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 29, 2017

Why Read This Report

Software-as-a-service (SaaS) is a popular element of a sound technology strategy. While almost all SaaS vendors explicitly state that protecting data is the customer's responsibility, infrastructure and operations (I&O) leaders usually send critical data to those providers without any plan for ensuring data resiliency. Back up 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. This report helps I&O leaders navigate the landscape of SaaS services and data recovery.

This is an update of a previously published report; Forrester reviews and updates it periodically for continued relevance and accuracy.

Key Takeaways

Backing Up SaaS Application Data Is Your Responsibility

Nearly every SaaS provider explicitly states in its terms and conditions 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 to custom-develop adapters or connectors that protect SaaS application data. You must engage 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, William McKeon-White, and Bill Nagel

December 29, 2017

Table Of Contents

Related Research Documents

Best Practices: Mitigating Insider Threats

Identify And Estimate The Costs Of Downtime On Your Business

The State Of Business Technology Resiliency, Q2 2017

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 verticals to meet a broad range of industry applications. Forrester predicts that the SaaS market will grow to $157 billion in 2020; some providers have more than $1 billion in revenue and are growing strongly.[1] This rapid increase in SaaS usage means a proportional growth in the movement of customer business data from on-premises to cloud instances. While firms were accustomed to protecting this data on-premises, they're not investing in protecting SaaS-based data the same way — which is a problem, as customers expect firms to protect *all* of their data and deliver trustworthy services. I&O leaders assume that their SaaS providers have "assured backup" in place — a dangerous and likely untrue assumption.[2] Enterprises *can* lose their cloud business data. One global pharmaceutical and life sciences firm lost data from some of the more than 100 SaaS services that it uses; in most cases, it could not completely recover the data. Firms must build their own data protection for SaaS applications to cover potential problems with:

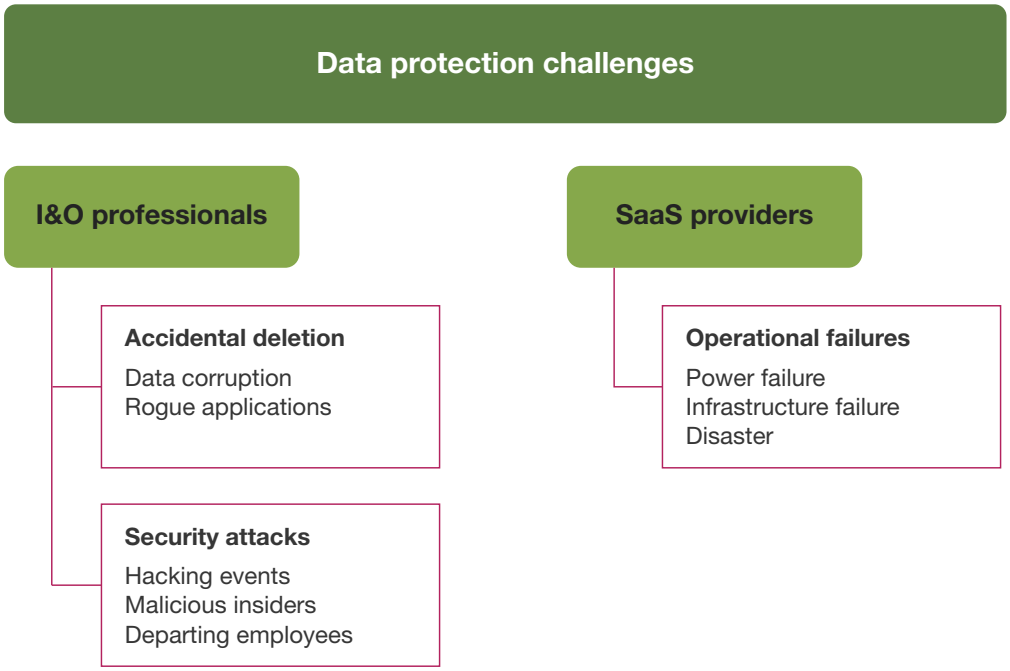
- **Accidental deletion.** This is the most basic and common cause of the loss of both on-premises and cloud-based data. This can be problematic, especially if the user fails to immediately notice the deletion and the data ages out of their trash can.[3] Accidental deletion can also take the form of 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. Most 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. Quite often, the client is responsible for securing the data hosted in SaaS.[4] 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.[5]

