EBOOK

backupify
a datto company

Making the Executive Case
For Cloud-to-Cloud Backup

INTRODUCTION: WHAT NOBODY TELLS YOU ABOUT THE CLOUD

Everything you've read about what Software-as-a-Service (SaaS) and cloud-based storage can do for your business is true -- to a point. It is often safer and cheaper to run cloud-based software applications than to use traditional, locally installed software.

The cloud is safer, but not infallible.

No software is foolproof, not even software in the cloud, and cloud vendors have no incentive to point out their vulnerabilities. That sounds obvious, but common sense is often left at ground level when companies start operating in the cloud.

Smart companies back up on-premise data. They do so because they don't want to have a single point of failure for their irreplaceable information. That doesn't stop being a good idea just because you move to the cloud.

User error is the unpreventable problem

The single biggest reason companies lost data before the era of cloud computing was hardware failure. A power supply overloaded, a motherboard shorted out or a hard drive crashed. Cloud vendors have legitimately solved this problem with massive, industrial-scale hardware redundancy. By copying your data onto several backup hard drives in several places, cloud vendors have made it nearly impossible for hardware failures to permanently destroy your information.

Google even goes so far as to promise the loss of an entire data center -- as in the failure of an entire campus of buildings full of servers -- won't keep you away from your data for more than 24 hours. Hardware failure is a solved problem in the cloud.

User error isn't. User error never will be.

User error is when you tell Google or Microsoft to permanently purge a bunch of emails you don't think you'll ever need again, only to find out later you just erased valuable, legally required customer correspondence. User error is when you accidentally write over parts of this year's sales spreadsheet with last year's data -- and you can't tell which fields are valid and which are completely wrong. User error is when you didn't configure that Salesforce add-on correctly and it marked every open opportunity as a Closed: Won -- even the ones you didn't close or win -- and now you can't tell which are the real wins and which are just wishful thinking.

No software program can tell the difference between intentional and unintentional commands -- and not every action you take in the cloud has a quick undo command.

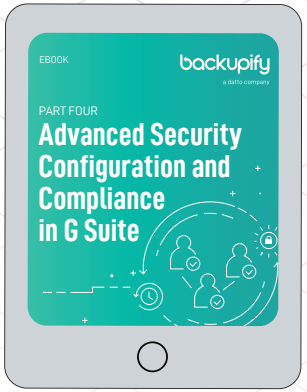
The cloud can save your business from unreliable hard drives. It can't save you from yourself.

And neither can your cloud vendor.

The cloud can save your business from unreliable hard drives. It can't save you from yourself.

Google recommends you use third-party G Suite backup tools in their own security policy.

You may also be interested in:



Advanced Security Configuration and Compliance in G Suite
DOWNLOAD NOW

Why your cloud vendor doesn't want to hear about your data loss

If you lose data in Office 365, there is no defined process or rules for recovering it. You can call their support team, but the level of help they offer depends on the scenario. In general, Microsoft support doesn't have the best reputation for getting people their data back. Their support team is tiered, so the responsiveness will also depend on how much you're paying for a subscription.

G Suite customers can get online and phone support, but Google still tries to push as many of their customers as possible to the self-service Google Support Forums.

Office 365 and Google are selling low-overhead, highly reliable cloud software. They go out of their way to ensure they will never lose your data. That means any data you lose was probably lost by you. And, as we mentioned above, neither Google nor Microsoft nor any other cloud vendor can protect you from yourself -- which makes user error a great big cost center these vendors can't control.

If Google had to put a support rep at your disposal every time you accidentally delete a Gmail message or Google Doc, G Suite would never make any money. The same is true for any cloud solution.

That tier-based support Microsoft offers is their way of ensuring that only people who really, really want and need to find lost data actually ask for help in recovering it. Google is subtler in trying to force their customers to solve their own data-loss problems, but it too wants to avoid undue responsibility when your data goes missing.

And, lest you think we're misreading the purpose of these data recovery policies, Salesforce flat-out tells users to perform their own backups. Google recommends you use third-party G Suite backup tools in their own security policy. Cloud vendors want you to be responsible for correcting your own data loss errors. They are explicit about that stance.

This is where cloud-to-cloud backup comes in.

