HYCU®

The HYCU State of SaaS Resilience Report **2025**

As SaaS adoption accelerates, is data resilience getting left behind?

Table of Contents

Executive Summary

With SaaS Risk Rising, Data Protection Is Falling Short

Software-as-a-Service (SaaS) applications have become the backbone of digital business. Organizations across industries increasingly rely on SaaS to adapt quickly, collaborate globally, and scale rapidly. But as SaaS portfolios expand, the risks multiply, and data protection is not keeping pace. Based on a survey of 500 IT and business decision-makers worldwide, our *2025 State of SaaS Resilience Report* reveals some sobering findings, highlighting the need for more effective data protection.

SaaS adoption is growing rapidly

Use of SaaS applications is on the rise across industry verticals, establishing its place at the center of business.

- Organizations use an average of 139 SaaS applications.
- 96% of respondents have increased SaaS adoption in the last few years.
- 46% have seen a dramatic increase in SaaS use.

Threats to SaaS data are increasing

SaaS-related data breaches are becoming commonplace, with costly consequences. Yet organizations report low confidence in their ability to prevent or recover from SaaS data disruptions.

- 65% of respondents experienced a SaaS-related breach in the past 12 months.
- 87% admit they have at least one SaaS application at risk due to inadequate protection.
- The average cost of downtime is $405,770 per day, $2.3 million over a five-day recovery period.

SaaS data resilience planning is not keeping pace with threats

More than half of organizations surveyed say data protection challenges have increased their exposure to cyber threats. IT is often not in control of SaaS applications, hampering visibility, security, and compliance.

- 66% of respondents believe SaaS vendors are solely responsible for protection, yet more than half lack confidence in vendors' protection capabilities.
- 43% of survey respondents say no one truly owns SaaS security, creating critical gaps in accountability.
- 44% struggle to respond to audits and regulatory requests.

Executive Summary

Most organizations are under-protected and unprepared for these threats

While protection gaps are widespread, the majority of organizations surveyed fail to meet even the bare minimum of SaaS data protection.

- Only 30% perform policy-driven backups for some of their SaaS applications.
- Only 26% have offsite data retention for some of their applications.
- Only 25% have resilience testing in place for some of their applications.

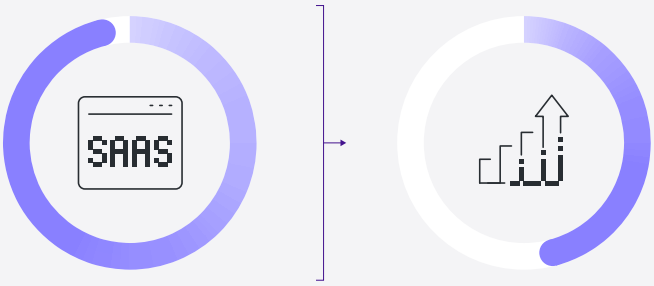
While SaaS platforms have unlocked tremendous value for organizations, our report reveals that customer data resilience strategies remain fragmented, underfunded, and misaligned with today's risk landscape. The path to increasing resilience lies in adopting a more unified, automated, and proactive approach to SaaS data protection.

SaaS Adoption Is Booming And Risk Is Growing

SaaS adoption is showing no signs of slowing. Nearly every organization has added more SaaS applications in the past two to three years. The average number in use today is **139**, but that number rises dramatically among organizations that have faced repeated breaches. Companies hit by multiple incidents reported running closer to **159 applications**, while those that avoided breaches averaged **116**.

This finding shows a direct link between SaaS sprawl and vulnerability. Every new app brings new integrations, new permissions, and new places where sensitive data may live. As one UK board member in education put it:

> *The attack surface grows with the number of SaaS applications in use, increasing the possible points of entry for cybercriminals.*



96%
of organizations have increased their use of SaaS applications in the past 2-3 years

