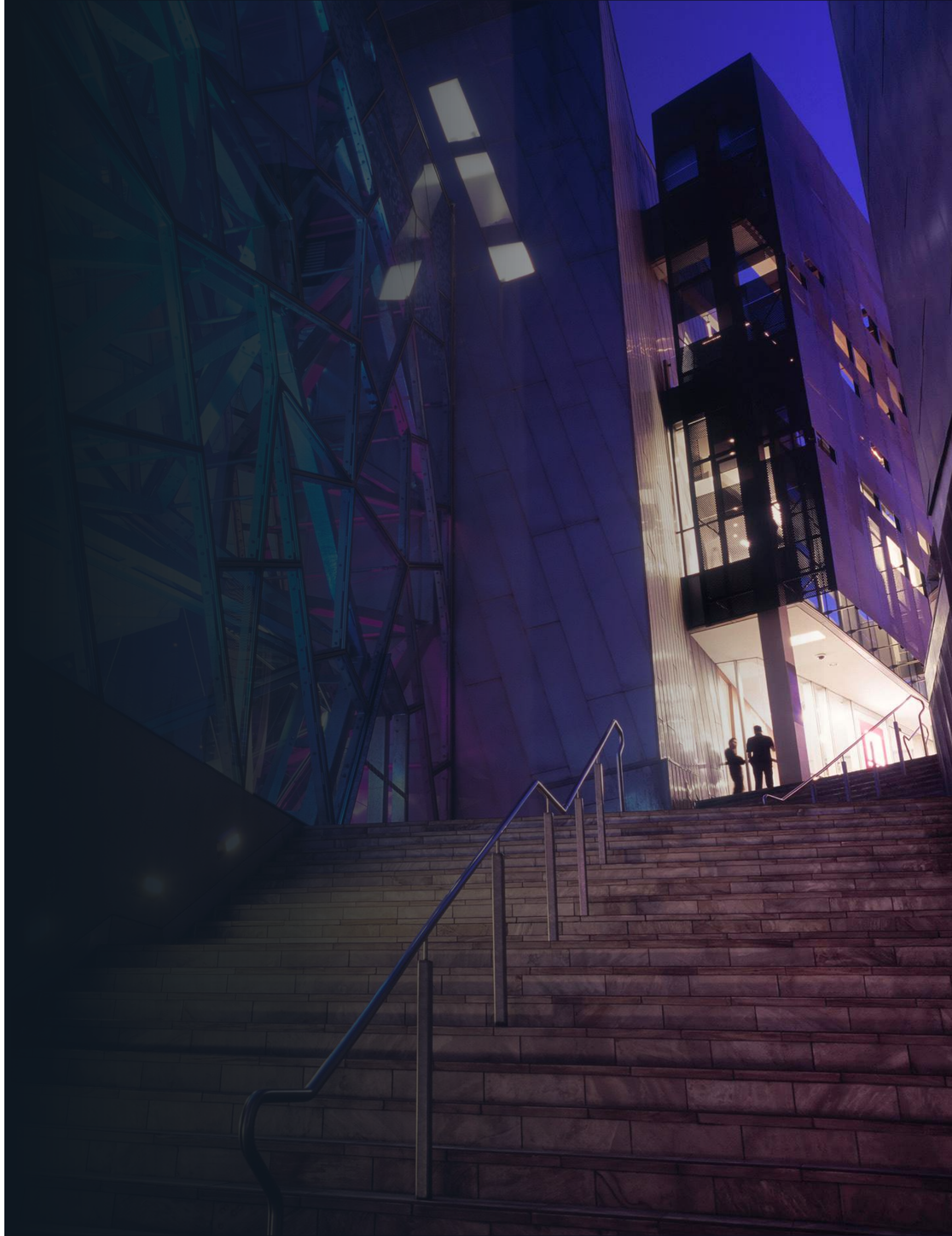
Enterprise Strategy Group | Getting to the bigger truth.™

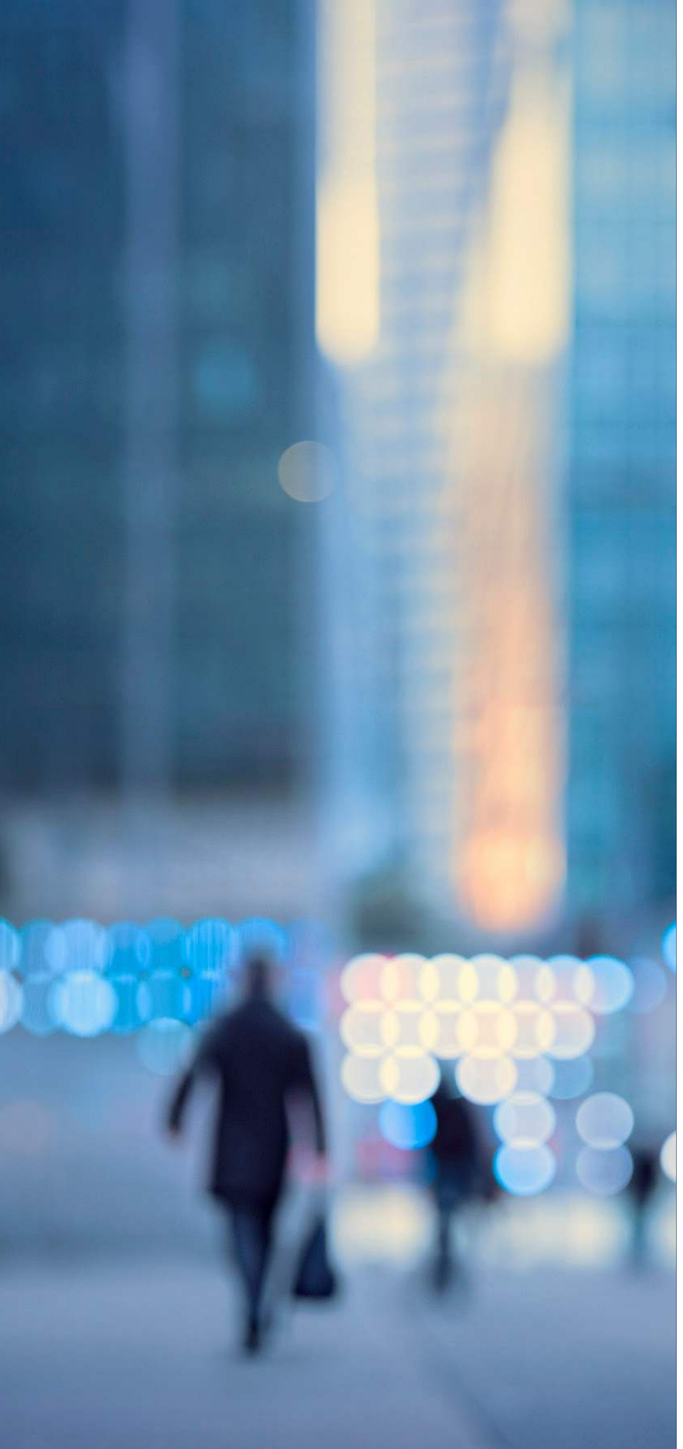
SaaS Data Backup: Transforming from Insurance Policy to Strategic Value Driver

Christophe Bertrand, ESG Senior Analyst

CONTENTS



This ESG eBook was commissioned by GRAX and is distributed under license from ESG.



