Segurança do Dropbox Business

Whitepaper sobre o Dropbox

Dropbox

Conteúdo

Visão geral

Com a transformação digital contínua em vários setores, é vital que os dados, as equipes e os dispositivos estejam protegidos onde quer que estejam. As organizações que confiam em soluções de nuvem, como o Dropbox Business, para permitir fluxos de trabalho remotos e distribuídos, precisam simplificar a colaboração, gerenciar riscos de nuvem proativamente e implementar controles efetivos que garantam a confidencialidade de sua propriedade intelectual, a integridade dos dados armazenados e compartilhados e a disponibilidade de dados por meio de um serviço de nuvem gerenciado e resiliente.

Mais de 600.000 empresas e organizações confiam no Dropbox Business como a solução para que equipes remotas e distribuídas colaborarem com segurança. A principal solução do Dropbox Business inclui o espaço de trabalho inteligente para colaboração e os recursos de sincronização e compartilhamento de arquivos. Nossas soluções são respaldadas pela infraestrutura líder do setor, bem como por recursos corporativos avançados de segurança, segurança de equipe e conteúdo, assinatura eletrônica, transferência segura e governança de dados. As informações deste whitepaper, exceto quando sinalizadas, se aplicam a todos os produtos do Dropbox Business (Standard, Advanced e Enterprise) e do Dropbox Education. O Paper é um recurso do Dropbox Business e do Dropbox Education.

O Programa de Confiança do Dropbox, nosso programa abrangente de segurança, está no centro do Dropbox Business e adota uma abordagem multicamada para a segurança, que é essencial na evolução das abordagens globais para o trabalho remoto.

Este whitepaper detalha os recursos de segurança de produtos do Dropbox Business, as medidas de segurança operacional do Dropbox, nosso compromisso de privacidade e transparência, bem como políticas de back-end, certificações independentes e medidas de conformidade normativa que fazem do Dropbox a solução segura para sua organização.

As informações deste whitepaper, exceto quando sinalizadas, se aplicam a todos os produtos do Dropbox Business (Standard, Advanced e Enterprise) e do Dropbox Education. O Paper é um recurso do Dropbox Business e do Dropbox Education.

Nos bastidores

Nossas interfaces fáceis de usar são respaldadas por uma infraestrutura que trabalha nos bastidores para garantir sincronização, compartilhamento e colaboração confiáveis e velozes. Para que isso aconteça, estamos constantemente aprimorando nosso produto e nossa arquitetura para agilizar a transferência de dados, melhorar a confiabilidade e para nos ajustarmos às mudanças no ambiente. Nesta seção, vamos explicar como os dados são transferidos, armazenados e processados com segurança.

Infraestrutura de arquivos

Os usuários do Dropbox podem acessar arquivos e pastas a qualquer momento a partir de computadores, navegadores da internet e dispositivos móveis, ou por aplicativos de terceiros conectados ao Dropbox. Todos esses clientes se conectam a servidores seguros para fornecer acesso a arquivos, permitir o compartilhamento de arquivos com outras pessoas e atualizar os dispositivos vinculados quando arquivos são adicionados, alterados ou excluídos.

A infraestrutura de arquivos do Dropbox é composta dos seguintes componentes:

- ***Servidores de metadados***

  Algumas informações básicas sobre dados de usuário, chamadas metadados, são mantidas em seu próprio serviço de armazenamento independente e funcionam como um índice para os dados das contas de usuários. Os metadados incluem informações básicas sobre a conta e o usuário, como endereço de e-mail, nome e nomes de dispositivos. E também incluem informações básicas sobre arquivos, inclusive nomes e tipos de arquivos, o que ajuda a viabilizar recursos como histórico de versões, recuperação e sincronização.

- ***Bancos de dados de metadados***

  Os metadados do arquivo são armazenados em um armazenamento de chave-valor transacional com controle de simultaneidade de várias versões e são fragmentados e replicados conforme necessário para atender aos requisitos de desempenho e alta disponibilidade.

- ***Servidores de blocos***

  Como padrão, o Dropbox foi desenvolvido para fornecer um mecanismo de segurança único, que vai além dos métodos tradicionais de criptografia ao proteger os dados do usuário. Os servidores em bloco processam os arquivos dos aplicativos do Dropbox, dividindo cada arquivo de blocos, criptografando cada bloco de arquivos usando cifras fortes e sincronizando apenas os blocos que foram modificados entre as revisões. Quando um aplicativo do Dropbox detecta um novo arquivo ou novas alterações em um arquivo existente, o aplicativo informa os servidores de blocos sobre a mudança, e os blocos de arquivos novos ou recém-modificados são processados e transferidos para os servidores de armazenamento em bloco. Além disso, usamos servidores de blocos para entregar arquivos e mostrar a visualização prévia para usuários. Para informações detalhadas sobre a criptografia utilizada por esses serviços, tanto em trânsito quanto em repouso, acesse a seção Criptografia abaixo.

- ***Servidores de armazenamento em bloco***

  O conteúdo real dos arquivos dos usuários é armazenado em blocos criptografados nos servidores de armazenamento em bloco.

  Antes da transmissão, o cliente do Dropbox separa os blocos de arquivos para prepará-los para o armazenamento. Os servidores de armazenamento em bloco funcionam como um sistema de Armazenamento de Conteúdo Endereçável (CAS), e cada bloco de arquivos criptografado individualmente é recuperado com base em seu valor de hash.

- ***servidores de visualizações prévias***

  Os servidores de visualizações prévias produzem visualizações prévias de arquivos. A visualização prévia é uma renderização de um arquivo de usuário em um formato diferente, mais adequado para apresentação rápida em um dispositivo de usuário final. Os servidores de visualizações prévias recuperam blocos de arquivos dos servidores de armazenamento em bloco para gerar as visualizações prévias. Quando uma visualização prévia é solicitada, os servidores de visualizações prévias recuperam

a visualização prévia no cache dos servidores de armazenamento de visualizações prévias anteriores e a transferem para os servidores de blocos. A visualização prévia é mostrada para o usuário pelos servidores de blocos.

- ***Servidores de armazenamento de visualizações prévias***

  As visualizações prévias no cache estão armazenadas em um formato criptografado nos servidores de armazenamento de visualizações prévias.

- ***Serviço de notificações***

  Esse serviço separado monitora se houve ou não alterações nas contas do Dropbox. Nenhum arquivo ou metadado é armazenado aqui ou transferido para cá. Cada cliente estabelece uma conexão Long Poll com o serviço de notificação e aguarda. Quando ocorre alguma alteração de qualquer arquivo no Dropbox, o serviço de notificação sinaliza uma mudança para os clientes relevantes, fechando a conexão Long Poll. O encerramento da conexão indica que o cliente deve se conectar aos Servidores de metadados de forma segura para sincronizar as alterações.

