Security in the Cloud with NetDocuments

Learn how cloud-based solutions improve security, maximize data encryption and reduce compliance risk.

netdocuments®

Safe Ready Proven

NetDocuments can simplify your work by providing one platform for secure content management, email filing, and collaboration. We deliver software-as-a-service to protect your most valuable information, using advanced security controls, encryption key management, and complete information governance, all validated by third-party audits. As client demands increase and new working patterns emerge, NetDocuments can grow and adapt with your changing needs while protecting critical content.

Our simple, secure content services platform enables organizations across the globe to improve workplace productivity and protect against potential security threats or cyber breaches. Through our efforts to embed security and resilience into our products and processes, we have been deemed safe, ready and proven by more than 2,500 customers worldwide.

> "NetDocuments' cloud platform is purpose-built to safeguard data and is coupled with advanced encryption and multi-layered security controls to provide a robust 'Security-as-a-Service' solution for client data."
>
> – Alvin Tedjamulia
> CTO, NetDocuments

PROTECTING CUSTOMER DATA

Security Backed by Hardened Infrastructure

Customer data is protected in transit using HTTPS and TLS security protocols. NetDocuments currently supports both TLS 1.2 and 1.3. We will begin deprecating TLS 1.2 once adoption of TLS 1.3 is completed by key vendors and equipment manufacturers.

Data is protected at rest in storage facilities with maximum entropic encryption applied by the NetDocuments service (Service). NetDocuments encrypts each file with a unique AES-256 Object Encryption Key (OEK). Each OEK is further encrypted with an AES-256 Master Encryption Key (MEK) stored in highly-secure Hardware Security Modules (HSMs) certified as compliant with FIPS 140-2 Level 3. The HSMs supports KMIP (Key Management Information Protocol) to maximize platform interoperability. KMIP enables platform companies like NetDocuments to consume the highest-grade encryption products while maintaining customer flexibility.

A customer may also choose to further encrypt the OEKs of selected documents with specific encryption using an AES-256 Customer-Managed Encryption Key (CMEK). All CMEKs are stored either in NetDocuments' HSMs or in customer-owned, Service-compatible HSMs.

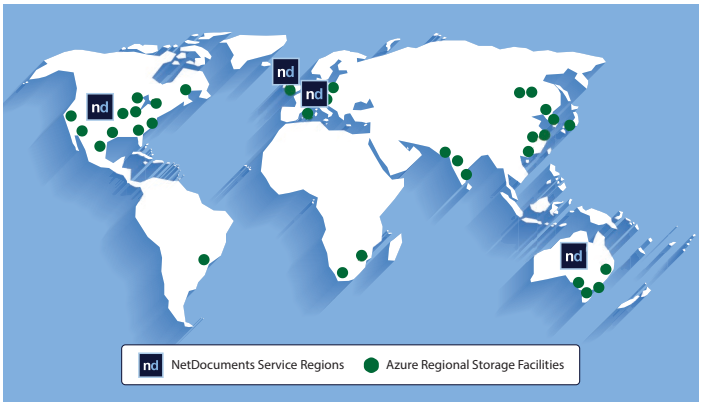
All AES-256 encryption keys created by the Service are generated using maximum entropy (randomness), hardware-based quantum random number generators. The result is 100 percent encryption key entropy and industry-leading cryptography for all customer content, without impacting performance.

PROTECTING SERVICE NETWORKS

NetDocuments employs a comprehensive range of procedures, tools, and independent resources to secure the Service, including:

1. **Network Perimeter Defense**
   - Independent, third-party Web Application Firewalls (WAFs) (Akamai)
   - DDoS protection by Prolexic
   - Internal, redundant, stateful firewalls
   - Load balancers (stateless firewalls)
   - Intrusion Detection System (IDS)
   - DMZ hosting for all web servers
2. **Server Security**
   - Real-time monitoring
   - Activity logging with log review and extended log retention
   - Strong passwords
   - Restricted access
   - Regular firewall rule reviews
   - Hardened server images regularly updated and deployed
   - Automated deployment including scheduled destroy-and-replace of all virtual machines (VMs)
3. **Data Center Security**
   - Physical perimeter barriers
   - Gated, monitored and controlled access
   - Visitation by pre-authorized appointment only - validated by government-issued photo ID with guests being accompanied by data center employees at all times
   - Internal and external 24x7 CCTV on all entries and key access areas - feeds are monitored and logged
   - Live security guards with regular security patrols
   - Segregated security zones requiring authorized access
   - On-site redundant backup power generation with extended fuel supplies
   - Redundant ISP access connections