From Data Backup to Data Intelligence

As organizations adopt more cloud services and applications, they also need to extend data protection SLAs to sensitive customer data stored in third-party cloud applications. Additionally, on-premises backup and disaster recovery workloads are leveraging cloud destinations, resulting in hybrid data protection topologies with varying service levels, end-user tradeoffs, and opportunities.

At the same time, the need for organizations to reuse data for strategic and operational business purposes beyond "just" backup is increasing. Vast amounts of data can increasingly be found in SaaS applications. Unfortunately, a chasm exists between traditional "dumb" data backup, in which data is only moved around but not leveraged to drive or support business outcomes, and data management, in which data is better understood and reused for other technical or business purposes.

RESEARCH METHODOLOGY

In order to understand how this confluence of changes is creating a disconnect between customer needs and currently offered solutions, ESG surveyed IT professionals at organizations in North America (US and Canada) responsible for data protection and management technology decisions for their organization across several studies[1]. All respondents were provided an incentive to complete surveys in the form of cash awards and/or cash equivalents.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

[1]Sources: ESG Research:

ESG Master Survey Results, *Data Protection Cloud Strategies,* June 2019.
ESG Research Report, *The Evolution from Data Backup to Data Intelligence,* February 2020.
ESG Research Report, *Real-world SLAs and Availability Requirements,* October 2020.

Back to Contents

Executive Summary

SaaS applications have taken over in many organizations as mission-critical applications. As such, they require enterprise-class levels of data protection and strong backup methodologies. After all, data is always your responsibility. But can you do more with it and what does it take?

With so much data now in SaaS environments, the prominence of SaaS backup and data protection technology is the linchpin to data reuse. These solutions can be leveraged as one of the mechanisms to support prerequisite processes. Organizations need to classify and sanitize data in order to make it re-usable. Organizations that embrace advanced data management like data classification and data sanitization may help provide the market with a roadmap to success, leading them to revisit how they approach data and how to make it a business asset that can be leveraged.

Data reuse is the key to many business benefits. Organizations should focus on the common denominator: the data itself, and its intelligent management. In order to realize the benefits of data reuse, organizations need to adjust their focus on their data management and data operations practices.

Back to Contents

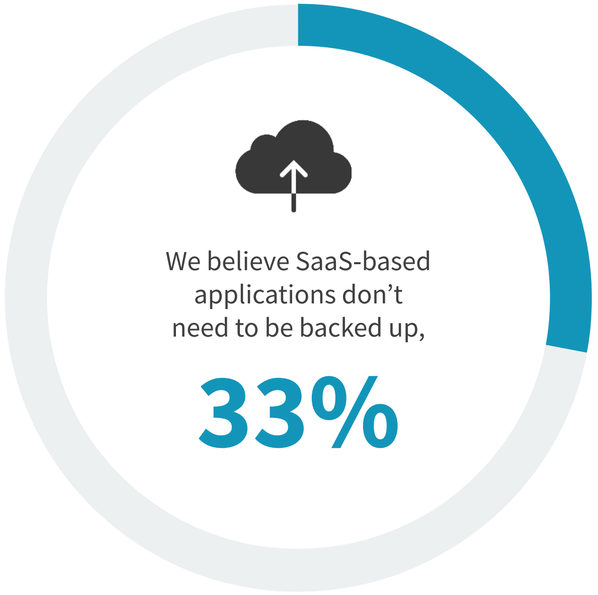
SaaS Data Backup: It's Your Responsibility

SaaS and Data Protection: The BIG Disconnect

ESG research reveals that SaaS usage is ubiquitous[1], and many organizations are relying on these cloud-based applications for mission-critical requirements. That's where ESG has identified a major disconnect: most people assume that SaaS application data still doesn't need to be protected. They conflate service availability — "My SaaS application is running" — with responsibility for backing up the data hosted in the service.

The responsibility for data and its governance does not change hands: it is always the organization's job to ensure that its data is compliant, protected, and recoverable. In other words, organizations need to protect the data in their SaaS services. The SaaS vendor will not do it for you! The recent end of life of the optional (and limited) data recovery service from a prominent SaaS should be a call to action for its users. User organizations must leverage ecosystem vendors in most cases to perform backup, disaster recovery, data compliance, and data management for them.

> ***"It is always the organization's job*** *to ensure that its data is compliant, protected, and recoverable."*