Why two clouds are better than one

If we might quote our own cloud backup glossary, cloud-to-cloud backup is a service that replicates data in one cloud and stores that duplicate data in another cloud system. Cloud-to-cloud backup is different from cloud backup in that it does not involve any data stored on your local hard drive.

Cloud-to-cloud backup systems are also optimized to restore data from backup directly back into the primary web application with sufficient speed and fidelity to minimize downtime and lost productivity.

That second part is very important. There are lots of ways to replicate data found in your cloud applications. A true cloud-to-cloud backup solution isn't just a data downloader or data duplicator. Cloud-to-cloud backup solutions are designed to get data back into your cloud apps as quickly and accurately as possible, so that data loss doesn't cost your organization excess time and money.

All the reasons you moved your primary applications into the cloud are the same reasons you should move your backups to the cloud.

All the reasons you moved your primary applications into the cloud are the same reasons you should move your backups to the cloud.

Making the case for cloud-to-cloud backup

Still not sure your cloud applications need their own cloud-based backups? Read on as we outline scenarios for every member of the executive suite explaining the relevance and necessity of cloud-to-cloud backup.

WHY THE CIO CARES ABOUT CLOUD-TO-CLOUD BACKUP

As the Chief Information Office of your organization, you are responsible -- literally, it's there in the job title -- for not losing any of your business's vital information. That job entails deploying security and disaster recovery solutions and policies, which in the case of cloud services depend greatly on cloud-to-cloud backup.

Every browser is now a (vulnerable) workstation

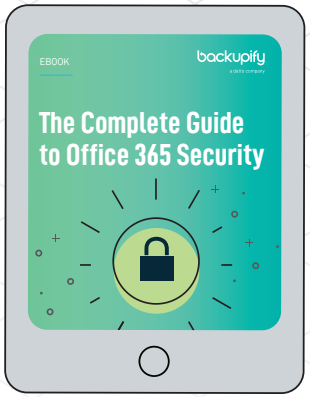
The beauty of the cloud is that most of its applications are accessible by any modern web browser, meaning employees can do work anywhere, anytime from almost any device. The terrifying danger of the cloud (at least for CIOs and security officers) is that any browser can potentially access your cloud applications -- including the buggy, spyware-riddled browsers on your employees' personal computers, tablets and smartphones.

Be honest: you had a hard enough time keeping the browsers on corporate workstations locked down and free of security threats. You can't reasonably expect that moving to the cloud will make it harder for your employees to have their passwords stolen and their data corrupted.

Once your employees work in the cloud, you'll need a backup and recovery solution that can undo the damage of their browser-based shenanigans as quickly as possible. That requires cloud-to-cloud backup.

Having backups of your cloud data means that, even in the worst of all possible cloud failures, you still can get at a copy of your data.

You may also be interested in:



The Complete Guide to Office 365 Security
DOWNLOAD NOW

Social engineering just got (terrifyingly) easy

Just as cloud CIOs like you must now treat every browser as a vulnerable workstation, you must also treat every Wi-Fi network as a vulnerable workplace. That means the sneaky social engineers that used to have to pose as delivery or repair personnel to gain access to your employees can now simply accost them at a coffee shop, airport lounge or trade show panel.

If your users can do damage to your cloud data accidentally, imagine what a social engineer armed with your user's access credentials could do intentionally.

Disaster recovery no longer includes physical control of servers

If a natural disaster befalls your old-fashioned co-located data center, you always have the last resort option of physically visiting the facility and accessing your server racks to get at your data. That worst case option doesn't exist in the cloud. And while it may be entirely unprecedented for Google or another SaaS application to permanently lose your data, do you want to be the CIO that has to tell your CEO that your data is permanently lost because you just assumed Google (or Box or Salesforce) was good for it?

Having backups of your cloud data means that, even in the worst of all possible cloud failures, you still can get at a copy of your data. That's more than just good policy; that's job security -- and it requires cloud-to-cloud backup.

WHY THE CFO CARES ABOUT CLOUD-TO-CLOUD BACKUP

Considering the consequences -- both fiduciary and regulatory -- of losing financial data, it's easy to see why if anyone needs their data backed up and secure, it's you, the Chief Financial Officer. Lost data equals lost dollars; the question is the exchange rate.

