




The State of SaaS Data Protection in 2024



New research exploring cyber threats to SaaS apps — and how leaders can protect their businesses

Businesses around the world have embraced Software-as-a-Service (SaaS) applications for a variety of business-critical workflows. The average small- to medium-sized organization relies on more than 200+ SaaS applications and industry analysts predict that SaaS adoption will continue to grow.

As businesses become increasingly reliant on SaaS solutions, it is critical to consider how vulnerable they are to cyber threats—and how resilient their processes are if this software were to fail or be breached. To explore this topic, HYCU conducted primary research among hundreds of decision makers from around the world. The results underscore some critical gaps in the way most organizations protect their data.



Key Takeaways

SaaS applications are a major vector for cyberattacks

More than a third of survey respondents reported being victims of ransomware attacks—and SaaS applications were the source of attack for the majority (61%) of breaches. When applications are hit, 90% of businesses report they cannot recover encrypted SaaS data within an hour, creating costly downtime and business disruption.

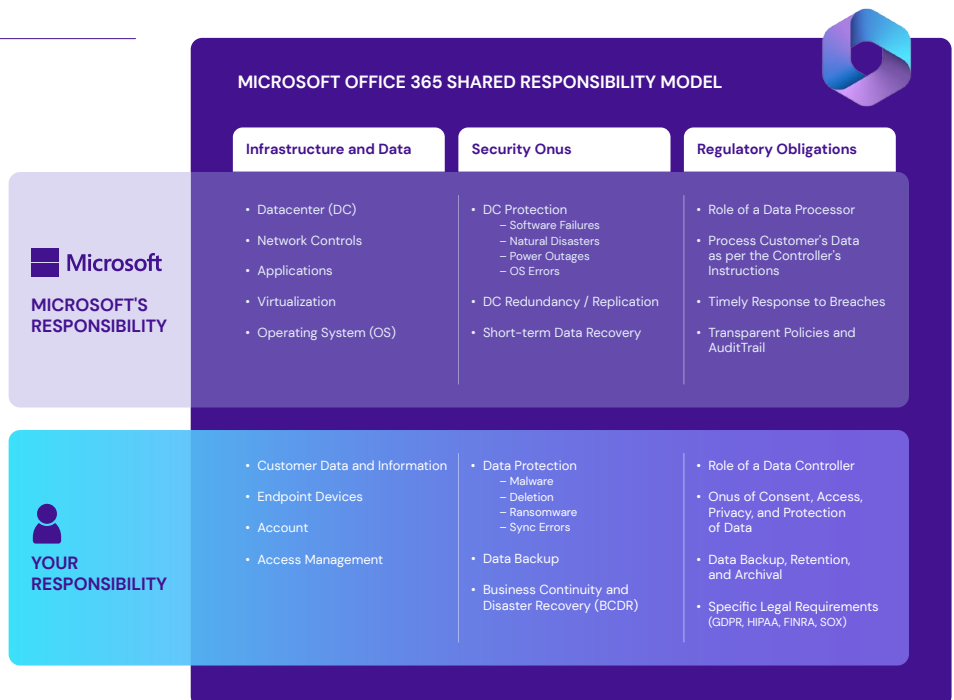


61%
of breaches have SaaS applications as the source of attack.

Business leaders may be unaware of the true scope of their SaaS estates

Survey respondents reported that their businesses, on average, use 22 SaaS applications—yet the average small-to medium-sized business uses ten times that number. This disconnect suggests that businesses are not aware of what they need to protect and, therefore, are not adequately prepared to protect the solutions that lines of business increasingly rely on.

In the Microsoft 365 shared responsibility model, the **customer is responsible for safeguarding their data** regardless of deployment option.



Single Sign-On (SSO) and Identity and Access Management (IAM) solutions need protection

Intended to enable secure access to SaaS applications, SSO and IAM solutions present critical single points of potential failure if attacked. Three quarters of survey respondents said their businesses would be meaningfully impacted if their Active Directory, SSO and IAM data were to suddenly become unavailable. The ability to safeguard this data is a crucial consideration for an effective data protection strategy.

