SaaSAssure℠

Eliminate Risk | Empower Control

EBOOK

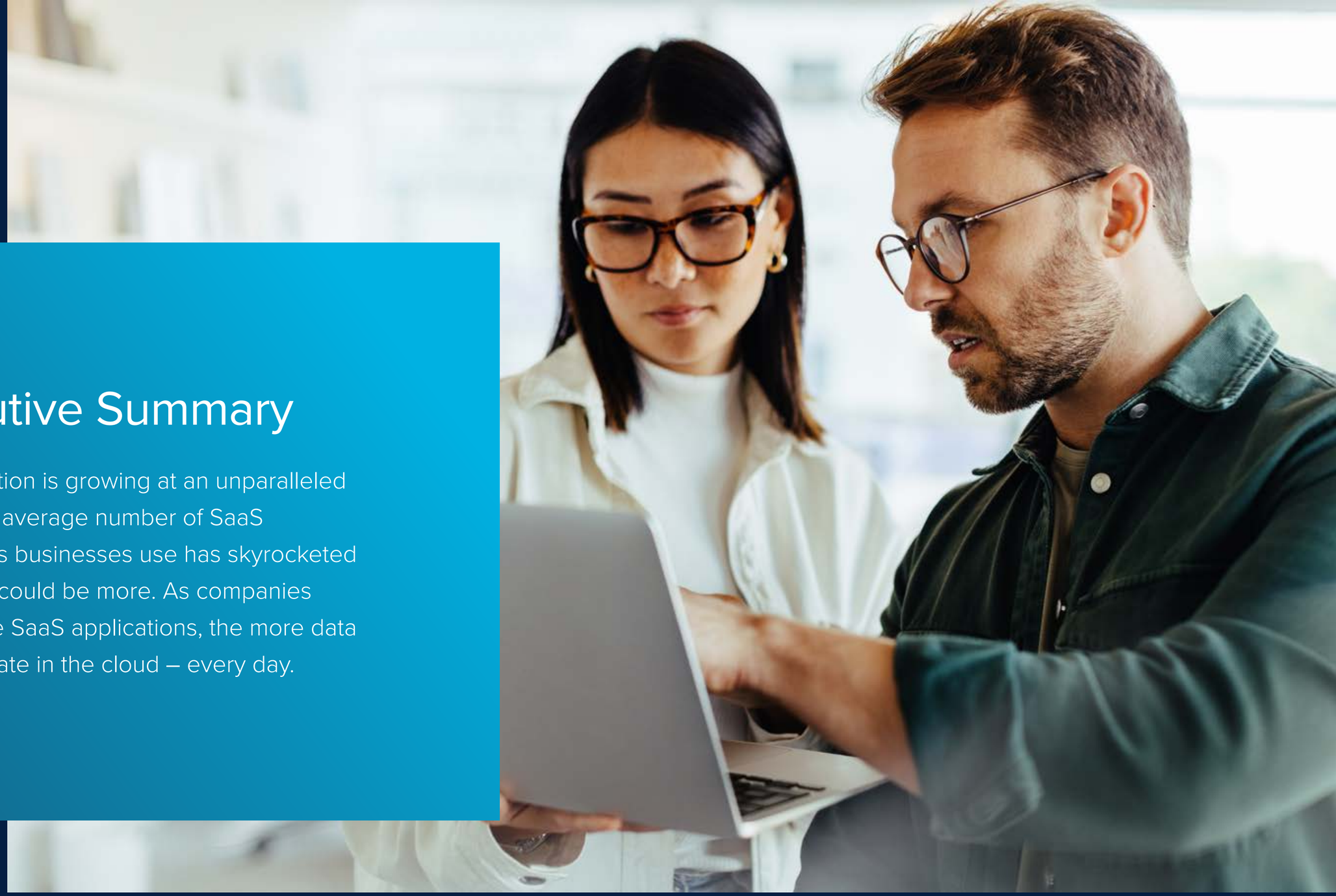
Closing the SaaS Backup Gap

A Must For Ensuring Data Security

Table of Contents

Executive Summary

SaaS adoption is growing at an unparalleled pace – the average number of SaaS applications businesses use has skyrocketed to 130 and could be more. As companies adopt more SaaS applications, the more data they generate in the cloud – every day.



