GRAX

E-BOOK

# 3 Reasons You Need to Take Back Ownership and Control of your SaaS Data

# Table of Contents

INTRODUCTION

# Who owns your data in your SaaS cloud applications? What about your data in 3rd party apps that plug into those apps?

## INTRODUCTION

# The question of data ownership in cloud applications turns out to be a significant one, not just for compliance and security reasons, but for reasons directly tied to an organization's ability to maximize the strategic value of its data for things like customer retention and revenue growth.

In this e-book, you will learn about:

- A new definition of data ownership in a world of SaaS cloud applications
- Three ways data ownership can be used to unlock business continuity and growth
- Critical implications for compliance, security and business continuity
- Real-world examples of organizations using data ownership for revenue growth
- What you can do to get your organization on the right path

1. DATA OWNERSHIP

# A new definition in a world of SaaS applications

## 1.1 DATA OWNERSHIP - A NEW DEFINITION

While almost all SaaS applications tell you that your organization retains “full ownership” of the data, which you store in their tools, this often stands at odds with reality. Particularly when you try to do something more than what you initially intended to do with your data. Some use your data to lock you into their app by transforming it into a proprietary format. While others might give you a raw data export in a static format, which you then have to manually manipulate to maximize value. Nuances and limitations abound, and the reasons for their existence are often not nefarious – designing true data ownership into SaaS customer experiences is laborious and is not always immediately valued (or paid for) by all customers.

But this is rapidly changing – fueled in equal measure by both regulatory pressures and competitive dynamics in just about every single market. In a world where our data traverses numerous systems, geographies, data silos, and 3rd party clouds, “data ownership” must be redefined across two key dimensions:

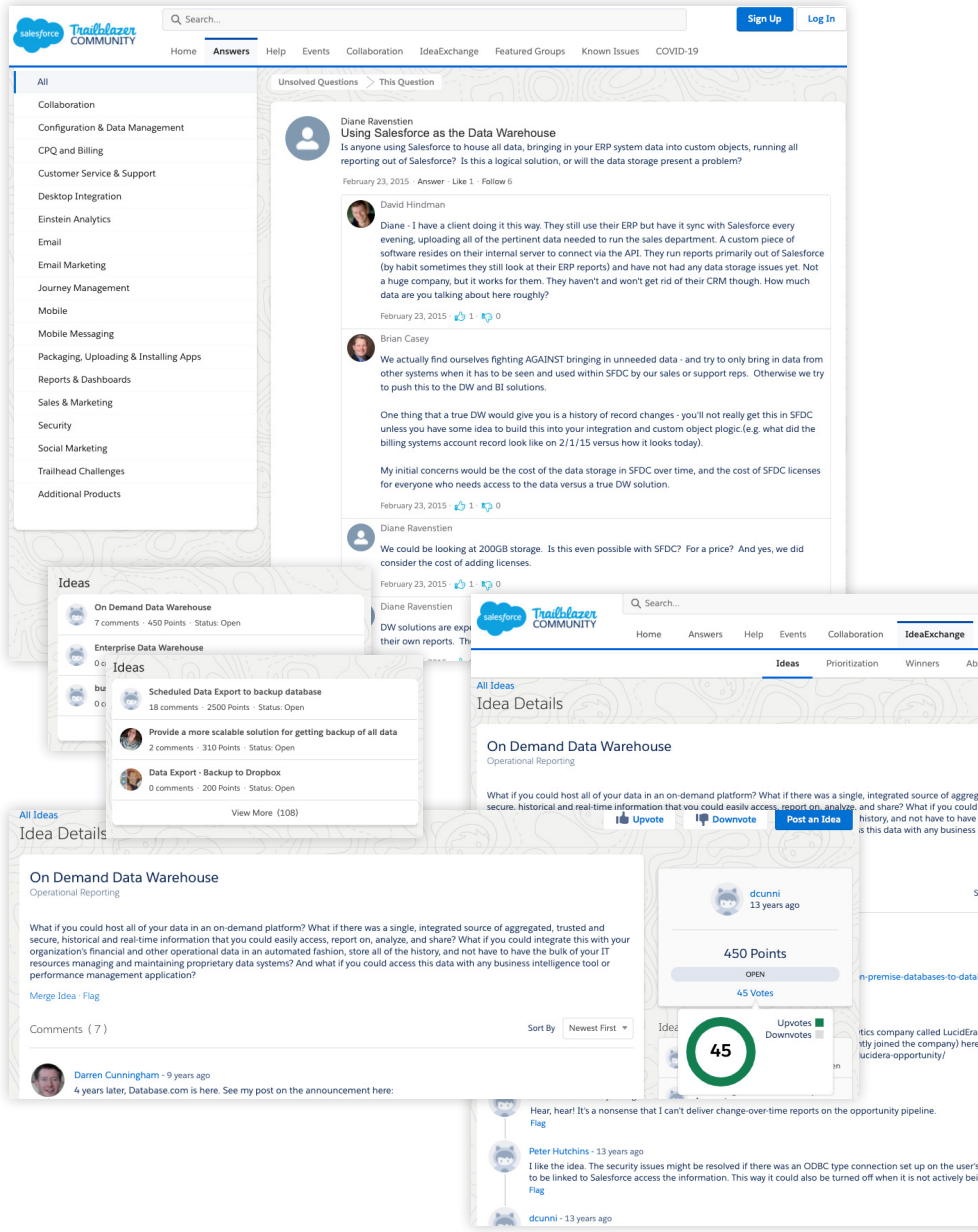
### Transmission

How and where the data moves

### Storage

Where data resides

In the example of a CRM, such as Salesforce.com, customer data is both stored and transmitted not only on Salesforce’s infrastructure, but also across a myriad of 3rd party applications and custom API integrations with customer systems. There are thousands of discussions happening in the Salesforce Trailblazer community, where members are asking each other for advice about how to best move data into or out of Salesforce. The ultimate intent is to maximize the strategic value of all data both inside and outside of the application by taking action on it everywhere it can deliver impact.



# Regulations Require a New Way of Thinking

Regulatory, governance and security pressures create a tremendous amount of constraint here, particularly for larger organizations. Highly-regulated industries often require organizations to maintain full auditability of their data's Digital Chain of Custody,[1] not to mention full ownership or control of where sensitive data is stored.[2] The need goes well beyond merely having direct access to critical application data during an application outage. But it's not just regulators or CISOs that care, at least indirectly, about the transmission and storage of SaaS application data. Product development, business intelligence, customer success, and revenue teams also care about this, even if they are unable to consciously acknowledge it. They call on Data Operations teams to make data available outside of cloud applications for downstream consumption, for use in new digital products, global selling initiatives, forecasting, and analytical projects – the list goes on.

With these two competing tensions – security, governance, and regulatory pressures on one side and the desire to maximize the availability of data on the other – data professionals are often left trying to do the impossible: balancing the two while trying to please everyone.

**Digital Chain of Custody**

/'dɪdɒɪt(ə)l / tʃeɪn / ɒv / 'kɒstɒdi

An irrefutable record of ownership and changes that data undergoes as it travels across all systems over time.

**[1]** See Appendix A.
**[2]** FINRA and WORM are examples of regulations that require ownership and control of storage environments. See Appendix A for more information.

## 1.2 DATA OWNERSHIP - REGULATIONS

The result is a partial compromise on all fronts that sometimes exposes organizations to undue security or compliance risk and compromises an organization's ability to get long-term revenue impact and value out of their data. It's no wonder billions of dollars continue to be paid in fines related to sensitive data breaches that are often difficult or impossible to trace,[3] while other organizations leave upwards of $60M of topline revenue on the table every year due to data quality or access-related issues.[4] There is also a downstream impact on the analytical value of data, with organizations like Gartner estimating that 80% of analytical insights actually don't deliver any business value whatsoever.[5]

> **"$60M of topline revenue on the table every year due to data quality or access-related issues."**
>
> "HOW TO CREATE A BUSINESS CASE STUDY FOR DATA QUALITY IMPROVEMENT"
>
> **GARTNER**

**[3]** Cost of a Data Breach Study. (2020). IBM. https://www.ibm.com/security/data-breach
**[4]** Moore, S. (2018, June 19). How to Create a Business Case for Data Quality Improvement. Smarter With Gartner. https://www.gartner.com/smarterwithgartner/how-to-create-a-business-case-for-data-quality-improvement/
**[5]** White, A. (2019, January 3). Our Top Data and Analytics Predicts for 2019. Gartner. https://blogs.gartner.com/andrew_white/2019/01/03/our-top-data-and-analytics-predicts-for-2019/

2. SAAS DATA BACKUP

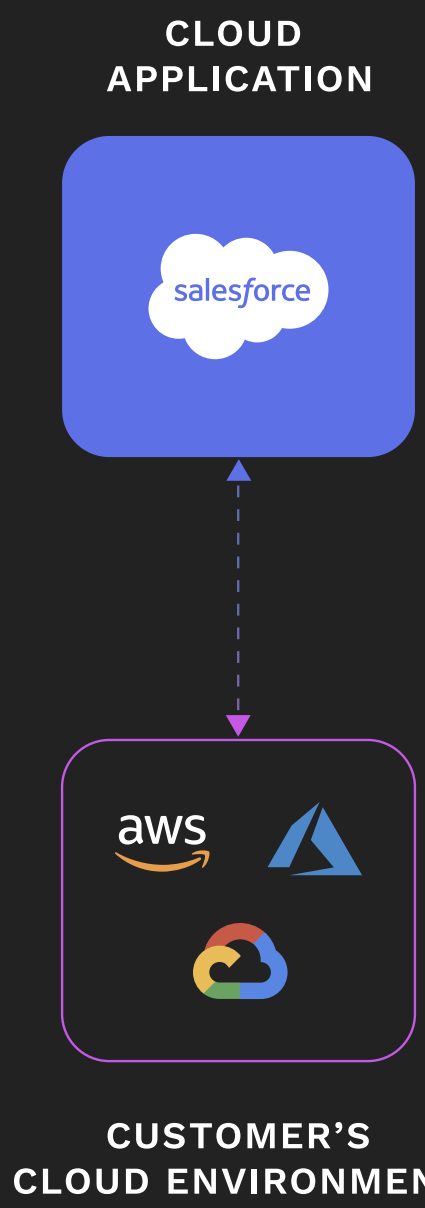
# The Cloud Application Data Ownership Hat Trick