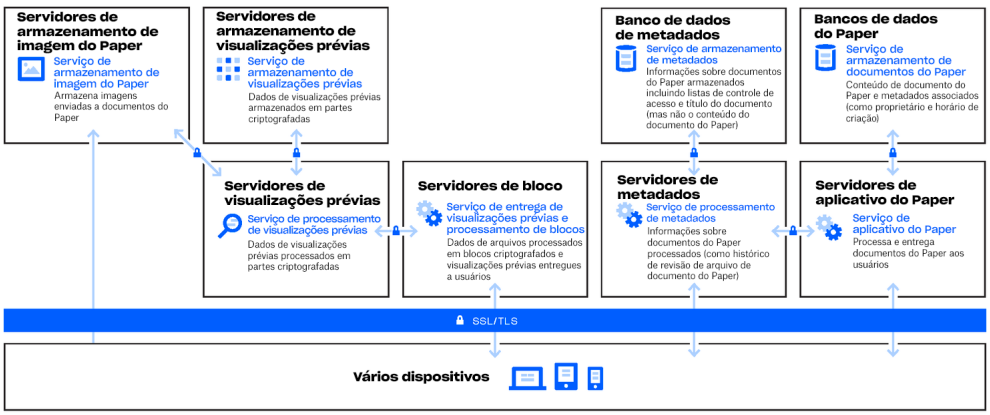
Armazenamento de dados de arquivos

O Dropbox armazena primariamente dois tipos de dados de arquivos: metadados dos arquivos (por exemplo, a data e o horário em que um arquivo foi modificado pela última vez) e o conteúdo real dos arquivos (blocos de arquivos). Os metadados de arquivos são armazenados nos servidores do Dropbox. Os blocos de arquivos são armazenados em um de dois sistemas: Amazon Web Services (AWS) ou Magic Pocket, o sistema de armazenamento interno do Dropbox. O Magic Pocket consiste em software e hardware patenteados e foram desenvolvidos desde sua concepção para oferecer confiança e segurança. Em ambos os sistemas, Magic Pocket e AWS, os blocos de arquivos são criptografados em repouso, e os dois sistemas atendem aos mais altos padrões de confiabilidade. Para mais detalhes, consulte a seção Confiabilidade abaixo.

Infraestrutura do Paper

Os usuários do Dropbox podem acessar documentos do Paper de clientes da web e de dispositivos móveis, ou por aplicativos de terceiros conectados ao aplicativo Dropbox Paper. Todos esses clientes se conectam a servidores seguros para fornecer acesso aos documentos do Paper, permitir o compartilhamento de documentos com outras pessoas e atualizar os dispositivos vinculados quando os documentos são adicionados, alterados ou excluídos.

A infraestrutura do Dropbox Paper é composta dos seguintes componentes:



- ***Servidores de aplicativo do Paper***

  Os servidores de aplicativo do Paper processam solicitações de usuários, renderizam a saída de documentos editados do Paper de volta ao usuário e operam serviços de notificação. Os servidores de aplicativo do Paper gravam edições de entrada do usuário nos bancos de dados do Paper, onde são colocados em armazenamento persistente. As sessões de comunicação entre os servidores de aplicativo do Paper e os bancos de dados do Paper são protegidas com o protocolo HTTPS (Secure Hypertext Transfer Protocol).

- ***Bancos de dados do Paper***

  O conteúdo real dos usuários de documentos do Paper, bem como determinados metadados sobre esses documentos, são criptografados em armazenamento persistente nos bancos de dados do Paper. Isso inclui informações sobre um documento do Paper (como título, proprietário, horário de criação e outras informações), bem como conteúdo dentro do próprio documento do Paper, incluindo comentários e tarefas. Os bancos de dados do Paper são fragmentados e replicados conforme necessário para atender aos requisitos de desempenho e alta disponibilidade.

- ***Servidores de metadados***

  O Paper usa os mesmos servidores de metadados descritos no diagrama de infraestrutura do Dropbox para processar informações sobre documentos do Paper, como histórico de revisão de arquivos de documentos do Paper e participação em pastas compartilhadas. O Dropbox gerencia diretamente os servidores de metadados, localizados em centros de processamento de dados de terceiros.

- ***Bancos de dados de metadados***

  O Paper usa os mesmos bancos de dados de metadados descritos no diagrama de infraestrutura do Dropbox para armazenar informações relacionadas a documentos do Paper, como compartilhamento, permissões e associações a pastas. Os metadados de documentos do Paper são armazenados em serviços de banco de dados MySQL e são fragmentados e replicados conforme necessário para atender aos requisitos de desempenho e alta disponibilidade.

- ***Servidores de armazenamento de imagens do Paper***

  As imagens transferidas para os documentos do Paper são armazenadas e criptografadas em repouso nos servidores de armazenamento de imagens do Paper. A transmissão de dados de imagem entre o aplicativo do Paper e os servidores de armazenamento de imagens do Paper ocorrem em uma sessão criptografada.

- ***Servidores de visualizações prévias***

  Os servidores de visualizações prévias produzem visualizações prévias tanto para as imagens enviadas para os documentos do Paper quanto para os hiperlinks incorporados aos documentos do Paper. Para as imagens transferidas para os documentos do Paper, os servidores de visualizações prévias buscam dados de imagem armazenados nos servidores de armazenamento de imagens do Paper, por meio de um canal criptografado. Para os hiperlinks incorporados aos documentos do Paper, os servidores de visualizações prévias recolhem dados de imagens e fazem a renderização, usando criptografia como especificado no link de origem. A visualização prévia é mostrada para o usuário, por fim, pelos servidores de blocos.

- ***Servidores de armazenamento de visualizações prévias***

  O Paper usa os mesmos servidores de armazenamento de visualizações prévias descritos no diagrama da infraestrutura do Dropbox para armazenar visualizações prévias do cache. Os blocos de visualizações prévias no cache estão armazenados em um formato criptografado nos servidores de armazenamento de visualizações prévias.

