atlantic.net
Secure Cloud Services

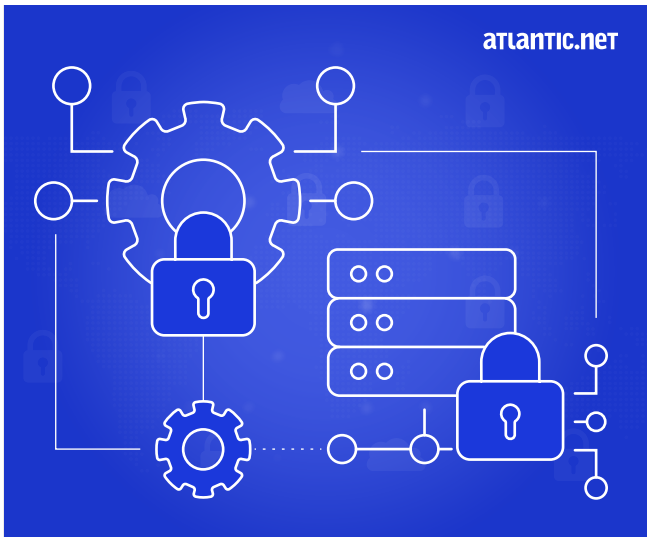
CELEBRATING 30 YEARS OF EXCELLENCE

WHAT ENCRYPTION DOES ATLANTIC.NET USE?

The implementation of leading-edge encryption standards throughout all of Atlantic.Net products and services provides cornerstone protection to all of our clients and their critical data.

Encryption is available at a system-wide layer, a network-wide layer, and even all the way down to encryption of individual files and folders. The recommended encryption standard depends on your implementation.

Atlantic.Net engineers will always recommend a tested, certified, and secure standard that protects your sensitive data in case of an accidental or deliberate data breach. If you are opting for one of our compliance services, then encryption will likely form a mandatory baseline requirement.



WHAT IS ENCRYPTION?

To briefly recap, there are three types of encryption protection standards used to encrypt data. The first is encryption at rest, which refers to encryption that is applied to the entire data layer of your technical solution. The most common way to do this is to use full-disk encryption, a method that protects all data that is stored on your server.

Full disk encryption works on system disks. Your operating system can be encrypted as well as any attached storage you may have, such as Atlantic.Net Secure Block Storage (SBS). Atlantic.Net implements full disk encryption on all of our consumable platforms by default, including our Cloud Hosting, HIPAA-Compliant Hosting, and more.

Next is encryption in transit. Data in transit is information that is moving from one system to another over the network. Our experts recommend that you encrypt not only sensitive data onsite using a tool like BitLocker or PGP, but also when transferring this data to Atlantic.Net servers; when transferring data, you need to use a secure network protocol such as sFTP over a secured VPN.

Encrypting data with an SSL certificate at the server level and using even more complex methods locally creates a secured data transfer approach that protects your data when traversing over the network or the public internet, preventing unauthorized snooping.

The final type is encryption when live. This is how data is encrypted when active in a production environment. Consider database encryption; live data stored in a database must be encrypted. Also, live servers also need to be encrypted, such as protecting the local disks and operating systems with BitLocker.

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

atlantic.net
Secure Cloud Services

CELEBRATING 30 YEARS OF EXCELLENCE

WHAT ENCRYPTION DOES ATLANTIC.NET USE?

PCI COMPLIANCE AND ENCRYPTION

The payment card industry has some of the highest required security standards to achieve compliance. The Payment Card Industry Data Security Standard (PCI-DSS) is all about protecting financial data and standardizing how a merchant processes card payments per customer.

PCI-DSS is a global standard for securing transactions, and unsurprisingly, there are several rules regarding encryption:

Protecting Transactions: Atlantic.Net systems use AES256 encryption as a minimum standard, and our teams are highly trained in security best practices when handling sensitive transaction data. All employees are vetted before employment, and we conduct regular training for the team.

AES encryption scrambles data when at rest, and only a valid key holder can decrypt the data. Combine this approach with the PCI requirements of PAN obfuscation (permanent account numbers), and any PCI data is in the best possible state for protection.

PCI-DSS requires that secret and private keys are used to encrypt/decrypt cardholder data within a secured cryptographic host. This is achieved by the Atlantic.Net KMS Key Managed Service.

Protecting Data in Transit: The PCI Security Council takes a hard line on data in transit because sensitive data can be vulnerable when transmitted, especially over an open network. Trusted Keys and Certificates (TLS/SSL) are mandatory and strong cipher suites are needed.

Thankfully, you will find all of these requirements and more are met by Atlantic.Net PCI-Compliant Hosting.

