FORRESTER®

FOR INFRASTRUCTURE & OPERATIONS PROFESSIONALS

Back Up Your SaaS Data — Because Most SaaS Providers Don't

Cloud-To-Cloud Backup Is The Only Practical Option For SaaS Data Protection

by Naveen Chhabra

December 19, 2016

Why Read This Report

Software-as-a-service (SaaS) cloud providers are popular elements of a sound business technology (BT) strategy. While the vendors provide the applications, almost all mention explicitly in their terms and conditions that protecting data is the client's responsibility. Yet infrastructure and operations (I&O) leaders send critical data to SaaS providers without any plan for ensuring data resiliency. Back up your SaaS data or risk losing customers, partners, and employees. Stop leaving the door open to data loss, and start proactively protecting cloud data — before it's too late.

Key Takeaways

Backup Of SaaS Application Data Is Your Responsibility
Every SaaS provider explicitly calls out that clients are responsible for protecting their own data. You must plan data protection for every new SaaS service to which you subscribe.

Cloud-To-Cloud Backup Is The Only Practical Option
It's not practical for you to custom develop adaptors/connectors that protect SaaS application data. You must engage with cloud-to-cloud backup providers, as they can leverage their experience to add support for new services quickly.

Back Up Your SaaS Data — Because Most SaaS Providers Don't

Cloud-To-Cloud Backup Is The Only Practical Option For SaaS Data Protection

by Naveen Chhabra
with Glenn O'Donnell, Liz Herbert, Michael Caputo, William McKeon-White, and Diane Lynch
December 19, 2016

Table Of Contents

2 Few Firms Protect Their Cloud Data From Obliteration

Wake Up To The Reality: You Are Responsible For Your Data . . .

. . . And Your SaaS Provider May Not Be Able To Restore Your Lost Data

10 You Can — And Must — Mitigate The Risk Of Losing SaaS Data

Cloud-To-Cloud Backup Is An Increasingly Viable And Preferred Option

Recommendations

13 Don't Make Assumptions: Grill Your SaaS Provider About Backup

15 Supplemental Material

Notes & Resources

Adobe, Google, and Microsoft provided Forrester with information for this report; we obtained all other information from publicly available product feature lists on company websites.

Related Research Documents

The Public Cloud Services Market Will Grow Rapidly To $236 Billion In 2020

TechRadar™: Cloud Computing, Q4 2015

Vendor Landscape: Data Resiliency Solutions, Q3 2016

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Few Firms Protect Their Cloud Data From Obliteration

SaaS adoption is growing across all industry verticals and a wide range of industry applications. Various SaaS provider firms have crossed the billion-dollar mark and are cruising ahead with strong growth rates. Forrester predicts that the SaaS market will grow to $157 billion in 2020.[1] This rocketing growth in SaaS usage produces a proportional growth in the movement of customer business data, from on-premises to the cloud instances. Your customers expect you to protect all data involved in delivering trustworthy services. Firms used to protect that data when it was on-premises but are not investing in protecting SaaS-based data the same way. I&O leaders assume that their SaaS providers have “assured backup” in place — a dangerous assumption that’s likely not true.[2] Enterprises can lose their business data. As an example, a global pharmaceutical and life sciences company that uses 100-plus SaaS services encountered data loss and was unable to recover it completely. Reasons that firms can face unrecoverable data loss within SaaS applications include:

- **Accidental deletion.** While this is the most basic cause of data loss, it’s also the most common for both on-premises and cloud-based data. This can be especially problematic if the user fails to notice deletion immediately and the data ages out of the user’s trashcan.[3] Accidental deletion can also take the form of accidentally overwriting correct information with incorrect information — something that many SaaS providers can’t easily reverse in their platforms.

- **Departing employees.** As employees leave your organization, what happens to the data associated with their accounts in your SaaS application? The rules vary significantly from vendor to vendor, but for many, deactivating a user account also means deleting the data stored there. Many organizations wish to keep this data but may not have a good way of exporting it or transferring it within the application.

- **Hacktivists.** Every news cycle brings a new story of a cyberattack. Today, cybercriminals most often target on-premises systems, but they’ll quickly shift targets as enterprises store critical data in SaaS and other cloud-based systems. Financially motivated criminals want to steal copies of customer data and intellectual property that they can easily monetize. Politically and socially motivated cybercriminals (known as hacktivists), however, may expose or destroy data in retaliation for some real or perceived offense.