## 2.1 SAAS DATA BACKUP

This balancing act represents a more resonant parable that we all learn at one point or another in life:

> ***how* you do things is often just as important as *doing* them in the first place.**

In the context of SaaS application data, one solid move that organizations can make early on is to take back control of where their data is stored and how and where it is transmitted. At first glance, this might seem like a liability or perhaps “nice in theory but impossible in practice,” there are a number of “easy buttons” becoming available in the market – tools that let customers store their SaaS application data in their own cloud environments (AWS, Azure, GCP), and to transmit that data over trusted, customer-controlled data pipelines. Whether organizations realize it or not, they are already liable for their sensitive customer data stored in 3rd party SaaS applications – ownership is no longer a liability – it’s a strategic advantage.



## 2.1 SAAS DATA BACKUP

One way of taking ownership of SaaS application data is to use an old tool for a new purpose. Deploying a backup and archive tool for your cloud application(s) can be a deceptively simple method of capturing both historical data (backup) and production (archive) data into your organization's data lake. While these tools are commonly thought of as an insurance policy in the disaster recovery space, some vendors are now looking beyond Recovery Point Objectives (RPO) and Recovery Time objectives (RTO) by allowing customers to store their backup and archived data in their own cloud data lakes. A handful of vendors are even eliminating the need to have customer data transmitted over their servers altogether. Customers can then take full ownership and control of their cloud application data, with no middleman or proxy for sensitive customer data in transit. A few vendors even allow backup and archived data to remain available in production in the SaaS application itself – effectively allowing customers to move their data completely under their governance umbrella, without losing actionability on the data in their cloud application environments.

Some of the most iconic companies in the world – that we buy from daily, wear on our wrists, have in our pockets, put in our bodies, or rely on to power the internet – have already started to take ownership and control of their SaaS application data using cloud data backup tools. What does this idea of SaaS application data ownership do for them?

> **Is it just an insurance policy or are there more strategic and competitive dynamics at play here?**

# The Impact of SaaS Data Ownership on Compliance, Customer Retention and Growth

The truth is that cloud applications are some of the most critical endpoints where organizations take action on their data. Actions include the need to:

- Meet regulatory needs – such as fulfilling GDPR, FDA, FINRA, or other requests
- Optimize customer retention – by delivering excellent customer service and support experiences
- Drive revenue growth – new product development, e-commerce, account-based selling and marketing, business intelligence and analytics, etc.

The friction, lack of visibility, or siloing of data between these applications require a combination of careful vendor selection, manual data management, and centralized data repositories (such as cloud data warehouses) in order to create the plumbing necessary for data to flow between systems freely. According to McKinsey, this is now a major imperative for most organizations as

> **"Leaders need to unearth the valuable data residing in discrete silos across the organization and build the right plumbing to deliver game-changing insights. And do it fast."[6]**

Even when that data freely or flexibly flows between systems, organizations lose important attributes of the data, such as metadata and change data. These losses in fidelity happen when the data leaves one application and traverses the DataOps ecosystem into another application – and they all serve to diminish the long-term strategic value and impact of data.

**[6]** Gottlieb, J., Ho, T., Kanagasabai, K., Rowshankish, K., & Weinberg, A. (2019, February 14). How to maximize the returns from your data. McKinsey & Company. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-blog/how-to-maximize-the-returns-from-your-data

# The Great Migration of Cloud Application Data to Customer Data Lakes

More and more organizations are taking their production and historical SaaS application data (and metadata) and moving it into their cloud data lakes – making all of it fully accessible to their entire data operations ecosystem.

> **The critical compromise that more advanced organizations are no longer willing to make is this: they don't want to remove the data from the cloud application production environment(s).**

However, this poses significant challenges, particularly when data storage issues in the cloud application negatively impact application performance or simply become too cost-prohibitive based on what the application provider charges for storage overages. Inevitably, a 'data archiving strategy discussion' ensues – where organizations have to make decisions about which data to keep in the application and which they would be willing to "put in cold storage" by archiving it out of the application. All of this stands in strong dissonance with the reality that we all live and breathe today: data storage is cheap and ubiquitously available in the cloud.

