How NetDocuments is Helping You Meet – and Exceed – Your Security and Governance Requirements

netdocuments®

Contents

INTRODUCTION

Today's realities for establishing and maintaining data security and governance controls have changed significantly in recent years. The global health crisis has highlighted the criticality of cyber-security while working from home. Regulatory and government agencies, clients, and auditors are imposing stricter controls on data protection, best practices, independently verified certifications and attestations, and end-user oversight.

The global health crisis has highlighted the criticality of cyber-security while working from home.

Information assurance is an industry term that describes protecting your information assets at all levels. Information Assurance provides a framework for describing the products, features and functionality available from NetDocuments for protecting your information assets. It encompasses:

- **Confidentiality** – restricting access or limiting the actions that can be taken with information
- **Integrity** – ensuring that information can only be accessed or modified by authorized users
- **Availability** – ensuring information is available and ready for use by authorized users
- **Authentication** – ensuring users are who they say they are
- **Non-repudiation** – ensures that actions taken on information cannot be denied

NetDocuments has developed a computing platform that complements your comprehensive approach to security. This document will demonstrate how NetDocuments' security and governance offering can help your end-user security. The first sections address current and upcoming products which will be made available as part of NetDocuments PROTECT which provides additional solutions for customers looking for enhanced security options. The concluding sections address the standard security features of NetDocuments.

INTRODUCING NETDOCUMENTS PROTECT

NetDocuments PROTECT is a solution compromised of additional security products designed to further protect document repositories and the data they store. PROTECT is comprised of the following products:

- **Workspace Security Manager (WSM)** for managing scalable ethical walls and need-to-know security, and providing easy to manage governance for content segregation, effective rights reporting, contractor or temporary walls, and other processes usually managed by the risk teams. WSM is included as part of PROTECT. A further description of WSM is found on page 5.

- **Data Loss Prevention (DLP)** for restricting end-user actions that may cause harm to or loss of data due to end-user naivety, carelessness, or malicious behavior. Establishing strong walls via WSM is an essential but partial solution, because authorized users with access to data may still inadvertently or intentionally leak contents to unauthorized external or internal parties via email, secure delivery, collaboration, downloads, or printing. DLP complements WSM to provide comprehensive management of user access to data. Like WSM, DLP is included as part of PROTECT. A further description of DLP is included on page 6.

- **Customer Managed Encryption Keys (CMEK)** for managing granular dual-custody cryptography. CMEK allows customers to control access to their documents and can help restrict against access from external parties. It is an optional PROTECT solution add-on offered by NetDocuments.

- **FlexStore (FS)** and **FlexStore Pro (FSP)** for allowing customers to store selected digital files in specific countries as required to meet local residency requirements and for improving performance. FS and FSP help customers meet the goal of having a single library spanning multiple storage facilities across multiple continents to promote a "one firm" strategy, while also allowing regional data storage and local data cryptography processing. Like CMEK, FlexStore and FlexStore Pro are offered as an optional PROTECT solution add-on.

Please contact NetDocuments for additional information on these solutions.

ABOUT NETDOCUMENTS WORKSPACE SECURITY MANAGER

Workspace Security Manager (WSM) is a practical technology designed to manage at-scale the confidentiality of client matters, workspaces and digital files stored in NetDocuments via access control and ethical walls. As one of the products included in PROTECT, WSM is intended to streamline security settings already natively present in the NetDocuments platform and to reduce the effort involved in managing complex need-to-know security and litigation hold environments.

A summary of WSM's capabilities is described below:

- Provides a modern and intuitive user interface and scalable methods for creating, managing, and applying security polices and ethical walls to workspaces
- Allows policies set at the workspace level to be pushed downstream to all associated documents, emails, folders and sub-folders, discussions, sets, and tasks
- Enables "need to know security" and temporary access to selected content (contractor walls), even when walls have been put in place
- Allows walls to be built around any metadata used to organize the workspaces in a Cabinet, such as Author, Practice Group, or Office, and not just Client/Matter
- When used in conjunction with DLP, disallows users from making unauthorized access control modifications to digital files that are contrary to official workspace security settings
- Can generate an Effective Rights Report for clients, regulatory agencies, or OGC inquiries, detailing the rights assigned and the controls set by the walls and need-to-know policies, at any time during the creation or during the life of the matter
- Has a low impact on system resources and is totally integrated with the NetDocuments cloud, including its entropic cryptography and authentication services, its search and navigation systems, and its global data distribution platform
- Can operate on a stand-alone basis or alongside existing integrations with external third-party ethical-wall services such as those from Intapp Walls, Prosperoware Confidentiality Manager, and others. NetDocuments walls can also be controlled from Physical Record systems such as File Trail and iComply.
- DLP, as with all NetDocuments products and offerings, will continue to be enhanced and improved in future versions.

