Keeping Cloud Data Secure

Whenever confidential data is stored in the public cloud, security is a major concern. There are many ways to protect data from unauthorized access, for example, by implementing user authentication and access controls, but nothing beats encryption. When data is encrypted, it is undecipherable even if authentication and access controls are breached, which provides the ultimate in confidentiality (if implemented properly, of course).

Traditional Approaches

Encryption in the public cloud can be either be client-side or server-side. Encryption keys can also be managed by the user or the cloud provider. These four elements influence the security level of data stored in the cloud, but also the setup and operation complexity.

The easiest but least secure method is server-side encryption with cloud-provider-managed keys, where the cloud provider controls the entire encryption and decryption process. This means we are relying on the cloud provider for security; the cloud provider itself or hackers attacking the cloud infrastructure could also have the ability to decrypt our data.

> Keeping data confidential in cloud is always a compromise between the convenience of cloud and the security of local encryption. COSNIM gives the best of both worlds.

On the other hand, client-side data encryption and user-managed encryption keys are much more secure, as nothing is disclosed to the cloud provider, but they are also the most complex to implement. Usually, applications will need to be enhanced to support client-side encryption, and secure mechanisms must be put in place to protect the encryption keys against application breaches. Moreover, since client-side encryption hides all information from the cloud provider, the latter cannot process this data any further (for example, to perform searches). Because of this constraint, users often end up encrypting only part of their data, leaving the rest in clear form for the provider to process and organize.

COSNIM Technology

COSNIM provides filesystem services directly on the local server and encrypts all data at the edge, right before the data is about to be stored on a local disk or sent to the cloud. This gives applications the

convenience of a fully functional storage system, as would normally be provided by a cloud provider, with all the security of client-side encryption, without any refactoring or adaptations.

100% Encryption, Including Metadata

In COSNIM, absolutely everything is encrypted locally, including data, metadata, and all control information. Nothing ever leaves a server or gets stored on local storage unencrypted, even if it's shared with other systems. Even the names of the capsules are fully encrypted. Since all encryption keys remain local and are never shared with cloud providers, they are also much less vulnerable to cloud attacks. In fact, without encryption keys, no hacker or cloud provider can figure out anything about what COSNIM storage capsules contain, not even the type or size of data or files, the directory structure, or any other metadata.

> COSNIM provides ultimate, 100% encryption coverage, with no compromises.

Military-Grade, Quantum-Resistant

COSNIM always encrypts data symmetrically, and by default uses military-grade AES-256 encryption, meaning that all data stored in capsules and in the cloud is fully protected with the best technology, resistant to even foreseeable quantum computers.

Multi-Keys and Multi-Algorithms

Each COSNIM capsule is physically independent and can be encrypted with any number of different encryption keys and/or algorithms, irrespective of other capsules in the Continuum. To further shield data against attacks, capsules may also be encrypted using randomly selected encryption keys, new encryption keys can be added at any time without re-keying existing capsules, and existing capsules may be re-encrypted with different keys or algorithms at any time, without coordination with any peers or servers.

Ultimate Zero-Trust

Traditional solutions typically implement zero-trust security by encrypting data before it leaves a server and decrypting it on the receiving end before processing. Data is frequently re-encrypted and decrypted as it goes through each system for processing. Since typical zero-trust implementations also use asymmetric encryption such as TLS for transport, this data is potentially vulnerable to quantum computing attacks.

In COSNIM, all capsules and their contents are fully encrypted before they leave the server and remain fully encrypted throughout their entire journey, in transit and at rest. When a system reads data from a Continuum, capsules are read and transmitted already fully encrypted, remain encrypted throughout their journey, and are decrypted only by the target application server. There is no intermediary decryption or re-encryption in COSNIM, even when sharing data with other users and servers, providing the ultimate zero-trust security.

User-Controlled Encryption Modules

Encryption in COSNIM is an independent process and occurs at the very last step before sending data to storage. Users can provide their own encryption modules to implement their own encryption algorithms, manage their own keys, or integrate with custom cryptographic hardware, without ever exposing any of this information to COSNIM. This ensures a superior level of confidentiality and security by completely removing COSNIM from the encryption process. COSNIM encryption modules are extremely simple to implement and are provided with sample code.

COSNIM goes beyond Zero-Trust. It can give the most demanding users easy and complete control over the entire data encryption and storage processes.

User-Controlled Storage Modules

As with encryption, users may also provide their own storage modules to handle the actual storage of capsules at their destination. This can be used, for example, to support non-standard storage services or to completely hide cloud access credentials from COSNIM. Since encryption and storage cycles are the very last stages of a COSNIM data flow, when users implement both encryption and storage modules, COSNIM itself can be fully isolated and sandboxed, with no access to the network, encryption keys, or access credentials. This gives even the most demanding users complete confidence in the security of their data, without compromising any of COSNIM's features.

Cloud confidentiality is extremely important, but not always easy to implement, and not always perfect. COSNIM provides the most advanced quantum-proof encryption and zero-trust model possible, with all the security of client-side encryption and the convenience of a fully integrated storage and filesystem.