- **Rogue applications.** With the ecosystem of add-on applications for popular SaaS solutions growing by the day — Salesforce's AppExchange now boasts more than 3,300 apps and more than 4 million installations — we're seeing growing concern about rogue third-party applications causing damage.[6] What happens when the app that's supposed to consolidate duplicate records accidentally deletes or corrupts unique records?
- **Prolonged outages.** An unexpected and prolonged outage at your SaaS provider can be the remote incident that cripples your business. Unless you have a plan for how to handle such circumstances, it's highly unlikely that you'll have access to your data. Insurance brokerage firms in the UK using services from SSP Worldwide were rendered helpless when SSP faced a three-week-long outage.[7] Brokers could not issue new policies, look up the expiration dates of existing policies, or communicate with their clients. SSP Worldwide couldn't recover some clients' data from backup instances — and to brokers' utter dismay, SSP Worldwide assumed no responsibility for losses they suffered due to the outage.
- **Data retention policy for audit or compliance purpose.** While your organization's policy or regulatory compliance mandates require you to retain data for few months or years, your SaaS providers won't preserve data for that long. ServiceNow only keeps a rolling backup of the past 28 days and the Oracle SaaS service retains data for 60 days from the last backup.[8]

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. Providers explicitly call this out in their terms and conditions. However, in situations such as disasters or infrastructure failures, SaaS providers do assume responsibility and take operational measures 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 most enterprise-grade SaaS offerings have robust methodologies for backing up and restoring data within their scope of responsibility, they may not make this technology available to users (see Figure 2). If you lose data through no fault of the provider — such as when one of your employees accidentally deletes data — it may not entertain requests to retrieve data from its backups. Even if it does, you'll likely encounter delays, restrictions, and even significant fees.[9] Salesforce charges a minimum of $10,000 to recover customer data, and it can take several weeks.[10] If you've categorized a SaaS service as critical, it's time to work with the provider 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 vendors.

FIGURE 2 SaaS Vendors Have Varied Backup And Restore Strategies

Vendor	Backup-and-restore methodology to prevent data loss	Restore policy if customer loses data
Adobe	Adobe uses Amazon Web Services (AWS) public cloud infrastructure to host its cloud applications; as part of the S3 redundancy functionality, files are replicated across AWS availability zones for backup.	Adobe commits to a basis AWS S3 restore policy. Once an end user deletes data within an Adobe cloud solution, Adobe deletes the data according to the customer agreement and its privacy policy.
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 registration and account information.	Information was not publicly available.
athenahealth	Information was not publicly available.	Information was not publicly available.
Box	Box stores and processes customer data at three third-party data center hosting facilities in Northern California and in third-party cloud computing and hosting facilities inside and outside of the US. Current disaster recovery arrangements include near-real-time replication of the production environment to a facility in Las Vegas. In addition, all customer data is replicated on a third-party storage platform located inside and outside of the US.	Customers can choose to enable or disable the trash, determine who can permanently delete content in the trash, and set the duration that items will remain in the trash of managed users' accounts. In most cases, legal holds and retention policies will trump trash settings. If the trash is set to "Nobody," "Never Delete," or "Legal Hold," nothing gets deleted. In the event of issues like primary file storage unavailability, customers can retrieve or restore files from Box's cloud-based secondary storage systems.
Cisco Systems	Aside from Global Site Backup, Cisco WebEx uses traditional backup methods and has the ability to restore data if and when necessary.	Information was not publicly available.

FIGURE 2 SaaS Vendors Have Varied Backup And Restore Strategies (Cont.)

