

Evaluating Cloud Storage Security

Date: July, 2009

Author: Terri McClure, Analyst, and Jon Oltsik, Principal Analyst

Abstract: By far, the number one question users considering a move to cloud storage ask is whether or not their data will be secure. Storing data offsite doesn't change data security requirements; they are the same as those facing data stored onsite. Security should be based on business requirements for specific applications and data sets, no matter where the data is stored. Users evaluating cloud storage service providers should demand the same type of security controls they would in their own data centers with regard to physical security, data encryption, and network security.

Overview

There are a lot of compelling reasons for businesses to deploy cloud-based storage. For a new business, start-up costs are significantly reduced because there is no need to invest capital up front for an internal IT infrastructure to support the business for the first year or two—just swipe a credit card and capacity is available. For businesses with limited IT resources, storage capacity is available instantly, without making investments in manpower to support and manage more capacity or floor space to house it. Large enterprises with deep investments in existing IT infrastructures can benefit from the storage-on-demand dynamic the cloud offers to quickly deploy temporary capacity or to create an efficient offsite storage tier for latency-tolerant data. Across the board, businesses can benefit from the flexibility cloud storage provides through subscriber-controlled on-demand capacity. New projects can be kicked off without the long, multi-month waiting period to provision new capacity typical of a large enterprise IT shop. Temporary capacity can be easily deployed if a new business opportunity arises, allowing the business to quickly react to new opportunities.

Keeping up with data growth is consistently a top IT storage challenge for the storage buyers ESG surveys. Consider that 30% of the more than 500 midsize enterprise storage professionals surveyed in mid 2008 said that one of their greatest problems is that they are running out of floor space in the data center. Another 31% cited keeping pace with overall data growth as one of their greatest overall IT challenges.¹ Larger enterprises feel it, too; a late 2008 survey indicated that 26% of the respondents were running out of floor space.² Shifting capacity to a cloud storage provider can significantly reduce these headaches.

Interestingly enough, the bulk of data stored is rarely accessed and could be moved to secondary and tertiary storage tiers—this is data that does not need sub-second performance. Wait times of a second or two to access data are completely acceptable. Since cloud storage may have some inherent latency related to network bandwidth and geographic distance, secondary and tertiary data may be good candidates for cloud storage.

There are many compelling benefits for users to deploy cloud storage, but an inhibitor has been concern about cloud storage security. Data security requirements don't change when data is stored offsite. Onsite or off, there are varying security requirements for different types of data. The first step users should take is to understand what those requirements are. Once data security requirements are defined for each data type, users can evaluate cloud storage providers against them.

Security Considerations for Cloud Storage

Storage security first came into focus when storage started getting attached to a network rather than sitting locked behind a server. But taking the storage out of the data center brings up new concerns. There is a perception that, since users don't control cloud storage security, they need to be convinced of the security of the cloud storage

¹ Source: ESG Research Report, *Medium-Size Business Server & Storage Priorities*, June 2008.

² Source: ESG Research Report, *ESG 2008 Enterprise Storage Systems Survey*, November 2008.

service provider. But users do control cloud storage security—through thorough audits and evaluation of the provider's technology and security processes. Users evaluating cloud storage service providers should take control and ask the same questions they do in their own data centers about physical security, data encryption, and network security.

ESG has assembled the following lists of storage infrastructure security questions that should be addressed whether data is housed internally or at an offsite cloud storage service provider.

Physical Security

- Is physical access to the data center restricted? Which security methods are required for access (example: biometric hand geometry readers)?
- Is the data center staffed and monitored 24 x 7?
- Is there a record or an ability to audit who has had access to the data center (example: video surveillance, audit logs)?
- Are background checks performed on employees with physical or managerial access to the infrastructure?
- Are there intrusion alerts and is there a documented response plan in case of a breach of physical security?
- Is the data center secured with surveillance cameras? If so, how is this video monitored?
- Has the data center ever been breached? If so, what were the details?

Storage Architecture Security

- What authentication methods are used between users and storage products (example: between storage administrators and management tools)?
- Are there secure configurations that mandate changes to default passwords as part of the installation process? Secure configurations should deny any and all services, features, and functions unless users specifically activate them.
- What types of security diagnostics and logging are in use? Device diagnostics must provide the ability to detect security events and log them accordingly. Users should have the ability to send security alerts to management consoles, element managers, pagers, e-mail, etc.
- How is multi-tenancy deployed—what technologies are used?

Network Security

- Are there secure configurations that mandate changes to default passwords as part of the installation process? Secure configurations should deny any and all services, features, and functions unless users specifically activate them (example: all switch ports should be turned off unless they are turned on by an authorized administrator).
- What types of security diagnostics and logging are in use? Device diagnostics must provide the ability to detect security events and log them accordingly. Users should have the ability to send security alerts to management consoles, element managers, pagers, e-mail, etc.
- If there is a Fibre Channel network in use, does it support security features for configuration and management? These should include a) secure zoning, b) fabric authentication of switches and hosts, and c) secure administration of individual switches and the entire fabric.
- Are network permissions and passwords audited, and how often?
- Are systems servicing each customer segregated from other network zones both logically and physically? There should be separate firewalled areas for Internet DMZ, production databases, development, staging, and backoffice applications.