Armazenamento de documentos do Paper

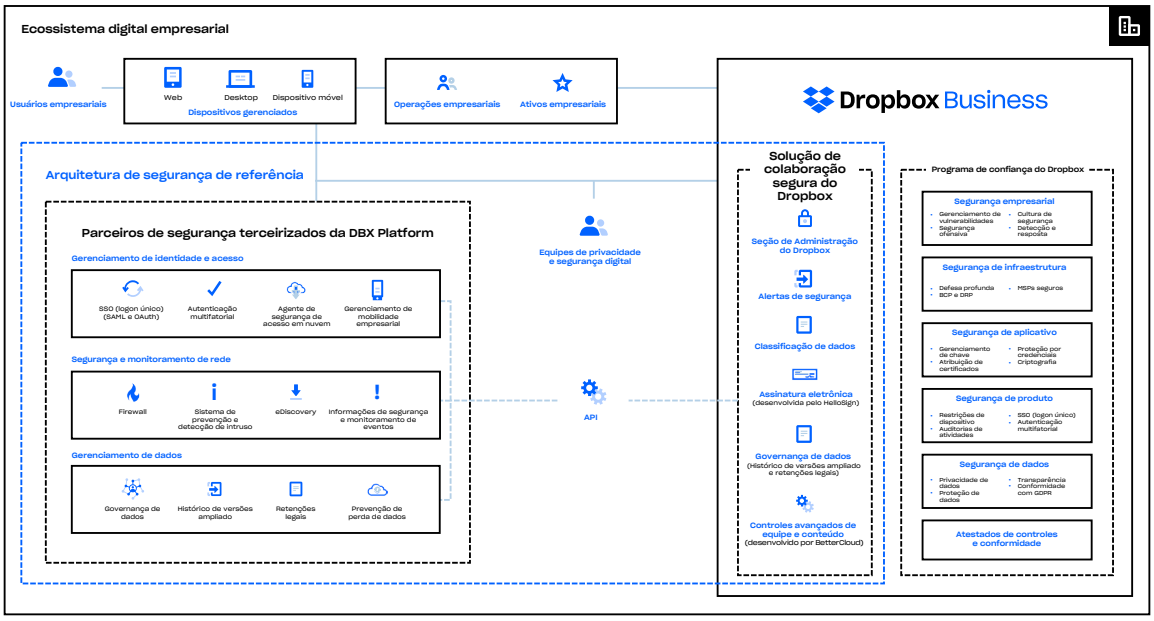
O Dropbox armazena primariamente os seguintes tipos de dados nos documentos do Paper: metadados dos documentos do Paper (por exemplo, as permissões compartilhadas do documento) e o conteúdo real dos documentos do Paper transferidos pelo usuário. Esses tipos são chamados coletivamente de dados de documentos do Paper, e as imagens transferidas para os documentos do Paper são chamadas de dados de imagens do Paper. Cada um desses tipos de dados é armazenado no Amazon Web Services (AWS). Os documentos do Paper são criptografados em repouso no AWS, que atende aos mais altos padrões de confiabilidade. Para mais detalhes, consulte a seção Confiabilidade abaixo.

Programa de confiança do Dropbox

A confiança é a base do nosso relacionamento com milhões de pessoas e empresas ao redor do mundo. Apreciamos a confiança que você deposita em nós e assumimos a responsabilidade de proteger suas informações com seriedade. Para merecermos sua confiança, criamos e continuaremos a expandir o Dropbox com ênfase em segurança, privacidade, transparência e conformidade.

O Programa de confiança do Dropbox estabelece um processo de avaliação de risco, que é designado para responder a riscos ambientais, físicos, de usuários, de terceiros, de leis e regulamentações aplicáveis, de requisitos contratuais e vários outros que possam afetar a segurança, confidencialidade, integridade, disponibilidade ou privacidade do sistema. Análises de desempenho ocorrem anualmente, no mínimo. Mais informações sobre o Programa de confiança do Dropbox estão disponíveis em dropbox.com/business/trust.

Seguimos uma abordagem multicamada para proteger a empresa, a infraestrutura, os aplicativos e os produtos que afetam sua organização.



Segurança de categoria empresarial

O Dropbox estabeleceu uma estrutura de gerenciamento de segurança da informação que descreve o propósito, a direção, os princípios e as regras básicas sobre como mantemos a confiança. Esse objetivo é alcançado por meio da avaliação de riscos e da constante melhoria da segurança, confidencialidade, integridade e disponibilidade dos sistemas do Dropbox Business. Revisamos e atualizamos regularmente as políticas de segurança, oferecemos treinamento em segurança, executamos testes de segurança em aplicativos e na rede (incluindo testes de penetração), monitoramos a conformidade com as políticas de segurança e realizamos avaliações de riscos internos e externos.

Nossas políticas

Estabelecemos um conjunto completo de políticas de segurança que são aplicadas pela equipe de segurança e abuso do Dropbox. Todas as políticas de segurança são revisadas e aprovadas pelo menos anualmente. Os funcionários, estagiários e prestadores de serviço participam do treinamento de segurança obrigatório quando entram para a empresa e passam por uma educação continuada de conscientização de segurança.

- ***Segurança da informação***

  Manter as informações do usuário e do Dropbox seguras.

- ***Autenticação***

  Descreve como os funcionários do Dropbox se autenticam para acessar sistemas de informação e dados.

- ***Segurança do dispositivo***

  Os requisitos mínimos de segurança para dispositivos móveis usados para acessar as informações da empresa.

- ***Controle de acesso lógico***

  Manter o acesso seguro aos sistemas, usuários e informações do Dropbox. Abrange o controle de acesso a ambientes corporativos e de produção.

- ***Segurança de dados***

  Descreve como o Dropbox protege os dados por meio de requisitos específicos de armazenamento, acesso e uso.

- ***Segurança em viagem***

  Descreve o que os funcionários do Dropbox devem fazer antes de viajar para o exterior.

- ***Diretrizes de segurança de vendas e experiência do cliente (CX)***

  Manter as informações do usuário seguras, proteger nossos funcionários e fornecer atendimento aos usuários.

- ***Segurança física***

  Manter um ambiente seguro para pessoas e propriedades no Dropbox.

- ***Diretrizes de segurança física de produção***

  Gerenciamento do acesso físico às instalações de produção.

- ***Resposta a incidentes***

  Descreve a forma como o Dropbox lida com segurança, privacidade e eventos do site relatados e documenta para cada incidente um plano de resposta.

- ***Materiais não autorizados com copyright***

  Proibir os funcionários de usarem o Dropbox ou os sistemas do Dropbox para armazenar ou compartilhar conteúdo não autorizado.

- ***Gerenciamento de alterações***

  Gerenciamento de alterações nos sistemas de produção. Destinado a todos os funcionários do Dropbox, prestadores de serviço e estagiários com acesso a sistemas.

- ***Privacidade de dados do usuário***

  Proteger e lidar com informações de usuários e dados de usuários no Dropbox em conformidade com nossa Política de Privacidade.

- ***Política de continuidade de negócios e gerenciamento de emergência***

  Descreve a preservação, a proteção e a segurança das pessoas (funcionários do Dropbox), a propriedade e os processos (empresariais).

- ***Programa de privacidade do Dropbox***

  O propósito, os princípios e a responsabilidade do Programa de Privacidade do Dropbox.

- ***Programa de confiança do Dropbox***

  Descreve como o Dropbox funciona e é digno de confiança.

- ***Segurança do ambiente de pagamentos***

  Proteger e manter o ambiente de pagamento exclusivo usado no Dropbox para aceitar pagamentos com cartão de crédito.