- **Malicious insiders.** Whether it’s a disgruntled employee, a resentful contractor, or some other insider with the intention to do harm, malicious users are another common cause of data loss, both on-premises and in cloud environments. The scope of damage will depend on the access and authorizations granted to the user. If it’s an individual contributor with a narrow range of responsibilities, the damage may be limited, but if it’s a power user, the damage can be extensive.[4]

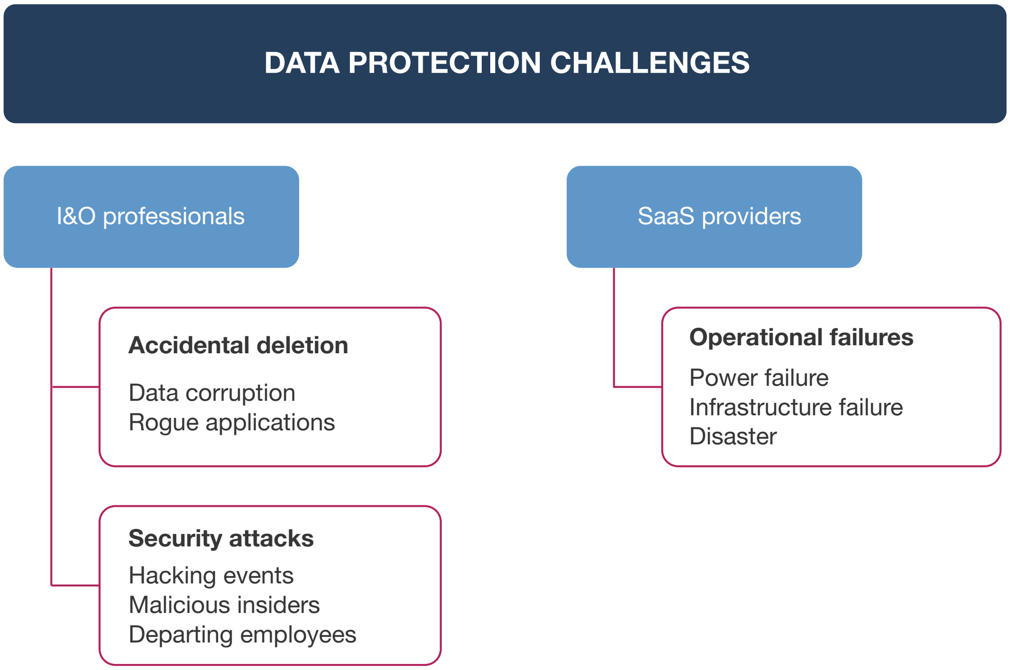
- **Rogue applications.** With the ecosystem of add-on applications for popular SaaS solutions growing by the day — Salesforce’s AppExchange now boasts more than 3,100 apps and more than 4 million installs — we’re seeing growing concern about rogue third-party applications causing damage. What happens when the app that’s supposed to consolidate duplicate records accidentally deletes or corrupts unique records?

- **SaaS providers' prolonged outage.** As the saying goes, "If anything can go wrong, it will." An unexpected, prolonged SaaS provider outage can cripple your business. Unless you have a plan in place for how to handle such a crisis, it's highly unlikely you'll have access to your data in these circumstances. For example, insurance brokerage firms in the UK using SaaS services from SSP Worldwide became inoperable when SSP faced a three-week-long outage.[5] Brokers were unable to issue new policies, couldn't look up the expiration dates of existing policies, and were unable to communicate with their clients. For some clients, SSP Worldwide wasn't able to recover data from backup instances. To the brokers' utter dismay, SSP Worldwide assumed no responsibility for broker losses resulting from this outage.

Wake Up To The Reality: You Are Responsible For Your Data . . .

A SaaS provider can't detect genuine data loss, so it doesn't accept responsibility for customer data. These providers explicitly call this out in their terms and conditions. However, SaaS providers assume responsibility and take operational measures in certain situations — such as a disaster or an infrastructure failure — so you don't lose your data (see Figure 1). It's your responsibility to keep the other risks covered.