3. KEY REASONS

# 3 Keys to Maximizing SaaS Application Data Value

# Ownership, Access, and Fidelity

It turns out that there are three critical keys to maximizing the long-term organizational value of data locked in SaaS cloud applications:

**Ownership**

Taking true ownership of where SaaS application data is transmitted and stored

**Access**

the ability to access data both inside and outside of the SaaS application(s)

**Capture**

the fidelity or frequency with which changes in data are captured

# Reason #1: Data Ownership

The first principle has as much to do with regulatory compliance as it does with growth. If you can take full ownership of your SaaS application data, you will be in a better position to maximize its strategic value across your organization. But before we go there, it's important to linger on the regulatory, security, and governance impacts of data ownership.

Most global and regional regulations require organizations to[7]:

FDA

"IMPLEMENT CONTROLS, INCLUDING AUDIT TRAILS..."

**(FDA, PART 11)**

PCI DSS COMPLIANT

"IMPLEMENT AUTOMATED AUDIT TRAILS"

**(PCI-DSS)**

"IMPLEMENT TARGETED POLICIES AND PROCEDURES TO ENSURE ONGOING MONITORING OF CLOUD-BASED PLATFORMS"

**(SEC RISK ALERT '19)**

**WORM**

"WRITE ONCE, READ MANY"

**(WORM)**

AICPA SOC

"CREATE AUDIT TRAILS PROVIDING SUFFICIENT CONTEXT"

**(SOC)**

Gramm-Leach-Bliley Act COMPLIANT

"KNOW WHERE SENSITIVE CUSTOMER INFORMATION IS STORED AND STORE IT SECURELY"

**(GRAMM-LEACH-BLILEY SEC 302, 404, 409)**

Coupled with the need for regional data segregation (particularly with European data), the requirements become untenable for most organizations. IT teams are often forced to either walk away from numerous SaaS applications that cannot satisfy such complex ownership and traceability needs, or run the risk of running afoul of global regulatory standards. Once again, professionals are faced with the tradeoff between agility on one side and compliance on another.

[7] See Appendix A.

## 3.1 REASON #1: DATA OWNERSHIP

The problem only gets worse when looked at through the lens of governance or security. Recovery Point Objectives (RPO) continually tighten from weeks to days to hours to minutes – often converging with traceability requirements that force organizations to ostensibly move to streaming change data capture in order to meet all needs.

A simple thought exercise on traceability can be illuminating:

- Say your customer data was a large pile of cash laid on a table in the middle of a big room full of people. The comparison bears a resemblance to reality since this is exactly how hackers view customer data stored in 3rd party systems.
- You train a camera on the pile of cash and even put an armed guard in place to watch over your tempting target, and just as you start to feel safe, you kick off the industry-standard operating procedure:
- You turn off the lights in the room and begin to briefly flip them on and off again at one day increments - this is called snapshotting.
- A governance or security expert comes along and says, “You should really flip those lights on and off again at one-hour increments. And in some cases, maybe in 15-minute increments.” You’ve now arrived at the current industry standard of ‘high-frequency’ snapshots.

## 3.1 REASON #1: DATA OWNERSHIP

But what about those 14 minutes and 59 seconds of darkness in between that 1 second of visibility? Is that enough time for someone to snatch the cash and cover up their tracks? In internet time, 14 minutes and 59 seconds is an eternity.

The other recourse organizations often have to protect their most prized possession is to turn to field audit trails available in certain applications, such as Salesforce.com. There, decisions have to be made about which data is traced and which is not (no truly unlimited audit trails exist), with the ultimate goal of closely watching the most critical data amid a sea of millions or billions of objects or records.

Ultimately, the more viable solution, in the long run, is for organizations to take ownership of their SaaS application data, to control the frequency with which it is captured, how it is transmitted, and where it is stored. SaaS data ownership once again forms the regulatory, governance, and security bedrock of an organization's modern data ecosystem.