EXECUTIVE OVERVIEW

Unfortunately, many organizations believe their cloudbased data is safe and secured by SaaS vendors. In fact, it is the SaaS customer's responsibility to back up their cloud data. Often, businesses are either unaware or ignore this or only back up data from a handful of SaaS vendors. This creates a growing gap between the amount of data that organizations are backing up and their growing data footprint in the cloud.

This growing gap requires enterprises to ensure an effective and secure solution for managing data across a wide variety of line-of-business applications, not just those considered "core." A SaaS data protection tool is a critical component of a comprehensive backup strategy and ensuring the tool covers the entire SaaS workload is key. Additionally, control of all data also makes it easier to comply with changing regulations on data retention, incident reporting and privacy laws.

130+ SaaS applications in use as SaaS adoption grows at an unparalleled pace.

The Cloud's Big Boom

The software-as-a-service (SaaS) boom is here to stay.

THE CLOUD'S BIG BOOM

The software-as-a-service (SaaS) boom is here to stay.

Organizations of all sizes are either evaluating or adopting new SaaS apps every day. This ever-growing roster of cloud-based apps help manage IT infrastructure, track budget and finances, and provide internal teams with productivity tools. Statista reveals a clear upward trend in the adoption of SaaS applications. The average count of SaaS apps in use among businesses grew from 80 in 2020 to 130 in 2022.

Given the many demands made on internal IT teams, it only makes sense to offload to the cloud the management of these apps. This frees internal IT teams to focus on more important work. However, along with this boost in flexibility, there lies a hidden danger. As the number of SaaS apps grows, so does the data footprint of the business utilizing them. More SaaS apps means more business-critical data is being created in the cloud every day, every hour, every minute.

Unfortunately, there is a false sense of security when using SaaS apps that all this growing data is somehow "safe." While some SaaS vendors provide periodic backups of some data, what is backed up and how varies across vendors. What's worse, even IT professionals may think that their cloud data is protected by the SaaS vendor and therefore safe and secure. ***It is not.***

