Quando você nunca precisa escolher entre produtividade e conformidade.

Isso é trabalho inspirado

A Solução
PROTECT

netdocuments®

PROTEGER

O **PROTECT** adiciona controles e proteções adicionais que estendem os recursos de segurança premiados e nativos do NetDocuments. Com ferramentas que permitem você criar e aplicar políticas de segurança em sua organização, proteja-se contra exfiltração não autorizada e crie uma estrutura de segurança robusta. O PROTECT oferece os recursos extras que você precisa para PROTECT seu conteúdo e reduzir o risco de violações de dados não intencionais ou maliciosas.

A tecnologia principal do PROTEGER inclui:

Prevenção de perda de dados (DLP)

Mantenha todos os seus dados e documentos confidenciais a salvo de uso não autorizado.

O NetDocuments DLP permite classificar o conteúdo, criar e aplicar políticas que controlam as ações do usuário, além de impedir que os documentos saiam da segurança do NetDocuments.

Gerenciador de segurança do espaço de trabalho (WSM)

Otimize e simplifique o gerenciamento de políticas de segurança.

O WSM facilita para que as pessoas certas criem, editem e apliquem políticas de segurança ao conteúdo em seus espaços de trabalho, para que você possa criar e gerenciar limites éticos ou ambientes de segurança com base na necessidade de conhecimento.

Opções adicionais de tecnologia:

FlexStore e FlexStore Pro

Gerencie e controle onde seu conteúdo está armazenado, para que fique mais próximo das pessoas que precisam dele.

O FlexStore oferece opções de armazenamento em nuvem ou híbrido que proporcionam controle sobre a localização física do seu conteúdo. Com o FlexStore, você pode aproveitar as vantagens dos centros de dados globais do NetDocuments, a tecnologia de armazenamento de objeto local em seus próprios centros de dados ou o Microsoft Azure Blob Storage para armazenamento em nuvem com reconhecimento geográfico — e gerenciar todas essas opções por meio de um console de gerenciamento conveniente. O FlexStore Pro adiciona o Serviço de criptografia distribuído (DCS), que criptografa e descriptografa o conteúdo mais próximo dos usuários finais.

Chaves de criptografia gerenciadas pelo cliente (CMEK)

Cumpra sua obrigação ética e profissional de proteger as informações que você detém.

As Chaves de criptografia gerenciadas pelo cliente (CMEKs) fornecem uma camada adicional de criptografia para suas informações mais confidenciais, deixando você com controle total das chaves de criptografia. O serviço NetDocuments padrão inclui duas camadas de criptografia. As CMEKs adicionam uma terceira camada, que fornece controle de custódia dupla. As CMEKs também permitem revogar e reaplicar as chaves conforme necessário e oferecem a flexibilidade de aplicar criptografia avançada a qualquer conteúdo específico que você escolher.

Prevenção de perda de dados (DLP)

À medida que os ataques internos aumentam, você precisa de uma estratégia de segurança holística para PROTECT suas informações mais confidenciais. O DLP alivia a pressão sobre suas equipes de TI sobrecarregadas usando políticas em camadas para gerenciar de forma simples e eficiente uma camada extra de segurança. Com o DLP, você pode impedir que usuários autorizados compartilhem, editem, enviem por e-mail ou baixem informações confidenciais de forma acidental ou maliciosa. E de forma fácil, você pode aplicar políticas em todo o seu conteúdo amplamente, ou usar metadados para aplicar políticas mais restritas no nível do perfil ou no nível do documento individual.

Previna ataques internos por funcionários descuidados, ingênuos ou maliciosos:

- **Mantenha o controle das suas políticas**
  Você precisa de flexibilidade para manter seus documentos e usuários seguros. O DLP oferece isso — com uma abordagem de política em camadas que permite aplicar controles ao conteúdo no nível de gabinete, perfil e documento. Isso possibilita adicionar camadas extras essenciais de segurança aos documentos específicos que precisam delas.
- **Economize tempo e esforço**
  O DLP fornece uma abordagem flexível para aplicar controles de acesso ao seu conteúdo. Com o DLP, você pode estender sua estratégia de segurança holística habilitando o DLP na fonte, em seu repositório NetDocuments.
- **Use a integração para elaborar uma estratégia de segurança mais holística**
  Você não tem como ficar seguro a menos que todas as suas soluções de segurança funcionem juntas. O NetDocuments DLP ajuda a tornar isso possível, proporcionando a capacidade de exportar políticas de DLP e rótulos de classificação para documentos do Microsoft Office como atributos de metadados personalizados. Isso permite que outras tecnologias de segurança acionem políticas com base nesses rótulos.

