Microsoft

StorSimple

Hybrid cloud storage security

IT professionals considering the StorSimple hybrid cloud storage solution may want to understand the security technologies provided. This paper explains the security measures that are used and the scenarios they address.

Hybrid cloud storage security

Four elements of hybrid cloud storage security: Account Administration; Data Access, Data In-Flight; and Data at-Rest

Security implementations for the StorSimple hybrid cloud storage solution from Microsoft address four different security scenarios, as depicted in Figure 1:

- User authentication to the Windows Azure account where the data is stored
- StorSimple system access to data stored in the cloud
- Security of data in-flight, as it is transferred from the StorSimple system to Azure storage
- Security of data at-rest, while it is stored within a cloud data center

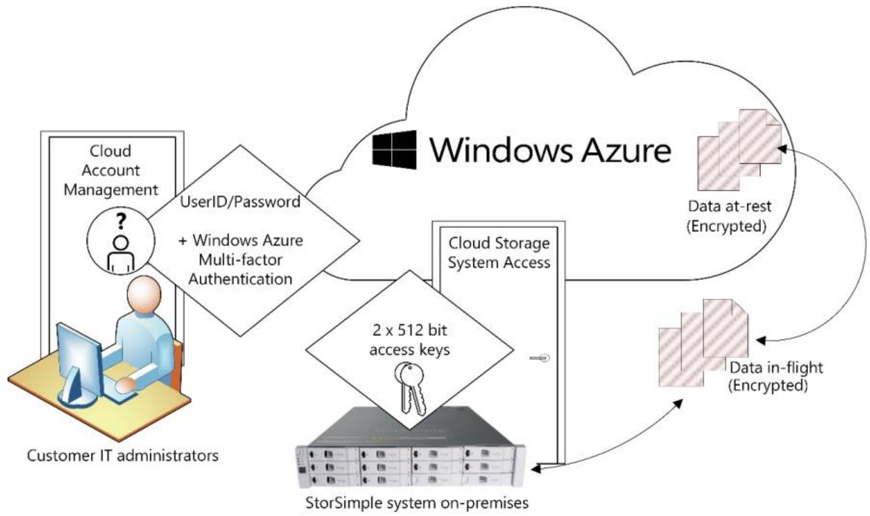

Figure 1. Security elements of the StorSimple hybrid cloud storage solution

StorSimple

Hybrid cloud storage security

User authentication to Windows Azure Storage: IDs, passwords, multi-factor authentication

The StorSimple hybrid cloud storage solution stores data in Windows Azure Storage, which is managed and accessed as a Windows Azure service. StorSimple system administrators control the use of cloud storage resources through the online Windows Azure Management Portal. Administrators authenticate to the Windows Azure Management Portal with a UserID and password, and can optionally use Windows Azure Multi-Factor Authentication to add another layer of security. Users with access to the Windows Azure Management Portal can change configuration parameters in addition to adding and deleting storage accounts and storage assets.

System access to Windows Azure Storage through storage access keys

Authentication of the StorSimple system to a Windows Azure Storage account requires the correct configuration of storage access keys. Two 512-bit keys are generated by Windows Azure for each storage account, one of which must match one of the two keys loaded into the cloud configuration of a StorSimple system. Storage access keys can be individually regenerated using a tool provided in the Windows Azure Management Portal. Alternating the regeneration of access keys lets administrators maintain cloud connections while generating new ones. Customers are advised to become familiar with changing access keys in the Windows Azure Management Portal and their StorSimple systems, and it is recommended that access keys be regenerated every 90 days.

Customers have a cloud storage subscription, which can have multiple storage accounts. StorSimple systems can connect to as many as 64 different storage accounts. Customers can use multiple storage accounts and their associated storage access keys to compartmentalize access to data in Windows Azure Storage by department, role, team, etc.

Data in-flight

Data in-flight encryption protects customers from scenarios where an unauthorized entity is able to tap the transmission of data at any point in the network linking the StorSimple system and Windows Azure.

Data transmission between the StorSimple system and cloud storage are encrypted using SSL, supporting up to AES 256 bit session encryption during data transfers between the StorSimple system and Windows Azure Storage. This encryption is distinct from the storage access keys and data at-rest encryption, although both of these measures are also in force when data is in-flight.

Data at-rest

Data at-rest encryption protects customers from scenarios where an intruder gains access to the storage access keys of a storage account and downloads data from it. It also protects customers from traditional scenarios where physical drives or tape media from a cloud data center are lost or stolen. With the hybrid cloud storage solution, cloud provider employees, contractors or other entities cannot read data as only the end customer has access to the keys.

StorSimple systems encrypt data stored in the cloud with a customer-provided encryption key using standard AES-256 encryption that is derived from a customer passphrase or generated by a key management system. With the ability of a StorSimple system to support up to 64 storage accounts, up to 64 different encryption keys can be used in a single StorSimple system.

Deduplication and data obfuscation

Deduplication also contributes to the obfuscation of data in a StorSimple system and in Windows Azure Storage. When data is deduplicated in the StorSimple system, it is translated from host-directed storage blocks into content-addressable data objects that are accessed by metadata mapping information. The deduplicated data objects are stored independently of the metadata and there is no storage-level context stored with them for accessing them based on volume, file system of file names. Data objects in Windows Azure Storage are distributed across many cloud data center physical disks. In general, 16 million objects are distributed across an indeterminate number of cloud storage disks for every 1TB of data stored in the cloud.