FIGURE 1 I&O Professionals And SaaS Providers Must Take Responsibility For Data Protection



. . . And Your SaaS Provider May Not Be Able To Restore Your Lost Data

While the majority of enterprise-grade SaaS offerings have robust methodologies for backing up and restoring data within their aforementioned scope of responsibility, they may not make this technology available to you as the user (see Figure 2). For example, if you lose data through no fault of the vendor — e.g., if one of your employees accidentally deletes data — it may not be able to work with you to retrieve data from its backups. In cases where the vendor can technically recover data, it's likely you'll encounter delays, restrictions, or even significant fees.[6] Salesforce, for example, charges a minimum of $10,000 to recover customer data, and it can take several weeks.[7] If you've categorized a SaaS application as a critical system, it's time to work with your sourcing and vendor management (SVM) people to find out if you can meet internal service levels and expectations. There are other benefits to having copies of your data outside of your primary SaaS provider, such as being able to lower the barrier to switching providers and having additional leverage when negotiating with your vendors.

FIGURE 2 Backup And Recovery Policies Of Popular Enterprise SaaS Solutions

Vendor	Backup-and-restore methodology to prevent data loss	Restore policy if customer loses data
Adobe	As part of the S3 redundancy functionality, files are replicated across Amazon Web Services (AWS) availability zones for backup.	Adobe commits basis AWS S3 restore policy of 4 hours.
ADP	Information was not publicly available.	Information was not publicly available.
Ariba (SAP)	Transactions made using the solution are initially stored in a database to prevent loss. All customer data resident on the systems is backed up daily. Backups are stored offsite at a secure third-party location. Backups include customer's registration and account information.	Information was not publicly available.
athenahealth	Information was not publicly available.	Information was not publicly available.
Box	Box replicates data between its data centers and backs up data to a third-party public cloud provider in near-real time. The backups are over 99.9% timely.	If a user accidentally deletes a file, it goes into the trashcan, where a user or administrator can retrieve it, depending on how it has been configured by the admin. Administrators can configure the Box service to keep trash content for 7, 14, 30, 60, or 90 days or can keep all trashcan content indefinitely if they so choose. Box admins can also configure trash controls so that admins only, admins and co-admins, or nobody within the organization can permanently delete content. In case of deletion from the account, customers can still retrieve the files by contacting Box support for 30 days. In the event of primary file storage unavailability or other issue, customers can retrieve/restore files from Box's cloud-based secondary storage systems.
Cisco Systems	Aside from Global Site Backup, Cisco WebEx utilizes traditional backup methods and has the ability to restore data if/when necessary.	Information was not publicly available.

FIGURE 2 Backup And Recovery Policies Of Popular Enterprise SaaS Solutions (Cont.)

Vendor	Backup-and-restore methodology to prevent data loss	Restore policy if customer loses data
Citrix ShareFile	Citrix webconferencing data is backed up at least daily. Citrix performs database backups of ShareFile to an alternate site with the capability to attribute metadata from either site if the integrity of the databases at the primary site is negatively affected. Citrix ShareFile stores uploaded data and customer files within third-party cloud providers and ensures that files are replicated locally and intra-geo. Adding extra resiliency, ShareFile can optionally back up customer files to a facility on the East Coast, which provides ShareFile the ability to recover customer files in the event of accidental deletion for up to 28 days.	ShareFile end users and admins can recover items from a recycling bin for up to seven days. The ShareFile operations team can recover files for up to 28 days before they're permanently purged. Podio users can recover only data through an API.
Concur Technologies	Concur employs a complete internal infrastructure to back up and monitor servers through secure connections. Backup media for Concur's online servers is fully encrypted with AES-128. Media that is stored offsite is safely transported by secure courier to a hardened offsite media storage facility.	Information was not publicly available.
Cornerstone On Demand	Cornerstone takes daily backups of full client databases. Hourly transactional backups are sent to separate hot disks. All backups are encrypted with AES-256 before being written to tape. Tapes are collected weekly and transported in locked boxes to secure vaults.	Information was not publicly available.
Google Apps	Data is replicated multiple times across Google's clustered active servers, so in the case of a machine failure, data will still be accessible through another system. It also replicates data to secondary data centers to ensure safety from data center failures.	Once an administrator or end user has deleted any data in Google Apps, Google deletes it according to the customer agreement and its privacy policy. Data is irretrievable once an administrator deletes a user account.

FIGURE 2 Backup And Recovery Policies Of Popular Enterprise SaaS Solutions (Cont.)