Políticas e acesso dos funcionários

Na contratação, cada funcionário do Dropbox deve passar por uma verificação de antecedentes, assinar um termo de reconhecimento da política de segurança e do contrato de confidencialidade e receber treinamento de segurança. O acesso físico e lógico aos ambientes corporativo e de produção é concedido apenas a indivíduos que concluírem esses procedimentos, conforme necessário para a condução de suas responsabilidades profissionais. Além disso, todos os funcionários participam de treinamentos de segurança anuais e recebem treinamento regular de conscientização de segurança via e-mails informativos, palestras/apresentações e recursos disponíveis em nossa intranet.

O acesso de funcionários ao ambiente do Dropbox é mantido por um diretório central e autenticado usando uma combinação de senhas fortes, chaves SSH protegidas por frase-senha e autenticação em dois passos. O acesso remoto exige o uso de redes virtuais privadas protegidas com autenticação em dois passos, e qualquer acesso especial é revisado e cuidadosamente examinado pela equipe de segurança. O acesso entre redes corporativas e de produção é estritamente limitado com base nas políticas definidas. Por exemplo, o acesso à rede de produção é baseado em chave SSH e restrito às equipes de engenharia que precisam do acesso como parte de suas funções. A configuração de firewall é controlada fortemente e limitada a um pequeno número de administradores.

Além disso, nossas políticas internas exigem a adesão dos funcionários que acessam ambientes corporativos e de produção às melhores práticas para criação e armazenamento de chaves privadas SSH. O acesso a outros recursos, incluindo centros de processamento de dados, utilitários de configuração do servidor, servidores de produção e utilitários de desenvolvimento de código fonte é garantido por meio de aprovação explícita pelo respectivo gerente. A gerência manterá o registro da solicitação de acesso, da justificativa e da aprovação, e o acesso será concedido pelas pessoas competentes.

O Dropbox emprega controles técnicos de acesso e políticas internas para proibir os funcionários de acessar arbitrariamente arquivos de usuários e restringir o acesso a metadados e outras informações relacionadas a contas de usuários. A fim de proteger a privacidade e a segurança do usuário final, apenas um pequeno número de engenheiros responsáveis pelo desenvolvimento dos serviços centrais do Dropbox tem acesso ao ambiente onde os arquivos dos usuários são armazenados. Quando um funcionário deixa a empresa, todos os seus acessos são imediatamente removidos.

À medida que o Dropbox se torna uma extensão da infraestrutura de nossos clientes, eles podem ficar tranquilos de que somos guardiões responsáveis de seus dados. Veja a seção Privacidade neste documento para mais detalhes.

Gerenciamento de vulnerabilidades

Nossa equipe de segurança realiza testes regulares de segurança automatizados e manuais e gerenciamento de correções e trabalha com especialistas de terceiros para identificar e corrigir possíveis vulnerabilidades e bugs de segurança.

Como componente necessário de nosso sistema de gerenciamento de segurança de informação, as conclusões e recomendações que resultam dessas avaliações são comunicadas à gerência do Dropbox, avaliadas e as ações apropriadas são realizadas conforme a necessidade. Problemas com alta gravidade são documentados, rastreados e resolvidos por engenheiros de segurança designados.

Gerenciamento de alterações

Todos os processos de desenvolvimento, resolução de problemas e de correção seguem nossa Política formal de gerenciamento de alterações definida pela equipe de engenharia do Dropbox para garantir que as alterações do sistema sejam testadas e autorizadas antes da implementação nos ambientes de produção. Alterações no código fonte são iniciadas por desenvolvedores que queiram fazer melhorias no aplicativo ou serviço do Dropbox. Todas as alterações são armazenadas em um sistema de controle de versão e são obrigadas a passar por procedimentos automatizados de versão de testes de Garantia de Qualidade (QA) para verificar se os requisitos de segurança estão sendo cumpridos. O sucesso nos procedimentos de controle de qualidade leva à implementação da alteração. Todas as alterações aprovadas pelo controle de qualidade são automaticamente implementadas no ambiente de produção. Nosso ciclo de desenvolvimento de software (SDLC) exige a adesão a diretrizes de codificação seguras, assim como à condução de uma triagem de alterações de códigos para verificação de potenciais problemas de segurança através de controle de qualidade e de nossos processos manuais de análise. Todas as alterações liberadas para o estágio de produção são registradas e arquivadas, e são enviados alertas automaticamente para a gerência da equipe de engenharia do Dropbox.

Alterações na infraestrutura do Dropbox são restritas somente às equipes autorizadas. A equipe de Segurança do Dropbox é responsável por manter a segurança da infraestrutura e garantir que o servidor, o firewall e outras configurações relacionadas à segurança estejam atualizadas em relação ao padrão do setor. Os conjuntos de regras de firewall e as pessoas com acesso a servidores de produção são revistos regularmente.

Varredura e teste de penetração de segurança (interna e externa)

Nossa equipe de segurança faz regularmente testes manuais e automáticos nos aplicativos para identificar e corrigir vulnerabilidades de segurança e falhas em nossos aplicativos para desktop, para a web (Dropbox e Paper) e para dispositivos móveis (Dropbox e Paper).

Além disso, o Dropbox contrata fornecedores independentes para realizar testes periódicos de penetração e vulnerabilidade nos ambientes de produção. Trabalhamos com especialistas de segurança independentes, com outras equipes de segurança do setor e com a comunidade de pesquisa em segurança para manter nossos aplicativos seguros. Também aproveitamos sistemas de análise automática para identificar vulnerabilidades. Esse processo inclui sistemas que desenvolvemos internamente, sistemas de código aberto que modificamos para nossas necessidades, bem como fornecedores externos que contratamos para análise automatizada contínua.

Manter conteúdo nocivo fora do Dropbox

Temos recursos de varredura que visam impedir o armazenamento e a distribuição de conteúdo nocivo no Dropbox. Nossos scanners aproveitam a crescente tecnologia doméstica, bem como recursos de ponta de parceiros como a Microsoft e o Google, para tornar o Dropbox um lugar seguro para nossos clientes.

Recompensas por identificação de bugs

Embora trabalhemos com empresas profissionais para realizar testes de invasão e conduzimos nossos próprios testes internos, as recompensas de bugs (ou programas de recompensas de vulnerabilidades) utilizam os conhecimentos da comunidade de segurança mais geral. Nosso programa de recompensas de bugs oferece um incentivo para que os pesquisadores identifiquem e divulguem de forma responsável os bugs de software. Esse envolvimento da comunidade externa oferece à nossa equipe de segurança uma verificação independente dos nossos aplicativos, colaborando para manter nossos usuários seguros. Nós nos esforçamos para estar entre os líderes do setor em recompensas por identificação de bugs, bem como em tempos de resposta e resolução.

