e-Guide

6 Reasons Cloud Storage is Now as Secure as Traditional Data Center Storage

Say “cloud storage” and some IT professionals cringe. The thought of using the cloud to store enterprise data evokes security, privacy, and compliance concerns. But advances in cloud technology – including the ability to deploy private cloud storage inside an enterprise data center – now bring security on-par with or ahead of traditional data center storage. This e-Guide offers 6 reasons why.

#1: Your Data is Encrypted … and You Hold the Keys

Do you lock your house? How about the valuables you keep in a safe or safe deposit box? Of course, the answer is yes.

If we translate this to files stored on a file server or Network Attached Storage (NAS) device in an enterprise data center, are they also protected? Traditional data centers typically use physical safeguards to protect against unauthorized access to facilities. But the bigger question is, how secure is the data within the facilities?

Increasingly connected networks, increasing attacks from within, and increasing sophistication of external malware and Ransomware attacks now make network breaches much more of a concern than physical breaches. Yet, files at rest in traditional data centers are typically not encrypted due to the age of the storage systems upon which they reside, as well as the cost and performance impact. This creates the same vulnerability as if you left your house or your safe deposit box unlocked.

By contrast, public cloud storage from vendors such as Amazon and Azure and private cloud storage from vendors such as Dell EMC and IBM, together with a global file system from a vendor such as Nasuni, ensure data is encrypted at rest and in flight. Nasuni uses AES 256-bit encryption keys to encrypt files as they are stored on Nasuni caching appliances in each location. They remain encrypted as they are transmitted over the network, and are still encrypted when they are written to cloud object storage.

Other cloud storage solutions also offer encryption. But going back to our original question, do you share copies of your house and safe deposit keys with everyone? Of course not. Nasuni takes this same approach with its encryption keys, giving you – and you alone – the ability to create and hold them. This way neither Nasuni nor the cloud storage provider can "see" the files that are stored.

Nasuni's file services platform also provides data deduplication and compression for all objects written to cloud storage. If some nefarious third party was to gain access to the data objects in the cloud, they would need to somehow decrypt the objects (without having access to the AES keys), but also know how to un-compress and reassemble the objects into usable files. This extra layer of camouflage is another reason why files stored with Nasuni and cloud storage are more secure than traditional data center storage.

#2: Cloud Storage Can Now Be Deployed in Your Own Data Center

Say "cloud storage" and some IT professionals think only of the public cloud – massive data centers around the world owned and operated by Amazon, Microsoft (Azure), and Google. Even with the security advantages described in #1, these IT pros would feel more comfortable hosting cloud storage within their own data centers and security perimeters.

Many enterprises are doing just that. They are now realizing the benefits of cloud storage – modular building blocks that are easy to scale at very low cost – from within the cozy confines of their own data centers.

These "private cloud" solutions include:

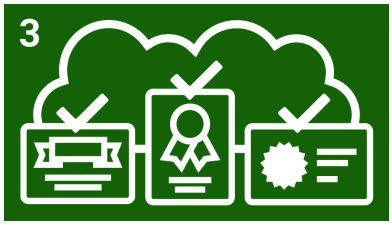
- Dell EMC Elastic Cloud Storage (ECS)
- IBM Cloud Object Storage (COS)
- Hitachi Content Platform (HCP)

and others. All provide highly scalable, cost-efficient storage deployed in your own data centers using software or appliances running on industry-standard, certified hardware. The systems are designed to scale easily by simply adding storage nodes for capacity or accessor nodes for more throughput.

The only component needed to let these private cloud storage platforms completely replace traditional file servers, NAS, backup, archive, disaster recovery, and multi-site file synchronization is a global file system from a vendor such as Nasuni.

So, if you don't feel comfortable putting your data in the public cloud, keep it inside your data center on your own private cloud. It will be more secure than traditional file storage, since all the encryption, compression, and deduplication camouflage layers still apply.

#3: Public Cloud Data Centers Have the Highest Certifications



The largest public cloud providers, including Amazon and Azure, have gone through extensive third party certifications to ensure data is protected – something that most enterprises forego in their own data centers.

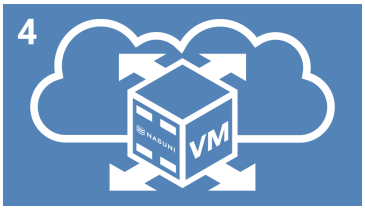
As a result, they now meet the highest industry compliance certifications and audit requirements, including:

- ISO 27001 certification for standardized management of information security
- AIPCA SOC 1 and SOC 2
- CSA STAR Certification including an available CAIQ
- PCI DSS (Payment Card Industry Data Security Standard) Level 1 compliance, required for handling credit cardholder personal information
- HIPAA-compliant applications involving health-related and other personally identifiable information (PII) as well as HITRUST
- FDA CFR Title 21 Part 11

These cloud providers can also provide detailed documentation of compliance as required by each standard.

Does your data center meet the compliance certifications above, and can you provide proof? If you move your data to the cloud, you get all this automatically, and likely raise the data security bar for your enterprise.