Storage Access and Management Security

- Do management tools or software applications that require user login store passwords in encrypted files?
- Is the management software configurable to mandate password length, type, and duration?
- Do the management products use support methods for secure end-user communications protocols like SSL, TLS, or SSH?
- Is there an active user session timeout?

- Do the management tools support multiple administrator profiles to provide granular security levels? Tools must have configuration options that restrict administrator access based upon time, day, function, etc. All administrator action should be logged for auditing and alerting.
- Does any management software requiring user login provide the ability to disable user accounts after 5 or fewer unsuccessful login attempts? This software should also have the capability to provide multiple types of alerts (examples: e-mail, SNMP to event console, pager, etc.).
- Is administrative traffic encrypted? (example: UNIX root, application admin).

Security Processes

- Does the service provider test all hardware and software in fully secure configurations to assess the vulnerability of the servers, networks, and applications?
- Is there a formal methodology to report and track security vulnerability alerts discovered within their products? This process must offer proactive (contact users directly) and specific (only contact vulnerable users) help to existing customers.
- Is there an established and documented security fix process for the distribution of critical software patches and non-critical security updates?
- Are security features, policies, and support processes documented in a common area of the Web site linked from the home page? All marketing material must include security features and functionality.
- Is there an established process for testing security in the QA process? This must include scanning software source code for buffer overflows, backdoors, and insecure features.

Other Considerations

- Has the service provider been through a SAS 70 or other type of audit? If not, why not? If so, would they be willing to share the results?
- Are there defined penalties for missing SLAs?
- What notification and escalation procedures are followed if data is not in compliance?

Nirvanix Security

ESG has not performed a security audit of the Nirvanix cloud storage infrastructure. However, Nirvanix has been through a successful SAS 70 type II audit and has shared the results with ESG. A full review of Nirvanix security capabilities is beyond the scope of this brief, but we have asked these and other questions and are satisfied that Nirvanix has a well thought out security strategy.

Nirvanix has considered and addressed the broad spectrum of security requirements discussed in this brief. It has documented physical, storage architecture, storage management, and security processes in place. The processes are standard and part of the base offering, so even data requiring minimal security is stored in a secure fashion. That said, cloud storage subscribers are not absolved of the responsibility to perform routine security audits—just as would be done in an internal data center.

Getting a Jump-Start with Cloud Storage

The list of security questions and considerations for cloud storage can be pretty daunting. At first blush, it seems like it would take forever to complete proper security audits and start to reap the benefits of outsourcing storage to the cloud. Shifting to cloud storage is a journey and there are some clear starting points, steps that can be taken to accelerate the process and begin the transition.

- If your company has an IT security team with defined IT vendor security policies and audit processes for products and services, typically driven from the top down by a CSO, get the security team involved when you are starting to evaluate cloud storage vendors. The security team will know what questions to ask and help to sort out the cloud storage vendors with weak security policies up front, saving time and money.
- If there are no defined IT vendor security policies in place, work with your internal security team to see how internal policies can be revised for applicability to IT vendors in a repeatable, measurable way. This is just good best practices and should be done regardless of a move to the cloud.
- There is typically some low hanging fruit: data that does not have stringent security requirements that can be moved offsite prior to the completion of an audit. The bulk of unstructured data is likely to fall into this

category and could move into the cloud prior to the completion of the audit. Often, this data will get higher levels of security from the cloud storage provider than from your internal IT group, since the service provider needs to have a fairly high minimum standard security level to even enter the cloud storage service market.

Taking a pragmatic approach can help accelerate the process and ease the transition into the cloud, allowing for immediate benefits in terms of easing onsite operational burdens such as power, cooling, floor space, and management overhead. No matter what approach you take, ensure detailed service level agreements (SLAs) are in place that define remedies in the event that data security is breached.

The Bottom Line

Cloud storage service providers' viability and revenue stream depend on meeting subscriber security requirements—and the service providers know it. Those cloud storage providers who survive will be those that don't match enterprise data center security requirements, they surpass them. Those that fail to rise to this level will pay the price in lost customers.

Because the service provider has to architect the cloud storage environment to meet security requirements for extremely sensitive data all the way down to bulk storage of public data, the applications that require only minimal security actually benefit from higher security levels. The cloud offerings from many service providers can exceed what many users do today to meet the security requirements for secondary and tertiary (or long term) data sets that are most suited to being stored at a cloud service provider.

Security is security; no matter where the data is stored, best practices need to be followed. Once data security requirements are determined for the application layer, the entire infrastructure needs to be audited to ensure compliance with those requirements, regardless of where the application data is stored. That responsibility still falls to the owner of the data. The questions provided in this brief should help form the foundation of a cloud storage service provider security evaluation checklist. In the meantime, there are steps that can be taken to begin reaping the strategic business flexibility and reduced capital expense benefits cloud storage services can provide by examining your data requirements and moving bulk unstructured data that does not have stringent security requirements into the cloud.