Estabelecemos um escopo para comunicações e aplicativos do Dropbox elegíveis, assim como uma política de divulgação responsável que promove a descoberta e o relato de vulnerabilidades de sistema e o aumento da segurança do usuário. Essa política estabelece as seguintes diretrizes:

- Compartilhe conosco problemas de segurança em detalhes.
- Seja respeitoso com nossos aplicativos existentes. Formulários de spam por meio de scanners de vulnerabilidade automatizados não resultarão em nenhum prêmio ou recompensa, já que eles estão explicitamente fora do escopo.
- Dê à nossa equipe um tempo razoável para analisar a questão antes de divulgar publicamente qualquer informação a respeito do problema de segurança.
- Não acesse nem modifique dados de usuários sem permissão do proprietário da conta.
- Não visualize, altere, salve, armazene, transfira ou acesse os dados e limpe imediatamente qualquer informação local ao denunciar a vulnerabilidade ao Dropbox.
- Aja de boa-fé para evitar violações de privacidade, destruição de dados e interrupção ou degradação de nossos serviços (incluindo negação de serviço).

Problemas podem ser relatados enviando um relatório para o Bugcrowd em: bugcrowd.com/dropbox.

Segurança física

Infraestrutura

O acesso físico a instalações de empresas subcontratadas que abrigam os sistemas de produção é restrito a funcionários autorizados pelo Dropbox, conforme necessário para o exercício de suas funções. Quaisquer indivíduos que necessitem de acesso adicional às instalações do ambiente de produção recebem acesso através da aprovação explícita do respectivo gerente.

A gerência mantém o registro da solicitação de acesso com a justificativa e a aprovação, e o acesso é concedido por pessoas autorizadas. Após a aprovação ser recebida, um membro autorizado da equipe de infraestrutura entrará em contato com a empresa subcontratada envolvida para solicitar o acesso para o indivíduo aprovado. A empresa subcontratada insere as informações do usuário em seu próprio sistema e concede ao aprovado pelo Dropbox o crachá pessoal para acesso e, se possível, acesso por biometria. Uma vez que o acesso seja concedido a indivíduos aprovados, é de responsabilidade do centro de processamento de dados garantir que o acesso seja restrito apenas àqueles indivíduos autorizados.

Escritórios corporativos

- ***Segurança física***

  A equipe de segurança física do Dropbox é responsável por promover políticas de segurança física e de supervisionar a segurança de nossos escritórios.

- ***Política de acesso e de visitantes***

  O acesso físico às instalações da empresa, além das entradas públicas e dos saguões, é restrito aos funcionários autorizados pelo Dropbox e a visitantes registrados que estejam acompanhados por alguém da equipe do Dropbox. Um sistema de acesso por crachá garante que apenas funcionários autorizados tenham acesso às instalações.

- ***Acesso ao servidor***

  O acesso a áreas contendo servidores corporativos e equipamentos de rede é restrito ao pessoal autorizado. O controle é feito por meio dos diferentes níveis de um sistema de acesso baseado em crachás. As listas de pessoas autorizadas a ter acesso físico a ambientes corporativos e de produção serão revistas no mínimo a cada três meses.

Resposta a incidentes

Temos políticas de respostas a incidentes e procedimentos para lidar com questões de disponibilidade, integridade, segurança, privacidade e confidencialidade do serviço. Como parte de nossos procedimentos de resposta a incidentes, temos equipes exclusivas, treinadas para:

- Responder a alertas de potenciais incidentes de forma imediata.
- Determinar a gravidade do incidente.
- Se for necessário, tomar medidas de mitigação e contenção.

- Comunique-se com as partes interessadas relevantes, internas e externas, incluindo a notificação a clientes afetados, para cumprir obrigações contratuais relativas a violações e à notificação de incidentes, além das leis e dos regulamentos relevantes.
- Reunir e conservar provas para auxiliar nos esforços investigativos.
- Documentar um post-mortem e desenvolver um plano de triagem permanente.

As políticas e os processos de resposta a incidentes passam por auditoria, como parte do nosso SOC 2, ISO/IEC 27001 e outras avaliações de segurança.

Segurança da infraestrutura

Segurança de rede

O Dropbox mantém atentamente a segurança da nossa rede back-end. Nossas técnicas de segurança de rede e monitoramento têm o objetivo de oferecer várias camadas de proteção e defesa. Empregamos técnicas de proteção padrão do setor, incluindo firewalls, varredura de vulnerabilidade de rede, monitoramento de segurança de rede e sistemas de detecção de intrusos, para garantir que apenas o tráfego admissível e não malicioso possa acessar nossa infraestrutura.

Nossa rede privada interna é segmentada de acordo com o nível de uso e risco. As redes principais são:

- DMZ exposta à internet
- DMZ com infraestrutura prioritária
- Rede de produção
- Rede cooperativa

O acesso ao ambiente de produção é restrito apenas a endereços IP autorizados e exige múltiplas autenticações em todos os pontos de extremidade. Os endereços IP com acesso são associados à rede corporativa ou ao pessoal autorizado do Dropbox. Endereços IP autorizados são revisados trimestralmente para garantir um ambiente de produção seguro. O acesso para modificar a lista de IP é restrito a indivíduos autorizados.

O tráfego da internet destinado à nossa rede de produção é protegido por meio de diversas camadas de firewalls e proxies.

Mantemos um limite rígido entre a rede interna do Dropbox e a internet pública. O tráfego de entrada e saída entre a internet e a rede de produção é cuidadosamente controlado através de um serviço de proxy exclusivo, protegido por regras rígidas de firewall.

O Dropbox utiliza sofisticados conjuntos de ferramentas para monitorar laptops e desktops com sistemas operacionais Mac e Windows e sistemas de produção, com o objetivo de detectar eventos mal-intencionados. Todos os registros de segurança são coletados em um local centralizado para fins forenses e de resposta a incidentes em conformidade com políticas de retenção padrão do setor.

O Dropbox identifica e reduz os riscos através de testes e auditorias regulares na rede, que são realizados tanto pelas equipes exclusivas internas de segurança quanto por especialistas em segurança independentes.

Pontos de presença (PoPs)

Para otimizar o desempenho do site para os usuários, o Dropbox aproveita redes de entrega de conteúdo independentes (CDNs) e pontos de presença (PoPs) hospedados pelo Dropbox em 31 locais diferentes no mundo. Nenhum dado de usuário é armazenado em cache nesses locais, e todos os dados transferidos são criptografados com SSL/TLS. O acesso físico e lógico aos PoPs hospedados pelo Dropbox é restrito somente à equipe autorizada do Dropbox. O Dropbox executa otimizações tanto na camada de transporte (TCP) quanto na camada de aplicação (HTTP).

Peering

O Dropbox tem uma política de peering aberto, e todos os clientes são bem-vindos para fazer peer conosco. Para mais detalhes, consulte dropbox.com/peering.

Confiabilidade

Um sistema de armazenamento só é bom quando podemos confiar nele. Para tanto, desenvolvemos o Dropbox com múltiplas camadas de redundância para proteção contra perda de dados e garantia de disponibilidade.