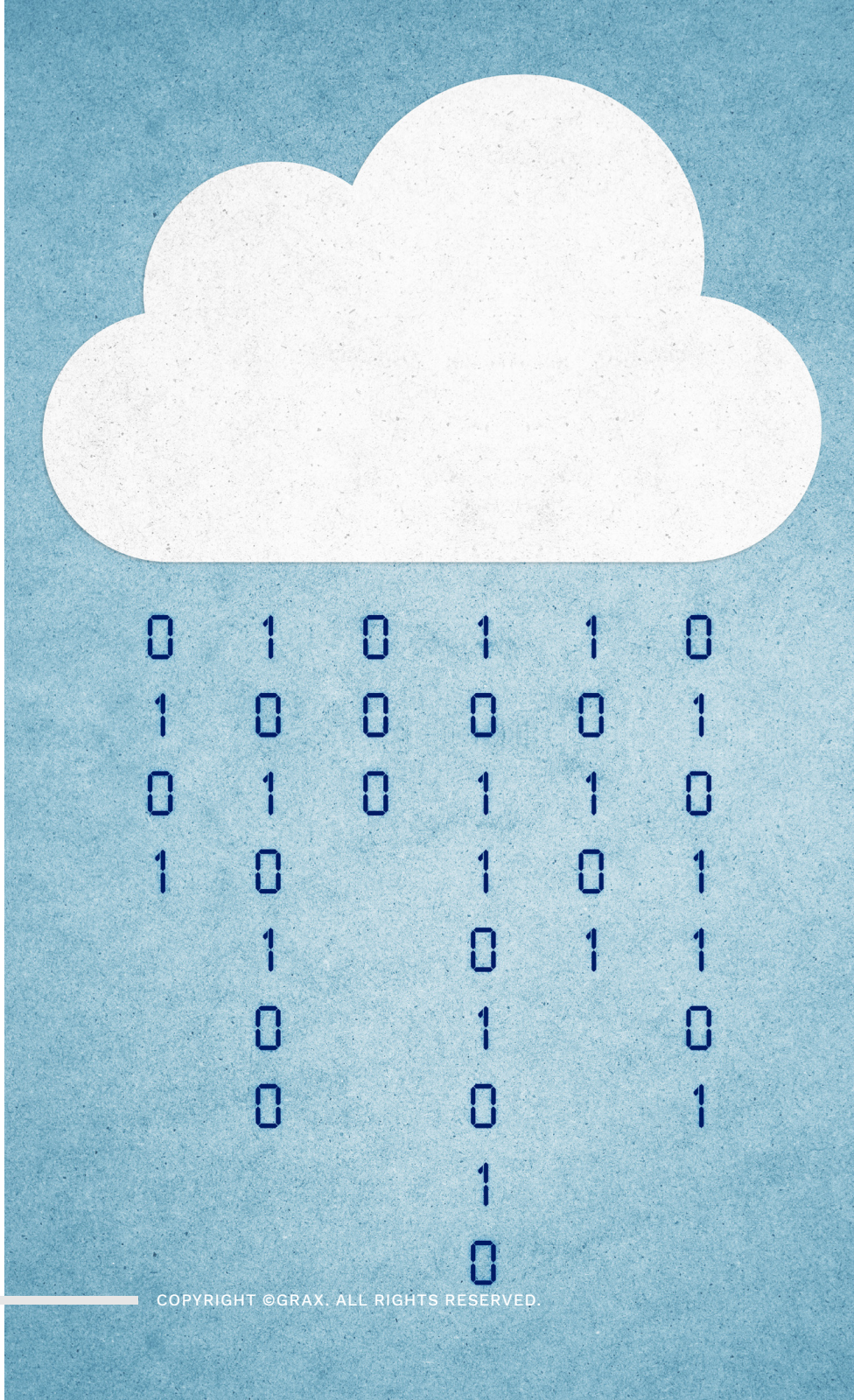
# Reason #2: Data Access

### The Key to Unlocking Data Flexibility and Agility

The second principle, Data Access, is critical because it allows organizations to capitalize on historical SaaS application data both inside and outside of the individual applications in which it is stored. The ability to 'color outside the lines' of intended purpose designed for data in the application itself unlocks creativity with multi-source data aggregation, new product development, digital transformation, and so on.

The dirty little secret with a lot of SaaS applications is that they use customer data to lock their customers into their services – a cynical view might go so far as to say that SaaS applications hold customer data hostage and lease it back to them. The truth here is, again, not always so clear cut. Customers amass large volumes of data and metadata inside of the SaaS tools as they use them - the "lock-in" or "stickiness" effect often naturally emerges from the continued use of the tool. Metadata, in particular, is often closely tied to the SaaS application itself – it is the layer that imposes additional taxonomy or structure, which in turn allows the organization to further action on the data inside of the cloud application.

> **So why would organizations want to access an application's data elsewhere in their DataOps ecosystem?**