Vendor	Backup-and-restore methodology to prevent data loss	Restore policy if customer loses data
IBM SmartCloud	Every data center is fully duplicated and backed up in near-real time (through data replication) to a remote alternate site. Every site, primary or alternate, is identical and fully capable of providing 100% of planned operational capacity. Within each data center there is a high degree of redundancy built into the service clusters for local resilience to failure.	IBM's safeguards against accidental deletion include a trashcan that gives users and admins a second chance to recover data within SmartCloud Notes. Admins can prevent users from emptying this trashcan for a configurable number of days (up to 90). Several end user safeguards have been made available to protect against accidental deletion — from standard trashcan second chances to a locked-down trashcan option (set by the client's admin) for SmartCloud Notes that prevents users from emptying trash for a configurable number of days (up to 90) followed by automatic delete.
Intuit	In addition to always maintaining two copies of data, Intuit automatically back up updated data every day. It's stored on firewall protected, redundant servers so data is safe from hardware and software failures, hackers, and viruses.	Since the records are updated upon every backup or with every change, it is not possible to restore files to a previous point in time.
Microsoft Dynamics 365 (field service, operations, project service automation, sales, and service)	A full backup of customers' data is performed on weekly basis and the incremental backup on a daily basis. Customers' data can be stored in multiple regions. Depending on the application, data is retained for 30 or 35 days on disk and archived on tape for 90 days.	MS support services team will help recover data in event of data loss. Clients need to raise a service request. MS does not charge any fee for data retrieval. Clients will have to engage with MS directly as MS does not let any third party access client data in such scenarios. MS commits to deliver recovered data within two days.
Microsoft Office 365	Microsoft backs up data both daily and multiple times per day. Resilience measures include local flash copies, off-line remote backup (encrypted), and the near-real-time replication to the DR data center. Multiple copies of client data exist at any given time in more than one location.	Microsoft backs up data both daily and multiple times per day. It also allows end users to recover accidentally deleted files from a recycle bin. Administrators can restore data — such as collections — as well as deleted users.

FIGURE 2 Backup And Recovery Policies Of Popular Enterprise SaaS Solutions (Cont.)

Vendor	Backup-and-restore methodology to prevent data loss	Restore policy if customer loses data
NetSuite	NetSuite conducts hot backups and stores data off-site in a secure location and safeguarded against almost any environmental conditions.	Information was not publicly available.
Oracle BigMachines	Oracle periodically makes backups of your production data in the services for Oracle's sole use, to minimize data loss in the event of an incident. Backups are stored at the primary site used to provide the Oracle Cloud Services, and may also be stored at an alternate location for retention purposes. A backup is typically retained online or offline for a period of at least 60 days after the date that the backup is made. BigMachines performs both weekly full data backups and hourly incremental data backups with ability to roll back at any time.	On an exception basis and subject to written approval and additional fees, Oracle may assist you to restore data which you may have lost as a result of your own actions.
Oracle Eloqua & Content Marketing	Oracle performs a weekly backup during the maintenance window. A backup is retained for a period of at least 30 days after the date that the backup is made.	Information was not publicly available.
Oracle Fusion CRM/HCM/ERP	To ensure that customer data is protected against accidental destruction or loss, backups are taken on a regular basis; backups are encrypted and are secured.	On an exception basis and subject to written approval and additional fees, Oracle may assist you to restore data which you may have lost as a result of your own actions.
Oracle Responsys	A backup is retained for a period of at least 21 days after the date that the backup is made.	On an exception basis and subject to written approval and additional fees, Oracle may assist you to restore data which you may have lost as a result of your own actions.
Oracle RightNow Technologies	Oracle backs up customer data once in each 24-hour period. Oracle may, but is not obligated to unless otherwise required by law, retain customer data in backup media for an additional period of up to 12 months.	On an exception basis and subject to written approval and additional fees, Oracle may assist you to restore data which you may have lost as a result of your own actions.

FIGURE 2 Backup And Recovery Policies Of Popular Enterprise SaaS Solutions (Cont.)