The shared responsibility model can leave critical data unprotected

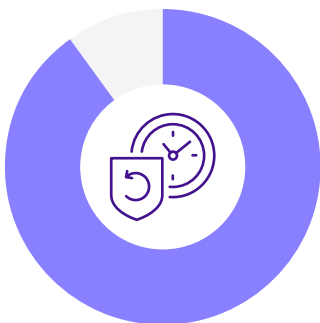
A large percentage of survey respondents said they rely on the SaaS provider to ensure their data is backed up. Yet this may leave them vulnerable in the event the provider goes down. That's because many cloud providers adopt a "shared responsibility" model. This generally means that vendors accept responsibility for things like the security, availability, and support of their infrastructure, while the customer assumes responsibility for data protection and recovery.

Business leaders should carefully review Service Level Agreements (SLAs) to ensure they clearly understand each party's responsibilities. While vendors may provide some backup features, ultimately the responsibility to recover data likely falls on the customer's shoulders.



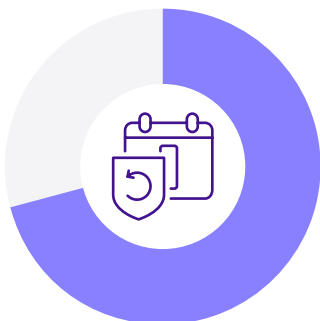
43%

of respondents lack staff with the skills to implement additional security processes.



90%

of the businesses surveyed reported that they could not recover encrypted SaaS data within an hour.



71%

of the businesses surveyed said they could recover data in less than a day.

Clear view of the challenges when it comes to recovering critical SaaS data?



6%

of senior managers report their businesses can recover data within an hour

VS



14%

of owners report their businesses can recover data within an hour

Many businesses lack the right people and processes for protecting SaaS application data

A majority of survey respondents reported that implementing additional security process is the main challenge with SaaS data protection. In addition, 43% of respondents said they lack staff with the skills to do so. As a consequence, less than half of businesses surveyed have implemented incident and disaster recovery plans for SaaS data, as well as reporting on SaaS protection for regulatory purposes. In many cases, businesses have implemented these measures only after they have been victims of a ransomware attack.

Slow speed of SaaS data recovery is a common problem

For businesses that do have procedures in place for backing up SaaS data, the speed of recovery is often poor. Of the businesses surveyed, 90% reported that they could not recover encrypted SaaS data within an hour. While 71% said they could recover data in less than a day, this downtime still represents a major business disruption.

Business leaders may not fully grasp the risk. While 6% of senior managers report their businesses can recover data within an hour, 14% of owners report that this is the case. This may signal that owners and senior leaders who are further removed from day-to-day operations may not have a clear view of the challenges their teams face when it comes to recovering critical SaaS data.

Leaders should be more involved in disaster recovery planning

This means assessing what would happen in a worst case scenario and how to respond to minimize the cost to the business. This includes conducting a business impact analysis to determine how much data their business can afford to lose (known as a Recovery Point Objective) and how much time they can tolerate without access to key applications (known as Recovery Time Objective).



Conclusion: How leaders can protect their businesses

Growth in SaaS usage shows no signs of slowing down. For businesses to operate successfully and minimize their vulnerability to attacks, they need effective solutions for protecting their data used by cloud-based platforms.

To meet today's SaaS data protection challenge, they must be able to:

- ✓ Successfully identify the true scope of their SaaS usage, including those tools that may fall under the label of "shadow IT."
- ✓ Navigate the modern shared responsibilities model so that they know exactly what they can and cannot expect from SaaS providers.
- ✓ Plan and implement disaster recovery procedures and policies that account for worst case scenarios and give regulators the overview they need to remain compliant as new requirements emerge around the world.
- ✓ Back up and restore data as rapidly as possible—nearly instantly—to avoid business disruption.

To achieve this final and most critical goal, leading organizations around the world are turning a pragmatic, proven solution for SaaS data protection:



HYCU provides storage-agnostic backup and recovery for commonly used SaaS platforms and applications, including:

- Salesforce
- Docusign
- GitHub
- Asana
- Miro
- Clickup
- ServiceNow
- Snowflake
- Microsoft
- Google
- Atlassian
- and over 70+ more

HYCU simplifies data protection while providing equivalent levels of backup and recovery support and simplicity across on premise, public cloud, and SaaS workloads.

For business leaders who recognize the realities of this new landscape and act decisively to protect their data, SaaS usage can be as safe as it is productive.