Frankly, it is almost impossible for you to put a general dollar figure of the intrinsic value of business data because so much of it is unpredictable. Losing a single Gmail message may not prove harmful -- unless that precise message happened to include an addendum to a contract that is needed for the meeting your CEO is in right now. Suddenly, the loss of that Gmail message is now equal to the dollar value of that contract, but building a risk model around this scenario is pretty challenging.

What you can predict is the amount of time spent recreating lost data which basically comes down to this: (Hours spent creating data) x (Employee hourly compensation) x (Frequency of data loss) = Value of lost data. If the value of the cloud data you expect to lose is higher than the cost of cloud-to-cloud backup, you should buy the backup.

Financial data is the most shared (and the least safe)

The vast majority of data in Salesforce could be considered financial data. Among the most shared items in G Suite are collaborative spreadsheets used to track sales and financial data. The appeal of cloud-based productivity solutions is that everyone involved in driving or tracking your company's transactions can input data at the same time into the same system, enabling real-time analysis of your organization's fiscal health.

As CFO, your best tactic to protect your cloud investment is to ensure your company doesn't have to write it off and pay to move back to expensive on-premise hardware and software.

Of course, that also means that every single one of those employees has direct access to your financial data, and the power to alter it. If user error is the unpreventable problem, financial data is the playground where user error has the most chance to occur, simply by virtue of enduring the most users making the most changes.

For CFO's like you, the equation is simple: Cloud-based financial data needs a cloud-based backup, period.

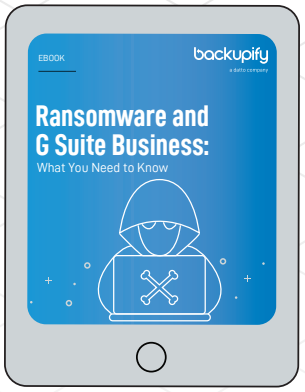
Protecting your cloud investment

The only thing worse than paying for software you don't use is having to pay for it twice: once when you adopt it, and again when you have to roll it back. As CFO, it's your job to help avoid that kind of figurative double taxation.

Plenty of cloud migrations have failed -- with plenty of dollars lost to systems integrators, trainers and consultants (to say nothing of lost employee productivity) -- because data was corrupted or destroyed soon after switching from on-premise systems to the cloud. New users are the most error-prone, and thus the early days of your cloud migration -- before your CIO has acknowledged the need for cloud-to-cloud backup -- are when you're most likely to lose cloud data to user error.

As CFO, your best tactic to protect your cloud investment is to ensure your company doesn't have to write it off and pay to move back to expensive on-premise hardware and software. The best way to avoid a reverse-migration is for smart CFOs (like you) to demand cloud-to-cloud backup.

You may also be interested in:



Ransomware and G Suite Business

DOWNLOAD NOW

WHY THE CLO CARES ABOUT CLOUD-TO-CLOUD BACKUP

As the Chief Legal Officer, you understand why your organization is legally obligated to retain cloud data. As a cloud CLO, you must also understand the need for third-party cloud-to-cloud backup.

Backups are not archives (and vice versa)

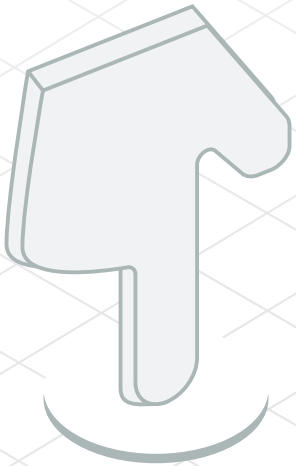
Here's an important rule of thumb: archives are for discovery; backups are for recovery.

Archiving tools like Google Vault are designed to make it easy to prove a chain of events to regulators and investigators. Archiving and compliance software keeps an explicit record of which user took what action when, and can often reproduce versions of files and messages as they existed at a certain point in time. Unfortunately, most of these tools are explicitly limited to communications platforms like Gmail and Google Talk. Archiving tools are about documenting the "he said, she said" of online communications, and assigning responsibility for any changes or transfers of data. Archiving tools are not designed to recreate or reproduce actual lost, altered or corrupted data.

Few if any archiving tools can help you if someone subpoenas your deleted Google Drive documents or wants to see an overwritten version of your Salesforce Sandbox.

Backup tools like Backupify, however, are designed to return lost data to the production application as quickly and seamlessly as possible. That means all data is held by a cloud-to-cloud backup even after it is deleted, and regardless of whether it's a document or a message or a decorative Google Sites image. If you as CLO need to produce a file that isn't an email, there's often no better source than a backup tool.