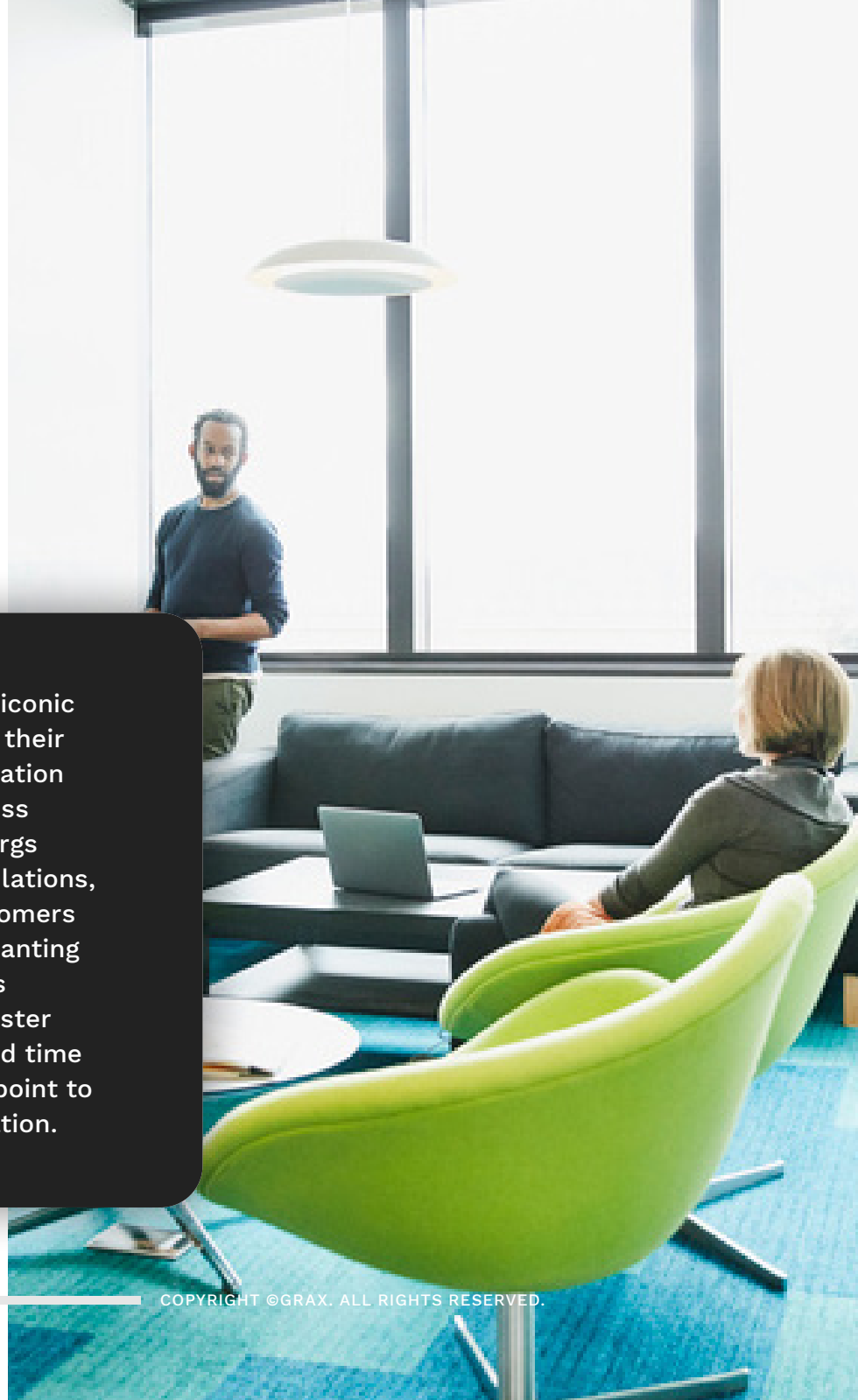


## 3.2 REASON #2: DATA ACCESS

### 360 Degree Visibility

It's very valuable to unify or "master" data across many disparate sources – this is why we are seeing technology giants like Salesforce and Snowflake talk about "Customer360." In the healthcare space, this takes on the name of Master Data Management (MDM) and Data Aggregation. Regardless of the name, it all tends to boil down to tokenizing a specific entity's record with the same unique ID across disparate systems and data sources, and then assembling a '360 degree view' of the entity comprised of all attributes across all sources. The ability to do this often has a direct revenue impact:

A global outsourcing leader who works with some of the most iconic companies in the world wanted to unify reporting across all of their customer accounts. Every month, 70 people across the organization took weeks to manually consolidate records of all activity across all customer accounts spread across hundreds of Salesforce Orgs globally. The organization needed to adhere to global data regulations, while at the same time be able to accurately invoice their customers for completed work. Mastering the opportunity record while granting multiple orgs access to it allowed for the record to reside in its original org while being visible and reportable in a separate master invoicing org. This 10x reduction in reporting-overhead improved time to revenue for the organization – and served as a jumping-off point to a much deeper digital transformation initiative for the organization.



## 3.2 REASON #2: DATA ACCESS

### Orchestrated Action

As we saw with the example above, data aggregation and mastering is often the beginning of an innovation S-curve for a business. Once customers develop ubiquitous visibility into their target entities (prospects, customers, partners, etc.), they can better orchestrate actions against those targets across disparate teams and systems in their business:

A multi-national payment processing organization in the midst of a mergers and acquisition transaction with another entity wanted to understand the overlap in target accounts between both entities, so that they could maximize cross-selling revenue potential immediately after the transaction was completed. Usually, what happens in these types of scenarios is that a monumental effort to merge people, process, and technology kicks off once the transaction occurs: data operations, sales, support, and other teams consolidate application instances (e.g., Salesforce Orgs) and teams begin the long process of alignment and "Org consolidation," while commercial operations teams scramble to cobble together a picture of the newly-formed entity via manual, ad-hoc reporting. The effort takes years and millions of dollars to accomplish – all while actually inhibiting competitive advantage for the newly-combined entity in the short term. In situations where organizations have overlapping SaaS applications, such as CRM instances, the issue is further exacerbated by each organization's internal data siloing. This naturally occurs within the same company across various regions (organizations often run separate instances or "orgs" of a CRM application depending on the region).