SERVER ENCRYPTION (DEDICATED SERVER/CLOUD SERVER)

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

To meet this requirement, Atlantic.Net upholds these encryption features:

- Data is automatically encrypted before 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.

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

atlantic.net
Secure Cloud Services

CELEBRATING 30 YEARS OF EXCELLENCE

WHAT ENCRYPTION DOES ATLANTIC.NET USE?

All consumable managed services from Atlantic.Net incorporate several encryption safeguards, and since all customers with either Dedicated or Cloud Servers (VPS) can access and utilize these managed services, we have built them from the ground up to be secure, robust, and fault-tolerant.

Cloud Storage: All customer data stored on the Atlantic.Net Cloud Platform is encrypted by default, with no action required by the customer. The encryption process takes place at the storage system layer automatically, and there is zero noticeable impact on performance.

Data is also encrypted at the storage device level with AES-256 for storage drives using a separate device-level key, which is different from the key used for encryption at the storage system layer. Typically, you run your operating system at the storage device layer.

Encryption of Backups: 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 that is different and independent from all other keys.

DEDICATED SERVERS (BARE METAL)

Our Bare Metal clients have the option to utilize local encryption on their private node, and while it is not mandatory, we highly recommend it. Ultimately the customer has the final say. However, when a customer opts to consume Atlantic.Net managed services, the same rules apply to all server endpoints; that encryption is enforced.

HIPAA COMPLIANCE AND ENCRYPTION

Atlantic.Net is famous for its HIPAA-compliant hosting services. You may be thinking that due to the security and privacy safeguard requirements of HIPAA, encryption would be mandatory. Encryption is surprisingly not a mandatory requirement of HIPAA-Compliance (if you choose not to encrypt, you must use an equal alternative), but as with all other Atlantic.Net services, our engineers enforce encryption at rest on all cloud storage devices used by HIPAA clients.

A major reason you should care about encryption is that the HHS's requirements for unencrypted information are much stricter than they are for encrypted data, so you need to have a good reason to not implement encryption to protect Protected Health Information (PHI).

PHI Data Governance: Think about where your data is - both on the client-side (mobile devices and workstations) and server-side. Once you know where the patient data is, you know what you need to encrypt. Atlantic.Net encrypts the entire hard disk drive by default.

atlantic.net
Secure Cloud Services

CELEBRATING 30 YEARS OF EXCELLENCE

WHAT ENCRYPTION DOES ATLANTIC.NET USE?

Consider PHI Data in Transit: To properly achieve encryption in transit, you typically will need a secure file server and transfer software. You only want the data accessible via password or some other type of key entry, for example, utilizing multi-factor authentication add-ons. Once files are uploaded to a secure server, it is possible to send out a link so that people can access the environment with the proper username, password, and MFA token (or through other means).

VPN ENCRYPTION

Protecting the VPN is essential when transferring files from on-premise to the cloud and vice-versa. Virtual Private Networks, or VPNs, are a method of employing encryption to allow users to access a private network securely and share data remotely through public networks.

Though VPNs connect over public interfaces, they're secure and appear as a private network. VPNs offer an inherent increase in security and are often used by SMBs and enterprise corporations as a way of connecting to remote data centers and remote users.

Atlantic.Net VPNs are encrypted by public-key cryptography, an asymmetric encryption methodology that seeks to maintain confidentiality without having to ever share a secret key over an insecure channel such as the public Internet. We also offer paired key encryption, another form of asymmetric encryption. The VPN encryption technology offered will depend on your technical solution.

OS-LEVEL ENCRYPTION

All modern operating systems have full system encryption available, and in most cell phones, tablets, and mobile devices, encryption is often enabled by default. It's very simple to enable encryption at the operating system level; to configure the setup only takes a few minutes. The only time-consuming part of the process is when your local disks are encrypted, and disk speed, disk type, and disk size will all play a factor in how long the encryption process takes.

If you use Windows Server or Windows Desktop professional products, the most straightforward option is to enable Windows **BitLocker. FileVault** for Mac is the Macintosh equivalent of Bitlocker and is also available out of the box. If you use Linux, then PGP for Linux is a great free option.

Your Security-Focused Hosting Partner

In addition to offering enterprise-grade end-to-end encryption in the Cloud, Atlantic.Net provides enterprise-grade managed solutions, including our fully-managed Atlantic.Net Firewall and Intrusion Prevention Security services. These are cost-effective options for any hosting environment looking to improve its security and reliability. Contact our Sales team today for pricing and availability of our Managed Security solutions! **sales@atlantic.net** or **+1-408-335-0825**

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