The Myths and Realities of Cloud-Based Data Protection

Setting the record straight is more important than ever in light of the rise of ransomware.

VERITAS

Sponsored

CIO FROM IDG

Cloud infrastructure is so easy to set up and manage that one can easily be lulled into an assumption that the cloud is a "set it and forget it" proposition. This is understandable: Cloud providers do an excellent job of abstracting away tasks such as load-balancing, infrastructure optimization, and routine systems administration. They provide predictable performance and nearly limitless scalability. They also maintain strong security for their own infrastructure.

But when it comes to protecting individual customer instances and data, the situation is more complex. Most cloud providers leave it up to customers to police access to their accounts and protect their own data. The simplicity of cloud infrastructure is so seductive that customers can easily forget that a cloud server guarded by a weak password is just as vulnerable as a server in their own data centers.

In most cases, the only significant difference between cloud and local infrastructure is location, says Anthony Cusimano, cloud solutions marketing manager at Veritas. "It's a myth that cloud is different from on-premises infrastructure," he says. "It's basically a data center with different scale and location. It's folly to believe that someone else's infrastructure is going to give you the same security you'd have in your own data center."

In fact, security risks are potentially even greater in the cloud because access often isn't protected by firewalls, virtual private networks, network segmentation, and other protections that are common in on-premises environments. As a customer's cloud footprint grows, "hundreds of people may have access to critical information," Cusimano says. "When it comes to social engineering or ransomware, if just one is compromised, it's a problem."

Data Protection Myths

Another common misperception is that cloud providers include data protection as part of their standard services. The reality is that none of the major cloud providers bundles backup into core server instances, although the service may be available as a paid option.

"You cannot rely on the cloud provider to do anything to protect and verify your data," says Dave Little, a Veritas senior distinguished engineer.

Nevertheless, this myth is pervasive. A recent Veritas survey of 1,200 senior IT and business decision-makers found that 83% believe that cloud providers bundle data protection into their standard services.[1]

One possible reason for the confusion is cloud providers' well-known practice of replicating data across multiple data centers for capacity management or load-balancing purposes. However, that is no guarantee of protection, because customers don't control what is essentially a housekeeping process. Furthermore, no cloud provider will guarantee the integrity of customer data, for reasons ranging from liability to insurance costs. In short, data protection is the customer's responsibility.

Setting the record straight on cloud data protection is particularly important in light of the rise of ransomware, a pernicious new form of malware that encrypts data on PCs and servers and demands payment of a ransom in exchange for a decryption code. Cybersecurity Ventures estimates that ransomware damages totaled more than $8 billion in 2018 and that a ransomware attack will happen every 14 seconds this year.

Ransomware attacks can cripple an organization for weeks if proper backup isn't place. Although early versions of this form of malware targeted mostly PCs, more-sophisticated ransomware variants have emerged more recently that target servers and even storage devices. More worrisome is that many variants now are self-propagating, meaning that once they infect a single computer, they can spider out across a network and disable hundreds more. The source and scope of the infection can be devilishly difficult to pinpoint.

“Malware can lie completely undiscovered, stealing client data and your resources,” Cusimano says.

Most ransomware spreads via social engineering, in particular through phishing attacks. Users click on an unknown link in an email and unwittingly install malware, which then spreads. Ransomware makes no distinction between targets; if the user is logged into a cloud service, the infection will spread to the cloud instance and may infect other virtual servers as well.

Healthcare and government organizations are particularly attractive targets for attack, because budgets are limited and equipment is less likely to be updated with the latest patches. In 2019 the city of Baltimore was hit with an attack that crippled critical services for a month and cost more than $18 million. In 2017 FedEx attributed a $300 million quarterly loss largely to a ransomware attack.

No Prevention

There is currently no way to prevent ransomware. The only protection is frequent backups of critical data, so that affected equipment can be wiped clean and data quickly restored. Users now have more options than ever for doing this, including snapshot images and backups to multiple media, both locally and in the cloud. The downside of this choice is complexity. There are pros and cons to each backup option.

