



EXPLICAÇÃO RESUMIDA DE SERVIÇOS E SEGURANÇA

netdocuments®

O NetDocuments é um sistema de gestão de documentos baseado em nuvem (DMS) que oferece gestão de documentos e e-mails, além de soluções de produtividade. Os usuários podem acessar os documentos de qualquer dispositivo aprovado com uma conexão à Internet enquanto aproveitam os benefícios de segurança e conformidade líderes do setor oferecidos pelo NetDocuments.

Este resumo de segurança descreve como o NetDocuments protege seus dados e redes de serviço para que você possa ter certeza de que suas informações estarão sempre seguras ao usar o DMS NetDocuments.

Proteção de dados do cliente

O NetDocuments foi projetado em uma base de segurança e inovação, com o entendimento de que a inovação não pode acontecer às custas da segurança. A plataforma NetDocuments foi arquitetada para proteger seus documentos com medidas de segurança robustas, incluindo várias camadas de criptografia e custódia controlada de forma independente das chaves de criptografia.

Cada documento que você coloca no DMS é criptografado com sua própria chave de criptografia de objeto (OEK) AES-256 exclusiva. Cada OEK é ainda criptografada com uma chave mestra de criptografia AES-256, ou MEK, que é armazenada em um módulo de segurança de hardware altamente seguro (HSM).

O NetDocuments oferece aos clientes a opção de criptografar ainda mais os documentos selecionados com uma terceira camada de criptografia usando uma chave de criptografia AES-256 gerenciada pelo cliente, ou CMEK. Todas as CMEKs são armazenadas em um segmento totalmente restrito de HSMs do NetDocuments, que só pode ser acessado pelo cliente, ou em um HSM de propriedade do cliente. Quando os dados do cliente estão transitando pela Internet, eles são protegidos por https com protocolos de segurança TLS.

SEGURANÇA DE REDE DA PLATAFORMA

A NetDocuments emprega uma gama abrangente de procedimentos, ferramentas e serviços independentes para fornecer segurança líder do setor para os documentos dentro da plataforma.

1. Segurança de rede

- Firewalls de aplicativos da Web independentes de terceiros
- Proteção contra DDoS
- Firewalls internos, redundantes e com monitoração de estado
- Balanceadores de carga (firewalls sem monitoração de estado)
- Sistema de detecção de intrusão (IDS)
- DMZ (Zona de rede desmilitarizada) que hospeda todos os servidores da web



2. Segurança de infraestrutura

- Infraestrutura totalmente redundante, sem ponto único de falha
- Monitoramento em tempo real
- Log de atividades com revisão de logs e retenção estendida de logs
- Senhas fortes
- Acesso restrito
- Revisões regulares de regras de firewall
- Imagens de servidor avançado atualizadas e implantadas regularmente
- Implantação automatizada, incluindo destruição e substituição periódica de todas as máquinas virtuais (VMs)



3. Segurança do centro de dados

- Barreiras físicas de perímetro
- Acesso fechado, monitorado e controlado
- Visitação somente por agendamento pré-autorizado, validado por documento de identidade oficial com foto
- Todos os visitantes são acompanhados por funcionários do centro de dados em todos os momentos
- Circuito fechado de televisão interno e externo 24 horas por dia/7 dias por semana em todas as entradas e principais áreas de acesso, monitoradas e registradas
- Guardas de segurança presenciais com patrulhas de segurança regulares
- Zonas de segurança segregadas que requerem acesso autorizado
- Geração de energia reserva redundante no local com suprimentos de combustível estendidos
- Conexões de acesso de ISP (Provedores de serviço de Internet) redundantes

4. Segurança de aplicações

- Segurança aplicada em múltiplas camadas: Documentos individuais, contêineres, perfil/metadados, projeto/caso, consumidor/cliente
- Permissões administradas pelo cliente: Listas de controle de acesso (ACLs), firewalls éticos
- Autenticação: Logon único ou Logon multifator implementado pelo cliente usando Identidade federada com aplicações compatíveis com SAML 2.0, ADFS ou RSA
- Revisões de código estático e dinâmico antes de cada lançamento
- Treinamento contínuo de desenvolvedor nas melhores práticas de segurança do OWASP
- Trilhas de auditoria