46%
have seen a significant increase

139 SaaS apps
used in organizations, on average

Those hit by more than one breach in the last 12 months use an average of

159 SaaS apps

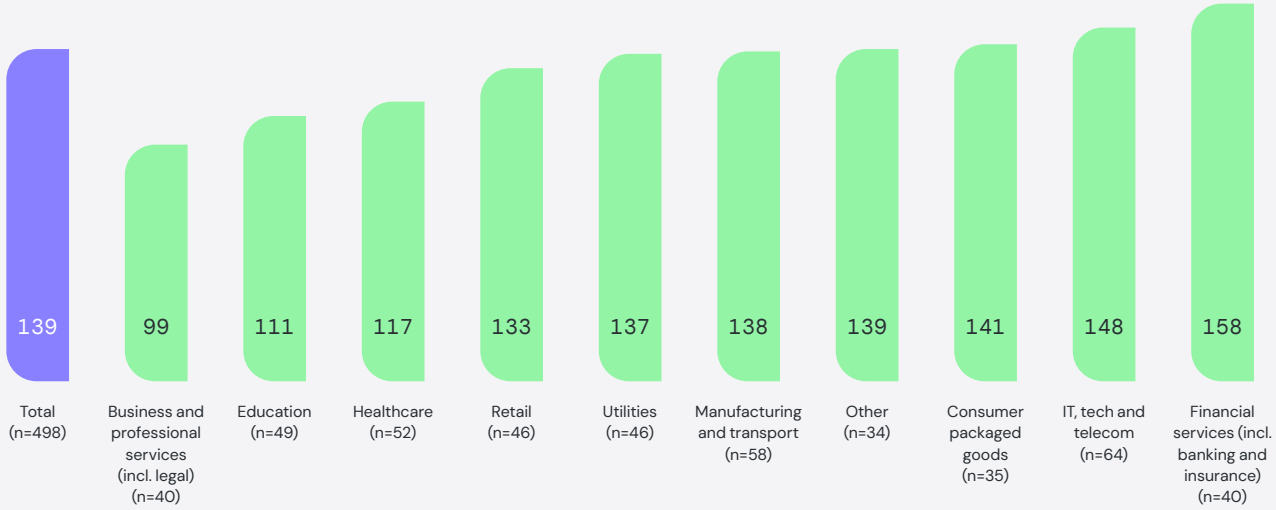
SaaS Growth Is Impacting All Verticals

Every sector is wrestling with SaaS expansion. IT and retail reported the highest levels of adoption, while healthcare and financial services are particularly sensitive to compliance challenges.

Despite industry differences, the underlying trend is consistent. SaaS has become embedded in daily business operations, and no single department or function has a complete view of what is in use. Shadow IT and decentralized adoption mean IT is often asked to secure applications it does not control.

For IT leaders, this creates a new governance challenge: protecting data in environments where visibility is partial at best, and accountability is often unclear.

Average number of SaaS applications, by vertical



SaaS Security Incidents Are Commonplace

65% of organizations experienced a SaaS-related breach in the past 12 months. This is no longer a fringe risk. It is a majority experience, and it is happening across industries, sizes, and regions.

What makes this particularly concerning is the correlation with SaaS adoption. The more apps an organization runs, the more likely it is to suffer a breach. Organizations with larger portfolios are not only breached more often, but they also report higher breach severity.

This means SaaS risk is not just theoretical. It is a measurable consequence of SaaS sprawl and inadequate resilience planning.

65%

have experienced a SaaS application data breach in the past year

2

average number of SaaS applications data breach incidents in the past year

Those with **more SaaS apps** are more likely to have had a breach

1–100 SaaS apps — 60%

101–200 SaaS apps — 66%

201+ SaaS apps — 77%

The High Cost of SaaS Disruption

The financial consequences of SaaS incidents are staggering.

- The **daily cost of SaaS downtime averages $405,770**.
- Recovery typically takes **five working days**, adding up to an estimated **$2.3 million in losses per incident**.
- For organizations running 200 or more SaaS apps, the cost of breach recovery is nearly **five times higher** than for those with smaller portfolios.

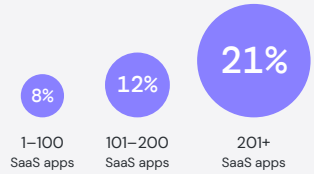
These numbers tell only part of the story. Beyond direct costs, IT leaders point to harder-to-measure losses: customer trust, regulatory penalties, and reputational damage. In many cases, these impacts far outweigh the technical costs of downtime.

Data breaches have substantial impacts on organizations, reinforcing the need for a strong defensive strategy

Of the **65%** that have experienced a data breach in the past year...

87% experienced some level of disruption.

Those with **more SaaS apps** are more likely to say that the breach was **critical**.



Cost and recovery impacts

$405,770
estimated average daily cost of SaaS data unavailability

1–100 SaaS apps	101–200 SaaS apps	201+ SaaS apps
$219,458	$262,976	$999,112

5 working days on average for **recovery time**

= **$2.3M** in potential losses

Visibility And Ownership Gaps Compound The Risk

A consistent theme from the research is the lack of visibility and accountability.

