When you never have to choose between productivity and compliance.

That's Work Inspired

The **PROTECT** Solution

netdocuments®

PROTECT

PROTECT adds additional controls and protections that extend NetDocuments' native, award-winning security capabilities. With tools that allow you to create and apply security policies across your organization, guard against unauthorized exfiltration, and create a robust security framework, PROTECT gives you the extra capabilities you need to secure your content and reduce the risk of unintentional or malicious data breaches.

Core PROTECT Technology Includes:

Data Loss Prevention (DLP)

Keep all of your sensitive data and documents safe from unauthorized use.

NetDocuments DLP allows you to classify content, create and enforce policies that control user actions, and prevent documents from leaving the security of NetDocuments.

Workspace Security Manager (WSM)

Streamline and simplify security policy management.

WSM makes it easy for the right people to create, edit, and apply security policies to the content in your workspaces—so you can build and manage ethical walls or need-to-know security environments.

Add On Technology Options:

FlexStore and FlexStore Pro

Manage and control where your content is stored, so it stays closer to the people who need it.

FlexStore provides cloud or hybrid storage options that give you control over the physical location of your content. With FlexStore, you can take advantage of NetDocuments' global data centers, local object store technology in your own data centers, or Microsoft Azure Blob Storage for geo-aware cloud storage—and manage all of those options through one convenient management console. FlexStore Pro adds the Distributed Cryptographic Service (DCS), which encrypts and decrypts content closer to end users.

Customer Managed Encryption Keys (CMEK)

Fulfill your ethical and professional obligation to protect the information you hold.

Customer Managed Encryption Keys (CMEKs) provide an additional layer of encryption for your most sensitive information, while leaving you in complete control of the encryption keys. The standard NetDocuments service includes two layers of encryption. CMEKs add a third layer, which provide dual-custody control. CMEKs also allow you to revoke and reapply keys at will, and they give you the flexibility to apply advanced encryption to whatever specific content you choose.

Data Loss Prevention (DLP)

As insider attacks rise, you need a holistic security strategy to protect your most sensitive information. DLP takes the pressure off your overburdened IT teams by using layered policies to simply and efficiently manage an extra layer of security. With DLP, you can prevent authorized users from accidentally or maliciously sharing, editing, emailing, or downloading sensitive information. You can easily apply policies broadly across all your content—or use metadata to apply policies more narrowly at the profile level or the individual document level.

Prevent Insider Attacks by Careless, Naïve, or Malicious Employees:

- **Keep Control of Your Policies**

  You need flexibility to keep your documents and users secure. DLP provides it—with a layered policy approach that allows you to apply controls to content at the cabinet, profile, and document level. This allows you to add essential extra layers of security to the specific documents that need them.

- **Save Time and Effort**

  DLP provides a flexible approach for applying access controls to your content. With DLP, you can extend your holistic security strategy by enabling DLP at the source—in your NetDocuments repository.

- **Use Integration to Build a More Holistic Security Strategy**

  You can't stay secure unless all of your security solutions work together. NetDocuments DLP helps make that possible—by giving you the ability to export DLP policy and classification labels into Microsoft Office documents as custom metadata attributes. This allows other security technologies to trigger policies based on those labels.

Protect Your Documents End-to-end

DLP is designed to work in tandem with Workspace Security Manager (WSM) and other NetDocuments security features to provide complete and layered protection for your information.

DLP provides the ability to export your security labels as attributes of Microsoft Office documents. These labels can automatically engage access and sharing controls, which provides seamless integration nto your overall security strategy.

Workspace Security Manager (WSM)

WSM gives you the freedom and flexibility to create and manage security policies, including access control permissions, locking permissions to create walls, enabling need-to-know sharing, and delegating security management to assigned individuals. These policies are applied at the workspace level and apply to all content within a workspace.

Free Up Your Time by Safely Delegating Workspace Controls

- **Safely Control User Access**

  Easily establish and control ethical walls for user access. Then, enable your IT team to authorize appropriate users to manage those ethical walls and other permissions at the workspace level within specific cabinets —while still maintaining access controls over those policy managers.

- **Create a True Need-to-Know Environment**

  The key to a need-to-know environment is only giving users access to the files they need. WSM provides the flexibility to authorize document access regardless of whether users are members of a workspace.

- **Use Clicks, Not Code**

  Make it quick and easy for authorized individuals to create and maintain need-to-know security environments, removing the need for complex code and specialized expertise.

- **Make Audit Trails Easy**

  WSM provides an audit trail of all changes made to a policy, which you can easily download as a report. This "rights report" shows the effective rights applied by a policy within the workspace, as well as other useful information.

Create a True Need-to-Know Environment

To create a secure and effective need-to-know environment, you must be able to easily create and manage ethical walls to control who has access to what within your service. You also need detailed and accurate information about who should access which documents. Since it's impossible for your IT team to be familiar with every matter and project across your organization, this involves delegating the creation and management of security policies to people with the knowledge and responsibilities that make them best-suited for those tasks.