Proteja seus documentos de ponta a ponta

O DLP foi projetado para funcionar em conjunto com o Gerenciador de segurança do espaço de trabalho (WSM) e outros recursos de segurança do NetDocuments para fornecer proteção completa e em camadas para suas informações.

O DLP oferece a capacidade de exportar seus rótulos de segurança como atributos de documentos do Microsoft Office. Esses rótulos podem envolver automaticamente os controles de acesso e compartilhamento, o que fornece integração perfeita com sua estratégia geral de segurança.

Gerenciador de segurança do espaço de trabalho (WSM)

O WSM oferece liberdade e flexibilidade para criar e gerenciar políticas de segurança, incluindo permissões de controle de acesso e permissões de bloqueio para criar barreiras, permitindo o compartilhamento com base na necessidade de conhecimento e delegando o gerenciamento de segurança a indivíduos designados. Essas políticas são aplicadas no nível do espaço de trabalho e abrangem todo o conteúdo de um espaço de trabalho.

Libere seu tempo delegando controles do espaço de trabalho com segurança

- **Controle com segurança o acesso do usuário**
  Crie facilmente grupos de Workspace Security Manageer (WSM) e capacite os usuários mais adequados para gerenciar as políticas de segurança adicionando-os, reduzindo a carga sobre sua equipe de TI. Em seguida, use as políticas para controlar o acesso e estabelecer barreiras éticas no nível da área de trabalho em gabinetes específicos.

- **Criar um ambiente de acesso somente para pessoas que deve acessar**
  O ponto critical para criar um ambiente seguro é apenas dar aos usuários acesso aos arquivos de que precisam. O WSM oferece flexibilidade para autorizar o acesso ao documento, independentemente de os usuários serem membros de um espaço de trabalho ou Workspace.

- **Use cliques, não código**
  Faça com que seja rápido e fácil para indivíduos autorizados criar e manter políticas de segurança que imponham controles de acesso, barreiras éticas e compartilhamento de necessidade de saber por meio de uma interface amigável com relatórios de ações completas.

- **Facilite as trilhas de auditoria**
  Você pode gerar um relatório de direitos efetivos que detalha as permissões de acesso, barreiras éticas e configurações de compartilhamento que você precisa saber ao criar ou editar uma política. Acesse (ou abaixe) um histórico completo mostrando quais mudanças foram feitas, e por quem, para cada política individual por meio a interface de administrador.

Crie um ambiente real com base nas necessidades de conhecimento

Para criar um ambiente seguro e eficaz com base nas necessidades de conhecimento, você deve ser capaz de criar e gerenciar barreiras éticas para controlar quem tem acesso a quê dentro do seu serviço. Você também precisa de informações detalhadas e precisas sobre quem deve acessar quais documentos. Como é impossível sua equipe de TI estar familiarizada com todos os assuntos e projetos em sua organização, isso envolve delegar a criação e o gerenciamento de políticas de segurança a pessoas com o conhecimento e as responsabilidades que as tornam mais adequadas para essas tarefas.

O WSM torna isso fácil, permitindo que os gerentes de política autorizados apliquem políticas de espaço de trabalho que incluem permissões para usuários internos e externos. Essa abordagem economiza tempo da equipe de TI e fortalece a postura de segurança da sua organização.

FlexStore e FlexStore Pro

À medida que as jurisdições e órgãos reguladores em todo o mundo continuam colocando mais restrições sobre como as informações são armazenadas e processadas, você se depara com um dilema recorrente: como manter suas equipes produtivas e oferecer boas experiências de serviço sem comprometer a governança de conteúdo e a segurança?

O FlexStore e o FlexStore Pro da NetDocuments abordam esse desafio diretamente, possibilitando que todas as suas partes interessadas experimentem a conveniência, eficiência e segurança das opções de nuvem híbrida e armazenamento em nuvem, independentemente de onde residam suas informações.

Duas opções para padronizar processos sem sacrificar o desempenho

- **FlexStore**

  Aproveite as vantagens do armazenamento global com reconhecimento geográfico

  O FlexStore é ideal se você tem clientes que exigem armazenamento local de documentos em locais de sua escolha. Com o FlexStore, você pode armazenar seu conteúdo na nuvem do NetDocuments, no Microsoft Azure ou localmente em seu centro de dados, enquanto desfruta de todas as eficiências de processamento e inovações que a tecnologia de nuvem segura tem a oferecer.

- **FlexStore Pro**

  Acelere a entrega do seu conteúdo

  Seus usuários desejam uma experiência de serviço consistente e confiável que inclua downloads rápidos e uploads ainda mais rápidos. Ao mesmo tempo, sua organização requer governança e controles de segurança consistentes, independentemente da localização. Com o FlexStore Pro, você pode ter os dois. O FlexStore Pro aprimora o FlexStore introduzindo criptografia e descriptografia de documentos localizados usando o Serviço de criptografia distribuído (DCS).

