EXECUTIVE SUMMARY

I/T organizations today are examining the use of cloud storage services to take advantage of the economic efficiencies, pricing flexibility, elasticity, and management simplicity that they provide. However, any discussion around cloud storage inevitably ends with a serious examination of security. Several questions are raised, seemingly without answers, including:

- Is my data secure? If so, how secure is my data?
- Who can access my data, and where can they access it from?
- What happens if my cloud storage provider loses a disk or a server?
- Am I in compliance, or out of compliance? How do I know?
- Can a former or malicious employee sabotage our data?

StorSimple’s cloud-integrated enterprise storage solution, coupled with leading cloud storage service providers, offers a framework by which the economics and elasticity of cloud storage can be realized without compromising performance, manageability, and even security of on-premises data center storage. This document explains how StorSimple and cloud storage service providers can:

- Ensure data confidentiality through industrial grade encryption
- Guarantee privacy by allowing only you to control encryption keys
- Mitigate compliance or privacy risk from lost media
- Control access and protect data through use of virtual private clouds
- Minimize threat of sabotage through multifactor authentication
Today’s storage environments require strict adherence to a well-defined set of technologies and processes. Data centers are typically locked and entry is restricted to ensure physical security. Management infrastructure access is controlled through roles-based access control (RBAC), centralized authentication and authorization, and communications are encrypted using SSL. Device interconnect is controlled through the use of numerous technologies including network access control (NAC), zones, and virtual fabrics. Similarly, authorization is managed through the use of technologies including challenge-handshake authentication protocol (CHAP), access control lists (ACLs), and LUN masking. Data at rest is protected through encryption to render it unusable without the appropriate key material. Data in motion is protected through SSL encryption, integrated authentication, and other mechanisms between tiers of a multi-tier application. Perimeter security is ensured through use of firewalls, intrusion detection/prevention systems, and even physical (separate physical networks) or logical (separate virtual networks) isolation. High availability is ensured through clustering, replication, redundant network fabrics, and load-balancing. To summarize, many of the obvious points of the ‘attack surface’ associated with storage infrastructure and the broader data center architecture are covered to minimize the possibility that security could be compromised. Using the traditional definition of the word “security”, this includes:

- **CONFIDENTIALITY**: Can an unauthorized user access my data, whether it is in flight from a user to an application server, between application server tiers, or at rest on a spindle?

- **INTEGRITY**: Can an unauthorized user or node access and change or delete my data, whether malicious or unintentional, at any point in the overall architecture?

- **AVAILABILITY**: Do single points of failure exist, or, vulnerabilities in my application architecture that—if compromised—could impact availability of service

**SECURITY CHALLENGES WITH CLOUD STORAGE**

Coming from an enterprise storage mindset, it is easy to see why so many concerns exist over cloud storage security. Fundamentally an organization’s data—the third most precious resource (behind customers and employees)—is being stored on a cloud storage service provider’s infrastructure and maybe even accessed over the Internet. In effect, the Internet is being inserted in between the application server and the storage system that it uses. Many of the best practices for security in an environment with cloud storage can be enforced, but given the fact that a third party is involved in the equation, some of those best practices cannot.

With a background rooted strongly in storage, application delivery, and data center infrastructure, StorSimple understands these concerns. The StorSimple appliance is designed to not only allow organizations to take advantage of the economics provided by cloud storage, but also ensure that your security posture is not compromised, as discussed in the next sections.
ENSURE DATA PRIVACY

While some cloud storage providers offer encryption—both for data at rest and data in motion—not all of them do. Additionally, those that do offer encryption may charge a premium to encrypt your data. However, allowing the cloud storage provider to encrypt your data is still not secure, as they retain control of the encryption keys—meaning they are fully able to release your data should litigation cause them to do so.

StorSimple provides encryption using AES-256 with Cipher Block Chaining (CBC)—the strongest commercially-available encryption—to encrypt your data prior to being stored on the cloud storage service. These keys can be generated using your existing Key Management System (KMS), and private key material can be used as an encryption key within the StorSimple appliance. Alternatively, you can use a passphrase as a seed to generating an encryption key within StorSimple. This means that your data is rendered unusable in the event that your cloud storage service provider is asked to turn over your data, because they will not have a copy of your key. Only you do.

