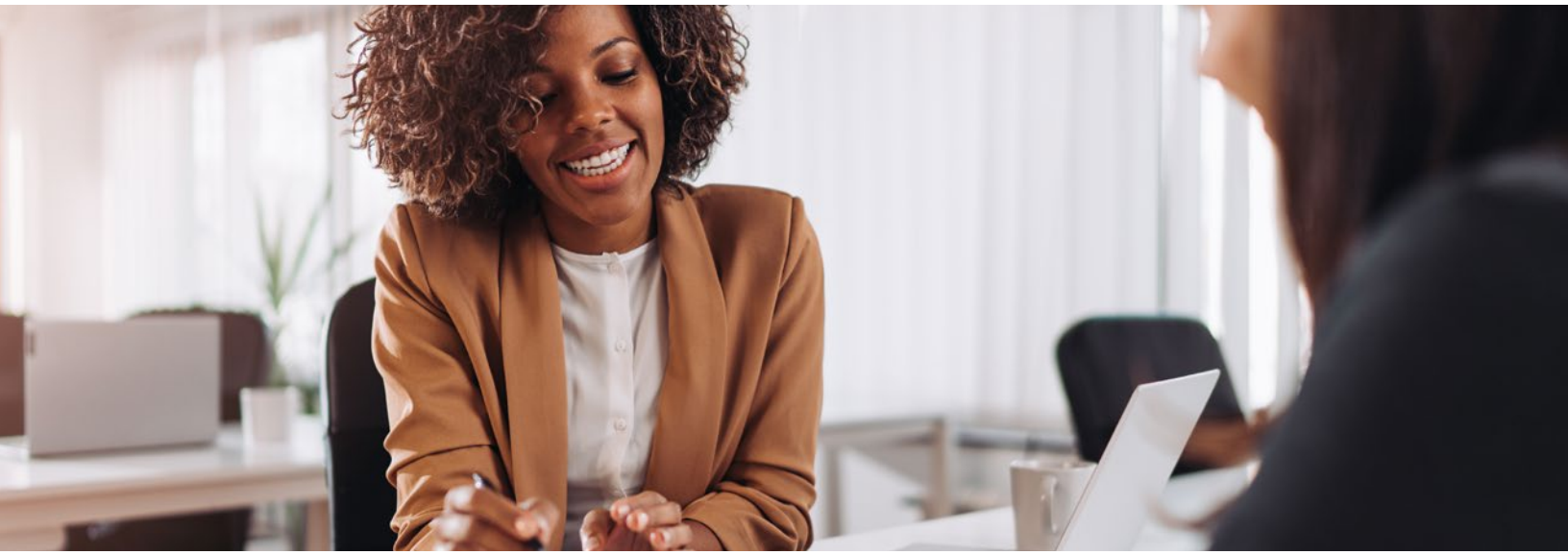
netdocuments®



DOCUMENT ENCRYPTION & WHY IT MATTERS

Encryption is crucial for the role it plays in security, compliance, and loss prevention.

Security

Safely storing business documents is a high priority. As files are shared digitally between people and devices, there are increasing opportunities for bad actors to attack systems and steal information. Encryption is an **essential layer** of protection to keep your content secure even if other security controls are breached.

Governance & Compliance

Information security and governance are critical operating requirements for organizations. Shaped by guidelines at the state, federal, and international level, companies need tools to store, manage, and defensibly dispose of documents. Encryption is a **key tool** for compliance with these standards.

Loss Prevention

The cost of data breaches extends far beyond merely improving security. Data breaches erode public trust and can have an incredibly damaging effect on a business' reputation—which can jeopardize existing and future customer relationships and revenue. Encryption **can prevent** a security incident from turning into a data breach.

netdocuments®

How NetDocuments Handles Document Encryption

Keeping your files safe is our job. With zero trust computing, NetDocuments uses industry-leading encryption practices to protect your business against data breaches, in addition to providing next-generation encryption infrastructure and key management. You can be confident your company's documents are protected at the highest levels available today within the NetDocuments Service.