Você não precisa escolher entre produtividade e conformidade

O FlexStore e o FlexStore Pro oferecem armazenamento com reconhecimento geográfico para ajudar a manter seus sistemas de arquivamento e políticas de segurança padronizados, não importa onde seus usuários estejam, o que acaba aumentando a confiança do cliente e das partes interessadas de que os documentos sempre permanecerão organizados, protegidos e em conformidade. Além disso, os locais de armazenamento do FlexStore e FlexStore Pro podem ser organizados por caso, cliente ou atributos de perfil do projeto para armazenar documentos específicos em um local específico. Isso significa que os usuários nunca precisam pensar onde seu conteúdo está armazenado e podem acessar tudo por meio de uma única interface.

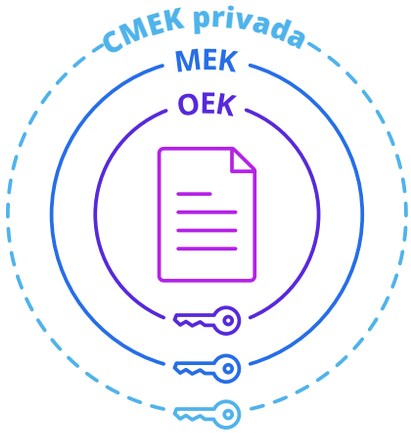
Chaves de criptografia gerenciadas pelo cliente (CMEKs)

Consumidores, clientes e partes interessadas geralmente têm requisitos de segurança exclusivos que exigem estratégias de segurança granulares, incluindo a capacidade de gerar e gerenciar suas próprias chaves de criptografia. As CMEKs se baseiam nos recursos de criptografia dupla da tecnologia existente de Gerenciamento de chaves de criptografia (EKM) da NetDocuments, adicionando uma terceira camada de criptografia a conteúdo específico.

Você pode escolher atribuir CMEKs a conjuntos específicos de conteúdo organizados por atributos de perfil de metadados, como cliente, caso ou projeto. Esse método de gerenciamento de criptografia permite remover o acesso a um conteúdo específico enquanto mantém o acesso do usuário a outros conjuntos de conteúdo.

Obtenha proteção incomparável de documentos com CMEKs

- **Chave de criptografia de objeto (OEK)**
  Sempre que um documento é carregado no NetDocuments, ele é criptografado usando uma nova OEK individual, única para cada documento.
- **Chave de criptografia mestre (MEK)**
  Assim que o documento é criptografado, a MEK é usada para criptografar, ou "empacotar", a OEK.
- **Chave de criptografia gerenciada pelo cliente (CMEK)**
  Se habilitada e aplicada ao documento de destino, uma CMEK é então usada para criptografar ou "empacotar" a OEK com uma segunda camada de criptografia, criando um total de três camadas de criptografia para seus documentos mais confidenciais.



O documento é criptografado pela OEK, que é então empacotada pela MEK. Se a CMEK estiver ativa, a MEK é empacotada pela CMEK, adicionando uma terceira camada de criptografia ao documento.

Segurança que excede as expectativas

Proteger informações não é uma responsabilidade única e genérica, e cada vez mais fica claro que algumas informações são tão confidenciais que exigem que sua organização tome todas as medidas possíveis para protegê-las. Com nossas opções de gerenciamento de nuvem e chave privada, as CMEKs não apenas aprimoram a tecnologia de criptografia líder do setor integrada ao NetDocuments, mas também aprimoram sua capacidade de oferecer suporte a diversas estratégias de segurança. Com CMEKs protegendo suas informações, você pode ficar tranquilo sabendo que já tomou todas as medidas para proteger seus dados até dos ataques cibernéticos mais perigosos.

Quando a segurança do documento diminui o risco e sua pressão arterial.

Isso é trabalho inspirado

As equipes de TI estão sempre em busca de estratégias inteligentes para fortalecer a postura de segurança da sua organização — sem sobrecarregar os usuários, clientes e outras partes interessadas.

Com a solução PROTECT, suas equipes de TI podem aprimorar a segurança de documentos líder do setor integrada ao NetDocuments, capacitar as melhores e mais experientes pessoas da sua organização para criar e gerenciar políticas de segurança adequadas e satisfazer as exigências dos seus requisitos de conformidade mais rigorosos — tudo isso enquanto remove tarefas administrativas complicadas.

Dê às suas equipes as ferramentas de que precisam para o *Trabalho Inspirado*.

Obtenha o PROTECT hoje mesmo.

Para saber mais, visite
www.NetDocuments.com
ou ligue para
+55 21 4040.4623.

netdocuments®