect customers from the most common causes of data loss: ransomware and malware attacks, user error, malicious behavior and sync or configuration errors.

Here are some key steps you can take to improve your Google Workspace data security.

ENABLE MALWARE PROTECTION

Malware (including ransomware) delivered through email is the most common (and generally the least sophisticated) threat to your domain. Gmail provides AI-enhanced spam-filtering for all users that automatically scans for viruses whenever an email is received or sent out of your Gmail account.

ENABLE PHISHING PROTECTION

Phishing represents the most effective way for threat actors to compromise Google Workspace credentials and accounts. Google provides advanced email security functionality, including the highly secure Advanced Protection Program, to all Gmail users.

IMPLEMENT MULTIFACTOR AUTHENTICATION

Google provides basic and advanced methods of authentication, including the option to use security keys to all customers. The 2-Step Verification adds an extra layer of security to your business data. You can access your Google account only by completing the two levels of authentication — first, your password, and second, by verifying using either your phone or a security key.

CREATE AND APPLY DLP FOR DRIVE

Data loss prevention (DLP) for Drive allows you to create and apply rules to control the information that your users can share in Google Drive files outside the organization. This helps in preventing unintended exposure of your organization's sensitive data.

BACKUP YOUR GOOGLE WORKSPACE DATA

Protecting your organization's Google Workspace data from accidental deletion, malicious behavior and synchronization errors, is vitally important to ensuring business continuity. Even more important is your ability to restore lost data and to trust in the solution and provider to deliver results when you need them the most. While Google provides some native functionality to help customers protect their domains from these threats, there are significant gaps that need to be addressed. Look for an efficient backup solution that is purpose-built for Google Workspace. You solution must enable rapid restore for all your critical Gmail, Drive (including Team Drives), Calendars, Contacts and Sites, in the event of a disaster.

CHECK OUT OUR GOOGLE WORKSPACE EVALUATION CRITERIA CHECKLIST TO FIND THE RIGHT BACKUP SOLUTION THAT MEETS YOUR ORGANIZATIONAL NEEDS.

BEST PRACTICES FOR SALESFORCE

Salesforce data centers are equipped with world-class disaster recovery capabilities to protect data from just about any infrastructure threat. However, you, not the vendors, are responsible for the most common causes of data loss — accidental deletions, insider threats and cyberattacks, to name a few.

Follow these steps to effectively secure your Salesforce org.

USE THE SALESFORCE HEALTH CHECK TOOL

Administrators can use the Health Check tool to conduct a security health check to identify and fix potential vulnerabilities in your Salesforce org. The Health Check tool provides a holistic view of your org's security settings and allows you to assess your security settings for vulnerabilities and misconfigurations. This helps reduce risk and improve overall security of your Salesforce org.

SET IP RANGE RESTRICTIONS

In Salesforce, admins can restrict users to access your Salesforce org instance only from allowed IP addresses, using IP range restrictions. Once administrators specify the range of valid IP address restrictions for a profile, users won't be able to log in from any other IT address apart from the ones defined. Restricting administrative access helps minimize the risk of unauthorized access in the event of account compromise.

USE SALESFORCE BACKUP AND RESTORE

Salesforce launched Backup and Restore (earlier Data Recovery Service) in September 2021. Backup and restore is a paid add-on service offered by Salesforce to help customers back up and recover their lost data. This can be useful if you do not have an alternative backup strategy. That being said, Salesforce encourages its customers to explore the Salesforce AppExchange if they are looking for a backup solution that provides more capabilities than the Weekly Data Export and Data Recovery Service.

USE A THIRD-PARTY BACKUP SOLUTION

While Salesforce Backup and Restore enables automated daily backups, you may want to make your backups occur more frequently. With a third-party backup solution, you will have the option to create recovery points for backups to occur on a more frequent basis. Salesforce replicates data for application availability and disaster recovery. However, the SaaS platform does not provide customers with backup data designed for restoration. Additionally, while Salesforce offers native backup and recovery options, they recommend you use third-party backup solutions because native options, like weekly export and recycle bin restore, are manual, time-consuming and do not guarantee full data recovery.

Salesforce administrators need a robust backup solution to ensure availability and performance. They need a reliable solution that will enable them to maximize productivity and make the best use of budget and resources.

USE OUR SALESFORCE EVALUATION CRITERIA CHECKLIST TO DISCOVER THE BACKUP SOLUTION THAT CAN HELP MEET YOUR DATA PROTECTION GOALS.

END-TO-END SAAS DATA PROTECTION

Spanning provides fast, affordable and reliable SaaS backup and recovery solutions for Microsoft 365, Google Workspace and Salesforce. Spanning backup solutions are powerful, yet easy to set up, manage and use, enabling administrators as well as users to restore data and quickly get back to work with minimal or no disruption.

Spanning 360 is the industry's only enterprise-class, end-to-end protection solution for Google Workspace and Microsoft 365. The solution is fully automated with an intuitive user interface, featuring advanced capabilities that prevents, anticipates and mitigates account compromise and data loss.

SPANNING 360 ENABLES YOU TO:

Prevent

Detect and block even the most sophisticated email threats.

Anticipate

Secure accounts at risk before a data loss incident.

Mitigate

Quickly find and restore data to its original state with just a few clicks.

DISCOVER HOW SPANNING PROVIDES COMPREHENSIVE SaaS DATA PROTECTION.

GET STARTED TODAY!

SPANNING
A Kaseya COMPANY

Spanning Cloud Apps, a Kaseya company, is the leading provider of backup and recovery for SaaS applications, helping organizations around the globe protect their information in the cloud. The company provides powerful, enterprise-class data protection for Microsoft Office 365, G Suite, and Salesforce. With data centers located in North America, the EU, and Australia, Spanning Backup is the most trusted cloud-to-cloud backup solution for thousands of companies and millions of users around the world.

START A FREE 14-DAY TRIAL AT
SPANNING.COM/START-FREE-TRIAL

@SPANNINGBACKUP
FOLLOW US ON LINKEDIN
FOLLOW US ON GOOGLE+
READ OUR BLOG

WWW.SPANNING.COM

+1 (512) 236-1277