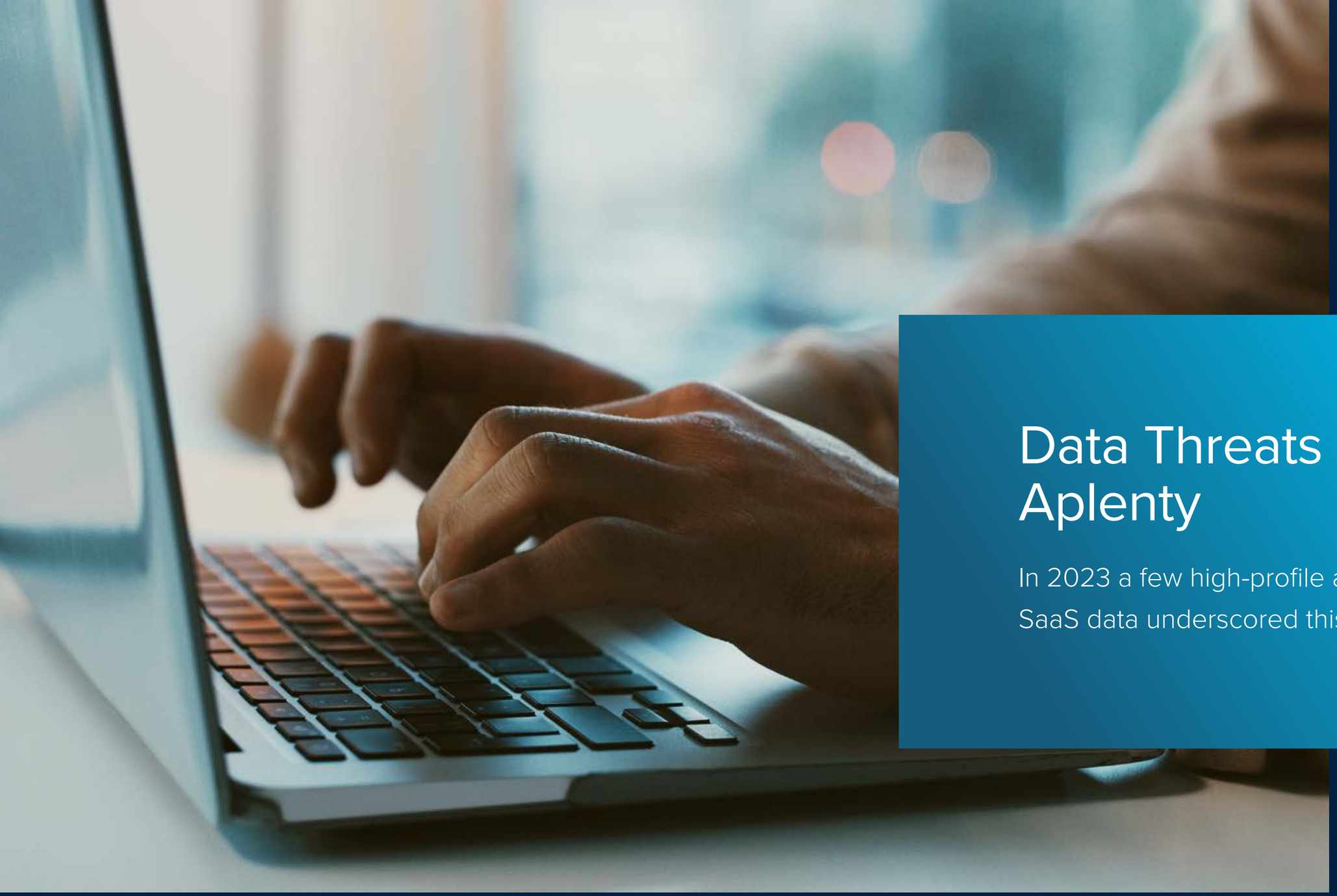
Your Data, Your Responsibility

SaaS vendors operate on what is known as the shared responsibility model.

YOUR DATA, YOUR RESPONSIBILITY

The shared responsibility model means that the SaaS provider agrees to be responsible for securing its cloud infrastructure (servers and network) and takes care of related maintenance and management. The customer, however, is responsible for the data generated or stored in that cloud environment from user accounts.

In other words, you create it – you're responsible for it. To keep the data "safe," then, means SaaS customers should be backing up their data themselves and storing it safely under their control. Many find it difficult to keep up with their growing cloud footprint. Some may ignore this task entirely while others opt to secure the data of just a few SaaS vendors. It may come as a shock, then, when organizations don't prioritize backups and SaaS data is lost, stolen, or compromised.