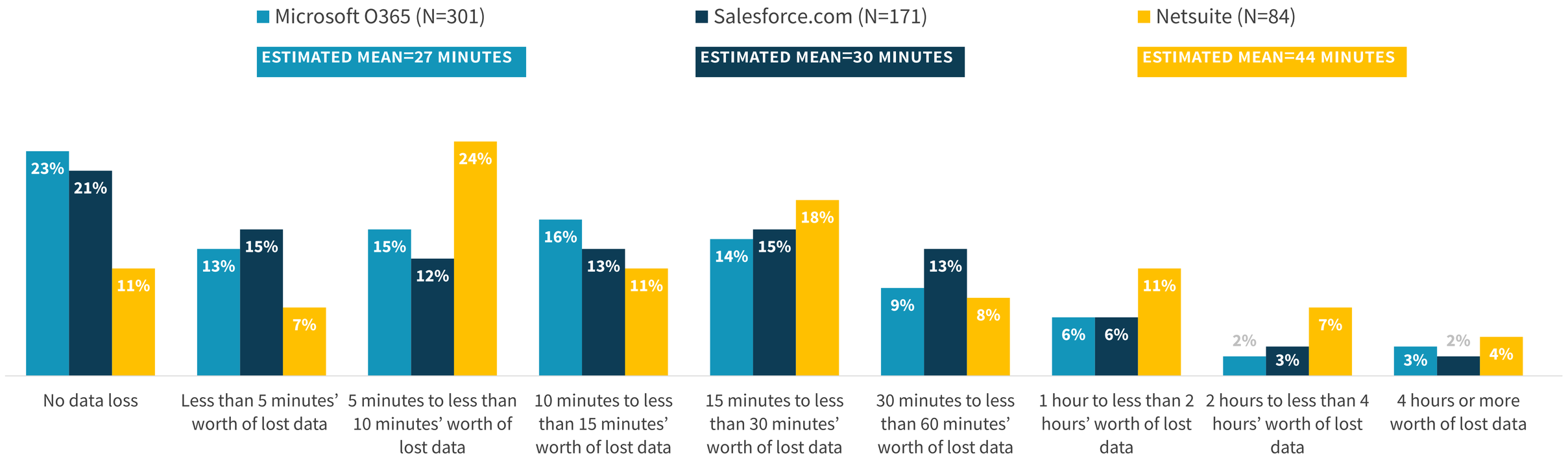
[1]ESG Research Report, *2020 Technology Spending Intentions Survey,* February 2020.

Back to Contents

SaaS RPO Tolerance

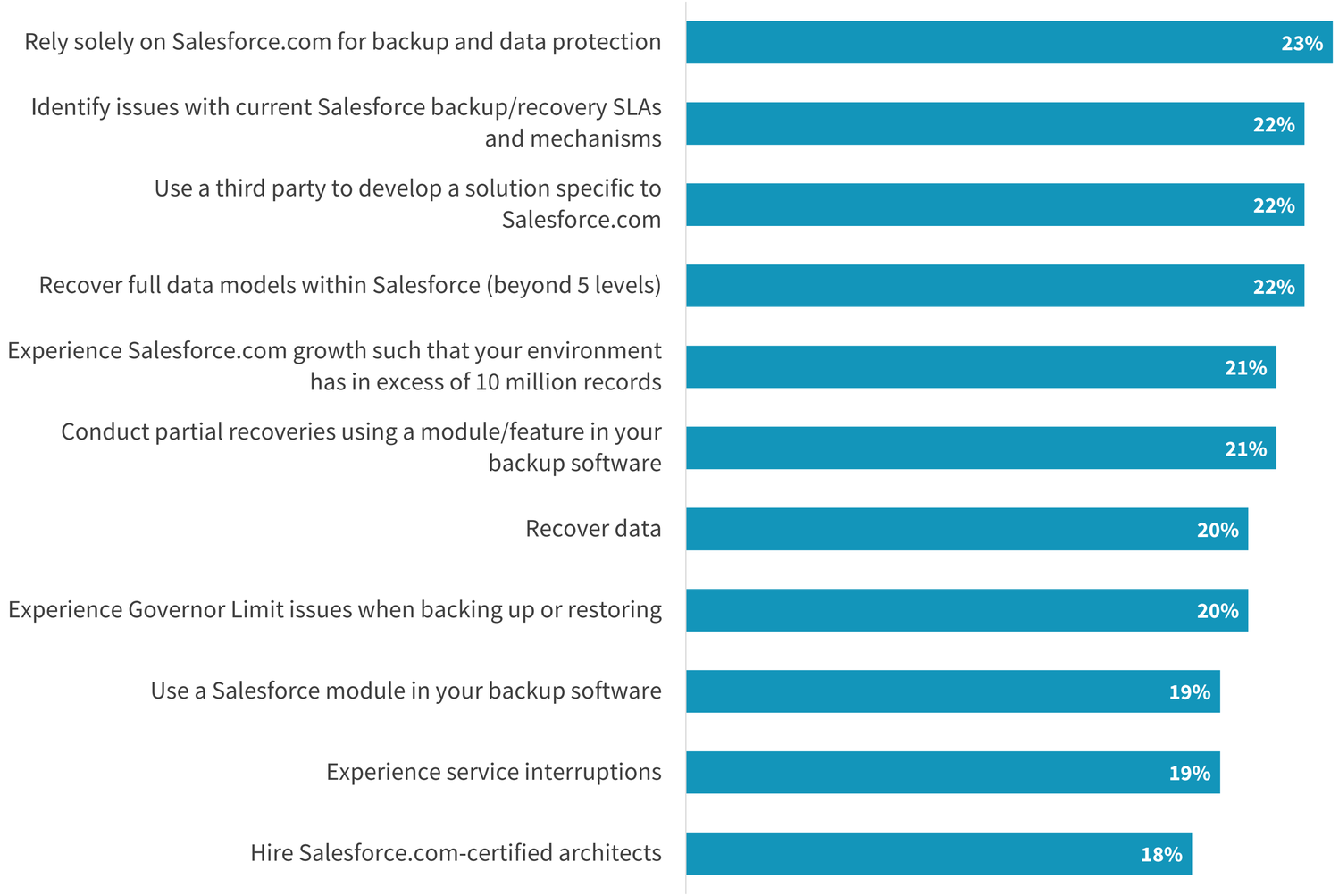
Zooming in on popular and mission-critical SaaS applications, never have expectations for RPO been so stringent. More than half of organizations expect RPOs lower than 15 minutes for Salesforce and Netsuite, and many expect zero data loss. This changes the game for IT professionals tasked with delivering on disaster recovery and business continuity: these data and processes are no longer in their data centers under their direct control, yet the business and IT KPI requirements remain.

RPO (i.e., amount of data loss) organizations can tolerate for the SaaS applications currently in use.



Back to Contents

Common Salesforce.com data protection issues.



Salesforce Data Protection Offers Many Challenges

The task at hand is far from easy in the context of an application like Salesforce. Beyond traditional best practices, additional complexity exists due to many challenges that can occur with this specific service. These warrant having a comprehensive backup solution in place. While the vendor offered a very basic backup, and in ESG's opinion, very inadequate service, it was recently discontinued (2020) in favor of the ecosystem. In order to protect Salesforce environments following enterprise best practices, in a way that is consistent with mission-critical KPIs, it takes a thorough understanding of the data models, schema, etc. This understanding helps foster consistent and unadulterated recovery… the full "state" of the application, in other words.