Vendor	Backup-and-restore methodology to prevent data loss	Restore policy if customer loses data
Citrix ShareFile	Citrix backs up webconferencing data at least daily. It backs up ShareFile databases to an alternate site with the ability 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 within geographies. For extra resiliency, ShareFile can optionally back up customer files to a facility on the US East Coast, giving 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 recycle 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 only recover 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 OnDemand	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 they're 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 SaaS Vendors Have Varied Backup And Restore Strategies (Cont.)

Vendor	Backup-and-restore methodology to prevent data loss	Restore policy if customer loses data
IBM Connections Cloud	Every data center is fully duplicated and backed up in near real time to a remote alternate site via data replication. 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 provides several safeguards to protect against accidental deletion and enable data recovery within IBM SmartCloud Notes. These range from standard trash can second chances to a locked-down trash can for IBM SmartCloud Notes that the client's admin can configure to prevent end users from emptying their trash for up to 90 days, followed by automatic deletion.
Intuit	In addition to always maintaining two copies of data, Intuit automatically backs up updated data every day. Data is stored on redundant, firewall-protected servers so it is safe from hardware and software failures, hackers, and viruses.	Because 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)	Full backups of customer data are performed weekly and incremental backups daily. Customer 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.	Microsoft's support services team can help recover lost data without a fee; clients need to raise a service request. Clients must engage Microsoft directly, as it does not let any third parties access client data in such scenarios. Microsoft commits to delivering 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, encrypted offline remote backup, and near-real-time replication to the disaster recovery 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 allows end users to recover accidentally deleted files from a recycle bin. Administrators can restore data, such as collections, and deleted users.
NetSuite	NetSuite conducts hot backups and stores data offsite in a secure location that is safeguarded against almost any environmental conditions.	Information was not publicly available.

FIGURE 2 SaaS Vendors Have Varied Backup And Restore Strategies (Cont.)

Vendor	Backup-and-restore methodology to prevent data loss	Restore policy if customer loses data
Oracle BigMachines	Oracle periodically makes backups of 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 the ability to roll back at any time.	On an exception basis and subject to written approval and additional fees, Oracle may help customers restore data that they may have lost as a result of their 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 help customers restore data that they may have lost as a result of their 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 help customers restore data that they may have lost as a result of their own actions.
Oracle RightNow Technologies	Oracle backs up customer data once in each 24-hour period. Oracle may retain customer data in backup media for an additional period of up to 12 months, but is not obligated to do so unless required by law.	On an exception basis and subject to written approval and additional fees, Oracle may help customers restore data that they may have lost as a result of their own actions.

FIGURE 2 SaaS Vendors Have Varied Backup And Restore Strategies (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. With the exception of Taleo Learn products, 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 help customers restore data that they may have lost as a result of their own actions.
Salesforce	All customer data submitted to the Covered Services, up to the last committed transaction, is automatically replicated in near real time to the secondary site. It is backed up on a regular basis and stored on backup media for an additional 90 days for production environments and 30 days for sandbox environments, after which it is securely overwritten or deleted. Any backups are verified for integrity and stored in the same data centers as their instance.	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 an online/hot database disk-to-disk backup of the entire instance.	ServiceNow can restore customer data from any of the backups (the last seven daily backups or the last four weekly backups). Customers can back up or restore data from their instance using ODBC.
Ultimate Software	With its 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 SaaS Vendors Have Varied Backup And Restore Strategies (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.	Zuora's database restore process operates at a shared level — colocated tenants' data is stored intertwined. It provides backups for infrastructure-level failures, not customer data loss due to application bugs or accidental deletion. As backups contain the intertwined data of multiple tenants, they cannot be exposed to clients. Customers are advised to use predefined interfaces such as AQuA to back up their data periodically.