Workspace Security Manager will become available in late 2020. To access WSM, you will need to subscribe to NetDocuments PROTECT.

ABOUT NETDOCUMENTS DATA LOSS PREVENTION

Where WSM modernizes access controls to digital files, Data Loss Prevention (DLP) modernizes the controls for actions users are permitted to perform on accessible files. When a user is not blocked by walls via WSM and is able to access certain workspaces or digital files, DLP policies may dictate what actions are allowed by a user in the NetDocuments platform while prohibiting other actions. For example, printing, copying or downloading may be allowed, but sending secured links, moving the file to different workspaces, or modifying access to the document may all be prohibited.

DLP is a practical technology designed to manage the permissible or prohibited actions against a matter, cabinet, or digital file, within the NetDocuments platform according to a flexible predefined Data Classification scheme defined by the Firm, or through direct assignment of specific DLP policies. Examples for data classification are "secret", "classified", "sensitive", and "internal". One of these classes is designated as default. Any of these classes can be assigned to a matter, which will automatically set all of its documents to receive the same classification, and the DLP rules assigned to that classification, unless such documents are specifically upgraded or downgraded to a different classification by a user authorized to take such action. For example, using the DLP rules, a user may be allowed to share digital files via Secured Delivery, Email, or CollabSpaces for "classified" matters, but prohibited from such actions for "secret" matters.

While WSM secures access to workspaces and files (border control or access enforcement), DLP controls the permissible actions once authorized users gain access to such contents (action control or action enforcement). A best practice approach to cyber security as part of a holistic information governance strategy requires both WWM and DLP.

Best practices require firms to monitor and track end-user actions to prevent data loss or misuse. Expecting all end-users to always comply with multitudes of different security policies for different clients and matters is an impossible task, potentially leading to disastrous data losses or unauthorized use or disclosure. Whether users are malicious, naïve, or careless, the security risks for data leaks are extreme. A truly holistic approach to DLP may combine specialist products at the network edge, along with the elegant simplicity of DLP being built into the central global repository.

A summary of DLP capabilities are described below:

- DLP provides a modern and intuitive user interface for managing the classification of data using Cabinet, document, or metadata attributes, and for defining policies for permissible and prohibited actions on digital files within the NetDocuments platform according to the data classification.
- Sample actions which can be controlled by DLP include:
  - Sending documents via email
  - Including in CollabSpaces
  - Copying a document
  - Delivering a document via Secure Link
  - Downloading documents outside of the ND Platform
  - Echoing the document
  - Modifying Explicit ACL controls
  - Moving a document out of its parent folder
  - Synchronizing via ndSync
  - Opening via Office Online
  - Printing a document
- DLP is fully integrated into NetDocuments. Action permissions are uniformly enforced across all NetDocuments interfaces, including web interface, ndOffice, ndMail, ndSync, and mobile devices.
- DLP policies deployed at the Cabinet, Profile, and Document level are additive and will not override each other, which allows you to create an additive DLP model. DLP only controls for actions for documents while those documents are in the document management system. DLP is not Digital Rights Management (DRM) which controls for actions outside the DM, such as when a file has been externalized via email attachment.
- Just like all NetDocuments security offerings, the DLP service will continue to be enhanced to cover more actions available in the document service.

To access DLP, you will need to subscribe to NetDocuments PROTECT.

OTHER SECURITY TECHNOLOGIES AND FEATURES THAT COMPLEMENT NETDOCUMENTS PROTECT

NetDocuments PROTECT complements existing data security and information governance features and technologies that already exist in the NetDocuments platform. When used in conjunction with the standard security features, PROTECT can be part of a layered approach to security. This section will detail some of

the key security features that are available to all NetDocuments customers today, regardless if PROTECT has been purchased.