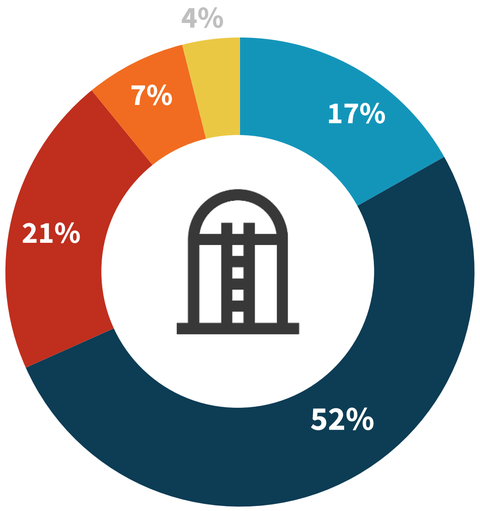
Back to Contents

Data Classification Is The Path To Successful Data Reuse

Most See Data Silos as a Problem Impacting IT Budgets and Strategies

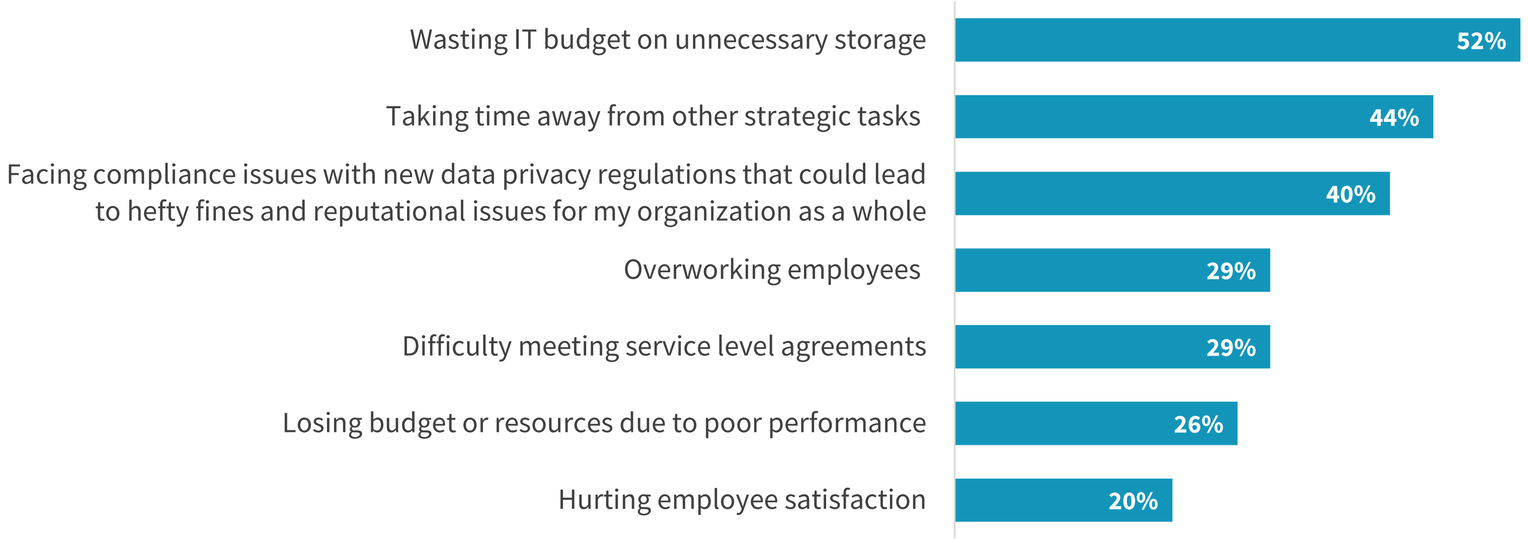
Most organizations see data silos as a problem impacting IT budgets and strategies. While there are integration tools, there are always challenges resulting in limitations to deliver on data protection KPIs. Silos are not good things for IT: they're expensive, distracting, and inefficient. Silos affect an organization's ability to deliver on compliance with data privacy regulations and often generate multiple copies of the same data, compounding the effects. Each SaaS application is yet another silo due to integration and API limitations pushing the limits of production environments. Organizations want to sometimes ingest the data into their engineering efforts or to create customer 360° views. In order to optimize the economics of data protection and data operations in general, including in the context of data originating from SaaS solutions, something has to change.

Are data silos a problem?



- Yes, it's a significant problem
- Yes, but we are making progress addressing the problem
- Not really
- Not at all
- Don't know

Risks attributed to data silos



Back to Contents

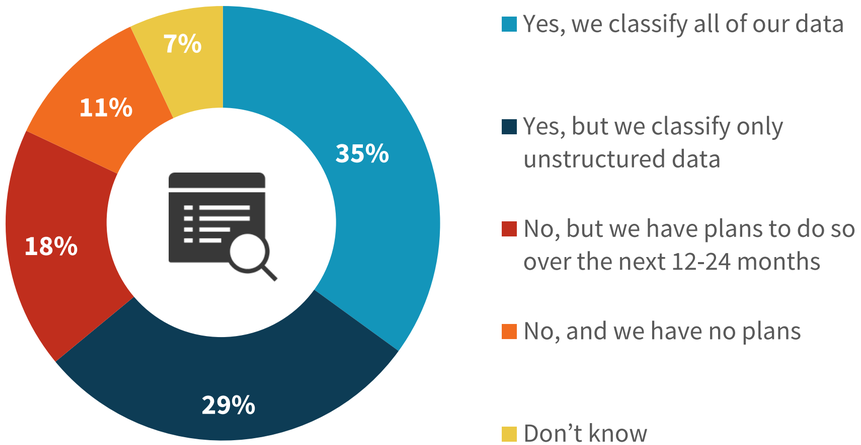
Most Classify and Sanitize Data to Some Extent

ESG research pinpointed that one way to alleviate the negative consequences of data silos is to classify all data. While a majority of organizations report classifying at least some of their data, classifying all data, meaning data both on-premises and in the cloud, leads to more effective business decisions and higher confidence levels. Specifically, organizations that classify all of their data are much more likely to make more informed business decisions and satisfy security and compliance requirements.