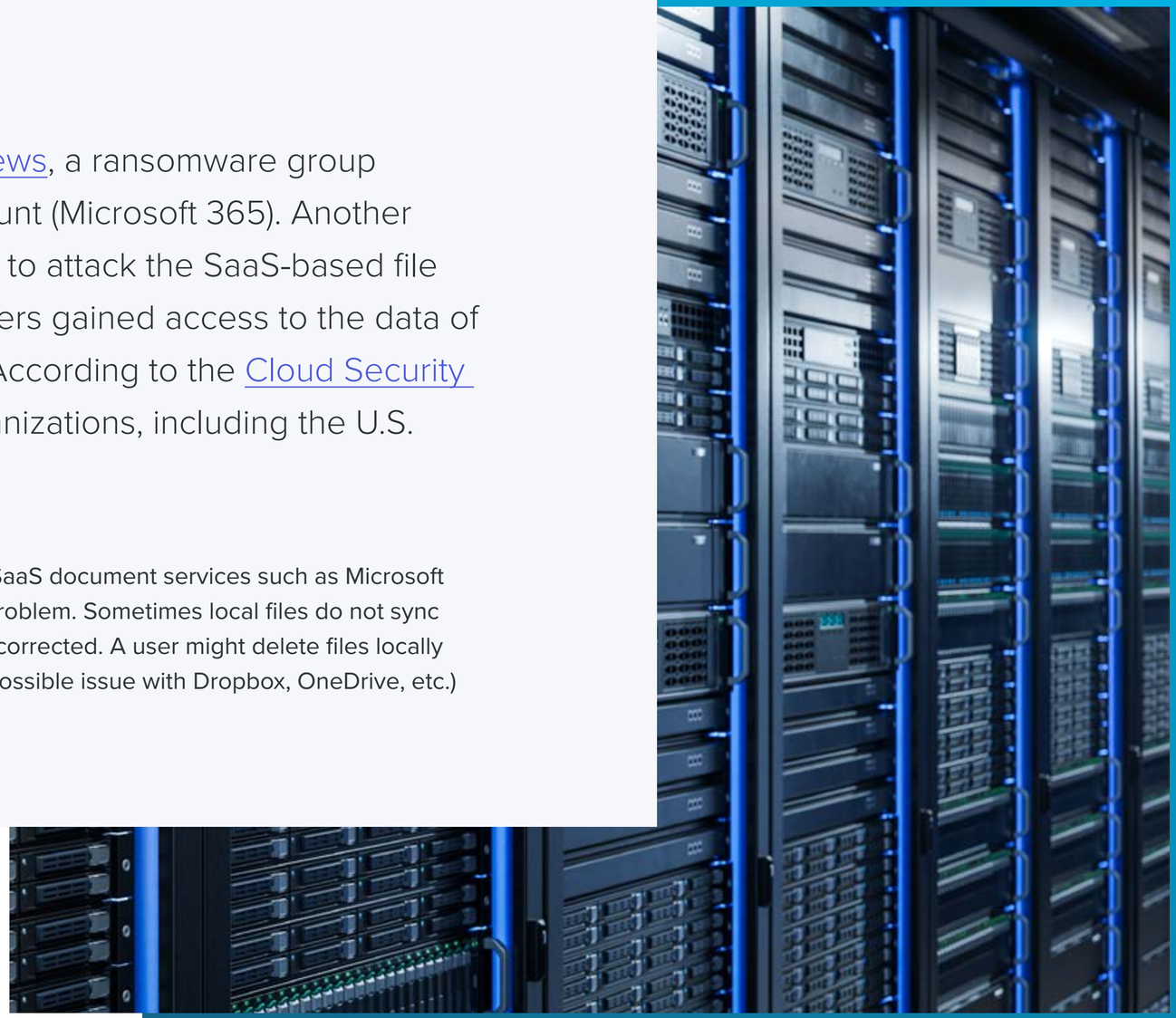
Data Threats Aplenty

In 2023 a few high-profile attacks on SaaS data underscored this risk.

DATA THREATS APLENTY

Early in 2023, as reported on Cyber Security News, a ransomware group successfully attacked a SharePoint Online account (Microsoft 365). Another ransomware gang used a zero-day vulnerability to attack the SaaS-based file transfer management application MOVEit. Hackers gained access to the data of thousands of employees and family members. According to the Cloud Security Alliance, the attack affected more than 100 organizations, including the U.S. Department of Energy and British Airways.

Ransomware gangs are just one kind of threat to data. With cloud SaaS document services such as Microsoft 365, Dropbox, Box and Google Drive, syncing issues are another problem. Sometimes local files do not sync properly, and sometimes file errors are synced before they can be corrected. A user might delete files locally and discover the deletions have been propagated to the cloud (a possible issue with Dropbox, OneDrive, etc.)