Metadados de arquivos

Cópias redundantes de metadados são distribuídas por dispositivos independentes dentro de um centro de processamento de dados em pelo menos um modelo de disponibilidade N+2. Backups incrementais são executados de hora em hora, e backups completos são feitos a cada 36 horas. Os metadados são armazenados em servidores hospedados no Dropbox e gerenciados por ele nos EUA.

Blocos de arquivos

Cópias redundantes de blocos de arquivos são armazenadas independentemente em pelo menos duas regiões geográficas separadas e replicadas de maneira confiável em cada região. (**Observação:** Para clientes que escolherem armazenar seus dados em infraestrutura alemã, australiana, japonesa ou do Reino Unido, os blocos de arquivos serão replicados somente dentro das regiões respectivas. Para mais informações, consulte os Centros de processamento de dados e provedores de serviço gerenciados abaixo.) Ambos os sistemas, Magic Pocket e AWS, foram projetados para fornecer durabilidade anual de dados de pelo menos 99,999999999%.

Os mecanismos de arquitetura, aplicativos e sincronização do Dropbox trabalham em conjunto para proteger os dados do usuário e torná-los altamente disponíveis. No raro caso de uma indisponibilidade de serviço, os usuários do Dropbox ainda têm acesso às cópias sincronizadas mais recentes de seus arquivos na pasta local do Dropbox nos computadores vinculados. As cópias de arquivos sincronizados na pasta do cliente do Dropbox para desktop/local estarão acessíveis na unidade de disco rígido do usuário durante quedas ou interrupções do serviço, ou quando você estiver off-line. As alterações em arquivos e pastas são sincronizadas com o Dropbox assim que o serviço ou conectividade é restabelecido.

Documentos do Paper

Cópias redundantes de dados de documentos do Paper são distribuídas por dispositivos independentes dentro de um centro de processamento de dados em um modelo de disponibilidade N+1. Backups completos dos dados de documentos do Paper também são realizados diariamente. Para o armazenamento de documentos do Paper, o Dropbox usa infraestrutura AWS nos EUA, desenvolvida para fornecer uma durabilidade anual de dados de pelo menos 99,999999999%. No caso raro de uma indisponibilidade de serviço, os usuários ainda têm acesso às cópias sincronizadas mais recentes de seus documentos do Paper no modo "off-line" no aplicativo do dispositivo móvel.

Sincronização de arquivos

O Dropbox oferece a melhor sincronização de arquivos da categoria. Nossos mecanismos de sincronização asseguram transferências de arquivos rápidas e responsivas, habilitando o acesso aos dados em todos os dispositivos, em qualquer lugar. A sincronização do Dropbox também é resiliente. Em caso de falha na conexão com o serviço do Dropbox, o cliente simplesmente retomará a operação quando uma conexão for restabelecida. Os arquivos somente serão atualizados no cliente local se tiverem sido completamente sincronizados e validados com sucesso junto ao serviço Dropbox. O balanceamento de carga entre vários servidores garante redundância e uma experiência de sincronização contínua para o usuário final.

Delta sync

Usando esse método de sincronização, apenas as partes alteradas dos arquivos são baixadas/transferidas. O Dropbox armazena cada arquivo em blocos independentes e criptografados, atualizando apenas os blocos que foram alterados.

Streaming sync

Em vez de esperar pela conclusão da transferência de um arquivo, a streaming sync começará a baixar os blocos sincronizados em um segundo dispositivo antes da conclusão da transferência de todos os blocos do primeiro dispositivo. Esse é um processo automático, usado quando computadores separados estão vinculados à mesma conta do Dropbox ou quando contas diferentes do Dropbox compartilham uma pasta.

Economizar espaço em disco rígido

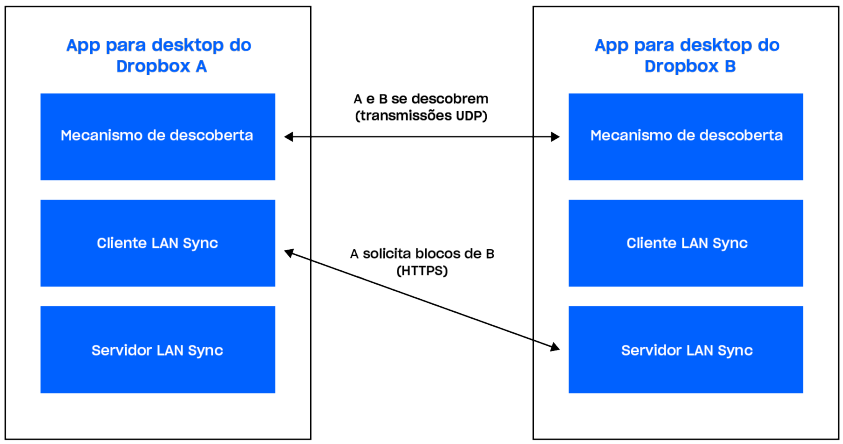
Os usuários podem liberar espaço de armazenamento no computador disponibilizando off-line somente os arquivos que desejam no disco rígido. Isso libera espaço no computador, mantendo tudo somente on-line no dropbox.com.

LAN sync

Quando habilitado, esse recurso baixa arquivos atualizados e novos de outros computadores na mesma rede local (LAN), economizando tempo e largura de banda comparado ao processo de baixar os arquivos de servidores do Dropbox.

Arquitetura

O aplicativo para desktop executa três componentes principais do sistema LAN sync: o mecanismo de descoberta, servidor e cliente. O mecanismo de descoberta encontra dispositivos na rede para sincronizar. Isso é limitado a dispositivos que têm acesso autorizado às mesmas pastas pessoais e compartilhadas do Dropbox. O servidor lida com solicitações de outros dispositivos na rede, servindo os blocos de arquivos solicitados. O cliente solicita os blocos de arquivos pela rede.



