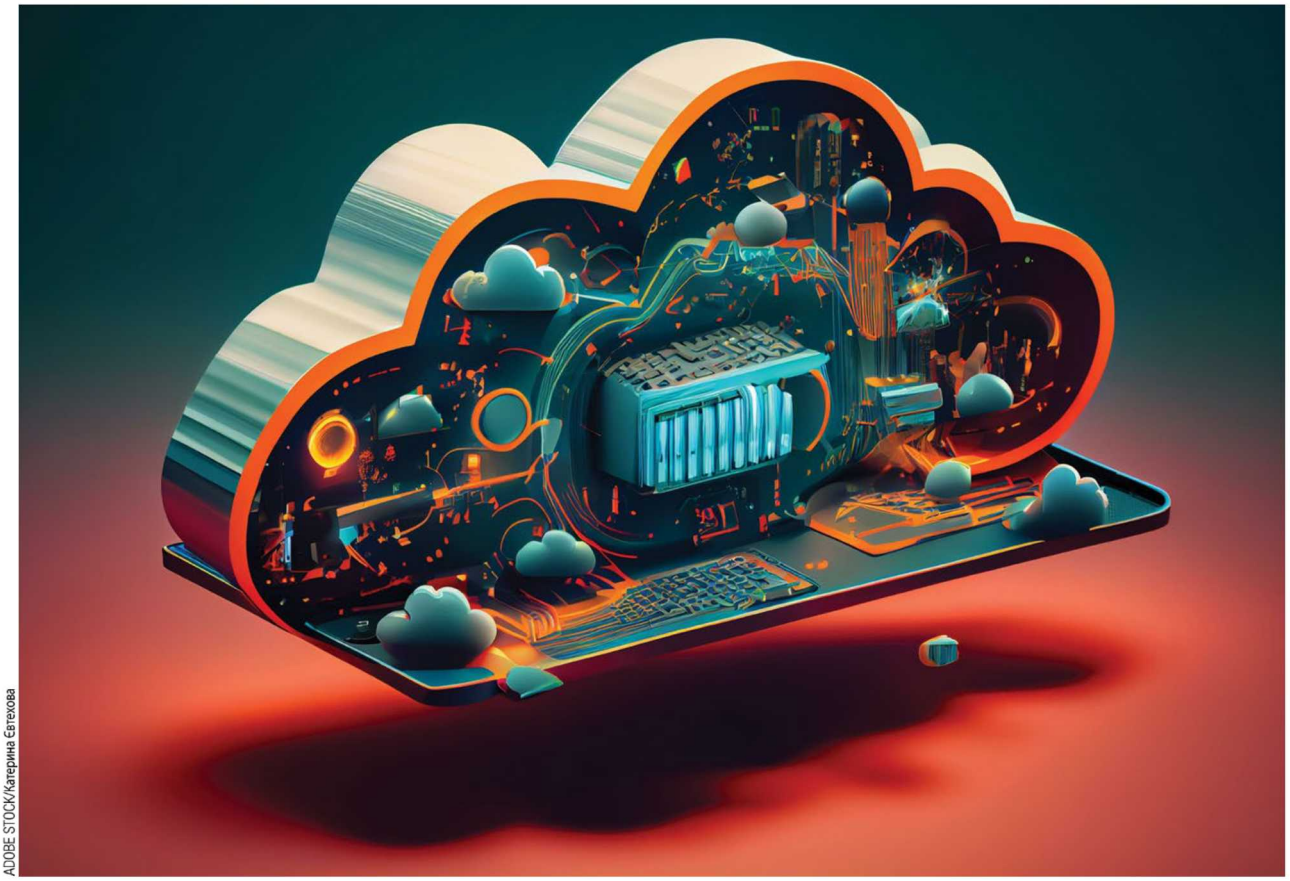
Safeguarding Data In a Multi-Cloud World

Chuck Cook | RENOVODATA



ADOBE STOCK/Катерина Евтехова

3PL references

Data-driven decision-making is increasingly crucial in today's business landscape. Protecting valuable data has never been more vital, yet it has also become more challenging. Third-party logistics providers and transportation companies often deal with sensitive data, including personally identifiable information and financial documents that constantly need to be safeguarded. As an ever-growing number of companies operate virtually and embrace cloud applications and multi-cloud environments, data management has become increasingly complex.

The data landscape is expanding rapidly, with approximately 92% of organizations now adopting a multi-cloud strategy. Consequently, "data sprawl" emerges, where files are scattered across multiple cloud platforms. This situation heightens the risk of exposing sensitive data to potential threats. If you're unaware of the type of data you have and where it lives, you are leaving your company vulnerable to public cloud security breaches, duplication, and sprawl. 3PL's are especially exposed to these perils due to data being shared across different platforms and systems with manufacturers, suppliers, and other logistics partners. Ensuring the backup of irreplaceable files

in secure clouds becomes imperative for maintaining business continuity.