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

Today's 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 is unacceptable, as is informing them that data is unrecoverable. As more critical data moves to SaaS, I&O leaders must proactively 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.** The number of cloud-to-cloud backup solution providers has grown tremendously in recent years; examples include Spanning, OwnBackup, and Datto Backupify. SaaS solution vendors themselves and these providers offer a simplified way to automatically back up 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 find and restore lost data with as little pain as is possible. Most of the solutions on the market today use Amazon Web Services or Microsoft Azure as the storage target.
- **Talk to your SaaS provider about its backup and restore policies.** Negotiate if you must. Several SaaS providers, such as Adobe, Box, and Microsoft, already have a strong backup and recovery story, and you may decide that 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 ask the provider to store backups in a different region or availability zone.
- **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 none offers 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

If you're considering investing in cloud-to-cloud backup services, a handful of vendors can help (see Figure 3). If you need to back up G Suite, Office365, or Salesforce, you have plenty of options. But if you must protect data from SAP, ServiceNow, Oracle, or Workday SaaS services, you'll struggle to find vendors that can help. Even leading cloud-to-cloud backup providers have made little progress adding support for SaaS providers, but pursue a partnership with them to build support for your next planned SaaS application. Continued SaaS momentum and growth require a fully functioning three-way ecosystem: 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.

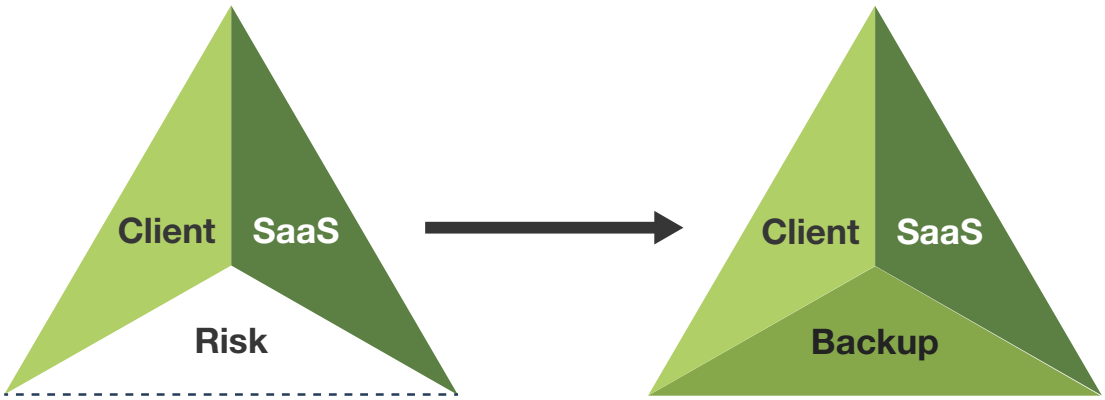
FIGURE 3 Cloud-To-Cloud Backup Solutions Don't Support All SaaS Apps

Vendor	SaaS apps protected	Number of users under management	Price	Storage targets
Asigra	• G Suite • Office 365 • Salesforce	360,000	Partner-led; does not sell direct.	MSP data centers, customers' on-premises storage target, or both.
AvePoint	• Dynamics 365 • Office 365 • Salesforce	Not available or the Forrester team could not arrive at a reasonable estimate.	$4/month/user; additional pricing plans available	Microsoft Azure; clients can bring in their own storage
CloudAlly	• Box • G Suite • Office 365 • Salesforce	400,000 (estimated)	$3/month/user or $30/year/user	AWS
Cloudfinder	• Box • G Suite • Office 365 • Salesforce	Not available or the Forrester team could not arrive at a reasonable estimate.	Does not sell direct.	Cloudfinder SafeHaven vault
Commvault	• G Suite • Office 365 • Salesforce	About 20,000	$7,250 per terabyte perpetual	Customers' on-premises protection storage
Datto Backupify	• G Suite • Office 365 • Salesforce	3.5 million	$3/month/user; flexible storage pricing plans also available	Datto Cloud
Druva	• Box • G Suite • Office 365 • Salesforce	175,000	Enterprise: $48/user/year Elite: $84/user/year ElitePlus: $144/user/year	AWS or Microsoft Azure
NetApp Cloud Control	• Office 365	Not available or Forrester team could not arrive at a reasonable estimate.	$45/year/user	AWS; Microsoft Azure blob storage; NetApp StorageGRID

FIGURE 3 Cloud-To-Cloud Backup Solutions Don't Support All SaaS Apps (Cont.)

