netdocuments®

CRIPTOGRAFIA DE DOCUMENTOS E POR QUE ISSO IMPORTA

A criptografia é crucial para o papel que ela desempenha na segurança, conformidade e prevenção de perdas.

Segurança

O armazenamento seguro de documentos comerciais tem uma alta prioridade. Como os arquivos são compartilhados digitalmente entre pessoas e dispositivos, há cada vez mais oportunidades para que os indivíduos mal-intencionados ataquem sistemas e roubem informações. A criptografia é uma **camada de proteção imprescindível** para manter seu conteúdo seguro, mesmo que outros controles de segurança sejam violados.

Governança e conformidade

A segurança da informação e a governança são requisitos operacionais fundamentais para as organizações. Moldadas por diretrizes em nível estadual, federal e internacional, as empresas precisam de ferramentas para armazenar, gerenciar e dispor de forma defensiva os documentos. A criptografia é uma **ferramenta chave** para o cumprimento desses padrões.

Prevenção de perdas

O custo das violações de dados vai muito além de uma simples melhoria em termos de segurança. As violações de dados corroem a confiança pública e podem ter um efeito incrivelmente prejudicial sobre a reputação de uma empresa, o que pode representar um risco para as relações e receitas atuais e futuras dos clientes. A criptografia **pode impedir** que um incidente de segurança se transforme em uma violação de dados.

netdocuments®

Como o NetDocuments lida com a criptografia de documentos

Manter seus arquivos seguros é nosso trabalho. Utilizando o modelo de computação "zero trust", o NetDocuments utiliza práticas de criptografia líderes no setor para proteger sua empresa contra violações de dados, além de fornecer infraestrutura de criptografia de última geração e gerenciamento de chaves. Você pode ter a confiança de que os documentos de sua empresa estão protegidos dentro do NetDocuments Service nos mais altos níveis disponíveis atualmente.

Criptografia multicamadas e Gerenciamento de Chaves de Criptografia (EKM)

O NetDocuments aplica múltiplas camadas de criptografia e utiliza tecnologia inovadora, incluindo um Gerador de Números Aleatórios Quânticos (QRNG), para criar uma chave de criptografia única para cada documento e e-mail salvo no Serviço. O QRNG usa mecânica quântica para gerar chaves de criptografia AES-256 totalmente entrópicas, em oposição à randomização baseada em software que pode ser decifrada por agentes estatais.

O NetDocuments Service realiza a criptografia e a decodificação em cada documento, em vez de utilizar métodos de segurança de baixo valor, tais como criptografia em nível de disco. Esse processo oculta todos os arquivos digitais dos administradores de armazenamento e rede, o que não é possível com a criptografia em nível de disco.

Cada documento salvo no NetDocuments é criptografado com sua própria Chave de Criptografia de Objetos (OEK) AES-256, única e totalmente entrópica. Após a criptografia, o documento é gravado na matriz de armazenamento de dados ("object store"), enquanto a OEK é armazenada separadamente em um banco de dados de chaves seguras.

Antes de serem armazenadas no banco de dados de chaves, as próprias OEKs são criptografadas usando uma Chave Mestra de Criptografia (MEK), que fornece uma camada adicional de segurança com criptografia. O NetDocuments protege e gerencia as MEKs em Módulos de Segurança de Hardware (HSMs) dedicados seguindo o FIPS (Federal Information Processing Standards, Padrões Federais de Processamento de Informações dos EUA) 140-2 Nível 3 com acesso restrito, usando a arquitetura Root of Trust para proteger totalmente a MEK. As MEKs são trocadas a cada seis meses. O FIPS é um padrão globalmente reconhecido para controles de segurança com criptografia. O nível 3 permite a separação física e lógica para maximizar a segurança da chave de criptografia.

A computação no modelo "zero trust" é obtida através do armazenamento de chaves de criptografia totalmente entrópicas em um HSM classificado no nível 3 do FIPS 140-2 e da utilização dos controles operacionais do NetDocuments Service.

Chaves de criptografia gerenciadas pelo cliente

Os clientes podem ter requisitos de segurança únicos e granulares. A criptografia pode ser usada para isolar diferentes conjuntos de conteúdo de outros documentos. Atendemos a essa necessidade oferecendo aos clientes a opção de utilizar Chaves de Criptografia Gerenciadas pelo Cliente (CMEKs), gerenciadas através de HSMs do NetDocuments ou HSMs gerenciados pelo cliente.

netdocuments®

Ao utilizar CMEKs, o NetDocuments Service aplica três camadas de criptografia separadas para cada documento. Os clientes controlam quando as CMEKs são aplicadas a documentos sensíveis que se enquadram nas políticas de regulamentação, de conformidade ou outras políticas de governança de dados exigidas.

Os clientes podem designar e revogar CMEKs para projetos ou grupos de documentos específicos, quando necessário. O gerenciamento de chaves de criptografia granular, baseado em metadados, permite às empresas revogar o acesso a conteúdos específicos enquanto outros conteúdos ainda estão acessíveis e protegidos por sua própria criptografia.

Criptografia em trânsito

O NetDocuments não protege apenas seus documentos enquanto eles estiverem armazenados na aplicação, o serviço também protege seus documentos enquanto eles estiverem sendo transmitidos para ou a partir do serviço, criptografando todas as transmissões do serviço pela Internet. O NetDocuments exige que todas as conexões ao serviço utilizem HTTPS e só permite a criptografia usando os protocolos de segurança TLS atuais (no momento TLS 1.2) para a segurança da transmissão de documentos.

Armazenamento resiliente de documentos

Um elemento chave da arquitetura de armazenamento do NetDocuments é o uso da tecnologia de armazenamento de objetos. Quando um arquivo é colocado no NetDocuments Service, ele é imediatamente criptografado e depois salvo em um depósito de objetos, onde acontece sua replicação automática ou seu "erasure coding" (dependendo do tamanho do arquivo) através de múltiplos data centers e múltiplos dispositivos de armazenamento físico dentro de cada data center. Essa dispersão pelos data centers geograficamente separados e altamente seguros garante total disponibilidade dos dados, integridade do conteúdo e os mais altos níveis de segurança.

Ao garantir que a criptografia seja utilizada em todo o NetDocuments Service, os documentos sensíveis tornam-se indecifráveis e inacessíveis a qualquer parte, incluindo o pessoal do NetDocuments.

A criptografia é um dos muitos elementos de um plano de segurança "zero trust" robusto

Embora a criptografia e o armazenamento de objetos sejam elementos essenciais de qualquer serviço seguro, eles representam apenas uma camada da governança de dados do NetDocuments Service. O NetDocuments fornece controles para gerenciar o acesso dos usuários a documentos e proteção contra perda de dados (DLP) para minimizar o risco de um vazamento de dados acidental ou malicioso.

Além disso, o NetDocuments mantém as certificações de segurança ISO 27001, 27017 e 27018 reconhecidas pelo setor, a nova certificação ISO 27701 para demonstrar a conformidade com a GDPR, e é periodicamente auditado para validar a conformidade com os controles SOC 2, para que você tenha o conforto e a garantia de saber que a infraestrutura de segurança do NetDocuments foi validada de forma independente por auditores credenciados, permitindo ainda que sua organização obtenha os benefícios da arquitetura de segurança abrangente do NetDocuments por meio da conformidade das transmissões.

Descubra como nossa criptografia líder do setor pode proteger ainda mais sua empresa.

Agende hoje uma demonstração do NetDocuments >