It's not a question of whether the CLO should choose an archiving tool or a backup tool for your cloud systems. A smart CLO like you wants both.



For more on Cloud-to-Cloud backup, Subscribe to the Backupify Blog

SUBSCRIBE

Your Terms of Service are no longer your own

If your company is using a cloud-based application to help deliver goods or services to your customers, the reliability of those cloud apps now directly affects any commitments you make to those customers. That means the availability of a cloud application -- and the accessibility and integrity of the data in your cloud apps -- can make or break your own service guarantees and contractual obligations.

If you've guaranteed in writing 90-day payment terms, or a 30-day project turnaround, or 24-hour product delivery, you need to be certain that your cloud-based financial records, your cloud-based order processing workflow and your cloud-based inventory management system won't lose data at any time in the transaction cycle. And just because your cloud vendor's Service Level Agreement hits all five key guarantees of availability doesn't mean that one of your employees won't delete the transaction data you need from inside those cloud applications.

A cloud-to-cloud backup means that lost data is back in place before you default on your own Terms of Service, SLA or contractual obligations. As CLO, your job is to ensure your organization can live up to the "commercially reasonable efforts" that a contract promises to make in meeting deadlines and standards. As a cloud CLO, you would be well advised to insist on a cloud-to-cloud backup of any SaaS application.

WHY THE COO CARES ABOUT CLOUD-TO-CLOUD BACKUP

As the Chief Operating Officer, you're charged with making sure that every process within, and every product of, your organization works smoothly. In this day and age, operations depends on data, which is why COOs like you are prime advocates for cloud-to-cloud backup.

Operational stability is spelled R-T-O (Restore Time Objective)

As COO, you should be the most discerning of cloud-to-cloud backup consumers within the executive suite. A savvy COO can tell anyone on the spot the likely financial impact of any momentary slowdown or stoppage of work. If your cloud applications lose data, work is slowed or stopped unless and until that data is recovered -- and as COO you are largely responsible for the productivity figures affected by such data loss.

A competent COO like you has processes and procedures in place to work around and through any data loss-related delays in operations. A key component of these procedures is your company's Restore Time Objective (RTO) -- the acceptable and expected amount of time it takes to notice and correct a data loss and return systems to normal standards of operation. The CIO may put the software and hardware in place that dictate a possible Restore Time Objective, but it's you, the COO, that has to live with that RTO, and oversee the processes that make it a reality.

As mentioned above, Google has never been shown to have permanently lost data, but it has suffered unplanned downtime. Salesforce does have expensive processes in place to recover lost data, but their minimum turnaround is three weeks. A three-week RTO may as well read DOA -- Dead On Arrival -- as it can prove fatal for any serious operation.

If you're a COO that cares about your RTO, then you can't help but demand a cloud to cloud backup.

Enterprise-grade cloud-to-cloud backup solutions can return lost data to production cloud systems in minutes. Not hours, and not days -- minutes. If your business relies on the cloud, the only way to maintain an adequate RTO for your cloud data is with cloud-to-cloud backup.

If you're a COO that cares about your RTO, then you can't help but demand a cloud-to-cloud backup.

Analytics are only true if the data is still there

Everyone in the executive suite is judged by numbers, but the numbers you manage as Chief Operating Officer are arguably the most vital. Whatever it is that your company is selling, it's you, the COO, that ensures what you're selling gets made. Your COO analytics dashboard includes numbers on all your company deliverables -- and it's those deliverables that underpin the profits recorded by the CFO and credited to the CEO.

And your COO dashboard is only accurate if you have all the necessary data. Lost cloud data means inaccurate operational performance indicators, which means you're worse than an uninformed COO -- you're a misinformed COO.

Cloud-to-cloud backup ensures that any lost data is recovered quickly, so you as COO can maintain an accurate KPI dashboard, and your company can hit its most important numbers.

WHY THE CEO CARES ABOUT CLOUD-TO-CLOUD BACKUP

In one sense, you as Chief Executive Officer care about cloud-to-cloud backup for all the reasons the rest of C-Suite cares about cloud-to-cloud backup: because as CEO you're ultimately responsible for everything. Still, there are explicit reasons why you would care about cloud-to-cloud backup -- because as CEO, your job is to manage the bigger picture.

