EVault®
A Seagate Company

The best case for the worst case.™

White Paper

Four Myths of Cloud Backup

Once touted in some circles as the centerpiece of future IT strategy, the cloud is undergoing a huge reality check that has dampened some of the enthusiasm. Costly disasters, random outages, and even concerns over government spying have slowed the growth of cloud adoption, particularly in the area of backup and recovery.

Many of the objections IT leaders have to the cloud today have sprung from myths that have reached urban-legend status. Simply put, cloud backup isn't as fraught with peril as some observers believe it to be. Moreover, while bad news, accurate or otherwise, travels fast, good news about cloud backup and recovery has been slower to reach many IT departments.

But that good news does exist. This paper will look at four of the popular and damaging myths surrounding cloud backup and recovery and set them straight—and in so doing, affirm that the cloud remains not only a viable option for backup but also the best one.

1 Myth No. 1:
It's Impossible to Maintain the Privacy of Data Stored in the Cloud

This might be the most pervasive and most damaging myth facing cloud computing today. By its very nature, the cloud leaves data exposed at some point, open to prying eyes of people who shouldn't see it, right? Isn't this the biggest drawback with cloud computing in general?

The answer to both questions is, "No—provided the cloud-based backup and recovery platform is set up correctly." Yes, a leaky cloud can rain data into places where it shouldn't fall, but proper encryption properly implemented can keep data airtight even in a cloud environment. Here's how.

Truth:
Properly Encrypted Data Is Equally Secure Anywhere—Including the Cloud

The first question any IT organization should ask when looking to back up data in the cloud revolves around how a cloud provider secures that data. How does the service provider encrypt it? Multipoint encryption is absolutely critical to data protection, a point many organizations either don't understand or choose to ignore.

Close the Backdoor

In the days of simple client-server computing, security backdoors were sometimes useful tools that allowed IT professionals to look into their networks without the hassle of dealing with encryption or authentication. But with the increased efficiency and lower costs of cloud computing have come more sophisticated attacks on corporate networks and greater responsibility to make sure that all data and all access to that data are protected at all times. That includes protecting and restricting data access by a cloud provider.

The first best practice in encryption is to encrypt at the source. The key is to find a tool that will encrypt data before it leaves the organization's own environment. Interestingly, a great deal of corporate data is not encrypted at the source, meaning that it's vulnerable while it's sitting in the data center, or on laptops or mobile devices. Find a cloud provider with multipoint encryption, and you'll have better data privacy protection than many corporate systems.

The next key target for encryption is data in transit. Data should always be encrypted as it moves across an organization's network, to and from a cloud provider. The final critical point for encryption is when data is "at rest" in the cloud data center.

Details matter where encryption is concerned. AES (Advanced Encryption Standard) is the only encryption standard that is certified by the government for classified materials, and it is the standard organizations should employ with their cloud providers or within private clouds.

NIST FIPS Certification

NIST FIPS certification validates best practices for cloud data security, such as:

- End-to-end encryption at all protected sites
- Encryption key safeguarding
- Password management and rotation
- Digital signature for every file and block of data
- Data destruction based on policy with certificate of destruction

Validation of cloud security is, therefore, extremely important. One excellent resource for validating cloud security is NIST (National Institute of Standards and Technology), an agency of the United States Department of Commerce. The NIST Federal Information Processing Standards (FIPS) provides the federal government and legal entities with a roadmap for cloud computing standards and controls, especially relating to cloud security and privacy.

Truth:

If You Control the Encryption Keys, You Control Privacy

The management of encryption keys is also an important consideration. These keys should be stored in a separate location from the encrypted data to avoid having a single point of compromise. In that same vein, a cloud provider should never maintain an organization's encryption key, nor should it require data to be unencrypted so that it can perform deduplication.

Organizations always need to maintain their own encryption keys and must demand encryption of data at all times. Anything less will compromise data security. Outsourcing to a cloud vendor makes sense—to a point. Giving away the keys to the kingdom, though, should not be part of an outsourcing agreement.

2 Myth No. 2:
It's Impossible to Control Who Has Access to Cloud Data

So, data is encrypted. But there's still the question of who has access to it. Popular belief among many in IT at the moment is that controlling access to cloud data is nearly impossible, or at least prohibitively complicated.

It is, in fact, not only possible to control cloud access, it's necessary. And it doesn't have to be overly complex. There are several ways of ensuring that only the right sets of eyes have access to data stored in the cloud.

Truth:
No One Can Access Your Cloud Data Unless You Let Them

Again, most importantly, organizations—not their cloud providers—should control encryption keys for unlocking their data. Furthermore, organizations must ensure that they've safeguarded network access back into their onsite IT infrastructures. Don't unknowingly create security backdoors.

It's critical that organizations ensure that the network firewall access they give cloud providers is narrowly defined, and that companies force authentication before giving any access to data. Also, customers should quiz service providers on how they monitor network traffic for anomalies that might suggest inbound DoS/DDoS attacks. Prevention plus the capability to recover is a far better strategy than recovery alone.

Another critical element of ensuring that only the right people have access to data is ensuring that only the right people have access to the data center. Physical systems that house user data should only be accessible by employees with a legitimate business need, and authentication and key management data centers must be completely inaccessible to noncredentialed employees.

If nonessential personnel or authorized contractors need access for any reason, they should be logged in and escorted by credentialed employees at all times. The best architectures are built to require two authorized employees before any data can be accessed. In many cases, a third-party provider is actually in a better position to provide these safeguards than an organization's internal IT department.