- **44% struggle to respond to audits and regulatory requests.**
- **55% lack confidence in vendors' protection capabilities.**
- **51% say their data protection challenges have increased exposure to cyber threats.**

Perhaps most telling: **43% of organizations say no one truly owns SaaS data resilience**. That lack of ownership creates confusion, delays, and weakens overall posture.

When no one owns data resilience, everyone is exposed.

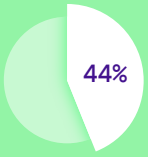
42%

Face limited visibility into data protection across SaaS applications

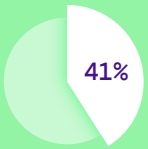
43%

say no one truly owns SaaS data resilience, creating risk and accountability gaps

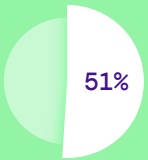
Impact of limited visibility



Difficulty responding to audits or regulatory requests



Loss of data or inability to recover deleted files

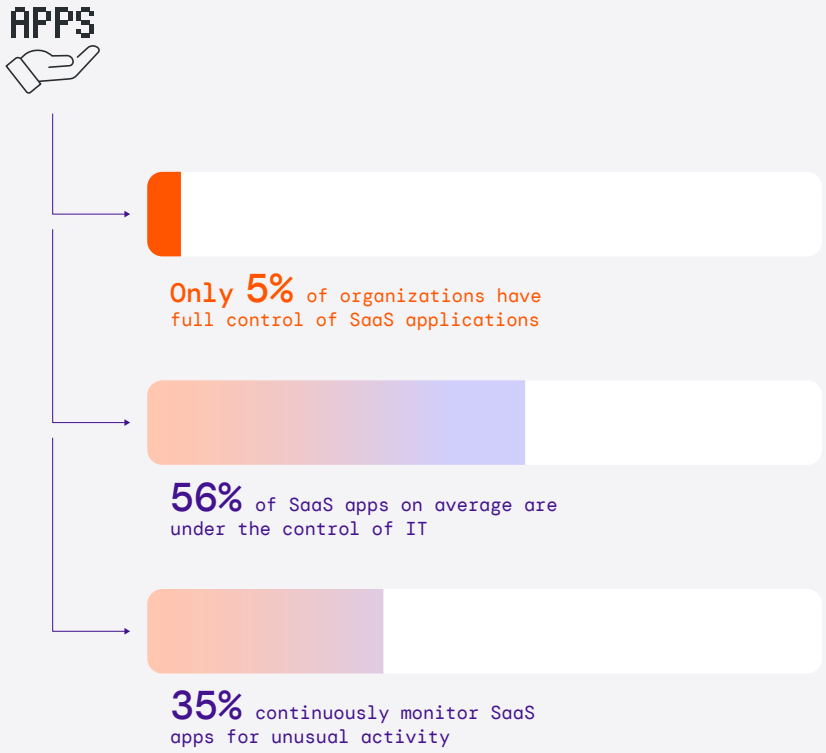


Increased exposure to cyber threats

IT Is Not Always In Control

The shift to SaaS has fundamentally changed IT's role. In the past, applications were hosted in centralized data centers, where IT had full control. Today, adoption is often driven by departments outside IT. Marketing buys its own CRM. HR onboards new collaboration tools. Finance spins up cloud-native platforms.

While this flexibility helps teams move faster, it also erodes centralized visibility and control. IT leaders are being asked to protect environments they had little say in selecting. The result is new challenges in security, compliance, and enforcement.



Protection Gaps Are Widespread

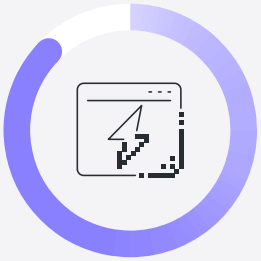
The survey findings confirm that protection has not kept up with adoption:

- **87% have at least one SaaS application unprotected**
- On average, **six apps per organization are at risk**
- **66% of respondents mistakenly believe their SaaS vendors are solely responsible for protection**

Overreliance on native vendor recovery is leaving organizations dangerously exposed. As one utilities executive explained:

> *We do not have full visibility into the security practices of every third-party vendor. That's a blind spot in our overall security posture.*

This misplaced confidence creates a dangerous reality. When a breach occurs, many organizations discover too late that the responsibility was theirs all along.