4. **Application Security**
   - Multilayer: documents, containers, profile/metadata
   - Customer-administered permissions: ACLs and ethical firewalls
   - Authentication: Username and password protected accounts or customer-implemented multi-factor sign-on using customer's authentication application
   - Federated Identity with SAML 2.0, ADFS, RSA
   - Static and dynamic code reviews prior to each release
   - Ongoing developer training on OWASP security best practices
   - Audit trails
5. **Data Protection**
   - At Rest: Documents encrypted with AES-256 encryption by the Application using fully entropic random keys
   - In Transit: Documents encrypted using HTTPS and current TLS security protocols
   - All data obfuscated within an Object Store using a non-enumerated storage architecture
6. **Best Practices**
   - Defective Media Retention (DOD 5520)
   - Hardened Operator Access: Two-Factor, VPN Tunnel, Removable Media Disablement
   - Independent penetration tests twice a year
   - Monthly vulnerability scans
   - Regular training for security, OWASP Top Ten, etc.
   - Annual background and credit checks for all employees
   - Password complexity requirements
   - Mandatory password change required every 90 days
   - Internet acceleration (Akamai)
   - Segregation of responsibilities and access
   - Annual SOC 2 Type 2 audits for security, availability, and privacy
   - ISO 27001 Certification with the additional controls of ISO 27017 and ISO 27018



SERVICE REGIONS

NetDocuments currently operates three Service regions. The United States (US) region uses three data centers located in Scottsdale, AZ, Las Vegas, NV, and Salt Lake City, UT. The United Kingdom (UK) region uses three data centers located in Redhill, UK, Newport, Wales, UK, and Harrogate, UK. The Australia (AU) region uses two data centers located in Sydney, NSW and Perth, WA . Each Service region is independent; customer data is not shared between regions. A customer selects a primary Service region to process and store data. Customers may choose to store data in multiple Service regions. A fourth NetDocuments Service region for continental Europe, using three data centers in Germany (DE), is projected to begin operations in Q4 2019.

Customers also have the option of using ndFlexStore to direct where subsets of their documents are stored. With ndFlexStore, customers can meet national residency storage requirements while still having a single, global library. ndFlexStore allows customers to use **Azure regional storage facilities**, compatible customer storage sites, or even compatible customer-client locations. No matter which storage option is selected, all documents are protected by NetDocuments' service-applied, multi-layered encryption technology.

Service levels for each region are updated every five-minutes and are publicly available at these locations:

Service Regions Status Pages

United States	https://trust-us.netdocuments.com
Europe	https://trust-eu.netdocuments.com
Australia	https://trust-au.netdocuments.com

SERVICE STATUS

To maintain peak service levels, the Service undergoes regular, scheduled maintenance during periods of low customer usage. During Scheduled Maintenance Windows (SMWs) platform engineers upgrade equipment and make other changes to ensure the Service is ready to support customer requirements. Whenever possible, NetDocuments announces SMWs one to two weeks in advance of the event. SMWs are not part of our published 99.9% uptime SLA.

OBJECT STORAGE FOR ADVANCED SECURITY MEASURES

All documents are saved in a highly-secure object store infrastructure using erasure coding which, depending on the size of the document, either synchronously writes the documents to multiple, geographically dispersed data centers or mathematically slices documents into multiple data slices which are distributed across various, geographically dispersed data centers.

As an additional measure of protection, each encrypted file stored in NetDocuments' object store is randomly saved in one of over one million logical directories using a non-enumerated file structure on the highly-secure NetDocuments storage array. This makes it impossible to independently navigate to individual customer files.

SECURITY CERTIFICATIONS AND REGULATORY COMPLIANCE

A SOC 2 audit demonstrates that an independent auditing firm has examined an organization's security control objectives and activities and tested those controls to ensure that they are operating effectively. NetDocuments undergoes annual SOC 2 Type 2 audits for security, availability and privacy and annual ISO 27001 certification audits which include testing for the additional controls in ISO 27017 and ISO 27018. The scope of the ISO 27001 certification includes all of the data centers which host NetDocuments' Services as well as key service providers used by NetDocuments. Undergoing both SOC 2 Type 2 and ISO 27001 audits provides additional value to customers because ISO establishes the framework for best practices around security controls while SOC 2 demonstrates the controls are in place and functioning.

NetDocuments is your security partner.

NetDocuments is committed to providing the most functional and secure content services platform available. We partner with our customers to implement and demonstrate the levels of security they and their clients require. This includes reviewing unique security specifications and supporting customer-sponsored security compliance audits.

NetDocuments actively reviews applicable industry security requirements as well as local, state, and national security regulations to determine appropriate compliance efforts. Examples include individual security requirements from various states within the US, the Privacy Shield agreement between the US and the EU, the General Data Protection Regulation (GDPR) adopted by the EU, and security requirements put forth by the Australian Signals Directorate. NetDocuments regularly modifies and expands its security controls to maintain the highest levels of security for customer data around the world by complying with appropriate standards and regulations.

PLANNING FOR THE FUTURE

NetDocuments continues to add security protocols, compliance certifications, new policies and additional Service features to enhance our existing set of service, compliance and security controls. Over the next year, we will be integrating our cloud email management, OCR functionality and instant messaging functionality into our current certification audits.

You can learn more about our compliance initiatives by visiting **www.netdocuments.com** or by emailing **compliance@netdocuments.com**.