100+ organizations affected from the attack

DATA THREATS APLENTY CONT'D

Another issue is SaaS service outages. Cloud systems can still fail, and data loss can occur. A recent article from CRN.com listed The 15 biggest Outages of 2023 and, yes, many big vendors and apps were on the list. Microsoft experienced outages for Teams, Microsoft 365, Azure, and Outlook. A fire in Paris, France, resulted in a significant outage in Europe of Google Cloud and many other cloud services.

It's easy to overlook, but both human error (misconfigurations, poor security training) and insider threats play a huge role in data breaches. As many an IT admin can attest, what employees are doing with access to data is difficult to monitor. In 2023 two Tesla employees leaked personal data of more than 75,000 former and current Tesla employees.

Whatever the reason, when a data disaster strikes, using backups to quickly restore operations is essential. The SaaS customer who does not back up their cloud data is left to work with provider-generated backups.

SaaS Vendor Backup: Hurdles and Hassles

Relying on SaaS vendors to provide backups can be a mistake.

SAAS VENDOR BACKUP: HURDLES AND HASSLES

In most cases, providers have some form of data retention policy, possibly some snapshots, but these are for a limited period. Depending on the industry, location, and regulations, this can range from 90 days to a year. How many employees can do without files and data more than 90 days old? In some cases, if a user account is deactivated, i.e., if they've been terminated or quit, their data is deleted along with the account.

Another hurdle comes from Application Program Interface (API) call restrictions (also called API caps). All SaaS services are multitenanted, so there is a limit on API calls customers can make. These caps ensure all customers have adequate access to the resources they need in the host's cloud. Providers can impose caps based on requests per day by minute, or by user per minute, according to Google.

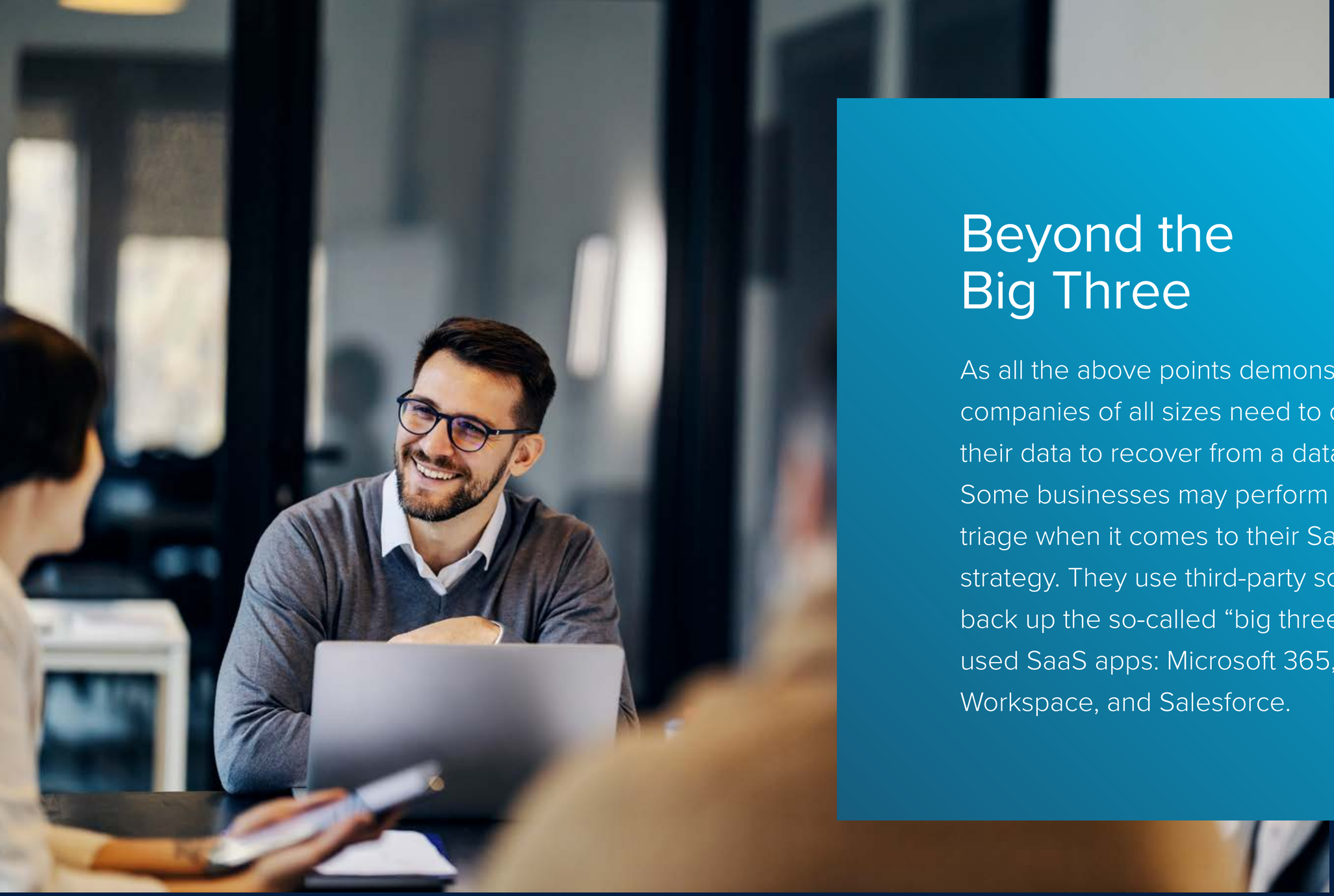
These caps may be a real problem when a data crisis unfolds. Users trying to recover data after a breach could encounter significant delays from their cloud provider. This can result in a backlog of API calls, or even blocked API calls if caps are exceeded. During a breach or emergency, the last thing a user needs is slowed or stalled service from their SaaS provider.