Vendor	Backup-and-restore methodology to prevent data loss	Restore policy if customer loses data
Oracle Taleo	Oracle runs nightly incremental backups of Taleo Learn products six days a week. The incremental backup data is stored to disk on Taleo's hosting infrastructure. It runs a full backup at least once per week. Except with respect to the Taleo Learn products, the full backup data is stored to disk on Taleo's hosting infrastructure on a weekly basis. The full backup data is then copied to disk at a physically separate location and encrypted.	On an exception basis and subject to written approval and additional fees, Oracle may assist you to restore data which you may have lost as a result of your own actions.
Salesforce	All customer data is automatically backed up to a tape library on a nightly basis. Backup tapes are cloned to an off-site facility to verify their integrity, and the clones are stored in a secure, fire-resistant location at that off-site facility.	As part of a last-resort process, Salesforce Support can recover customer data at a specific point in time, in the case that it has been permanently deleted or corrupted. The price for this service is a minimum of $10,000.
ServiceNow	ServiceNow uses online/hot database disk-to-disk backup of the entire instance.	ServiceNow can restore customer data from any of the backups (past 7 days, past 4 weekly). Customers can backup/restore data from their instance using ODBC.
Ultimate Software	With Ultimate Software's on-demand service model, Ultimate Software has total responsibility for all IT components, including installing and upgrading the system, maintaining and updating hardware, and performing backups.	Information was not publicity available.

FIGURE 2 Backup And Recovery Policies Of Popular Enterprise SaaS Solutions (Cont.)

Vendor	Backup-and-restore methodology to prevent data loss	Restore policy if customer loses data
Workday	Workday's master production database is replicated in real time to a slave database maintained at an offsite data center. A full backup is taken from this slave database each day and stored at the offsite data center facility. Workday's database backup policy requires database backups and transaction logs to be implemented so that a database may be recovered with the loss of as few committed transactions as is commercially practicable. Transaction logs are retained until there are two backups of the data after the last entry in the transaction log. Database backups of systems that implement interfaces must be available as long as necessary to support the interfacing systems. This period will vary by system.	Information was not publicly available.
Yammer	Multiple encrypted copies of all data are securely stored both onsite and offsite. Yammer's offsite backup is done multiple times per day through a provider called Zetta. Long-term, Yammer is moving to Microsoft Azure for backups; however, Zetta is still part of its backup solution at this time.	Yammer allows administrators to export data from the network for archiving purposes. This data can be reposted to Yammer in the case of accidental deletion or corruption.
Zuora	All data is backed up to disk at each data center, on a rotating schedule of incremental and full backups. The backups are cloned over secure links to a secure disk archive. Disks are not transported offsite and are securely destroyed when retired.	Information was not publicly available.

You Can — And Must — Mitigate The Risk Of Losing SaaS Data

We live in the era of "now": Your customers expect data and services, both on-premises and in the cloud, to be available immediately, regardless of time or context. Expecting customers to wait for days or weeks for you to recover lost data or informing them that data is unrecoverable is unacceptable. As more critical data moves to SaaS, I&O leaders must be proactive and invest in mitigating these risks now instead of waiting for data loss to occur. Forrester has identified several steps that you can take if you're concerned (and you should be) about losing critical data with a SaaS provider:

› **Work with a cloud-to-cloud backup provider.** During the past few years, a new class of backup software provider has emerged: cloud-to-cloud. A few notable examples include Datto Backupify, OwnBackup, and Spanning. SaaS solution vendors themselves, these providers offer an automated and simplified way to back up copies of your critical data (including metadata and audit logs) from one cloud to another. These tools often come with advanced search-and-browse features as well as granular recovery capabilities to make finding and restoring lost data as pain-free as possible. Most of the solutions on the market today use Amazon Web Services as the storage target.

› **Talk to your SaaS provider about its backup and restore policies.** Negotiate if you must. Several SaaS providers, such as Box and Microsoft, have a strong story on backup and recovery already, and you may decide you're comfortable relying on their services to restore lost data. Smaller providers may be open to negotiating an additional backup service on top of the original SaaS offering. In these cases, it's prudent to request that the provider store backups in an offsite location.

› **Define a manual process for exporting cloud data.** The least elegant solution to this challenge is to periodically and manually export data from the SaaS platform and store it elsewhere, either in your data center or with another cloud provider. Many SaaS providers offer data export tools that can facilitate this process, but few to none offer any automation or scheduling in these tools. Furthermore, granular restores are virtually impossible with this method, so you'd need to restore the data in an all-or-nothing fashion.