Additionally, StorSimple takes advantage of SSL for data in motion (when reading or writing to the cloud storage service) when supported by the provider. Using encryption for both data in motion as well as data rest helps ensure data privacy, and renders data useless should a hard drive or tape be lost by your cloud storage service provider.

PROTECT DATA CONFIDENTIALITY AND MITIGATE SABOTAGE RISK

Even with data encrypted in the cloud, the ability to access data still poses a threat to your data's integrity and availability. A common concern for those considering cloud storage services is “what happens if we have to terminate one of our administrators that happens to have access to our cloud storage service?”. Such scenarios expose one of the biggest challenges with securing data stored in a cloud storage service - that of a rogue employee who maliciously deletes data from the cloud storage service, tampers with data, takes a copy of data to bring along to their next employer, or renders your systems unable to access their data. This problem typically stops cloud storage initiatives in their tracks.

StorSimple has worked with cloud storage service providers to counter this risk. Virtual Private Clouds (VPCs) can be deployed, which effectively isolate and dedicate part of the cloud storage provider’s infrastructure for your use only. Virtual Private Networks (VPNs) can be established between your data center and the cloud storage service provider, which allow access into your resources in the cloud storage service provider network from only your data center network. This not only prevents users from accessing cloud storage resources from outside of your network, protecting you from a rogue employee threat, but also ensures that anyone capturing your network traffic from the internet will be unable to discern what your data is.

Additionally, StorSimple has worked with cloud storage service providers to support Multi-Factor Authentication (MFA). MFA is typically implemented using secure tokens, which must be presented when logging into or accessing various parts of the management console for the cloud storage service. This, coupled with granular roles-based access control (RBAC) to determine what privilege level users have on the cloud storage service management dashboard, minimizes the threat posed to your data and your service by either a malicious user or an unintended action. The threat from questionable or terminated employees can be eliminated by simply being proactive and revoking their access and their token, making it virtually impossible for them to access or manipulate your data or services.
An additional concern that arises with cloud storage is that of compliance with government or industry regulation. The list of compliance initiatives companies have to address continues to grow, and includes PCI, HIPAA, SOX, GLBA, and others. The fundamental premise of these initiatives involves how data is handled, shared, protected, and how the associated systems are secured. While a vendor may make a claim about how their product helps achieve compliance, we at StorSimple believe that each organization should evaluate each element of their infrastructure, each system of their architecture, and their policies and procedures to determine whether or not they are in compliance. However, for the common compliance use cases, StorSimple allows you to rest assured that:

- All data stored in the cloud is encrypted using the strongest commercially-available encryption (AES-256-CBC). Key material remains in the hands of your personnel, and is not given to third parties

- Storage data in flight between the StorSimple appliance and cloud storage service providers is encrypted using SSL (which takes advantage of 1024-bit or 2048-bit RSA encryption for generating the session key)

- Storage data in flight between servers and the StorSimple appliance can be isolated to a non-routable, unreachable, or physically separate iSCSI networks, and volume access can be controlled by IP address, IQN, and CHAP authentication, including mutual authentication

- Access to configuration, management, and monitoring elements of your cloud storage service can be controlled through use of multi-factor authentication, and virtual private clouds can be deployed to further secure access

- High availability is ensured with StorSimple as there is no single point of failure, redundant and hot-swappable components, automated failover, and integrated alerting and diagnostics

**Summary**

Enterprise IT organizations are rightfully concerned about security when considering use of cloud storage services. Being able to extend security best practices from traditional data center storage models to cloud storage services helps to minimize risk, increase confidence in cloud storage services, and reach near parity in terms of security between on-premises storage and off-premises cloud storage.

StorSimple’s solution enables organizations to realize the economic advantages provided by cloud storage without compromising performance or security. All data written to the cloud is encrypted using keys you control, which are not shared with third parties including the cloud storage provider. Data read or written from the cloud storage provider can be encrypted using SSL, and virtual private clouds and VPNs can be used to control the points from which cloud storage infrastructure can be accessed. Roles based access control and multi-factor authentication can be used to control who has what level of privilege, and is also an effective tool at mitigating risk caused by rogue employees as well as those activities that are accidental in nature.