5. Proteção de dados

- Em repouso: Documentos criptografados com criptografia AES-256 pela Aplicação usando chaves aleatórias totalmente entrópicas
- Em trânsito: Documentos criptografados com HTTPS usando protocolos de segurança TLS atuais
- Todos os documentos são salvos em uma infraestrutura de repositório de objetos altamente segura usando codificação de eliminação que, dependendo do tamanho do documento, grava os documentos de forma síncrona em vários centros de dados em localizações diversas ou divide matematicamente os documentos em várias fatias de dados que são distribuídas em diversos centros de dados em pontos geográficos dispersos
- Todos os arquivos de dados ou fatias são ofuscados pela colocação aleatória de arquivos individuais em mais de um milhão de diretórios lógicos dentro de cada centro de dados, usando uma estrutura de arquivo não enumerada dentro do repositório de objeto de armazenamento

6. Melhores práticas

- Retenção de mídia com defeito (DoD 5520)
- Acesso avançado do operador (acesso MFA, túnel VPN, desativação de mídia removível)
- Testes de penetração independentes duas vezes por ano
- Varreduras mensais de vulnerabilidades
- Treinamento regular
- Histórico anual e verificações de crédito para todos os funcionários
- Requisitos de complexidade de senha
- Alteração de senha obrigatória necessária a cada 90 dias
- Aceleração da Internet (Akamai)
- Auditorias anuais Tipo 2 SOC 2 para segurança, disponibilidade e privacidade
- Certificação ISO 27001 com os controles adicionais de ISO 27017, ISO 27018 e ISO 27701
- Atestado independente de conformidade com os requisitos de segurança da HIPAA e HiTECH aplicáveis

7. Segregação de responsabilidades e acesso

- Hardware – Operadores de centros de dados
- Aplicação – Engenharia e CQ
- Rede – Equipe de TI
- Servidores e armazenamento – Equipe de TI
- Segurança – Acesso de dois fatores pela Equipe de segurança com auditoria pela Equipe de conformidade independente
- Conformidade e auditorias – Equipe de conformidade independente

8. Planejamento para o futuro

- Expansão de protocolos e políticas de segurança
- Gestão integrada de e-mails na nuvem
- Funcionalidade OCR integrada
- Mensagens instantâneas integradas para colaboração segura vinculada a documentos ou projetos
- Desenvolvimento ativo de funções e recursos adicionais



CERTIFICAÇÕES DE SEGURANÇA E CONFORMIDADE NORMATIVA

A NetDocuments passa por auditorias anuais Tipo 2 SOC 2 de segurança e disponibilidade, além de auditorias anuais de certificação ISO 27001 que incluem os controles adicionais da ISO 27017, 27018 e 27701. A certificação ISO 27001 também inclui todos os centros de dados usados pela NetDocuments.

Além dessas auditorias anuais, a NetDocuments analisa ativamente os requisitos de segurança aplicáveis do setor, bem como os regulamentos de segurança locais, estaduais e nacionais para determinar os esforços de conformidade apropriados. Os exemplos incluem requisitos de segurança individuais de vários estados dentro dos EUA, o Regulamento Geral de Proteção de Dados (GDPR) adotado pela UE e os requisitos de segurança estabelecidos pelo Australian Signals Directorate.

A NetDocuments modifica e expande regularmente seus controles de segurança para manter os mais altos níveis de segurança para dados de clientes em todo o mundo, cumprindo com os padrões e regulamentos apropriados.

SEU PARCEIRO DE SEGURANÇA

A NetDocuments faz parceria com seus clientes para implementar e demonstrar os níveis de segurança exigidos. Isso inclui a revisão de requisitos de segurança exclusivos e o suporte a auditorias de conformidade de segurança do cliente.

A NetDocuments está comprometida em fornecer aos seus clientes o sistema de gestão de documentos mais funcional e seguro disponível. Você pode conhecer mais sobre as iniciativas de segurança e conformidade da NetDocuments visitando o site netdocuments.com ou entrando em contato com a Equipe de conformidade da NetDocuments pelo e-mail compliance@netdocuments.com.