Mecanismo de descoberta

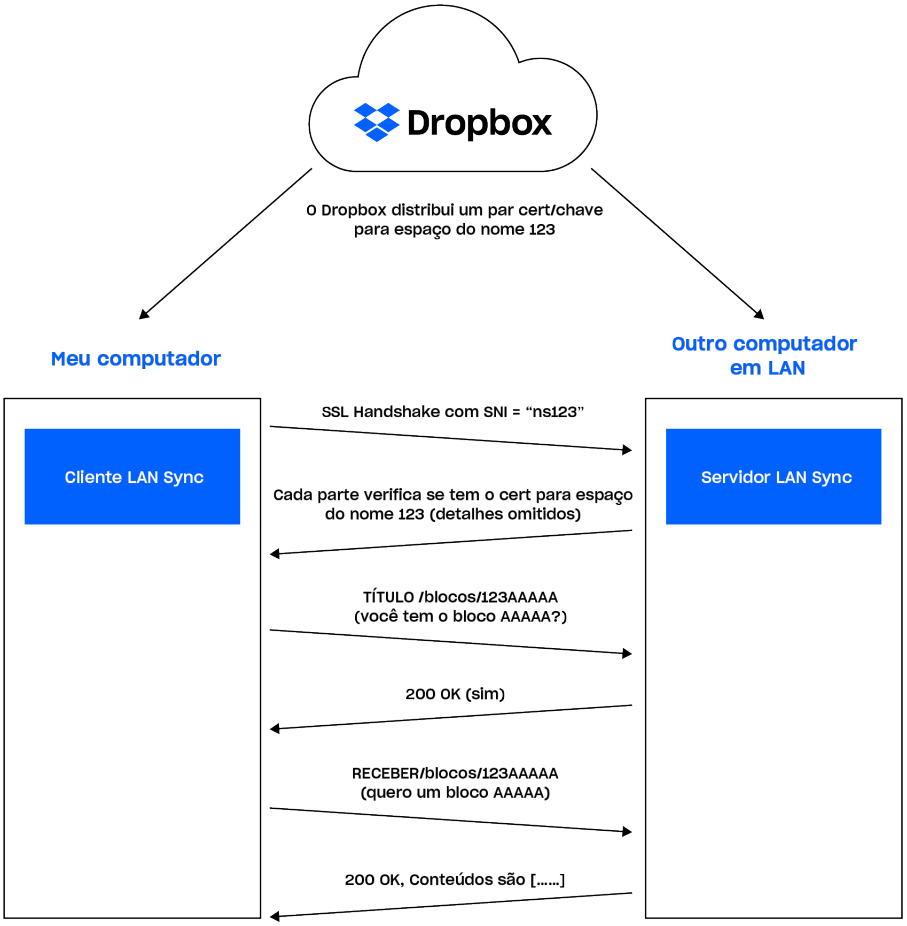
Cada dispositivo na LAN envia os pacotes de transmissão UDP e fica atento a eles em relação à porta 17500 (reservada por IANA a LAN sync). Esses pacotes contêm a versão do protocolo usada por determinado computador: as pastas pessoais e compartilhadas do Dropbox, a porta TCP usada para executar o servidor (que pode ser diferente da porta 17500, se ela estiver indisponível) e um identificador aleatório para o dispositivo. Quando um pacote é visto, o endereço IP do dispositivo é adicionado à lista de cada pasta pessoal ou compartilhada, indicando um potencial destino.

Protocolo

A transferência de bloco de arquivos real é realizada por meio de HTTPS. Cada computador executa um servidor HTTPS com pontos de extremidade. Um cliente poderá verificar muitos peers para ver se eles contêm blocos, mas apenas baixá-los de um servidor.

Para manter todos os dados seguros, nos certificamos de que apenas clientes autenticados para determinada pasta possam solicitar blocos de arquivos. Também nos certificamos de que computadores não possam fingir ser servidores de pastas das quais não têm controle. Para solucionar isso, geramos pares de chave/certificado SSL para cada conta pessoal do Dropbox ou pasta compartilhada. Elas são distribuídas dos servidores do Dropbox aos computadores dos usuários que estão autenticados para a pasta. Os pares de chave/certificado serão rotacionados sempre que houver uma alteração na participação de alguém, por exemplo, quando uma pessoa é removida de uma pasta compartilhada. Exigimos que ambas as extremidades da conexão HTTPS sejam autenticadas com o mesmo certificado (o certificado para o Dropbox ou para a pasta compartilhada). Isso prova que ambas as extremidades da conexão estão autenticadas.

Ao estabelecer uma conexão, informamos ao servidor a qual conta pessoal do Dropbox ou pasta estamos tentando nos conectar, usando a Indicação de Nome do Servidor (SNI), para que o servidor use o certificado correto.



Servidor/cliente

Com o protocolo descrito anteriormente, o servidor precisa saber apenas quais blocos estão presentes e onde encontrá-los.

Com base nos resultados do mecanismo de descoberta, o cliente mantém uma lista de peers para cada pasta de conta pessoal do Dropbox e compartilhada. Quando um sistema LAN sync obtém uma solicitação para baixar um bloco de arquivos, ele envia uma solicitação para uma amostra aleatória de peers que foi descoberta pela pasta da conta pessoal do Dropbox ou compartilhada, e em seguida solicita o bloco da primeira pasta que o contiver.

Para evitar latências, usamos pools de conexão a fim de permitir reutilizar conexões já iniciadas. Não abrimos uma conexão até que seja necessário e, uma vez aberta, ela é mantida viva, caso precisemos dela novamente. Além disso, limitamos o número de conexões a um único peer.

Se um bloco de arquivos não for encontrado ou baixado com sucesso, ou se a conexão parecer muito lenta, o sistema voltará a obter o bloco por meio dos servidores do Dropbox.

Centros de processamento de dados e provedores de serviços gerenciados

Os sistemas corporativos e de produção do Dropbox estão alojados em centros de processamento de dados de empresas independentes e provedores de serviço gerenciado localizados nos Estados Unidos. Os relatórios SOC e/ou os questionários de segurança do fornecedor e as obrigações contratuais dos centros de processamento de dados contratados são revisados ao menos uma vez por ano para controle eficiente da segurança. Esses provedores de serviços independentes são responsáveis pelos controles de segurança física, ambiental e operacional nas fronteiras da infraestrutura do Dropbox. O Dropbox é responsável pela segurança lógica, de rede e do aplicativo de nossa infraestrutura alojada em centros de processamento de dados de terceiros.

Nosso provedor de serviço gerenciado para processamento e armazenamento de conteúdos de arquivo, o Amazon Web Services (AWS), é responsável pela segurança lógica e de rede dos serviços do Dropbox fornecidos através de sua infraestrutura. As conexões são protegidas pelo firewall do provedor de serviço gerenciado, configurado com o padrão "negar tudo". O Dropbox restringe o acesso ao ambiente para um número limitado de endereços IP e funcionários.

Infraestrutura na Alemanha, Austrália, Japão e Reino Unido

O Dropbox oferece armazenamento em blocos de arquivos em regiões fora dos Estados Unidos para clientes qualificados. Nossa infraestrutura é hospedada pelo Amazon Web Services na Alemanha, Austrália, Japão e Reino Unido e replicada dentro da região respectiva para garantir a redundância e proteger contra a perda de dados. Os metadados de arquivos são armazenados nos Estados Unidos nos servidores próprios do Dropbox. Os documentos e visualizações prévias de todos os clientes do Paper são armazenados nos Estados Unidos, no momento.