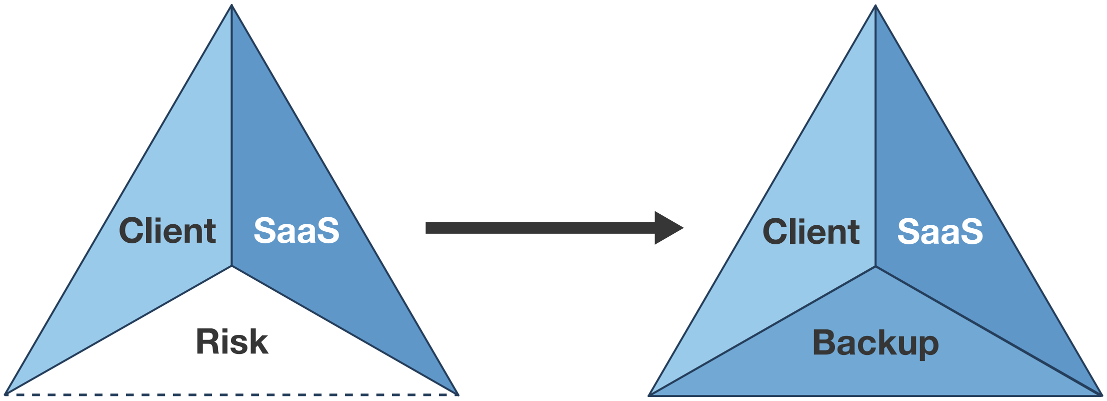
Cloud-To-Cloud Backup Is An Increasingly Viable And Preferred Option

Considering investing in cloud-to-cloud backup? Today, a handful of companies are offering cloud-to-cloud backup services to the most popular SaaS providers (see Figure 3). If you're looking to back up Google Apps, Office365, Salesforce, or a social media platform, you'll have plenty of options. If you have to protect data from one of SAP's or Oracle's SaaS solutions, you'll struggle to find third-party help. Leading cloud-to-cloud backup providers haven't made much progress adding support of SaaS providers, but pursue a partnership with them to build support for the next SaaS application you have in mind. Continued SaaS applications momentum and growth require a full three-way ecosystem consisting of the client (you), the SaaS provider, and the cloud-to-cloud backup provider (see Figure 4). This triad functions in a similar way to the discipline for on-premises applications.

FIGURE 3 Cloud-To-Cloud Backup Solutions Don't Support All SaaS Apps, So Prepare A Data Backup Plan

Vendor	SaaS apps protected	Number of users under management	Key customer references	Cost
Asigra	• Google Apps • Office 365 • Salesforce	N/A	Electronic Vaulting Services; Backup My Info; Phoenix IT Services	N/A; does not sell direct
CloudAlly	• AWS DynamoDB and SimpleDB • Google Apps • Office 365 • Salesforce • Yahoo Mail	200,000 (estimated)	N/A	$3/month/user
Cloudfinder	• Box • Google Apps • Office 365 • Salesforce	N/A	N/A	N/A; does not sell direct
Datto Backupify	• Facebook • Google Apps • Office 365 • PipelineDeals • Smartsheet • Salesforce.com • Twitter	150,000 (estimated)	Financial Times; Museum of Modern Art	$3/month/user. Flexible storage pricing plans also available
OwnBackup	• Facebook • Google Apps • LinkedIn • Salesforce • Twitter	>200,000	Allergan; MacMillan; NTT Data	$3/month/user
Spanning by DellEMC	• Google Apps • Office 365 • Salesforce.com	>100,000	McKesson; Pivotal; SoftBank; WWF	$40 or $48/year/user
SysCloud	• Box • Google Apps • Salesforce.com	120,000 (estimated)	University of Groningen	$4/month/user
Skyvia	• MS Dynamics CRM • QuickBooks • SugarCRM • Salesforce • ZohoCRM	80,000 (estimated)	N/A	Standard: $9/month/20Gb Professional: $99/month/20Gb Enterprise: $499/month/1Tb

FIGURE 4 A Full SaaS Triad Minimizes Risk By Including Cloud-To-Cloud Backup



Recommendations

Don't Make Assumptions: Grill Your SaaS Provider About Backup

Getting started means gathering more information. After reviewing dozens of contracts for language on resiliency, backup, and continuity, Forrester has found that many providers are vague and noncommittal regarding their efforts to recover lost customer data. Partner with your SVM team to review vendor contractual terms on backup and disaster recovery to see what you can expect if you lose data. If contracts are vague or inconclusive, reach out to your provider for further clarifications. If you're dissatisfied with the recovery options that your vendor provides, negotiate for additional services — some providers are more open to this than others are. Evaluate alternative SaaS platforms if your current choice is intransigent. Either way, contact a cloud-to-cloud backup provider for help. When reviewing contracts or talking to their providers, I&O leaders should ask these questions:

› **"What's your backup-and-restore methodology to prevent data loss?"** You'll want to look for vendors that do some type of disk-to-disk backup and move backups offsite relatively quickly. The provider should retain backups for at least 30 days.

