SpinOne

SaaS Data Protection Guide

- Data protection
- Compliance
- Threat prevention

Never before has data been under so much scrutiny from a regulatory perspective and in danger from security concerns and threats.

SpinOne

Contents

01

BUSINESS DATA PROTECTION CHALLENGES

SaaS Data Protection Guide

Data Protection, Compliance, and Threat Prevention – the Three-Fold Challenge for Business

Data is the new “gold” of businesses today. Everything is driven from collected data. Data is being stored in massive quantities and is being used for all kinds of purposes to further business interests and to make the customer experience more customized and tailored than ever before. However, **never before has data been under so much scrutiny from a regulatory perspective and in danger from security concerns and threats**.

Businesses today must meet the three-fold challenge of data protection, compliance, and threat prevention in order to be successful at using data in a way that is acceptable, useful, and secure.

02

KEY TAKEAWAYS

1. Don't rely on SaaS vendors for cloud data protection
2. Ensure data security to meet compliance standards
3. Employ prevention methods to stop security threats

Don't Rely on SaaS Vendors for Cloud Data Protection

There are often misconceptions about what responsibility the public cloud provider has towards data and what protections they offer.

"Every SaaS provider explicitly calls out that clients are responsible for protecting their own data. You must plan data protection for every new SaaS service to which you subscribe. It's not practical for you to custom develop adaptors/connectors that protect SaaS application data. You must engage with cloud-to-cloud backup providers, as they can leverage their experience to add support for new services quickly."

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

Ensure Data Security to Meet Compliance Standards

Most if not all organizations doing business today fall under some type of compliance regulation(s). Just in 2018, the General Data Protection Regulation or GDPR compliance regulation was introduced. GDPR makes it much more important for businesses doing business in or handling EU citizen's data to protect this data. GDPR has "real teeth" in terms of the penalties that can be levied against organizations found in breach of the new regulatory guidelines. This includes penalties up to 4% of annual turnover or 20 million euros, whichever is higher. This is no small penalty to be in breach of regulation!

GDPR, PCI, HIPAA, and other compliance regulations make it imperative that businesses make compliance an important part of the initial planning stages of new infrastructure including public cloud. One of the key aspects of GDPR compliance is “security by design”. Security as part of GDPR can no longer be an “afterthought”. It must be a primary consideration when building out IT infrastructure, processes, and services today.

Despite the penalties that can be levied against businesses in breach of compliance regulations, the end result is better security and a more focused approach to protecting customer data which is a good thing and a goal that all businesses today should and must strive for.

Hybrid infrastructure is making it more difficult for businesses to meet up with compliance regulations as public cloud tooling, processes, and required services such as backups are often missing from the solution. This creates gaps in the ability of businesses to effectively meet compliance goals.

Employ Prevention Methods to Stop Security Threats

Every week it seems there is a notable or high-profile breach in security or ransomware attack. There is no end to attack vectors or threat actors looking to compromise data. The number of threats and those looking to steal, compromise, or destroy data is not going away any time soon. Businesses today must be vigilant about security. A huge part of security vigilance is **threat protection**. Effective threat protection means organizations today go on the offensive and are **proactive** about security.

Hybrid cloud infrastructure that spans both on-premises and public cloud environments makes it more of a challenge for organizations to have the visibility and tools needed to properly manage, maintain, and secure their environments. Often, small to mid-sized businesses are in the sights of attackers due to fewer resources both financially and in terms of technology and personnel to ward off attacks. A recent study by healthsecurity.com found that 71% of ransomware attacks targeted small businesses for this reason. Threat protection is a key area of securing today’s technology infrastructures since it means organizations are proactively looking for threats and remediating them.

03

HOW TO MEET SECURITY CHALLENGES

Time and again, it is found that data breaches, leaks, and other security compromises such as ransomware attacks involve neglecting the basic security principles required to properly secure environments. Often, if best practice guidelines are implemented, security threats can be effectively neutralized before any real harm results.

Let’s look at a few basic best practice guidelines in the areas of data protection, compliance, and threat protection and see how these are important to the overall security posture of organizations today.

BACKUP RULE

Follow 3-2-1 backup rule

There is a key role in data protection called the 3-2-1 backup rule that serves as a best practice for protecting business-critical data. This best practice states you need to have (3) copies of your backups stored on (2) different mediums, with at least (1) stored offsite. The overall benefit of the 3-2-1 backup rule is you have multiple copies of your data and those copies are separated from one another in an intentional fashion.

This methodology is a little easier to get “hands around” on-premises since on-premises environments are controlled, provisioned, managed, and backed up in one’s own data center with chosen tools and solutions. However, with public cloud infrastructure, the 3-2-1 backup rule is often a much more difficult process for organizations to get a handle on compared to on-premises environments.

BACKUP STORAGE

Store cloud data backups separately from production data

Backups of public cloud data need to stored separately from the production environment as outlined in the 3-2-1 best practice methodology. Many public cloud SaaS backup solutions require businesses to store data in the same infrastructure that houses production data. However, businesses need a service that allows storing backup data in separate infrastructure than production to ensure completely autonomous data backups that can be restored or downloaded without any reliance on the production SaaS infrastructure.

LONG-TERM BACKUPS

Make long-term archived backups

Keeping multiple, versioned copies of data is a core requirement of data backups. Data backups usually fall into two categories – hot backups that are used for data recovery and archived backups used for long-term data inquiries.
Having the ability to store long-term backups for a designated period of time allows the ability to retain archival data. Archived backups serve the purpose of being able to restore or review information needed for data inquiries and other historic data purposes. Organizations using a backup solution of public cloud data services need to be able to satisfy both of these backup requirements to satisfy best practice guidelines.

