The 3 Major IT Risk Drivers
Your Organization Should Watch Out For

Businesses globally are increasingly moving to multicloud and hybrid cloud environments due to their numerous benefits. However, these technologies come with some key challenges that can put your organization at risk.

Protecting your data in the cloud: Would you risk IT?

Key data protection challenges associated with multicloud or hybrid cloud strategies:

- Lack of visibility into your data
- Complex and susceptible since data spans across multiple cloud providers
- Introduces new threat vectors and data risks

Over 80% of organizations have sensitive SaaS data that is exposed. On average, a terabyte of cloud storage contains over 6,000 files with sensitive information, and more than 3,900 folders are shared externally.[1]

The Three Major Risk Drivers in Your IT Organization

Your data in the cloud is constantly at risk due to the following three reasons:

1 Human-driven risks

Whether unintentional or deliberate, human actions significantly contribute to data loss in SaaS application environments.

HUMAN ERROR
More than 80% of data breaches are caused by human error, making it one of the key risk drivers in cloud data security.[2]

MALICIOUS INSIDER ACTIVITY
According to the 2024 Insider Threat Report, insider attacks have significantly increased, with the percentage of organizations reporting these incidents rising from 66% in 2019 to 76% in 2024.[3]

HACKERS
In Q2 2024, global cyberattacks rose by 30% year-over-year, with organizations experiencing an average of 1,636 attacks per week.[4]

2 Technology-driven risks

As reliance on new-age technology solutions grows, technology-driven risks also grow, increasing the chances of exposing your organization to a wide range of threats.

SYNC ERRORS
Sync errors due to weak connectivity, technical glitches or reliance on third-party applications can result in losing the information you need most.

VIRUS, MALWARE AND RANSOMWARE
Over 450,000 pieces of malware are created daily, representing a 50% increase in malware creation over the past two years.[5]

RELIANCE ON NATIVE TOOLS
According to the 2023 Data Protection for SaaS report, over 50% of respondents reported that their organizations had lost SaaS data.[6]

3 Process-driven risks

SaaS data protection is complicated since it involves numerous parties, technologies and processes that must come together to achieve the desired results.

LACK OF AN INCIDENT RESPONSE (IR) PLAN
Factors such as employee training, incident response (IR) planning and having an IR team were crucial in reducing the average breach cost by approximately $244,111.[7]

SECURITY MISCONFIGURATIONS
Cloud misconfigurations are responsible for 12% of initial attack vectors in security breaches, which cost businesses an average of $3.98 million.[8]

NON-COMPLIANCE
Fines, penalties and settlements due to data breaches and non-compliance cost companies hundreds of millions of dollars.[9]

Key steps to reducing risk with Spanning

Spanning Backup is a purpose-built, cloud-native backup and recovery solution, providing enterprise-class, end-to-end data protection for Google Workspace, Microsoft 365 and Salesforce.

Spanning helps prevent, anticipate and mitigate account compromise and data loss through:

1. **ROBUST SECURITY**
Spanning leverages industry-standard, application-level security (OAuth 2.0) instead of less secure privileged service accounts and passwords.
2. **PHISHING DEFENSE**
AI-enabled email security for protection against phishing, business email compromise (BEC), account takeovers (ATO) and more.
3. **SPANNING DARK WEB MONITORING**
Identify, analyze and proactively monitor your organization's compromised or stolen credentials on the dark web.
4. **END USER SELF-SERVICE RESTORE**
Empower end users to quickly find and perform non-destructive data restores without IT intervention.
5. **AUTOMATED DAILY AND ON-DEMAND BACKUPS**
Eliminate time spent tediously managing backup schedules, reduce the chance of inconsistencies and errors, and streamline compliance.
6. **CUSTOMIZABLE CLOUD RETENTION TERMS**
Easily customize policies based on your needs to meet regulatory or compliance requirements and SLAs.

Sources

1. https://info.varonis.com/en/great-saas-data-exposure-report
2. https://git-sicherheit.de/en/news/sicur-cyber-2024-82-percent-of-data-breaches-are-related-to-human-error
3. https://www.securonix.com/resources/2024-insider-threat-report/
4. https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/#:~:text=Key%20Statistics%3A,(1%2C999%20attacks%20per%20week).
5. https://www.av-test.org/en/statistics/malware/
6. https://www.techtarget.com/esg-global/research-report/research-report-data-protection-for-saas
7. https://www.ibm.com/reports/data-breach
8. https://www.ibm.com/reports/data-breach
9. https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html

Download the eBook to learn about these risk drivers and the steps to overcome them in detail.

SPANNING
A Kaseya COMPANY