Lower the downside risk of adopting the cloud

Every major change to your organization entails risk, and as CEO you must examine that risk by weighing the upside and downside of the particular tactic or strategy. CEOs are rewarded handsomely for achieving upside, and are often dismissed for experiencing too many downside events.

Adopting the cloud for any mission-critical application is hardly an unusual move these days, but "everyone else is doing" is rarely an acceptable excuse when a CEO oversees a poorly implemented cloud adoption or migration. Cloud-to-cloud backup removes nearly all the risk associated with adopting a cloud application, because it ensures that even if your own employees actively or passively corrupt your cloud data, it will be recoverable. Cloud-to-cloud backup shrinks the downside risk profile of any cloud adoption.

In the midst of cloud migration, cloud-to-cloud backup is the prudent CEO's best friend.

Avoid cloud vendor lock-in

There's a short term downside if you as CEO oversee a failed cloud adoption, but there's perhaps an even more significant upside risk if the cloud migration succeeds: vendor lock-in. While most cloud vendors have pretty explicit conditions on data ownership within their Terms of Service and Service Level Agreements, that's cold comfort if the vendor doesn't honor those terms.

Ready to take Cloud-to-Cloud backup for a spin?

SCHEDULE A DEMO!

What do you do if your cloud vendor suffers its own financial or technical setback and cannot meet its obligations to provide you access to your data? What if your cloud vendor is acquired and the new owners alter your Terms of Service (because most cloud ToS documents allow cloud vendors to unilaterally alter terms at any time)? What if your cloud vendor simply becomes an overwhelmingly dominant player in your industry and raises the price for their cloud solution beyond acceptable costs for your company?

Could you take your data -- and your meta-data -- out of your cloud solution and move it elsewhere in a timely fashion?

If your on-premise solution provider pulled any of these stunts, you still had physical possession of the hardware where your data and applications were stored. You had the power, and you could take your business elsewhere if need be. Cloud-to-cloud backup preserves this option with cloud applications. If your cloud vendor attempts to strong arm you -- to effectively hold your data hostage in their servers -- your cloud-to-cloud backup gives you anywhere, anytime access to a second copy of your business data.

That puts you, the CEO, in a much stronger bargaining position if your cloud vendor gets ruthless. Never bring a knife to a gunfight, and never bargain with your cloud vendor without having a cloud-to-cloud backup already in place.

Keep the option to leave the cloud

Perhaps the most underappreciated aspect of cloud-to-cloud backup is the fact that it's useful for companies who no longer want to operate in the cloud. The frank truth is that cloud solutions aren't appropriate for every organization, and while many tools exist to shift your company from one cloud solution another, few are prepared to migrate you from a cloud application back to on-premise systems.

backupify

a datto company

- **Unmatched cloud expertise** from the global leaders in SaaS protection
- **The cost-effective** choice for the Enterprise, offering a reliable, fast, automated, and scalable solution
- **Truly secure**, independent backup that is SOC 2 Type II & HIPAA compliant
- **Quickly recover data** from ransomware, accidental deletion, or human error with Backupify's infinite retention and unlimited storage

Find out why over 3 million users around the globe trust Backupify to protect their Office 365 and G Suite data.

Start your 15-day free trial at Backupify.com.

Cloud-to-cloud backup systems are ideal partners when migrating away from the cloud. Enterprise-grade cloud-to-cloud backup solutions can deliver your replicated cloud data in a number of formats, including as archives that can be downloaded in common filetypes usable by conventional installed software.

Experience proves that there are occasionally insurmountable regulatory, operational or security challenges around your company's use of cloud-based applications. Cloud-to-cloud backup provides a contingency that allows your organization to re-adopt on-premise systems with speed and ease. That's a backup plan every CEO can appreciate.

CONCLUSION

If you want to summarize this paper in one sentence, here it is: The only way for the cloud to live up to its promises is with cloud-to-cloud backup.

Every member of the C-Suite should repeat that sentence as a mantra. Your cloud applications cannot and will never protect you from user error, but a cloud-to-cloud backup offers you a "get out of user error free" card to be played whenever your own employees corrupt, misplace or destroy vital business data.

Smart executives understand the pros and cons of migrating to the cloud, but the smartest members of the C-Suite demand cloud-to-cloud backup.