› **"What's your policy surrounding data loss that occurs because of customer action?"** In the case of data loss that's not the fault of the vendor (e.g., accidental deletion or a malicious user), will the vendor restore your data? If so, how long will it take, and how much will it cost? Few vendors have set service-level agreements on this operational model.

› **"Can customers perform their own backups and restores of data from your offering?"** Some SaaS offerings include the ability for customers to manually export and download data. This is an alternative to using cloud-to-cloud backup providers if the vendor doesn't currently support your application or if you want to keep backup copies on-premises.

› **"What are your resiliency and continuity capabilities?"** While reviewing backup and recovery abilities, you should also review your vendor's disaster recovery capabilities. Get a detailed outline of how the vendor will recover or failover in the case of a large-scale event and whether you should expect service levels to change. Also, review the disaster recovery plans, testing policies, and test results of your vendors. Look out for language about force majeure, which allows the provider to abdicate responsibility in the case of "an act of God."

Supplemental Material

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Adobe

Google

Microsoft

Endnotes

[1] Firms across all industry verticals and a wide range of applications are using SaaS services. See the Forrester report "The Public Cloud Services Market Will Grow Rapidly To $236 Billion In 2020."

[2] Many large SaaS providers don't mention their plans around backup and recovery policy, practice, and readiness. Examples include ADP and athenahealth.

[3] Many SaaS providers, including Box, keep deleted data in the trash for 30, 60, or 90 days.

[4] We discuss various forms of insider threats in the following report; SaaS isn't immune to those insider threats, and you must develop plans to deal with the risks. See the Forrester report "Hunting Insider Threats."

[5] SaaS providers should assume data loss responsibility if losses occur because of operational mismanagement. Brokers faced data loss when SSP Worldwide failed to recover data. Source: Emmanuel Kenning, "SSP admits it will take weeks to restore customers fully," InsuranceAge, September 15, 2016 (http://www.insuranceage.co.uk/insurance-age/news/2470951/ssp-admits-it-will-take-weeks-to-restore-customers-fully).

SSP Worldwide assumed no responsibility to the "consequential losses" incurred as a result of using its software. Source: Caroline Donnelly, "SSP Worldwide customers call for revised compensation offer for two-week cloud outage," TechTarget, October 17, 2016 (http://www.computerweekly.com/news/450401120/SSP-Worldwide-customers-call-for-revised-compensation-offer-for-two-week-cloud-outage).

[6] The Oracle Responsys Cloud Service retains a backup for a period of at least 21 days after the date of the backup. On an exception basis and subject to written approval and additional fees, Oracle may assist customers to restore data that they may have lost as a result of their own actions. Source: "Oracle Cloud Enterprise Hosting and Delivery Policies," Oracle, December 1, 2015 (http://www.oracle.com/us/corporate/contracts/cloud-ent-hosting-del-policies-1881438.pdf) and "Oracle SaaS Public Cloud Services," Oracle, July 2016 (http://www.oracle.com/us/corporate/contracts/saas-public-cloud-services-pillar-3089814.pdf).

[7] Salesforce has a defined policy that lists the cost and time to recover the data from a particular point. Source: "Data Recovery Service and Cost FAQ," Salesforce (https://help.salesforce.com/apex/HTViewSolution?urlname=Data-Recovery-Service-and-Cost&language=en_US).

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO

B2B Marketing

B2C Marketing

Customer Experience

Customer Insights

eBusiness & Channel Strategy

Technology Management Professionals

CIO

Application Development & Delivery

Enterprise Architecture

› Infrastructure & Operations

Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research (Nasdaq: FORR) is one of the most influential research and advisory firms in the world. We work with business and technology leaders to develop customer-obsessed strategies that drive growth. Through proprietary research, data, custom consulting, exclusive executive peer groups, and events, the Forrester experience is about a singular and powerful purpose: to challenge the thinking of our clients to help them lead change in their organizations. For more information, visit forrester.com.