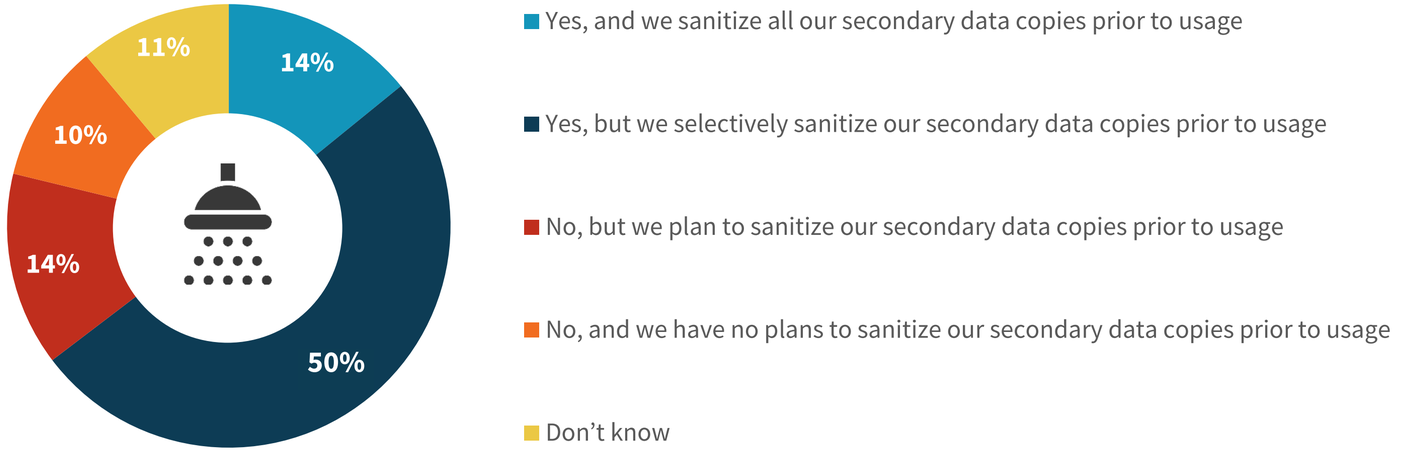
However, data classification is only a first step, in many ways. Once organizations know what data they have, what it is, where it lives, etc.—the context of it, in other words–it needs to be "sanitized." Understanding what the data is—the content—is a prerequisite to make the data compliant for reuse, in ESG's opinion. Organizations that report successful heightened business confidence based on their classification of data happen to be much likelier to also sanitize their data. This is an important process: organizations can't reuse data that is not compliant or they might risk perpetuating non-compliance across the business. Many recent privacy-focused regulations only emphasize this critical need and step in the data reuse process.

With so much data now in SaaS environments, the prominence of SaaS backup and data protection technology is even more evident, as these solutions can be leveraged as one of the mechanisms to support additional processes such as data classification and sanitization.

Data classification trends



Data sanitization trends



Back to Contents

PERCENT OF ORGANIZATIONS THAT:

	PROMOTERS (positive opinion of their organization's data reuse success)	PASSIVES (average opinion of their organization's data reuse success)	DETRACTORS (poor opinion of their organization's data reuse success)	"SUCCESS GAP" (between data reuse experience Detractors and Promoters)
Use cloud services for secondary data reuse	65%	48%	24%	41%
Classify all of their data	61%	41%	26%	35%
Sanitize all of their secondary data	39%	14%	11%	28%

* In order to segment according to the Net Promoter Score scale, respondents were put into one of the following groups based on the data reuse rating they gave their organization:

Promoters (score of 9 or 10): Positive opinion of their organization's ability to derive incremental business value from secondary data.
Passives (score of 7 or 8): Average opinion of their organization's ability to derive incremental business value from secondary data.
Detractors (score of 0-6): Poor opinion of their organization's ability to derive incremental business value from secondary data.

Data Reuse Promoters Profile May Provide Data Intelligence Blueprint

There is a strong correlation between certain data management activities and their impact on value-creation through secondary data use: making use of cloud services for secondary data reuse, classifying all data, and sanitizing all data. Indeed, IT professionals who have a positive opinion of their organization's data reuse success (i.e., promoters) tend to use cloud services for secondary data reuse (65%), classify all of their data (61%), and sanitize all of their secondary data (39%).* This creates a sharp contrast between promoters and detractors at the other end of the spectrum, or what ESG calls a success gap, which is one way to measure the intelligent data management chasm. Organizations that embrace advanced data management may help provide the market with a roadmap to success. These organizations need to revisit how they approach data and how they can leverage it as a business asset. In time, ESG expects that the success gap between experienced data "reusers" and those who aren't will translate into lasting competitive advantage differences – and the financial consequences that go with it.