Vendor	SaaS apps protected	Number of users under management	Price	Storage targets
OwnBackup	• ServiceNow • Salesforce • Slack	500,000 (estimated)	$3/month/user	AWS
Spanning	• G Suite • Office 365 • Salesforce	1 million	$40 or $48/year/user	AWS
SysCloud	• G Suite • Salesforce	200,000 (estimated)	$4/month/user	AWS
Skyvia	• Box • G Suite • FreshDesk • Magento • MS Dynamics 365 • MS OneDrive • NetSuite (beta) • QuickBooks • Salesforce • Shopify • SugarCRM • Zendesk • ZohoCRM	200,000 (estimated)	Standard: $9/month for 20 GB Professional: $99/month for 20 GB Enterprise: $499/month for 1 TB	Microsoft Azure
StorageCraft	• G Suite • Office 365	Not available or the Forrester team could not arrive at a reasonable estimate.	Partner-led	AWS or Microsoft Azure

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 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 sourcing and vendor management colleagues to review vendors' contractual terms on backup and disaster recovery to see what you can expect if you lose data. If contracts are vague or inconclusive, ask the provider for further clarification. If you're dissatisfied with the recovery options your vendor provides, negotiate for additional services — some providers are more open to this than others. 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:

- **"What's your backup-and-restore methodology to prevent data loss?"** Look for vendors that perform 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 vendor's fault (e.g., due to accidental deletion or a malicious user), you need to know whether the vendor restore your data — and if so, how long it will take and how much it will cost. Few vendors have set service-level agreements on this operational model.
- **"Can customers backup and restore their own 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 you review your vendor's backup and recovery abilities, you should also examine its disaster recovery capabilities. Get a detailed outline of how the vendor will recover or fail over in 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."

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. By default, deleted Office 365 data is nonrecoverable after a maximum of 30 days.

[4] The Oracle cloud master services agreement states that "You [the client] are responsible for any security vulnerabilities, and the consequences of such vulnerabilities, arising from your content." Source: "Oracle Cloud Services Agreement," Oracle (http://www.oracle.com/us/corporate/contracts/cloud-csa-v030917-us-en-3657533.pdf).

[5] SaaS isn't immune to insider threats, and you must develop plans to deal with the risks. For more information, see the Forrester report "Best Practices: Mitigating Insider Threats."

[6] Salesforce AppExchange lists all of the marketplace applications available. Source: Salesforce AppExchange (https://appexchange.salesforce.com/appxStore?type=App).

[7] SaaS providers should assume data loss responsibility if losses are due to 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," Insurance Age, 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 because of using its software. Source: Caroline Donnelly, "SSP Worldwide customers call for revised compensation offer for two-week cloud outage," ComputerWeekly.com, October 17, 2016 (http://www.computerweekly.com/news/450401120/SSP-Worldwide-customers-call-for-revised-compensation-offer-for-two-week-cloud-outage).

[8] ServiceNow retains 28 days of backed up data on a rolling basis. Source: ServiceNow (https://www.servicenow.com/company/trust.html#data-retention).

[9] On an exception basis and subject to written approval and additional fees, Oracle may help customers restore data that they may have lost due to their own actions. Source: "Oracle Cloud Hosting and Delivery Policies," Oracle, June 2017 (http://www.oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf) and "Oracle SaaS Public Cloud Services," Oracle, October 2017 (http://www.oracle.com/us/corporate/contracts/saas-public-cloud-services-pillar-3610529.pdf).

[10] Salesforce has a defined policy that lists the cost and time to recover the data from a point-in-time snapshot. Source: "Data Recovery Service and Cost FAQ," Salesforce Help & Training (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.

136661