Follow the DATA

TO CAPTURE MONTHLY RECURRING REVENUE FROM CLOUD BACKUP SERVICES

The move to cloud computing disrupts the traditional MSP business model. How can MSPs embrace the disruption?

THE ANSWER IS: FOLLOW THE DATA.

Data migration to the cloud is a real opportunity for MSPs who deliver cloud-oriented services, and can lead to new recurring revenue and increased relevance.

50%

50% of businesses will use cloud-based office systems like Google Apps for Work or Microsoft Office 365 by 2020[2].

60%

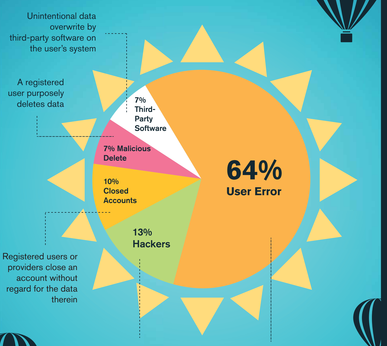
60% of total IT spending growth in 2015 was for cloud computing[1].

$282 Billion/year

$282 billion per year will be spent on public cloud services such as AWS and Microsoft Azure by 2018[3].

A comprehensive data backup strategy can prevent these

Five Most Common Data Loss Events[8]



Cloud office productivity and infrastructure services can help businesses save $$$ on IT infrastructure costs.

Most SaaS offerings provide data management and protection as part of their service.

Let's talk cloud reality

Cloud Reality #1
Cloud Platforms – Rampant Outages

Cloud platforms prioritize providing a highly available service of 99.9% uptime, but outages are rampant.

In 2015, AWS, Google Cloud Platform and Microsoft Azure cumulatively experienced 294 cloud platform outages that lasted a total of 24 hours and 53 minutes[5]. Backing up cloud-based data to somewhere other than the same cloud is essential.

Cloud Reality #2
SaaS – No Data Protection

SaaS applications do NOT offer cloud data management and data protection as part of a business's service agreement, AND almost NO legacy backup software can back up data stored in SaaS applications.

Only 41% of IT pros who have cloud office productivity and infrastructure services in their organization are using cloud backup and recovery services[6].

Cloud Reality #3
SaaS – Data Recovery is Expensive

Data recovery with SaaS office productivity providers, when possible, is EXPENSIVE and time-limited.

Salesforce.com charges $10,000 per recovery to recover deleted information more than 15 days old.

Cloud Reality #4
AWS – Protection Gaps

For organizations that leverage AWS for data storage, EBS snapshots are necessary to protect data stored in VMs and for strategic VM management and control.

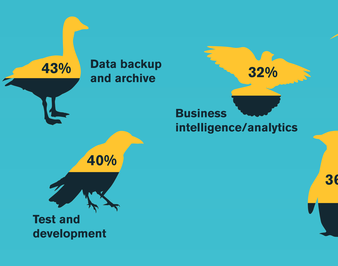
Writing complex, manual backup scripts to perform snapshots in AWS is technically challenging and very time consuming.

Cloud Reality #5
Ransomware Attacks Rising

Ransomware trojans like CryptoLocker can jump from an infected laptop to cloud-based apps with a simple sync of files, thus ENCRYPTING ALL FILES in both locations. Without data backup, restoring the data is impossible.

CryptoLocker attacks increased 50% in 2015 to more than 50,000 infected corporate machines[7].

Which IT workloads are migrating to the cloud[4]?



MSPs: Following the data will lead to monetization of the cloud.

Embrace new cloud data protection services

Design best practices and data protection strategies for your customers

Extend the conversation with customers about other cloud data management services

Asigra works with a global ecosystem of managed service providers who use Asigra Cloud Backup™, a comprehensive, secure software solution, to deliver cloud backup and data recovery services to SMBs and Enterprises worldwide protecting data born in cloud-based SaaS applications and platforms. Asigra supports all cloud deployment models – public, hybrid, and private clouds.

Follow the data, and discover new monthly recurring revenue opportunities with Asigra.

Learn more about becoming an Asigra partner at http://www.asigra.com/partnering

[1] Barron's – 2016 Will Be All About the Cloud
[2] Gartner Report – Do You Need to Cover Your SaaS to Prevent Data Loss?
[3] Gartner Forecast Analysis: Public Cloud Services, Worldwide, 4Q14 Update April 2015
[4] ESG Research Report, 2014 Public Cloud Computing Trends, March 2014.
[5] CloudHarmony: Analysis of downtime at IaaS public cloud providers in 2015
[6] Spiceworks 2015 State of IT Report
[7] Kaspersky Lab on business threats: 2015 saw the number of cryptolocker attacks double
[8] Aberdeen Group: Downtime and Data Loss: How Much Can You Afford?

Asigra.
Recovery is Everything™