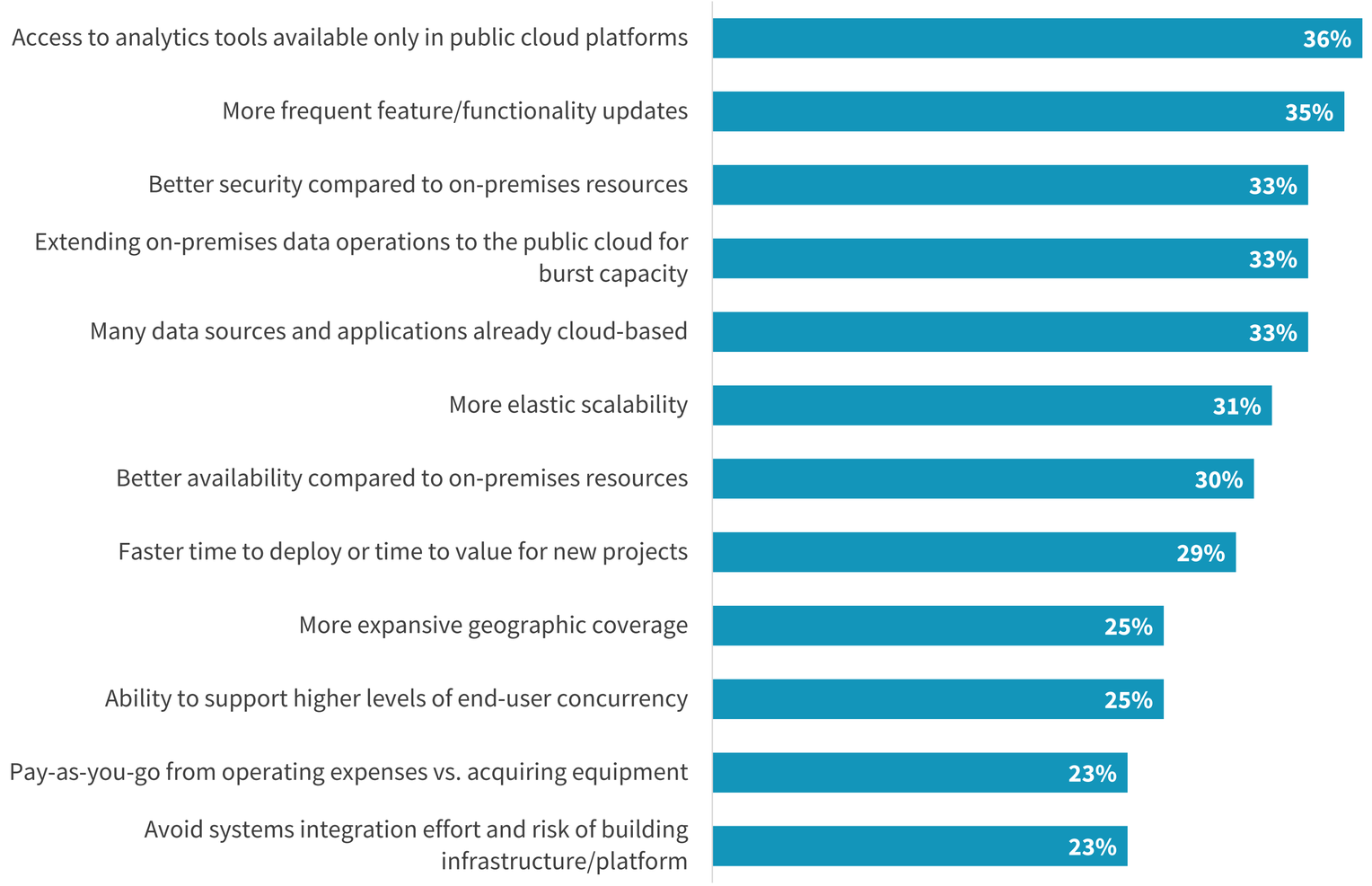
Back to Contents

Use Cases For Intelligent Data Management

Analytics and Operational Improvements Top Benefits of Public Cloud Secondary Data

Data reuse is the key to many business benefits. Data is the business, whether data-based services supplement physical goods or are the actual business. Against a backdrop of accelerated digital transformation due to the current health crisis, there has never been a more important time to optimize the return on one's data. Data reuse spans a variety of use cases, and benefits are reported in key areas such as operational efficiency, scalability and, topping the list, the ability to put analytics in play. On both the business and IT sides, it is worth noting that the top benefit is analytics. The more you can understand about the past and the present, the better you can model your business and operations. It should also be noted that the ability to optimize the development and operations of key business applications is also a top benefit, meaning that successful data reuse helps in optimizing the business directly where it happens.

Benefits attributed to sending secondary data to public cloud services.

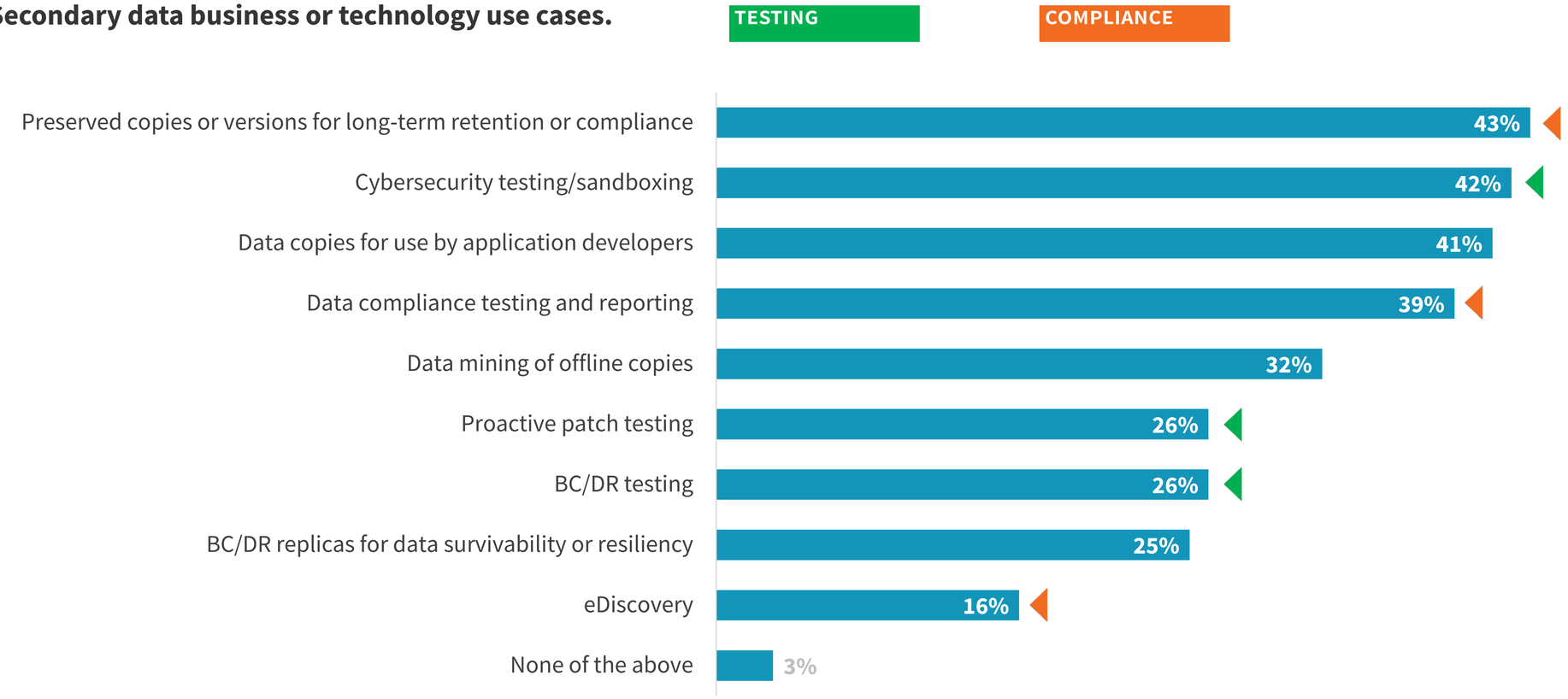


Back to Contents

Beyond Backup: Secondary Data Use Cases

There is a variety of use cases for data reuse that can be grouped in two main categories: testing and compliance. While these use cases are very different in their nature and objectives, they bring data and the need for advanced data operations to the forefront. Taking a closer look at the top use cases, we also see that they can all have significant business impacts but also require a high degree of data integrity and traceability.