## 3.3 REASON #3: DATA CAPTURE

Here, taking ownership of the application data and absorbing it into the organization's data lake for aggregation and cross-application exposure can significantly reduce time to value and drive immediate impact on top and bottom-line revenue growth. It's not often intuitive or direct, but the connection between SaaS application data ownership and business growth is often always lurking in the background.

# Key #3: Data Capture- a.k.a. Data Fidelity

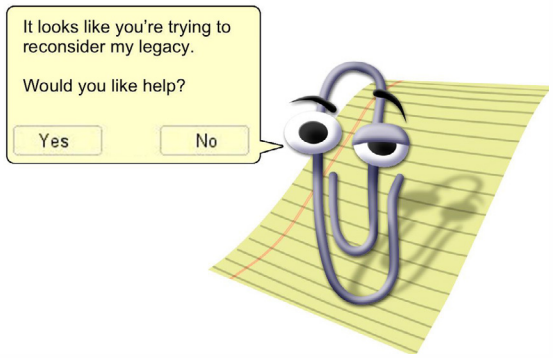
If you have taken ownership and control of your historical application data and you have maximized access to that data both inside and outside of the application, the only frontier left to conquer is the frequency with which you capture data – a.k.a. the "fidelity" of that data.

### Why is frequency important?

Beyond the security "thought exercise" given earlier in this paper, the frequency of data capture connects to a more fundamental principle of human nature: evolution. Humans and organizations are pattern-recognition machines, always trying to spot and capitalize on emerging patterns that either signal threats to their existence or opportunities for growth. The frequency with which one captures the most minute changes in an environment is akin to how closely one "pays attention."

## 3.3 REASON #3: DATA CAPTURE

# Global tech giants like Facebook, Google, and Amazon have known this and used this to their strategic advantage for years.




**- NEW YORK MAGAZINE**

The emergence of new patterns in purchasing behavior, content consumption, or website visits signal a change in an individual's needs, which in turn signal opportunities for organizations to fill that need in some way.

Some organizations are starting to understand that they don't actually need to amass the same breadth of data as the tech giants do in order to compete against them effectively. Increasing the fidelity with which it is captured (the frequency of data capture) can be more effective than increasing the breadth of data captured (the number of sources). More subtle patterns can be spotted as they emerge from minute changes in commonly discarded or overwritten data objects or fields. The analysis of covariance between data points that either precipitate one another or move in unison can yield far more effective results than broad swaths of data that may be unrelated or frozen in time. The Internet of Things (IoT) industry has known this for some time – subtle changes in narrower sets of leading indicators for part failure, user frustration, or environmental interaction can be easier and more meaningful to mine than the sum of all search data in the entire world.

This fundamental principle of 'data fidelity' also lies at the heart of one of our perpetual frustrations with predictive analytics and artificial intelligence. We feed horizontal, point-in-time snapshots of our data into intelligent agents or analytics tools and expect to be able to make incredible predictions based on that data. Instead, we often wind up with "Clippy," the Microsoft Office Assistant telling us, "it looks like you're trying to write a whitepaper."

