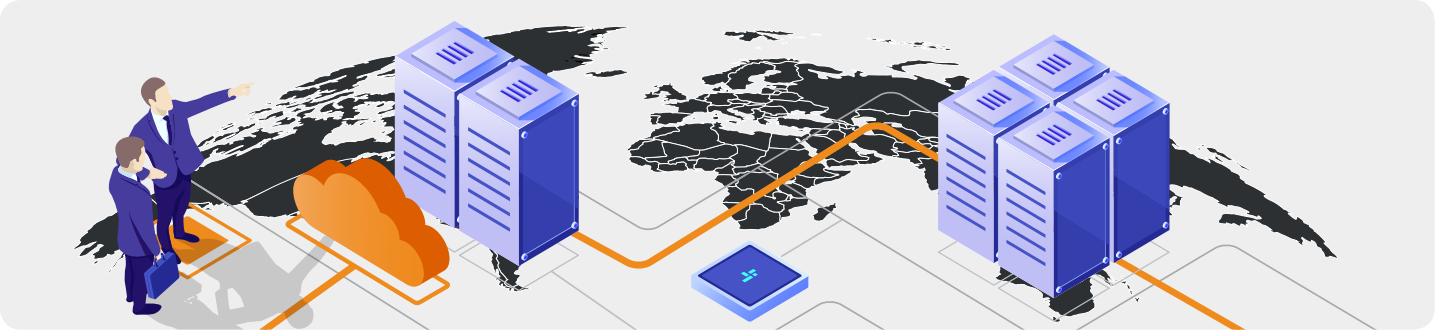
KeepItSafe®



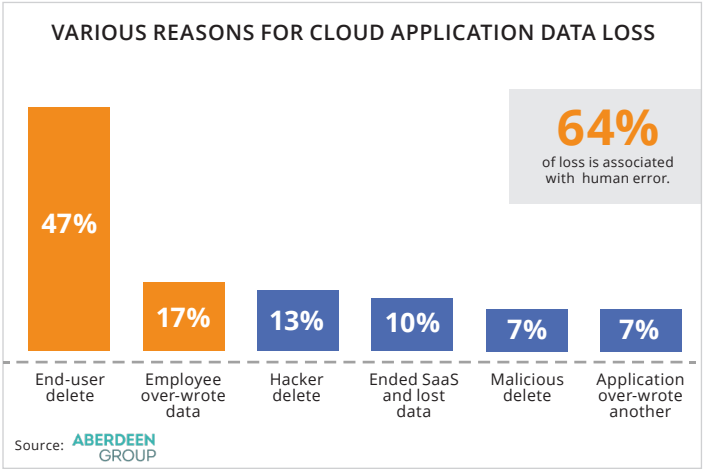
The Mission-Critical Data You're Probably Not Backing Up

If you're a backup admin, you've got network backup down pat. However, there are two critical data locations that you may not be backing up – either because you're not sure how, or because you don't know you should. These areas are SaaS/PaaS and mobile endpoints.

Here's the problem in the proverbial nutshell:

1. **Not backing up for data protection.** Your users are storing a lot of mission-critical information in your SaaS/PaaS infrastructure, and on their mobile devices. However, your SaaS/PaaS providers are likely not backing up your data past a few days. And you may not be backing up your mobile endpoints at all.
2. **Not backing up/archiving for eDiscovery and compliance.** If you're not backing up your mobile endpoints, you have no federated search capability. And although users may search their personal SaaS data, admins and attorneys have no federated search or legal hold capabilities.

Data protection and searchability are hard-wired into network backup. With 70% of organizations having either apps or infrastructure running in the cloud, per IDG, why is there a lack of backup for SaaS/PaaS and mobile endpoints?



THE CHALLENGE OF SaaS AND MOBILE ENDPOINT BACKUP

SaaS/PaaS

Aren't your SaaS and PaaS providers backing up your data? Not really. They're doing a good job at keeping it available. Backing up? Not so much. Yet there is a lot of risk to your online data.