Secondary data business or technology use cases.



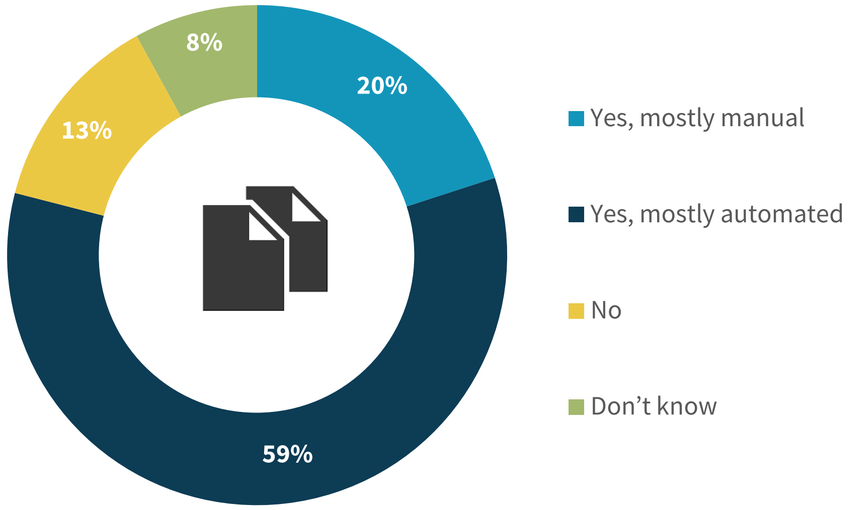
From a practical standpoint, “dumping” data from a SaaS workload, for example, without having performed full compliance checks on whether it can be reused or is not good enough. The data has to be clear of cyber threats, as well, which is where testing helps. It also has to be traceable, meaning organizations need to track data’s full chain of custody/events.

Back to Contents

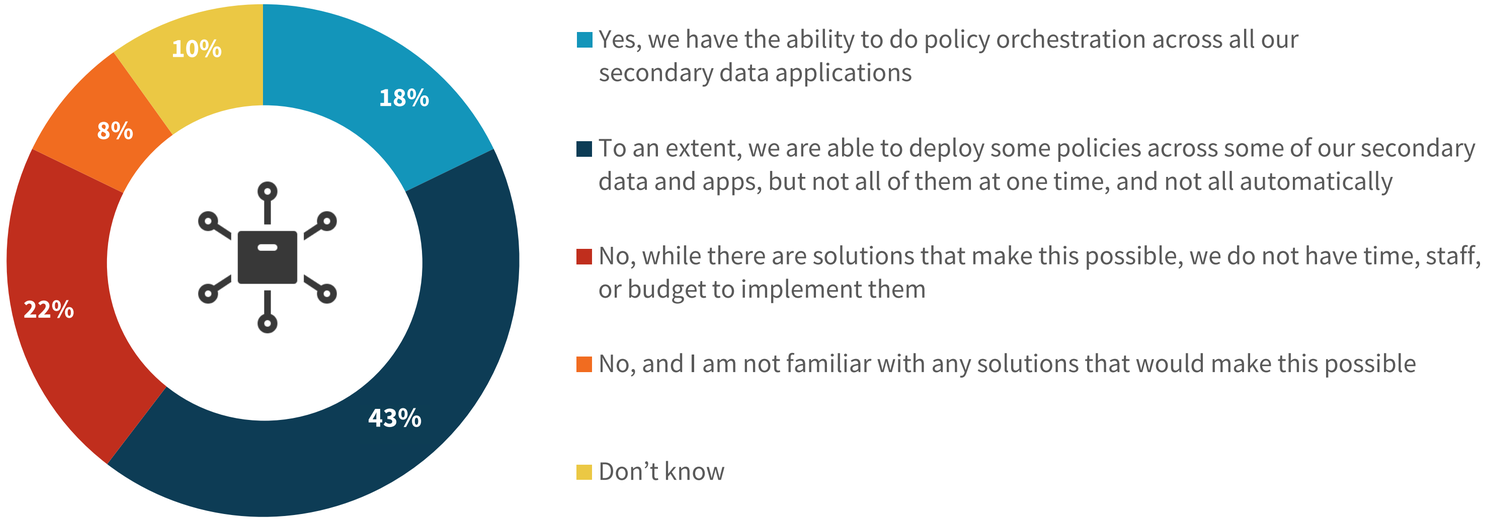
Majority of Organizations Have Built-in Copy Automation, But It is a Difficult Road to Secondary Data Reuse

As business needs evolve, the IT infrastructure has to follow and redesign itself. Current mechanisms for data reuse in place today were designed for needs that have significantly evolved and now require advanced automation and orchestration of data and processes. Data reuse automation has been "retrofitted" rather than built-in, which is why many organizations report limited implementation of uniform policies across all secondary data. Having the capabilities to automate and deploy uniform data policies is the next big challenge. In the new hybrid world of digital transformation and heavy reliance on cloud and SaaS, creating multiple, uncoordinated, and separate processes for different uses cases, tacking on disparate tools, and generating costly data replication is just not scalable. The focus has to be placed on the common denominator: the data itself, and its intelligent management.

Usage of technology that manages copies of data.



Ability to deploy uniform policies across all secondary data.



Back to Contents

The ESG Intelligent Data Management Model

The requirement for context and content about data is becoming more acute as new regulations and the need to use data to support digital transformation are changing the role of data in the enterprise. Data has to be more intelligent to be more easily shared across an organization. The ESG Intelligent Data Management Model highlights how organizations can evolve past the data management chasm.

Data that was originally on-premises is now also in the cloud, creating a hybrid infrastructure with enhanced complexity for IT. Data protection has evolved to not only provide data protection and data movement on premises, but also to the cloud and in the cloud. This cloud-enabled stage is where the market is today and where many organizations are adapting their data protection solutions. This is particularly important in the context of SaaS applications, a delivery model in which the data and service are not delivered by in-house IT. The data governance requirements placed on organizations that use SaaS solutions, however, do not change: it's their data and their responsibility to protect it. But protection is not enough to get to the next level.

In order to realize the benefits of data re-use, organizations need to adjust to focus on their data management and data operations practices . To "graduate" to the data intelligence stage and cross the data management chasm, they need to use modern solutions that do not exclusively focus on the traditional use case of backup and recovery, but rather look at data more holistically to understand its context – what type of data, what system produced it, etc., – and its content (personal identifier, for example) so that it can be reused.