Another factor affecting recovery time is complexity. Depending on the app, some recovery tasks involve multiple data tables that must be recovered in a precise order. A good example of this is Jira, the software development, collaboration, and project management app by Atlassian. It includes tables for project data, and tables for attachments, as well as tables for user accounts. When backing up manually, recovery takes several complex steps. Manual processes can chew up admin time and introduce a risk of data loss during recovery.

SAAS VENDOR BACKUP: HURDLES AND HASSLES CONT'D

Consider, too, that SaaS vendors typically do not provide individual account-level data protection. Restoring user accounts (setting them up again) falls to the customer's IT staff or admins. It's not that it's an impossible job – it's a question of how internal staff is using their time.

Even the best data emergency and backup plan will mean little if the Recovery Time Objective (RTO) can't be met. This is the maximum acceptable amount of time systems can be down before causing significant damage (financial or operational). This differs with each organization, but defining the RTO at least gives staff a "clock" to work to. The hard part of RTO planning is pinning down the time needed to get information from vendors and partners.



Beyond the Big Three

As all the above points demonstrate, companies of all sizes need to control their data to recover from a data disaster. Some businesses may perform a kind of triage when it comes to their SaaS backup strategy. They use third-party solutions to back up the so-called “big three” most-used SaaS apps: Microsoft 365, Google Workspace, and Salesforce.

BEYOND THE “BIG THREE”

But this strategy ignores the fact that the average organization has over 130 SaaS applications in use, and the average employee uses nine. Also, which applications are deemed important varies by department. Beyond the “big three,” these other SaaS apps have their own backup quirks and issues. Here are just a few examples:

Atlassian Jira

Jira doesn’t rollback individual accounts. They recommend all users backup their databases. Backup requires at least three separate tables that must be recovered in a specific sequence. Users must manually back up their service which can be time-consuming without some form of automation.

QuickBooks Online

Like other SaaS tools, users must initiate a manual backup of the service, but automated backups can be set up. But not all data is captured in automatic backups. Some of this is non-critical, but others can be very inconvenient and require significant time to rebuild, like recurring transactions, reports, and bank feeds.

Workday

Workday has a robust internal process to protect its system databases with strong replication and transaction logging, but account level backups are not as easy. Workday would require a user to export several data tables manually and not all data would be recoverable.