Multi-Layer Encryption and Encryption Key Management (EKM)

NetDocuments applies multiple layers of encryption and uses innovative technology, including a Quantum Random Number Generator (QRNG), to create a unique encryption key for each document and email saved to the Service. The QRNG uses quantum mechanics to generate fully entropic AES-256 encryption keys, as opposed to software-based randomization which can be deciphered by nation-state actors.

The NetDocuments Service performs the encryption and decryption on each document, rather than using low-value security methods such as disk-level encryption. This process conceals all digital files from storage and network administrators, which is not possible with disk-level encryption.

Each document saved to NetDocuments is encrypted with its own unique, fully entropic AES-256 Object Encryption Key (OEK). After encryption, the document is written to the data storage array ("object store"), while the OEK is stored separately in a secure key database.

Before being stored in the key database, OEKs are themselves encrypted using a Master Encryption Key (MEK), which provides an additional layer of encryption security. NetDocuments safeguards and manages MEKs in dedicated Federal Information Processing Standards (FIPS) 140-2 Level 3 Hardware Security Modules (HSMs) with restricted access, using Root of Trust architecture to fully protect the MEK. MEKs are rotated every six months. FIPS is a globally recognized standard for encryption security controls; Level 3 enables physical and logical separation to maximize encryption key security.

Zero trust computing is achieved by storing fully entropic encryption keys in an HSM rated at FIPS 140-2 Level 3 and using the NetDocuments Service operating controls.

Customer-Managed Encryption Keys

Customers may have unique, granular security requirements. Encryption can be used to isolate different sets of content from other documents. We meet this requirement by offering customers the option of using Customer-Managed Encryption Keys (CMEKs), managed through NetDocuments HSMs or customer-managed HSMs.

netdocuments®

When using CMEKs, the NetDocuments Service applies three separate encryption layers to each document. Customers control when CMEKs are applied to sensitive documents falling under regulatory, compliance, or other mandated data governance policies.

Customers may assign, and revoke, CMEKs to specific projects or groups of documents where needed. Granular, metadata-based encryption key management allows businesses to revoke access to specific content while other content is still accessible and protected by its own encryption.

Encryption in Transit

NetDocuments not only protects your documents while they are stored in the application, the Service also protects your documents while they are being transmitted to or from the Service by encrypting all Service transmissions over the Internet. NetDocuments requires all connections to the Service to use HTTPS and only allows encryption using the current TLS security protocols (currently TLS 1.2) for document transmission security.

Resilient Document Storage

A key element of the NetDocuments storage architecture is the use of object store technology. When a file is placed in the NetDocuments Service, it is immediately encrypted and then saved in an object store, where it is automatically replicated or erasure coded (depending on the size of the file) across multiple data centers and multiple physical storage devices within each data center. This dispersal across geographically separate, highly secure data centers ensures full data availability, content integrity, and the highest levels of security.

Ensuring encryption is used throughout the NetDocuments Service makes sensitive documents indecipherable and inaccessible to any party, including NetDocuments personnel.

Encryption is One of Many Elements of a Robust, Zero Trust Security Plan

While encryption and object storage are essential elements of any secure Service, they represent only one layer of NetDocuments' Service data governance. NetDocuments provides controls to manage user access to documents and data loss protection (DLP) to minimize the risk of an accidental or malicious data leak.

In addition, NetDocuments maintains industry-recognized ISO 27001, 27017, and 27018 security certifications, the new ISO 27701 certification to demonstrate compliance with GDPR, and is regularly audited to validate compliance with SOC 2 controls, so that you have the comfort and assurance of knowing NetDocuments security infrastructure has been independently validated by accredited auditors—and allowing your organization to claim the benefits of NetDocuments' comprehensive security architecture via pass-through compliance.

Discover how our industry-leading encryption can further protect your business.

Schedule a demo of NetDocuments today >