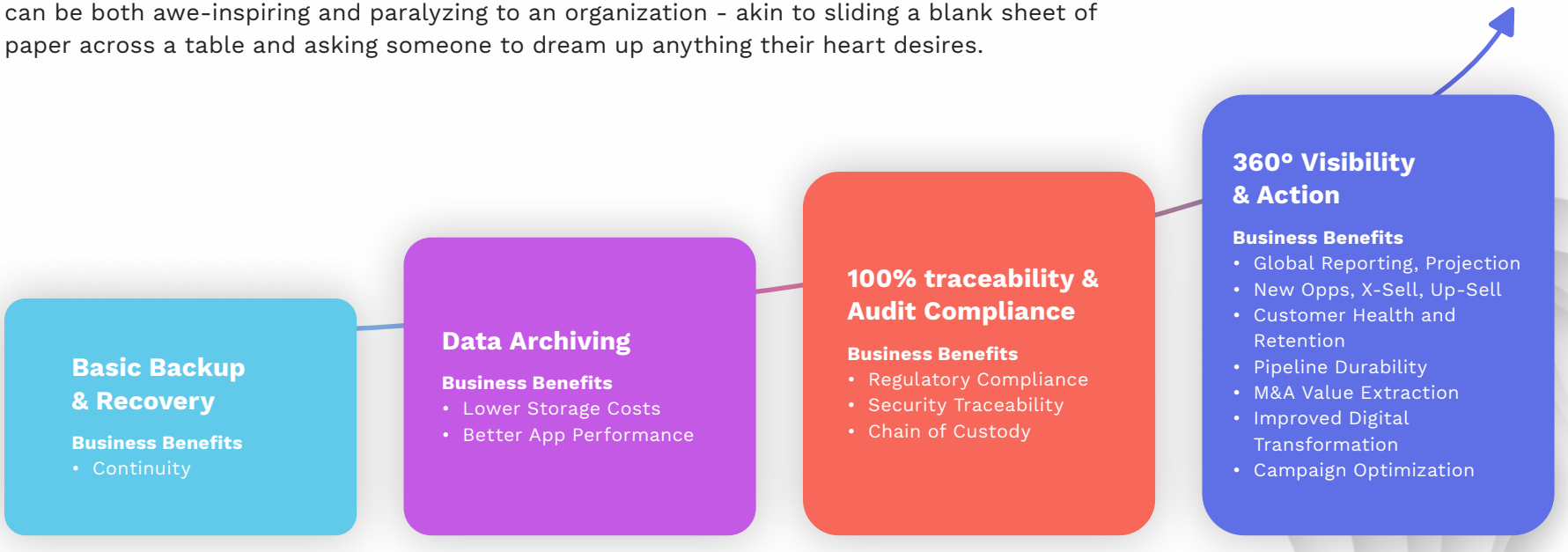
Most algorithms do a better job when pointed at narrower datasets with lots of time-series data, simply because it is easier to understand cause-and-effect patterns when looking at attributes that either covary, or don't, over time.

4. SUMMARY

# What We Learned and How to Get Started

## 4. SUMMARY

When it comes to an organization's cloud application data, possession seems to be even more than 9/10s of the law. Beyond the fundamental requirement to meet the most stringent of global regulations, SaaS data ownership precipitates optimization and growth. It holds the potential to put organizations on altogether new s-curve for innovation in their markets. It can be both awe-inspiring and paralyzing to an organization - akin to sliding a blank sheet of paper across a table and asking someone to dream up anything their heart desires.




**So what simple, actionable thing can organizations do to reap immediate and measurable benefits?**

4.1 STEP #1

# Take Ownership of Your Application's Data

The easiest place to start is to use an old tool, such as cloud data backup, in a new way – to take ownership of your cloud application data. True data ownership (control of where data is both transmitted and stored) unlocks data access - the ability to fully control and maximize how data is used across an ecosystem of applications. And access creates a forcing function for fidelity – the granularity with which data is captured, which is directly tied to an organization's ability to notice new or emerging change patterns in the data. Each becomes a steppingstone for long-term transformation, with even the first step having a tremendous impact on an organization's compliance, security, and governance posture.

To start, deploy a SaaS data backup and archive tool for a critical business application, such as Salesforce. To ensure the tool will allow you to take ownership and control of your data, it is imperative to prioritize tools that give you:

**True Data Owmership**

Control of where data is both transmitted and stored

**Full Ownership**

both over transmission and storage of your backup/archive data

**Complete Access**

allow you to continue to access both historical and archived data both in your production application environment and in your own cloud data lake

**Change Data Capture**

the ability to capture up to every single change in data over time

## 4.2 STEP #2

# Chart Your Next Best Desired Outcomes

After understanding the impact of the three principles above, it is essential to identify the handful of next best organizational outcomes of SaaS data ownership. These can include:

- Improving governance or compliance posture
- Driving business continuity
- Reducing DataOps overhead
- Reducing application storage costs
- Consuming application data in a data warehouse or other applications
- Driving cross-selling behavior across regions or teams
- Bringing external data into applications
- Actioning 360-degree customer views
- Developing new products based on application data

Immediate and tangible objectives, such as those listed above, become the bedrock for long-term ROI and impact cases for the business. They also force organizations to start thinking about their historical SaaS application data as a strategic asset to the business.

4.3 STEP #3

# Check out GRAX

## We are paving the way for change in our industry

GRAX helps organizations adapt faster by letting them get more strategic value out of their historical cloud application data. Customers can fully capture, own and access all of their historical SaaS application data anywhere, anytime, by simply backing it up or archiving it to their own cloud environment. GRAX delivers up to 4X higher ROI than leading competitors.

**Learn more at grax.com.**

### Backup & Restore

Backup, recover and act on historical data changes directly inside your applications

### Data Archive

Reduce impact of data on application performance and storage without removing it from the app

### Time Machine

Record, Recover And Act On Every Single Change In Your Data Over Time

### Data Hub

Create complete 360° customer views in any app without costly consolidation or manual coding

## APPENDIX A

GRAX | Adapt Faster.

## Get Started

help@grax.com

844-GRAXDVP

**grax.com**

## Follow Us

GRAX

@GRAXdv