When uploaded to the platform, each document receives and is encrypted by its own unique Object Encryption Key (OEK) which is then separately encrypted by a Master Encryption Key (MEK) at the repository level. Each key is created using fully entropic quantum random number generation. Because of this, documents can only be accessed by persons using authorized credentials.

Since each file is encrypted individually and at the repository level, the risk of transferring malicious code, including ransomware, from one document to others in the repository eliminated. Even if one corrupted file is uploaded to the system, it cannot spread its corruption to other files through the NetDocuments service. The Service provides circuit breaker functionality in ndSync, which can detect and stop mass uploads of files, if ndSync is enabled on the individual workstation that is uploading the documents.

Permissions for the platform are designed around access controls and profile-based security. Access to content can be granted based on View, Edit, Sharing, and Administrative permissions, and these can be applied to document or profile attributes. This allows firms to restrict access to content based on the metadata associated with it, meaning that if you have data regarding a certain project, you can restrict access for all files within that workspace that are tagged with that project's metadata attribute.

ABOUT NETDOCUMENTS TRUST SERVICES

In addition to the standard security features listed above, NetDocuments Trust Services is a corpus of material available under subscription which the Firm may use to respond to client and regulatory audits or use for learning about and validating the security, availability, and privacy of the NetDocuments Service. The materials are regularly updated and are made available by the NetDocuments Compliance Group. Upon subscribing to the service, the firm will have access to contents outlining NetDocuments policies and best practices and to material on the following NetDocuments certifications and attestations:

• AICPA SOC 2 on Security • AICPA SOC 2 on Availability • AICPA SOC 2 on Privacy	• ISO 27001 • ISO 27017 • ISO 27018	• ISO 27701 2nd half 2020 (for GDPR) • FIPS 140-2 Level 3 for HSMs • HiPAA/HITECH

NetDocuments also employs the following best practices in order to further protect your data: segregation of duties, defective media retention, removable media disablement, log isolation, 3rd party security scans,

static/dynamic source code scans, regular vulnerability tests, etc. These best practices are detailed in the Trust Services as well.

NetDocuments deploys datacenters in the US (3 facilities), UK (3), Germany (3), and Australia (2). In addition, storage facilities are available in Microsoft Azure in select global locations. NetDocuments is also working to complete the FedRAMP authorization process for a new, dedicated US Service region. NetDocuments anticipates achieving FedRAMP Ready status in July 2020 and full FedRAMP authorization in the fourth quarter of 2020 for the new Service region. Each datacenter used by NetDocuments follows or exceeds industry standards for security and availability of datacenter resources. Those standards include perimeter security, 24/7 external and internal surveillance, hardened entrances, preauthorized visitation with validation, multifactor access for physical security zones, fully redundant HVAC, water and fire detection and prevention, and extended on-site backup power generation capability. NetDocuments audits each datacenter is uses annually, and the datacenters are also within the scope of NetDocuments current ISO 27001 certification.

CONCLUSION

NetDocuments provides a strong information assurance platform for every customer, at every level, from data security to end user focused information governance features. Our security architecture, encryption techniques, and compliance controls demonstrate our commitment to keeping your data secure within the platform.

We are also committed to furthering our security offerings by continually improving controls within our Service infrastructure and complementing those with our PROTECT solution for customers who desire additional customer-managed security controls. These solutions allow firms more control over how data is accessed and what users can do with it.

ABOUT NETDOCUMENTS

NetDocuments is the leading cloud-based document and email management solution to securely store and organize documents on one platform. With NetDocuments, users can work securely on documents and file emails anywhere in the world on any device while collaborating with internal and external stakeholders alike—which makes it an ideal solution for remote work.

Backed by 20 years of experience in cloud innovation, over 2,750 companies worldwide trust us to secure their data while increasing productivity and team collaboration.

To learn more about maximizing productivity, mitigating risk, and building collaboration: Contact us at **(866) 638-3627** or visit **www.NetDocuments.com** to learn more today.