For example, snapshots provide the shortest-possible restore times but take a toll on performance, don’t work with all storage media, and don’t capture a full image of all stored data. Tape backup is relatively inexpensive to operate, but equipment can be expensive to install and maintain and tapes don’t permit fast access to individual files. Backing up to disk solves the access problem but is expensive. Cloud backup is limited by bandwidth and may be prohibited by regulations in some circumstances.

High-availability services aren’t a solution either. Although HA protects against server failures or outages by automatically replicating data to a mirrored server or storage device, it is no substitute for a full backup. In fact, HA may actually worsen the impact of a ransomware attack, by replicating malware and data deletion.

“HA makes your applications available by clustering or copying so that another server or disk takes over, but if you delete or corrupt something, it will be replicated just as quickly as the good stuff,” Little says.

Have It Your Way

The best solution gives users the flexibility of choosing the best options as circumstances dictate.

“The more places you can recover from and the more media types you can use, the safer and more recoverable the data is,” Cusimano says.

For many organizations, that means using a combination of backup solutions that can be deployed at different points in the lifecycle. For example, an organization may want to back up critical data to two cloud servers and to disk to optimize data protection and recovery speed. A week later, that data may be deemed less critical and moved to tape on-premises and to a single cloud archive.

Needs may also change over time as a result of new technology options, pricing changes, regulatory demands, acquisitions, and other factors. In addition, customers may want to fine-tune their backup strategies to take advantage of tiered options such as tape and other archival storage technologies. A single backup solution can make these transitions seamless and automated.

Backup is part of a robust data protection discipline that starts with understanding what data you have, what level of backup protection to provide, and what your recovery requirements are, according to Little.

"You should always architect the entire backup solution around recovery requirements," he says. Understanding these needs not only protects data but also reduces cost. "Most people keep too much data for too long," Little adds. For example, they may keep older data on backup servers when it can safely be archived for less.

Cusimano offers the following backup suggestions:

Back up as much as you can as often as you can. The optimal schedule depends on your business and may range from every few minutes to daily. A good strategy is to compare the cost of downtime to the cost of backup and look for the balance between the two.

Back up to multiple locations and/or cloud services. The greater the variety of backup options you use, the less risk of data loss. Leverage on-premises infrastructure for control and cloud backups for convenience. You may want to back up particularly critical data to an "air-gapped" server that isn't connected to the network.

Set clear time-to-recovery objectives, and test against them. Testing is critical, because unexpected events are inevitable and can be better anticipated through frequent testing. It's also a good hedge against media failure.

Test for ransomware attacks specifically. Having the latest patches and antivirus definitions is always recommended, but they won't necessarily protect against new strains of ransomware. Test scenarios in which large amounts of data are suddenly locked up, and develop a rapid-recovery plan.

Use good security practices. Log-in credentials should be changed frequently and access directories regularly reviewed. Backup infrastructure should have its own set of access controls and policies, so attackers who breach the main IT network can't compromise backup data.

Back up at the virtual machine level to enable quick recovery of machine states. This is no substitute for a comprehensive data backup, but it can significantly reduce total downtime.

The cloud is a great tool for enhancing your organization's agility and speed, but be aware of the data protection limitations of cloud services and plan accordingly. Modernizing your backup-and-recovery infrastructure not only protects against new threats such as ransomware but also reduces operating costs and improves flexibility.

Veritas NetBackup's unified data protection is a software-based, vendor-agnostic platform focused on the value of information rather than the underlying environment. It can protect workloads of any size and eliminates the need to juggle multiple point products. NetBackup helps ensure resilience and on-demand access from anywhere while reducing the risks and costs of storing growing amounts of data around the globe.

To learn more, go to www.veritas.com/solution/cloud

[1] "Truth in Cloud Report," Veritas Technologies, 2017