As organizations progress from one stage of the Intelligent Data Management model to the next, they encounter a number of hurdles along the way. While specific challenges vary drastically, each stage has a key linchpin that needs to be dealt with in order to progress:

Back to Contents

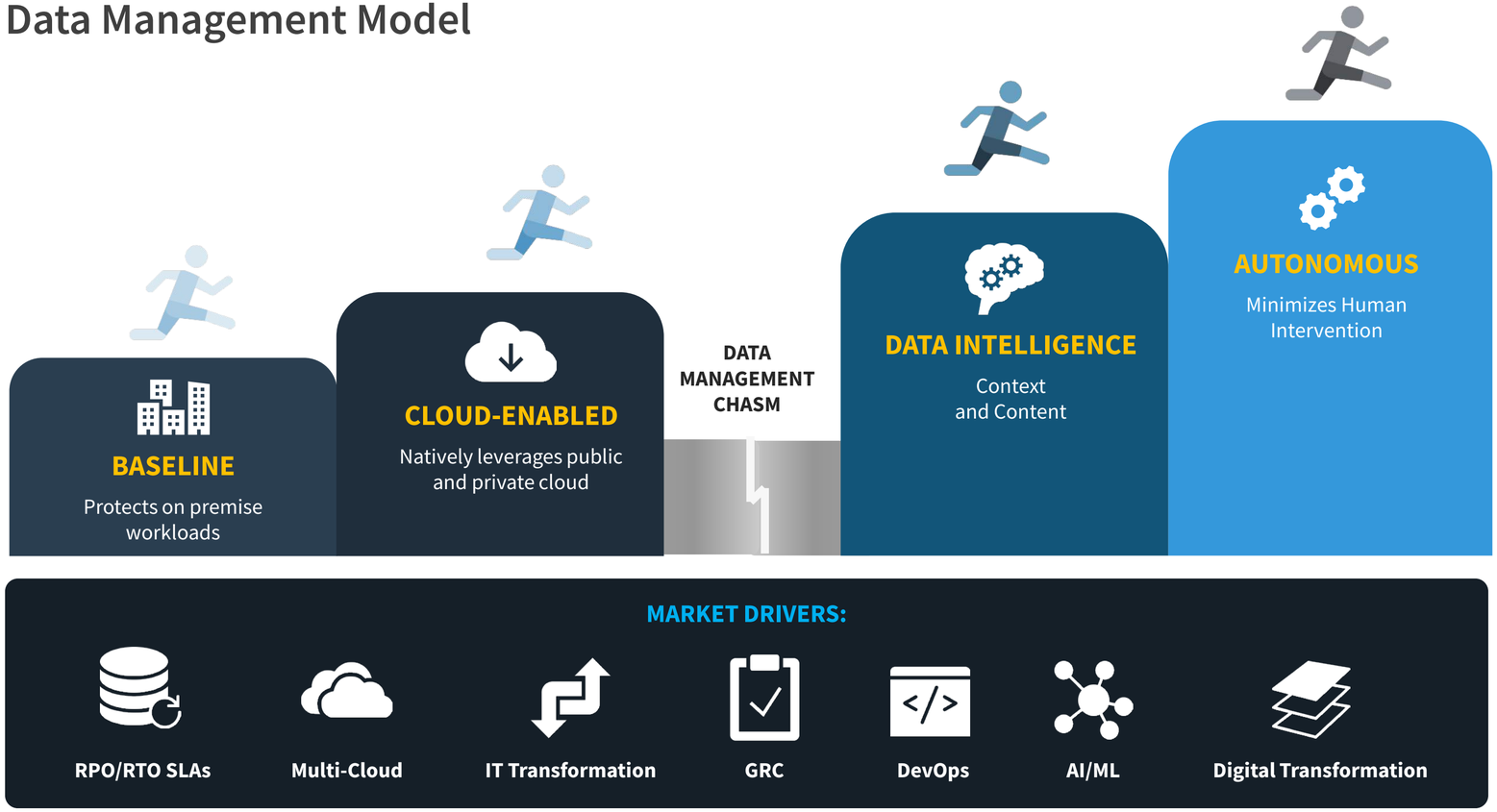
1. BASELINE:

To progress from this stage to "Cloud Enablement," an organization must acknowledge and extend the same levels of data protection that it uses for on-prem workloads to its broader ecosystem of third-party SaaS or cloud applications. The realization that compliance and regulatory requirements must be extended to an organization's sensitive data stored in SaaS applications is one of the key drivers here - but there are others.

2. CLOUD ENABLEMENT:

To progress from this stage to "Data Intelligence," an organization must identify and build specific data reuse cases that would impact revenue, customer retention, or security scenarios. This must be done in concert with business stakeholders. The recommendation here is to start small, i.e., if an engineering or business intelligence team is already reusing application data by ingesting it from a SaaS application, making that data available in a scalable, cost-effective cloud storage facility that is owned by the organization would likely reduce application impact, improve operational or storage costs, and make the data available to other parties within the organization.

The ESG Intelligent Data Management Model



3. DATA INTELLIGENCE:

The move from intelligent data use to taking autonomous or automated action based on that data is yet another big leap for most organizations. As repeatable reuse patterns emerge, organizations find themselves repeating manual actions based on what has worked in the past. Those actions can become more autonomous. In order to move from intelligence to autonomy, organizations need to identify and codify a set of automated actions triggered by change data. Examples might include rolling out a service crew to a connected device based on streaming data that indicated imminent failure, or automating alerting and action based on dips in NPS or CSAT score.

Back to Contents

Get More Value with GRAX

This report highlighted the tremendous benefits that can be derived by businesses that implement a SaaS data backup solution that enables them to traverse the maturity model from basic backup to data reuse. This is precisely why GRAX was built. GRAX is the only SaaS data backup, archive, and recovery tool that lets customers maximize the value of their historical cloud application data. It does this by letting them take full ownership and control of their data, store it anywhere, and access it everywhere. The most iconic companies in the world that we buy from daily, wear on our wrists, have in our pockets, or rely on to power the internet all use GRAX. For them, GRAX is more than just an insurance policy—it is a way to unleash the power of their historical application data and use it to drive business continuity, regulatory compliance, strategic advantage, customer retention, and revenue growth.

To get started, visit grax.com.

LEARN MORE

GRAX

ABOUT ESG:

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

Back to Contents