atlantic.net
Secure Cloud Services

CELEBRATING 30 YEARS OF EXCELLENCE

ENCRYPTION

Encryption in the Atlantic.Net Cloud Platform

The Atlantic.Net Cloud Platform encrypts customer data stored at rest by default with no additional action required by the customer. This is accomplished through industry standardized encryption mechanisms.

Atlantic.Net believes encryption of customer's data at rest shouldn't be an optional feature and is now a requirement of all computing. That's why our world-class encryption is implemented in a transparent manner, with no further need for configuration by the user.

KEY FEATURES

- Data is automatically encrypted prior to being written to the disk. Data is encrypted using Advanced Encryption.
- Standard 256-bit (AES-256). This encryption standard is the only publicly accessible encryption cipher approved by the National Security Agency (NSA) for top-secret information.
- Each encryption key used to encrypt data is itself encrypted with a set of master keys.

Note: Encryption of data stored at rest is an important part of a broader data security strategy and should not be considered the only mechanism for securing data.

WHAT IS ENCRYPTION?

In today's world, security should be a deciding factor when choosing a Cloud vendor. Atlantic.Net takes security and privacy seriously. We work around the clock to protect the data stored on our Cloud Platforms.

Encryption in transit and at rest are central components of our security strategy which help to ensure data can only be accessed by authorized services within our Cloud Platforms.

Encryption is the process of encoding information in a way that only authorized entities can access it in a decipherable way. The method of encrypting the information typically uses a publicly available algorithm, but relies on a key which is kept private to encrypt the information. To decrypt the information back to a decipherable format, the private key will be required. This means that even if someone were to gain access to the encrypted information they will not be able to understand it without access and use of the private key. Although the above concept of encryption and decryption applies to many facets of computing, here we will cover data encryption at rest on storage systems.

atlantic.net
Secure Cloud Services

CELEBRATING 30 YEARS OF EXCELLENCE

ENCRYPTION

WHY ENCRYPTION IS ESSENTIAL TO PROTECTING DATA?

Encryption of data stored at rest is an important part of a broader data security strategy. Encryption helps ensure that if data is somehow obtained in an unauthorized fashion, the person will not be able to access the data without also having access to the encryption keys. This means that even if someone obtains the storage devices, they will not be able to decrypt the data on the storage devices.

Additionally, encryption is an important part of how Atlantic.Net helps ensure the privacy of customer data while still allowing our engineers to maintain and support all infrastructure, while providing a built in mechanism to protect access to customer content.

HOW STORAGE IS ENCRYPTED

Within the Atlantic.Net Cloud Platform all customer data is encrypted by default, with no action required by the customer. This encryption takes place at the storage system layer.

Each chunk of customer data is encrypted prior to being written to the storage system and then is distributed across the storage system in chunks. An unauthorized user would need to have access to not only all chunks that make us the data they want to access, but also the encryption key(s) corresponding to that encrypted data.

The encryption keys are protected by controls that ensure data access is granted by authorized roles at authorized points-in-time. This further helps prevent unauthorized access to data, increasing data security and privacy.

Data is encrypted using Advanced Encryption Standard 256-bit (AES-256). This encryption standard is the only publicly accessible encryption cipher approved by the National Security Agency (NSA) for top-secret information and is often included as part of customer compliance requirements.

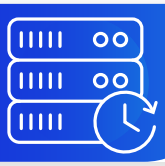
In the Atlantic.Net Cloud Platform, the AES-256 encryption is implemented at the storage system layer in a cipher mode of XTS-plain64, using a hash algorithm of sha256, and key size of 512-bits with half of the bits used for the cipher key and the other half used for the XTS key.

In addition to the storage system level encryption described above, data is also encrypted at the storage device level, AES-256 for solid state drives, using a separate device-level key, which is different than the key used for encryption at the storage system layer.

atlantic.net
Secure Cloud Services

CELEBRATING 30 YEARS OF EXCELLENCE

ENCRYPTION



ENCRYPTION OF DATA BACKUPS

Atlantic.Net's backup systems ensure that all customer data remains encrypted throughout the entire backup process, including data transport. To further enhance security and privacy, all data backups are encrypted with an encryption key which is different and independent from the keys mentioned in the previous section.

KEY MANAGEMENT

Atlantic.Net utilizes a centralized key management service (KMS) that is replicated in peer-to-peer fashion. This KMS makes storing, encrypting, and decrypting data on a massive scale manageable. Additionally, utilizing the KMS allows us to efficiently track and control data access.

The key used to encrypt data on a storage system is called the data encryption key (DEK). DEKs are generated on the storage systems and sent to the KMS where they are encrypted with the receiving system's key encryption key (KEK), then passed back to the originating storage system to be stored for future use.

When a storage system needs to decrypt data, it retrieves the DEK and passes it to the KMS. The KMS then verifies that the requesting service is authorized to use that key. If it is authorized, the key is decrypted using the KEK and returned to the originating service. The service then uses the key to decrypt the data.

All keys stored in the KMS are encrypted with AES-256. All encryption and decryption of keys can only be done within our KMS. This further enhances security by helping to prevent unauthorized use and provides a consistent audit trail.

The KMS automatically rotates KEKs at a regular interval. Our standard rotation period is 90 days. KEKs are stored as a key set. We keep one KEK active for encryption purposes and a set of historical KEKs for decryption purposes.

KEK access is managed by control lists on a per-key basis. Only authorized services and users can access a key. Each key request is verified for authentication and logged for auditing.

The KMS is itself protected by a master key called the key management service key which encrypts and decrypts all the KEKs in the system. The master key is only present in RAM on the KMS systems. When a KMS instance is restarted, it will obtain the master key from its peer instances.

atlantic.net
Secure Cloud Services

CELEBRATING 30 YEARS OF EXCELLENCE

ENCRYPTION

For disaster recovery purposes, the master key is encrypted with AES -256 and stored in an off-line master key management system that is physically secured in multiple locations. Access to this off-line key management system should only be necessary if all KMS instances need to be restarted at the same time. Less than ten employees have physical access to the off-line master key management system.

The KMS system as described above is still being phased in to upgrade a system that operated in a similar manner but was not peer-to-peer.

SUMMARY

- Data chunks are encrypted with DEKs.
- DEKs are encrypted with KEKs.
- KEKs are stored in the KMS and encrypted with the KMS master key.
- KMS is replicated in peer-to-peer fashion globally.
- KMS master key is present in RAM on the KMS systems and obtained from peers KMS systems when a KMS instance needs to be restarted.
- If all KMS instances need to be restarted at the same time, the KMS master key is stored in multiple locations on secure hardware that less than ten employees have access to.

Find Out More

Atlantic.Net stands ready to help you attain fast compliance with a range of certifications, such as SOC 2 and SOC 3, HIPAA, and HITECH, all with 24x7x365 support, monitoring, and world-class data center infrastructure. For faster application deployment, free IT architecture design, and assessment, visit us at **www.atlantic.net**, call **+1-408-335-0825**, or email us at **sales@atlantic.net**.

ATLANTIC.NET MANAGED & SUPPORTED IN THE USA INVESTING IN AMERICAN JOBS