Millions of people use Office 365 for mission-critical work, and many organizations are only relying on Microsoft's geo-distributed Database Availability Groups to protect against data loss from user error, ransomware, and other threats. This backup exists primarily so Microsoft can restore massive data volumes in case of a catastrophic event. This gap in its native capabilities can cause a multitude of operational, security and legal headaches down the road.

Microsoft does backup user data to a point. For example, SharePoint Online data is available up to 29 days. And under certain conditions and within 90 days, Office 365 users can restore deleted messages and mailboxes. But after those time periods, you are out of luck unless you have set up complicated policies on your Office 365 account.

> *"As you move to cloud applications, unless you're using one of the few SaaS data-protection solutions, your data has just gone from well protected to unprotected."* - ***Jason Buffington, Senior Analyst, Enterprise Strategy Group***

To be fair it's not only Microsoft but rather most SaaS services like Box, Salesforce, Google Apps, etc. suffer from the cloud backup gap. Although their cloud data is protected in case of corruption, this does not mean that your SaaS provider will be able to restore content in a way that meets your needs or internal service level agreements. Nor do they create individual customer archives for long-term data retention and searches. You will need to look to a cloud to cloud (C2C) backup offering to get the protection your data needs.

Endpoint Protection

It's the nature of the beast that employees will store data on laptops, tablets, desktops, and smartphones – yet mobile devices are at constant risk of damage, loss, and theft. Multiply that risk by the sheer number of devices out there: an average of 3 devices per employee. That's a lot of mobile endpoints to protect. And BYOD (Bring Your Own Device) exacerbates the problem. How do you secure and protect an individual's personal device without compromising personal information?

> *"... the dispersion of data — which can now be stored across millions of endpoints and cloud applications — is causing heightened concern within the enterprise. The decentralized nature of the modern enterprise is great for increased productivity among the workforce, but it has created a nightmare for business executives in terms of security and risk."* — ***IDC***

Yet backing up endpoint devices is critically important to your business. You need a solution that will protect corporate data on employee mobile devices by capturing it, backing it up to the cloud, rendering searchable backup/archives, and enabling RTO/RPO in case of data loss or corruption.

Best Practices for SaaS/PaaS Backup and Endpoint Protection

Whether you are backing up from SaaS/PaaS or from mobile endpoints, look for the following capabilities in your solutions:

- ✔ Combine multiple views and backup administration in a centralized management console.
- ✔ Provides integrated data protection across hybrid clouds and multiple clouds.
- ✔ C2C should at least support Office 365, not only Exchange but also SharePoint Online and OneDrive.
- ✔ Extra points for additional SaaS support like Salesforce or Google Apps. And your mobile endpoint solution should cover laptops, tablets, smartphones, and desktops.
- ✔ Enable federated searchable archives. This capability supports eDiscovery projects and legal holds, as well as compliance investigations.
- ✔ Granular solution that backs up and restores files, folders, and volumes. Enable IT to assign different backup policies to differing RTO/RPO requirements.
- ✔ Highly secure cloud infrastructure with SAS-70, SSAE-16, or SOC1 certifications. Multi-zone redundancy is optional but attractive. Secure encryption at-movement and at-rest; robust user access security.
- ✔ Optimize WAN utilization with fast high-volume data transfers between the SaaS provider and backup cloud, and from mobile endpoints to the backup cloud.
- ✔ Remember AWS backup for long-term data protection and management. Public clouds are highly concerned with availability, but not with individual customer backup past 30-90 days.

There are several solutions out there that have these capabilities but differ in execution. Some offerings are SaaS offerings themselves and run exclusively from the cloud. Others are backup products that add C2C backup capabilities to their on-premise offerings. Some backup mobile endpoints only, others SaaS/PaaS only, and some do both.

Choose the solution or combination of solutions that work best for your data protection and business needs. To be sure, choosing and deploying the solutions you need can be time-consuming and complicated. Uncomplicate it by partnering with a trusted provider for comprehensive C2C and endpoint backup.

KeepItSafe offers comprehensive cloud data availability solutions — contact us.

888 965 9988 | www.keepitsafe.com | sales@keepitsafe.com