DATA SHARING

Monitor sharing of data inside and outside SaaS environments

SaaS environments such as Office 365 and G Suite allow sharing access to users who are outside the environment. This can create tremendous security and compliance challenges. Organizations must monitor access to files and data shared outside the organization to be able to effectively meet compliance regulations. Otherwise, there will always be questions about what data is shared, accessed, and potentially in violation of compliance regulations. Again, this requires effective tools to monitor and manage sharing across the SaaS landscape.

DATA MONITORING TOOLS

Use tools to monitor data inventory

One of the most difficult things to do in public cloud environments is to monitor data inventory. While there are many tools found within the public cloud Saas environment, often, these can be cumbersome to use, have separate logins and dashboards aside from the SaaS environment and each produce information difficult to aggregate or correlate across the different tools and utilities.

To add to the complexity, public cloud SaaS environments can be vast, with thousands of users and various permission levels. Users can be coming from multiple sanctioned locations or even the public Internet when accessing business-critical data. Many businesses struggle with monitoring access to files and having the ability to effectively audit access to these resources. If this cannot be done with native tooling, businesses must use third-party solutions to be able to effectively gather and consume the data needed to keep in line with compliance best practices.

ARTIFICIAL INTELLIGENCE

Leverage Artificial Intelligence to monitor SaaS data

The complexity and the sheer enormity of data housed in SaaS are simply too much for a human to manage and monitor in terms of security and compliance. Organizations looking to successfully conquer the security and compliance challenges of both today and tomorrow must use artificial intelligence. AI tools can correlate, aggregate, and parse data exponentially faster, more powerfully, and 24x7x365, unlike an actual person performing the same tasks. These types of AI-enabled tools are going to be required to stay on top of complex and challenging security and compliance obstacles in hybrid environments.

DATA ENCRYPTION

Encrypt data in-flight and at-rest

Encryption is a key technology in the world of security and compliance. Businesses must make data unreadable to any unauthorized individual both as it is transmitted over the network and as it is stored. This underscores the need to encrypt data in-flight and at-rest. Encryption of data makes it unreadable to anyone without the key to decrypt the data.

To keep with compliance and security objectives to protect business-critical and customer data, encryption is a crucial basic necessity. Clear text and unencrypted data make data leakage a very real possibility. Even if other mechanisms fail to prevent leaking data outside cloud environments, encryption helps to ensure any leaked data is unreadable.

ACCESS MANAGEMENT

Use identity and access management

Proving a user's identity is one of the basic requirements of keeping an environment secure and in compliance with regulatory requirements. Even though the concept of identity is easy to understand, putting it into practice in a secure way is more difficult that might seem to be the case. Typically, establishing identity is accomplished by using some type of credentials. The most basic way this is carried out is by using a username and password. However, organizations are finding the traditional username and password to be less than effective when it comes to securing environments and their data. Weak passwords and lack of two-factor authentication leads to accounts easily being cracked. This leads to more modern approaches being needed to establish identity.

The other component of allowing access to data resources is **access management** and involves linking permissions with a set of credentials. A best practice methodology with identity and access management is assigning only the absolute least amount of privileges needed to perform a specific job role. This least-privilege access methodology helps to ensure a user does not have more access than needed. Additionally, it helps to contain any security fallout of compromised user credentials.

This concept of identity and access management is a fundamental requirement of securing and keeping with modern compliance regulations.

06

MAKE THE BEST CHOICE

When it comes to data protection, compliance, and threat protection, these tasks can be extremely difficult to achieve in public cloud Software-as-a-Service environments such as Office 365 and G Suite. As has already been mentioned, public cloud environments are often “black boxes” with data access being difficult to monitor, control, and secure correctly. Additionally, there are no native backup mechanisms in place with Office 365 and G Suite environments. This is a tremendous problem for organizations looking to migrate or already migrating business-critical services and data to public cloud SaaS environments.

As outlined in GDPR requirements, security by design must be implemented from the outset and not simply be an afterthought to modern SaaS implementations. This requires that organizations properly engineer data protection, compliance, and threat protection mechanisms to uphold the security by design methodology. Ideally, businesses need to be able to monitor, manage, and configure data protection, compliance, and threat protection mechanisms using a single pane of glass.

SpinOne – Next Generation Data Protection, Compliance, and Threat Prevention Technology

SpinOne uses artificial intelligence technologies to “learn” the SaaS environment and profile what is normal. This way our system can recognize the unusual or potentially threatening activity. Having powerful machine learning algorithms working at securing SaaS environments is like having an intelligent sentry guarding the environment 24x7x365.

We provide a one-stop solution for businesses looking to solve data protection, compliance, and threat protection challenges in either Office 365 or G Suite public cloud SaaS environments. Learn more about our offerings:

1. **SpinSecurity to protect from ransomware →**
2. **SpinAudit to assess the risks of third-party SaaS apps and Chrome extensions →**
3. **SpinBackup to securely back up cloud data →**

SpinOne

ABOUT SPINONE

SpinOne is a multi-tenant platform created by Spin Technology and designed to simplify the complexity of cloud data security. As an all-in-one platform, SpinOne combines three solutions that make business data bulletproof from the security breach and insider threats: SpinSecurity, SpinAudit, and SpinBackup.

SpinOne is trusted by over 1,500 organizations worldwide including HubSpot, Vopak, IBT Industrial Solutions. We have more than 1,200,000 business users in more than 100 countries.

Try SpinOne Free →

Spin Technology Inc

2100 Geng Rd Suite 210

Palo Alto, CA 94303, USA

USA and Canada Toll Free:

+1-888-883-2993
(9am to 5pm PST)

EU, CIS and Asia:

+48-22-602-2440
(7am to 4pm GMT)