87%

have at least one SaaS application type at risk due to inadequate backup or reliance on native recovery

6

SaaS application types at risk per organization, on average

66%

think responsibility for data protection should lie with their SaaS vendor

Applications In Spotlight

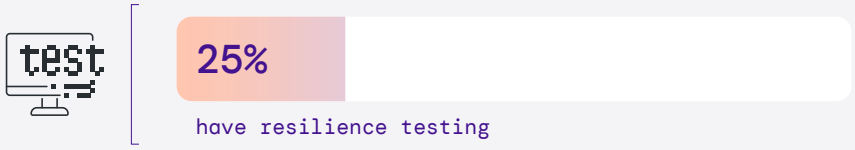
Respondents consistently called out enterprise SaaS platforms as their highest areas of concern. The reasons varied, but the theme is consistent: these applications are deeply integrated, widely accessible, and hold business-critical data.

Application	Reasons Provided by Respondent
salesforce	» Salesforce CRM and our Collaboration platforms pose the most security risks. This is because they handle sensitive data, have broad access, and integration capabilities. Misconfigurations, weak access controls, and unauthorised access are vectors for attacks. « Board Member of an IT Company
GitHub	» GitHub represents the most significant security risk to our organization due to its role in storing and managing source code, credentials and configuration files that are critical to our operations. « Board Member of an IT Company
okta	» As our identity and access management (IAM) platform, Okta acts as the central gateway to virtually all other SaaS tools and internal systems. If compromised, it could provide an attacker with access to: Internal and customer-facing applications administrative tools and privileged systems. « Senior Manager of an IT Company
Microsoft 365	» Ensuring Microsoft 365 application comply with data protection regulation can be complex, which is the biggest security risk for my organization. «
box	» It's Box, so many teams dump important stuff there, if someone outside got access, we would not even know right away. «
slack	» For many businesses Slack is essential communication tool but a breach could expose confidential internal discussions file attachments and chat logs. «
Google Workspace	» Due to its suite of applications, Google Workspace presents a broad attack surface. The potential for phishing attacks, data breaches, and unauthorized access to sensitive information is constant. We are implementing robust security measures, including multi-factor authentication and data loss prevention, to protect our Google Workspace environment. «
zoom	» Zoom meeting minutes contain a lot of confidential internal information, especially the content of negotiations with suppliers, and if this data is intercepted or downloaded, our losses can be very large. «
zendesk	» Zendesk because having complexity of setting up and managing permissions for these integration lead to misconfigurations by the client and granting overly broad access to third-party apps or services. «
Dropbox	» Without proper security controls Dropbox could result in the unauthorized sharing of sensitive document posing a threat to company privacy and compliance. «
HubSpot	» HubSpot is tied into our entire sales funnel. Losing data here would be more than just inconvenient. «

Under-Protected And Under-Prepared

Most organizations failed to meet the bare minimum when it comes to SaaS data protection:

- 30% perform policy-driven backups for *some of their apps*
- 26% have offsite data retention for *some of their apps*
- 25% have resilience testing in place for *some of their apps*



Methodology

The HYCU State of SaaS Resilience Report 2025 is based on a global survey of **500 IT and business decision-makers** conducted in 2025. Respondents represented organizations actively using SaaS applications across a range of industries.

Participants ranged from board-level executives and C-suite leaders to senior and mid-level managers, ensuring a balanced perspective across both strategic and operational roles.

To qualify, all respondents had to work at organizations currently deploying SaaS applications. Survey questions explored SaaS adoption trends, security incidents, data protection strategies, resilience confidence, and the business impact of downtime or breaches.

Responses were analyzed globally, with regional coverage including North America, Europe, and Asia-Pacific. This provides a representative view of how SaaS adoption and resilience challenges are playing out across markets with different regulatory and operational pressures.

The goal of this research is to shine a light on how organizations are adapting their data protection and security strategies in a SaaS-first world, where adoption continues to accelerate but resilience has not yet caught up.

500 IT decision-makers

From board members; C-level to Mid-level management operating in:	
IT	n=64
Healthcare	n=52
Retail	n=46
Financial services	n=40
Consumer packaged goods	n=35
Manufacturing	n=58
Education	n=50
Utilities	n=46
Business and Professional services	n=40
Government	n=40

Regions

North America	125
EMEA	225
APAC	150


USA 125


UK 75


Germany 75


France 75


Singapore 50


Japan 50


Australia 50

The HYCU State of SaaS Resilience Report **2025**