10 Reasons Why MSPs Need Cloud-to-Cloud Backup and Recovery

January 2014

Introduction

The tremendous growth in cloud services and their improved reliability and security have led many managed services providers and their clients to the erroneous belief that data in the cloud will never be lost or lead to business continuity issues.

It is true that clients who have moved to the cloud won't experience old-school on-premises problems stemming from hard drives crashing, motherboards failing or power supplies being accidentally knocked out. But the reality is there is still a risk of data loss in the cloud, and managed services providers (MSPs) need to help clients prepare for potential problems. Here are 10 reasons why MSPs need an effective cloud-to-cloud backup solution to better serve clients and improve their businesses:

Reason No. 1: User Error

Problems around user error don't go away when a client organization moves to the cloud. In fact, in some cases there may even be the potential for users to make more mistakes in the cloud. That's because there's more opportunity for user error when so many data updates are made in real time through cloud-based applications. For example, a user may delete an email or voicemail that has been delivered to his email, thinking the retention policy for this type of communication is months, not weeks—only to learn that the item has been deleted at a system level after only 30 days. Knowledge workers struggling with the flood of inbound communications often will put off "important non-urgent" items, only to learn later that the emails and voicemails have been deleted completely.

Users are still going to make mistakes, and they're still likely to accidentally delete files or delete specific data without realizing what they've done, until it is too late. MSPs can help clients head off potentially aggravating and egregious data-loss issues through cloud-to-cloud backup and recovery.

Reason No. 2: Malicious User Activity

In addition to accidental data loss from everyday user activity, there's also the risk that malicious users can wreak havoc in cloud accounts, even after they've been terminated and left the premises. Are your clients ready for the possibility of a disgruntled employee logging into Google Apps and dragging all of their relevant emails into the trash can, so it is deleted for good?

Similarly, do your clients have controls in place to prevent criminal employees from hiding fraudulent behavior through the same means? In other cases, hackers may gain access to sensitive internal systems and threaten data deletion if a ransom is not paid. Like negotiating with terrorists, paying ransom to hackers rarely ends well. The safest solution to a threat like this is a complete system-level backup, geographically and logically separated from the production systems.

MSPs can provide some mitigation against this risk through a full slate of cloud-to-cloud backup services.

Reason No. 3: Flawed Migrations

Many organizations depend on their MSPs to help them perform routine migrations while servicing cloud accounts. Whether it is moving records from one user account to another or migrating a whole set of data from an old service to a new service, there's always potential for a migration process to go wrong.

Should the migration cause overwriting of data or accidental deletion of a massive number of accounts, a repository of data outside the service that is linked to granular recovery points can provide much-needed peace of mind for the MSP and the client.

Reason No. 4: Third-Party Software

Syncing data with other solutions may severely corrupt data, causing manual rework or requiring all data to be regarded as incorrect and re-entered from scratch. For example, if a user's inbox goes missing after a new email client is utilized, it can be restored from a cloud-to-cloud backup solution. In other instances, third-party software or sync tools can sometimes corrupt data or render it useless. This frequently occurs with contact data.

With point-in-time recovery, a user's entire contact database can be restored from an earlier point in time in a correct state, saving countless hours of rework. As the hybrid world becomes increasingly complex, third-party software interaction with cloud data is a looming risk. MSPs can help shield their clients from this risk.

Reason No. 5: Data Fragmentation

As line-of-business leaders increasingly purchase cloud services directly for their departments, data has begun to creep across a whole host of cloud platforms. MSP clients are increasingly in need of a way to help solve a resultant data fragmentation problem that makes it difficult to track, search, back up and recover relevant business data.

eFolder Cloudfinder currently services the four major business-to-business Software as a Service (SaaS) players—Microsoft Office 365, Google Apps, Salesforce and Box. eFolder's vision is to expand to support dozens more SaaS platforms, so that managed services providers can use Cloudfinder to help clients solve the fragmentation problem.

Cloudfinder allows for the data to not only be centrally backed up and protected for simple restoration, but also easily searched, with reporting on exactly where it resides.

Reason No. 6: Compliance Violations

With so many MSP clients operating in regulated industries that require strict privacy controls around user information, patient information, customer information and so on, the cloud can present a minefield of potential compliance violations. Often, native cloud applications don't provide enough data control to stem the tide of compliance issues.

Backup and recovery services may not be a panacea for cloud security issues, but MSPs can use them to at least help organizations address some important compliance requirements. Built with appropriate reporting, backup and recovery services can greatly aid in data discovery and understanding where it sits. Similarly, such services can also ensure that data is protected from fraudulent or accidental deletion. Additionally, they can aid in mirroring and restoring data when incident responders must engage in forensic examination of systems.

Reason No. 7: Self-Service Client-Level Restoration

Anytime a client picks up the phone to call help desk for assistance with a problem, it costs someone time and money. MSPs can leverage cloud-to-cloud backup and recovery solutions to help individual clients automatically restore data when users in the organization have lost or deleted data on their cloud accounts. This can greatly reduce the cost of help desk and technical support, and help MSPs maintain high levels of client satisfaction in the process.

Reason No. 8: No Cloud Provider Is Perfect

While most cloud providers have made great headway in improving the resiliency and reliability of their services, at the end of the day clients are betting their business operations on the ability of that provider to offer constant access to critical business data in the cloud.

Backup and recovery services will give MSP clients some insurance on that bet, so that if outages or system failures do occur, they're not left in the lurch as a result. MSPs can ensure that client employees never miss a beat, even if a cloud service someday performs less than perfectly.

Reason No. 9: Maintaining a Seamless Experience Across the Hybrid Gap

Whether a workload is running on customer premises, in a public cloud or in a hybrid cloud, MSPs with full administrative engagements with clients are ultimately on the hook for ensuring consistency across the entire IT experience. Cloud-to-cloud backup and recovery services can help MSPs guarantee a seamless technology experience while still giving clients the option to maintain hybrid IT environments.

Reason No. 10: Cementing Your Position as a Trusted Advisor

That seamless technology experience is critical in establishing an MSP's role as a trusted advisor for clients. Just because a service has the Microsoft or Google name on it doesn't mean it doesn't need management and extra support.

Many of these public cloud services lack the kind of robust support that clients have come to expect when engaging MSPs for on-premises services. MSPs that can allow clients the flexibility and cost savings of these cloud services without forcing them to give up that deep support will be valued as true technical partners to the business.

About eFolder Cloudfinder

eFolder Cloudfinder is an advanced cloud-to-cloud backup service designed for easy reselling and repackaging by value-added resellers and MSPs. Cloudfinder helps service provider partners add backup, search, restoration and reporting to Office 365, Google Apps, Salesforce and Box. When clients use it for multiple platforms, Cloudfinder enables unified visibility across the cloud portfolio for a more complete IT service offering.

Corporate Headquarters
2340 Perimeter Park Drive, Suite 100, Atlanta, GA 30341, (678) 888-0700, www.efolder.net, sales@efolder.net