WSM makes that easy—by allowing authorized policy managers to apply workspace policies that include permissions for both internal and external users. This approach saves your IT staff time and strengthens your organization's security posture.

FlexStore and FlexStore Pro

As jurisdictions and regulatory bodies across the world continue to place more restrictions on how information is stored and processed, you are faced with a recurring dilemma: How do you keep your teams productive and provide them with good service experiences without compromising content governance and security?

FlexStore and FlexStore Pro from NetDocuments directly address this challenge—by making it possible for all your stakeholders to experience the convenience, efficiency, and security of hybrid-cloud and cloud-storage options no matter where their information resides.

Two Options to Standardize Processes Without Sacrificing Performance

- **FlexStore**

  Take Advantage of Geo-aware Global Storage

  FlexStore is ideal if you have clients that require local document storage in locations of their choosing. With FlexStore, you can store your content in the NetDocuments cloud, on Microsoft Azure, or on premises in your data center, while still enjoying all of the processing efficiencies and innovations that secure cloud technology has to offer.

- **FlexStore Pro**

  Accelerate Your Content Delivery

  Your users want a consistent, reliable service experience that includes quick downloads and even faster uploads. At the same time, your organization requires consistent governance and security controls, regardless of location. With FlexStore Pro, you can have both. FlexStore Pro enhances FlexStore by introducing localized document encryption and decryption using the Distributed Cryptographic Service (DCS).

You Don't Have to Choose Between Productivity and Compliance

FlexStore and FlexStore Pro offer geo-aware storage to help keep your filing systems and security policies standardized no matter where your users are, which ultimately increases client and stakeholder confidence that documents will always stay organized, protected, and compliant. Plus, FlexStore and FlexStore Pro storage locations can be organized by matter, client, or project profile attributes to store specific documents in a specific location. This means users never have to think about where their content is stored, and they can access everything through a single interface.

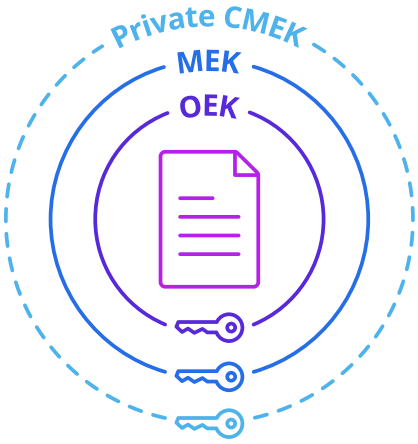
Customer-Managed Encryption Keys (CMEKs)

Customers, clients, and stakeholders often have unique security requirements that demand granular security strategies, including the ability to generate and manage their own encryption keys. CMEKs build on the dual-encryption capabilities of NetDocuments' existing Encryption Key Management (EKM) technology—by adding a third layer of encryption to specific content.

You can choose to assign CMEKs to specific sets of content organized by metadata profile attributes such as client, matter, or project. This method of managing encryption allows you to remove access to specific content while maintaining user access to other sets of content.

Get Unmatched Document Protection with CMEKs

- **Object Encryption Key (OEK)**
  Whenever a document is uploaded to NetDocuments, it is encrypted using a new, individual OEK which is unique for each document.
- **Master Encryption Key (MEK)**
  As soon as the document is encrypted, the MEK is used to encrypt, or 'wrap', the OEK.
- **Customer Managed Encryption Key (CMEK)**
  If enabled and applied to the target document, a CMEK is then used to encrypt, or "wrap" the OEK with a second layer of encryption—creating a total of three layers of encryption for your most sensitive documents.



The document is encrypted by the OEK, which is then wrapped by the MEK. If CMEK is active, the MEK is wrapped by the CMEK adding a third layer of encryption to the document.

Security That Exceeds Expectations

Protecting information is not a one-size-fits-all responsibility, and it's becoming increasingly clear that some information is so sensitive that it requires your organization to take every possible step to secure it. Through our cloud and private key management options, CMEKs not only enhance the industry-leading encryption technology built into NetDocuments, they improve your ability to support diverse security strategies. With CMEKs protecting your information, you can rest easy knowing that you've taken every step to secure your data from even the most dangerous cyberattacks.

When document security lowers your risk and your blood pressure.

That's Work Inspired

IT teams are always searching for smart strategies to strengthen their organization's security posture—without adding extra burdens for users, clients, and other stakeholders.

With the PROTECT solution, your IT teams can enhance the industry-leading document security built into NetDocuments, empower the best and most knowledgeable people across your organization to create and manage appropriate security policies, and satisfy the requirements of your most rigorous compliance requirements—all while removing cumbersome administrative tasks.

Give your teams the tools they need to *Work Inspired*.

Get PROTECT today.

To learn more, visit
www.NetDocuments.com
or call **(866) 638-3627.**

netdocuments®