#4: File Access is Only Allowed Thorough Hardened Edge Caching Appliances



Providing high performance access to files without having to go to the cloud or pay costly egress charges is the primary function of the Nasuni Edge Appliance. These physical or virtual appliances can be

deployed wherever high performance file access is needed. They look just like traditional file servers and NAS devices, with one important difference: they only cache active files.

The full set of file data and metadata is stored in cloud object storage by Nasuni UniFS®, Nasuni's cloud-native file system. UniFS extends out to each edge appliance, caching only enough of the file system metadata and active files needed for local, high performance access. This means you only need typically 20% of the file storage capacity you needed before with your NAS devices and file servers. That's an 80% savings, plus more savings in power, cooling, and floor space.

How does that make modern cloud-based file storage more secure than traditional file storage? As discussed in #1, Nasuni data and metadata is encrypted and is not usable in its at-rest format in cloud object storage. To access the data, a Nasuni edge appliance is required, and many security features have been added to these appliances to harden them against attacks:

- All non-used protocol ports are closed.
- All data in flight from the edge appliance to cloud object storage is encrypted and you, the customer, hold the encryption keys.
- There is no open customer or hacker-accessible back-end access. The appliances do have remote support capabilities, but this connection is controlled and only enabled by the customer. Remote support requires the customer to enable access, all Nasuni Support personnel require secure authentication, and all support troubleshooting commands are logged for review.
- SMB3 encryption between the client and the directory shares on Nasuni appliances is supported.
- Nasuni hardware appliances are available with self-encrypting drives, providing extra security should someone remove a drive or appliance from the data center.

The sum of these capabilities far exceeds what most file servers and NAS devices offer today for traditional data center storage.

#5: The Same Active Directory and LDAP Authentication Policies are Still Used

One way to ensure cloud storage is at least as secure as traditional data center storage is to use the same authentication and access tools and procedures.

When you use Nasuni's global file system with any brand of cloud storage, that's what you get.

All client connections to Nasuni Edge Appliances are through standard file sharing protocols including SMB1, 2, and 3 as well as NFS v3 and v4. Active Directory and LDAP authentication control which users can access which files or sets of files, just like with traditional, full-sized file servers and NAS devices.

Active Directory (AD) permissions provide access only to data that is visible to the authenticated user, protecting data that is not visible through user and group security policies. These permissions are controlled by the system administrator, not the user. Direct access to data outside Nasuni Edge Appliances is not permitted – there is simply no way for end users to directly access the cloud storage.

Nasuni also supports AD Trust relationships, allowing policies to be applied across users and domains integrated through company acquisitions.

#6: File Data is Immutable, with Infinite Version Histories

Ultimately, we want to know our data is safe and secure, and not subject to change by accidental or intentional mistakes or system failures. This is one area where cloud storage now exceeds the capabilities of traditional data center storage.

Traditional NAS systems and file servers are generally reliable, but data corruptions do occur. Disk blocks or sectors can be changed, overwritten or corrupted. Local snapshots, which typically point to these same blocks or sectors, can also be corrupted. Backups are not always available, and even when they are, they may not be able to recover data to the point in time right before the corruption.

With cloud storage and a continuously versioning file system like Nasuni, data corruptions cannot occur. All data written to cloud storage uses a Write Once Read Many (WORM) model in which new data and metadata are always appended. Nothing is ever overwritten.

This provides the capability to immediately recover any set of data should a problem occur with an edge caching appliance. If snapshots are occurring at 15-minute intervals, simply roll back or restore to the last point in time version. The restore is extremely fast, since it is metadata only, and the newly restored metadata points to "gold copy" objects that cannot be overwritten or corrupted.

While this method protects against occasional software or hardware failures, it also provides the added benefit of immediate restores of data accidentally corrupted by malware that may have slipped through antivirus and other systems.

On a traditional disk system, the blocks and sectors can be locked up and unusable. With cloud storage and Nasuni, the local files may indeed get corrupted or locked up. However, since the data in cloud storage is WORM, a restore of the last snapshot puts all data back as it was before the malware event.

With traditional NAS or file server storage, this restore could take hours or even days, and may never be able to restore data close to the point of the corruption. With cloud storage and Nasuni, restores happen in minutes to the point in time right before the corruption.

Conclusion

We have covered only 6 of the many ways that cloud storage with a global file system like Nasuni provides security that equals or exceeds traditional data center storage. If unfounded security fears are causing your enterprise to miss out on these benefits of private or public cloud storage:

- Up to 60% cost savings by consolidating NAS, file servers, replication, backup, DR, archive, and remote access;
- Infinite capacity for group shares, project directories, and home drives;
- High speed file synchronization across any number of locations to boost distributed workforce productivity;
- Simpler management for IT;

then share this E-Guide with your colleagues. Then, start a proof of concept with Nasuni to validate these 6 reasons why cloud storage is now more secure than traditional data center storage.

About Nasuni

Nasuni enables enterprises to store and synchronize files across all locations at any scale. Powered by the Nasuni UniFS® global file system, Nasuni file services stores unstructured data in object storage from providers such as Amazon, Dell EMC, IBM, and Microsoft, while caching actively used data wherever it is needed – on-premises or in the cloud – for high performance access. By using Nasuni to collaborate on files across multiple sites and consolidate Network Attached Storage (NAS) and remote office file servers, customers maximize workforce productivity while reducing IT cost and complexity.