BEYOND THE “BIG THREE” CONT’D

The current SaaS backup market has many vendors covering different parts of the SaaS pie but are mostly focused on “the big three.” This forces organizations into a patch-work approach to backing up SaaS data when a comprehensive strategy is what’s needed.

Many organizations, whether they know it or not, are experiencing an alarming and growing gap between what should be backed up from SaaS vendors and what is backed up. Over time, if unattended, the SaaS backup gap will widen. Huge amounts of business-critical data in the cloud and not quickly available for recovery can become the weak link in a crisis.

Take Command of SaaS Data

When it comes to comprehensive cloud SaaS backup solutions, there is finally a solution that will help small, medium, and large businesses to close the SaaS data gap. Asigra is introducing a new platform to build an ecosystem of support for many SaaS apps that have no backup support today.

TAKE COMMAND OF SAAS DATA

SaaSAssure℠ powered by Asigra is building deep integration into dozens of SaaS services, providing the benefit of continuous data protection and advanced recovery options. Partners will ultimately have access to a Software Development Kit to enable backups for new SaaS apps.

SaaSAssure will solve many of the challenges that customers face in protecting their SaaS data. SaaSAssure is designed to make SaaS backups extremely easy to manage. It is fully automated, meaning more efficient oversight and restoration when data disasters strike.

It's multitenanted and built for Managed Service Providers (MSPs), integrators, and other IT providers. Through a single console, an administrator can back up and recover across many SaaS services, efficiently and quickly. There's no software or agents to install and no need to rip and replace existing software. Backup data can be stored in AWS or any S3-compatible storage that service providers already use to minimize storage costs.

The goal is to simplify restoration steps to improve recovery speed. In addition to a simplified, rapid restoration process, select services will have granular restoration capabilities. For those services where granular restores are available, RTO will improve dramatically.

TAKE COMMAND OF SAAS DATA CONT'D

Most importantly, SaaSAssure provides advanced security for SaaS data. Cybercriminals are directly targeting backups as a rich source of actionable data SaaS data is particularly at risk, especially if it's manually backed up as a series of CSV files.

A recent example came from the LastPass hack. Attackers were able to steal the credentials of a senior developer and then use those credentials to access their backup service, where they then stole the master vault of all users' stored credentials.

Multiperson Approval (MPA)

An industry first, this requires multiple people to approve a potentially destructive action that can result in data loss Even if an attacker has access to admin credentials, they will not be able to proceed with harmful actions without additional approvals from other specified users.

Multifactor Authentication (MFA)

This requires users to authenticate using a six-digit Time-based one-time password application, such as Google or Microsoft Authenticator, when signing in or attempting to perform a potentially destructive action. MFA is a great first step at protecting systems but fails if an attacker has remote access to a system that an admin has logged into. Once the admin has logged into a service, someone with remote access could take control. Additional MFA requests prevent attackers from proceeding unnoticed.

Encryption

Asigra uses 256-bit encryption in flight and at rest to protect data with the highest security and compliance standards.

SaaSAssure gives organizations more control over their data. This is increasingly important as privacy and data retention laws continue to evolve and change. When outsourcing data storage to many SaaS providers, organizations may be placing their data under different jurisdictions with different privacy, retention, and incident reporting laws.

SaaSAssure is ultimately part of the broader picture of data management.

Total control over data, or data sovereignty, solves many problems. However, backing up the fast-growing mountain of data from SaaS apps is a daunting task. Partial solutions only paper over the need for future work. What's needed is a way to close data gaps, keep up with data growth, and even make comprehensive backups stable and secure not just now but in the future. SaaSAssure helps businesses of all sizes accomplish that.

SaaSAssure℠
Eliminate Risk | Empower Control

www.saasassure.com

Join the forefront of SaaS data protection with SaaSAssure.

Request a Demo

© 2024 SaaSAssure is a servicemark of Asigra Inc. All other brand and product names are trademarks of their respective owners. [02/24]