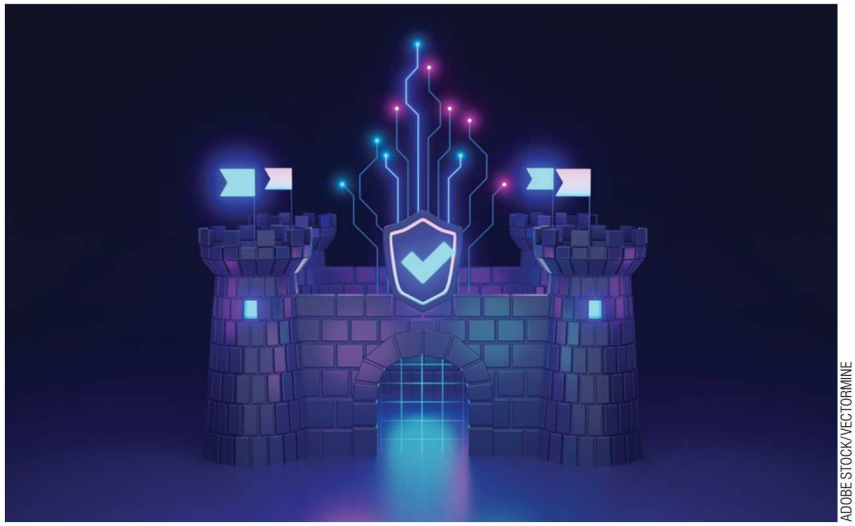
The utilization of cloud-based applications by organizations has witnessed a significant surge, increasing by 35% since 2022. Similarly, the trends of data creation are projected to amass at a rate of 35% year over year until at least 2025. Moreover, an alarming statistic reveals that one in five employees resort to personal apps for uploading, creating, sharing, and storing sensitive company information, further complicating security risks.

Studies show that 71% of respondents consider data sprawl to be a significant issue for their organizations. Such sprawl can result in privacy breaches, or even costly compliance violations. Duplicated data backups due to sprawl squander financial resources and can lead to confusion. Furthermore, failure to effectively track critical systems, applications, and backups can severely impact data recovery in the event of a disaster. Worst of all, data sprawl exposes organizations to unnecessary security risks, legal liabilities, and substantial IT downtime. Each of these risks incurs significant expenses for remediation and can even push companies to the brink of closure.

Steps to Tackle Data Sprawl

Gaining control over data sprawl requires a systematic approach. Firstly, businesses should establish a robust framework for classifying data and managing applications and systems. Next, it's essential to protect critical data, systems, and applications whether stored locally or in the cloud. Equipping employees with the necessary tools, access standards, and policies to educate them on proper interactions with company data is equally important. Finally, implementing appropriate life cycle management policies completes the basic strategy.

Data classification is an often-underestimated facet of data security. 3PL's are constantly creating, sending, and receiving a breadth of data of vastly different security levels. Without a solid structure in place, the task of categorizing data for secure and convenient access becomes insurmountable. A well-defined classification policy provides a framework for safeguarding data throughout its life cycle—from creation and storage to processing and transmission. It facilitates accurate documentation of data locations, ensuring efficient backup procedures.



ADOBE STOCK/VECTORMINE

Classification Strategy

A useful approach to data classification involves categorizing an organization's data types based on their sensitivity levels. For instance, employing a four-step system that considers the potential damage caused by a data breach can classify most data sets:

1. Public: Data that can be freely shared with the public, such as marketing materials, website content, and contact information.
2. Internal: Information not intended for public disclosure, such as sales playbooks or organizational charts.
3. Confidential: Sensitive data that could have adverse consequences if widely disclosed. This category includes vendor contacts and employee/HR data, which businesses are legally obligated to protect.
4. Restricted: Highly sensitive business and customer data that, if exposed, would pose significant financial or legal risks. Examples include intellectual property, HIPAA-protected data, credit card information, social security numbers, and other personally identifiable information.

Managing and securing all this data, as well as how it is stored and shared, may appear challenging. However, addressing the fundamentals will establish a baseline of security and provide peace of mind. Armed with this knowledge, you can confidently implement a four-step management system: identifying the location of data, hardware, and software assets; classifying each data set based on its significance; testing and documenting a plan to mitigate unforeseen events' impact; and ultimately allocating resources to protect your data where it matters most.

Identifying and safeguarding your data is important to minimize your risk and liability. Transportation organizations are increasingly adopting cloud-based platforms that help streamline operations. Unfortunately, without a calculated plan to mitigate data sprawl, these additional clouds can cause just as many headaches as they solve. A data classification system gives you the freedom to adopt new cloud solutions and classify, organize, and properly protect your data and limit exposure. Leverage data security practices and data protection & recovery tools that provide visibility to your organization and make you more resilient to data sprawl and growth.