3 Myth No. 3:
The Cloud and Compliance Don't Mix

Yes, compliance is complicated, and it's critical. Particularly in industries such as finance and healthcare, compliance can make or break an organization, literally. Many organizations, fearing compliance issues, choose not to back up data in the cloud.

They don't have to reject the cloud, though. Done properly, cloud backup and recovery can be well within the parameters of compliance. The key is to find a service provider that has credibility with compliance issues and the credentials to back it up.

Truth:
Compliance Can Actually Get Easier with an Audited Cloud Provider

It's absolutely critical that cloud service providers know and abide by the laws governing compliance and data access, and that they submit to or have submitted to audits verifying the security of their systems. Due diligence is the best practice here.

EVault Customers and Superstorm Sandy

In part thanks to advance warning and preparation from EVault, EVault customers were in recovery mode before Superstorm Sandy even hit and, once the storm had passed, their total recovery times were remarkably fast. One manufacturing customer with a 48-hour service-level agreement (SLA) was online after just six hours despite flooding and a loss of power.

With EVault, during and after Sandy, businesses kept running in the cloud even while dealing with washed out roads, flooded buildings, and extended power outages. Geographically dispersed data centers kept data safe even though the entire eastern seaboard was knocked out. And managed services were there every step of the way. IT attended to immediate emergencies while relying upon managed services to recover systems.

Audits provide cloud consumers with assurances that cloud providers are in compliance with federal, state, and other regulatory mandates to ensure data privacy and data protection. For example, under California law, service providers must notify customers as well as the state if data privacy is compromised. Furthermore, state law mandates service providers submit information showing they are using best practices to ensure protection of consumer information.

Formal independent audits with SSAE 16 and ISO 27001 can verify that the cloud provider's data centers have met rigorous requirements around physical security, physical access, and internal controls. The audit process also allows cloud providers to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. This is especially important for FIPS and HIPAA compliance.

Also, IT professionals should always ask "what if?" questions of cloud providers. These are the questions IT pros would have to answer if the FBI, the CIA, the SEC, or corporate lawyers came knocking on their door. The most important among these is: What if the provider is asked to turn over an organization's data? Also related to compliance is expiration of data. If an organization is only required to retain data for six years, IT pros should understand exactly how a cloud vendor will retire or permanently destroy that data in a way that ensures no one has access to it.

4 Myth No. 4:
Cloud Backup Doesn't Provide Fast Recovery

A final prevailing myth about the cloud is that while it might be an inexpensive option for backup, it's a useless option for backup's more important cousin, recovery. After all, backing up data does no good if an organization can't recover that data quickly after a disaster. Many IT pros prefer to back up data onsite, cost or no cost, due to the belief that recovering data in-house is more efficient than recovering from a cloud model.

This myth is simply not true—as long as the cloud provider has ensured a safe and recoverable setup for an organization's data.

Truth:
Cloud Recovery Can Be as Fast—or Faster—Than Onsite Recovery

Among the key factors for customers to investigate here are the number and location of a cloud provider's data centers. How redundant will backed up data be, and are data centers dangerously close together such that one disaster could affect two or more of them?

Customers also need to make sure they understand a service provider's guaranteed recovery time and ensure that it fits their organization's needs. Can a business survive on a 24-hour recovery turnaround, or does it need to be four hours?

Preventive action from cloud providers can be a great asset here. For example, a cloud vendor can monitor weather reports and let customers know when a disaster might be headed their way.

When organizations do their due diligence and find a service provider who lives up to or exceeds their agreements, recovery time is not only not a problem, it's generally much faster than it would be onsite.

In Conclusion: All Clouds—and Cloud Vendors—Are Not Created Equal

The myths about cloud backup and recovery aren't without some basis in truth. Cloud disasters do occur, and organizations and cloud vendors alike have to be diligent to keep a secure, recoverable cloud platform up and running. When they do, the results can be tremendous, and the myths are easy to dispel.

There is no question that businesses can benefit from moving data to the cloud. The cloud is elastic and efficient. It can improve user productivity and unburden IT staff, saving time and money. It can accommodate anything from simple file sharing to mission-critical data backup. But it's important to remember that all clouds or vendors are not created equal. Organizations must:

- Understand which technologies and operational best practices are necessary to enable an iron-clad, rock-solid cloud environment
- Know the business track record of a service provider, what its core competencies are, and how well they map to business requirements
- Realize that a service provider is an extension of an IT team and should serve as a trusted adviser when disaster strikes
- Be aware that outages occur, but if that translates to business interruption, then organizations need to have a clear picture of how their service providers define SLAs associated with recovery—and make sure the SLA is guaranteed

Armed with the truth about cloud backup and recovery, along with a better understanding of the underlying processes, personnel, and technology issues involved, IT pros can transform cloud backup from a source of uncertainty and doubt into a business advantage. And they may experience something they might never have expected from a move to the cloud: peace of mind.

About the Author

David A. Chapa, EVault Chief Technology Evangelist, has more than 25 years in the storage industry, focusing specifically on data protection, disaster recovery, and business continuity. He has held senior-level technical positions with companies such as Quantum, OpenVision (VERITAS), ADIC, Unisys, NetApp, and the Enterprise Strategy Group (ESG). He has been a featured speaker at major industry conferences and is a recognized blogger and author. He is coauthor of *Implementing Backup and Recovery* and technical editor of "Cloud Security," "Security 2020," and "Web Commerce Security Design and Development."

2013.12.0003_wp_us (updated 12/27/2013)