Continuidade de negócios

O Dropbox criou um sistema de gerenciamento de continuidade de negócios (BCMS) para abordar a forma de retomar ou continuar a prestar serviços aos usuários, bem como de funcionar como uma empresa, caso os processos e as atividades críticas de negócios sejam interrompidos. Conduzimos um processo cíclico que consiste nas seguintes fases:

- ***Avaliações de impacto e riscos de negócios***

  Conduzimos uma avaliação de impacto de negócios (BIA) pelo menos uma vez por ano, para identificar processos críticos ao Dropbox, avaliar o impacto potencial de transtornos, definir prazos prioritários para recuperação e identificar nossos vínculos e fornecedores críticos. Além disso, conduzimos uma avaliação de risco em toda a empresa pelo menos uma vez por ano. Ela ajuda a identificar, analisar e avaliar sistematicamente o risco de incidentes disruptivos para o Dropbox. Juntas, a avaliação de risco e a BIA informam sobre prioridades de continuidade e estratégias de mitigação e recuperação para os planos de continuidade de negócios (BCPs).

- ***Plano de continuidade de negócios***

  Equipes identificadas pela BIA como críticas para a continuidade do Dropbox usam essas informações para desenvolver BCPs para seus processos críticos. Esses planos ajudam as equipes a saber quem é responsável por retomar os processos se houver uma emergência, quem em outro escritório ou local do Dropbox pode assumir os processos delas durante um transtorno e quais métodos de comunicação devem ser usados ao longo de um evento de continuidade. Eles também nos ajudam a nos prepararmos para um incidente disruptivo, centralizando nossos planos de recuperação e outras informações importantes, como quando e de que forma o plano deve ser usado, informações sobre contatos e reuniões, aplicativos importantes e estratégias de recuperação. Os planos de continuidade do Dropbox estão ligados ao plano de gestão de crises de toda a empresa (CMP), que estabelece o gerenciamento de crises do Dropbox e equipes de resposta a incidentes.

- ***Teste/exercício de plano***

  O Dropbox testa elementos selecionados de seus planos de continuidade de negócios pelo menos uma vez por ano. Esses testes, em conformidade com o escopo e os objetivos BCMS, têm como base cenários apropriados e são concebidos com objetivos definidos de forma clara. Eles podem variar quanto ao escopo, desde exercícios de decisão a simulações completas em escala real de incidentes verdadeiros. Com base nos resultados do teste, assim como na experiência de incidentes reais, as equipes atualizam e melhoram seus planos para resolver problemas e fortalecer a capacidade de resposta.

- ***Revisão e aprovação de BCMS***

  Pelo menos uma vez por ano, nossa equipe de executivos revisa o BCMS, já que isso faz parte da revisão do Programa de Confiança do Dropbox.

Recuperação de desastres

Para atender aos requisitos de segurança da informação durante uma grande crise ou catástrofe que possa impactar as operações do Dropbox Business, mantemos um plano de recuperação de desastres. A equipe de engenharia do Dropbox revisa esse plano anualmente e testa determinados elementos pelo menos uma vez por ano. Pontos relevantes são documentados e monitorados até a resolução.

Nosso Plano de recuperação de desastres (Disaster Recovery Plan, DRP) lida com desastres de disponibilidade e durabilidade, definidos nos seguintes termos:

- Um desastre de durabilidade consiste nas seguintes situações:
  - Uma perda completa ou permanente do centro de processamento de dados primário que armazena os metadados, ou de vários centros de processamento de dados que armazenam blocos de arquivos.
  - Perda da capacidade de comunicar ou fornecer dados de um centro de processamento de dados que armazena metadados, ou de vários centros de processamento de dados que armazenam conteúdo de arquivos.

- Um desastre de disponibilidade consiste nas seguintes situações:
  - Uma interrupção maior que dez dias.
  - Perda da capacidade de comunicar ou fornecer dados de um serviço de armazenamento/centro de processamento de dados que armazena metadados, ou de vários serviços de armazenamento/centros de processamento de dados que armazenam blocos de arquivos.

Definimos um Objetivo de Tempo de Recuperação (Recovery Time Objective, RTO), que é o período de tempo e um nível de serviço no qual o processo ou serviço comercial deve ser restaurado depois de um desastre e um Objetivo de ponto de recuperação (Recovery Point Objective, RPO), que é o período máximo tolerável no qual os dados podem ser perdidos na ocorrência de uma interrupção de serviço. Também medimos o Tempo Real de Recuperação (Recovery Time Actual, RTA) durante os testes de Recuperação de Desastres, executados anualmente, no mínimo.

A resposta a incidentes, a continuidade de negócios e os planos de recuperação de desastres do Dropbox são testados em intervalos planejados e no caso de alterações organizacionais ou ambientais significativas.

Segurança de aplicativos

Interfaces de usuário do Dropbox

Os serviços do Dropbox podem ser utilizados e acessados por meio de diversas interfaces. Cada uma tem configurações e recursos de segurança que processam e protegem dados de usuários, ao mesmo tempo que permitem a facilidade de acesso.

- ***Web***

  Essa interface pode ser acessada através de qualquer navegador web. Ela permite aos usuários enviar, baixar, visualizar e compartilhar seus arquivos. A interface web também habilita os usuários a abrir versões locais de arquivos já existentes, usando o aplicativo padrão do computador.

- ***Desktop***

  O aplicativo do Dropbox para desktop é um poderoso cliente de sincronização que armazena os arquivos localmente para acesso off-line. Ele oferece acesso completo às contas do Dropbox e pode ser executado nos sistemas operacionais Windows e Mac. Os arquivos são visualizados e podem ser compartilhados diretamente dentro dos navegadores de arquivos do sistema operacional.

- ***Dispositivos móveis***

  O aplicativo do Dropbox está disponível para dispositivos iOS e Android, permitindo aos usuários acessar todos os seus arquivos onde quer que estejam. O aplicativo móvel também permite aos usuários disponibilizar arquivos para uso off-line.

- ***API***

  As APIs do Dropbox oferecem uma forma flexível de ler e gravar dados nas contas de usuários do Dropbox, assim como acesso a funcionalidades avançadas como busca, revisão e restauração de arquivos. As APIs podem ser usadas para gerenciar o ciclo de vida do usuário de uma conta do Dropbox Business, executar ações para todos os membros de uma equipe e habilitar o acesso à funcionalidade de administrador do Dropbox Business.

Interfaces de usuário do Paper

Os serviços do Paper podem ser utilizados e acessados por meio de diversas interfaces. Cada uma tem configurações e recursos de segurança que processam e protegem dados de usuários, ao mesmo tempo que permitem a facilidade de acesso.

- ***Web***

  Essa interface pode ser acessada através de qualquer navegador moderno. Ela permite aos usuários criar, visualizar, baixar e compartilhar seus documentos do Paper.

- ***Dispositivos móveis***

  O aplicativo móvel do Paper está disponível para smartphones e tablets iOS e Android, habilitando os usuários a acessar documentos do Paper onde quer que estejam. O aplicativo móvel foi desenvolvido como um aplicativo híbrido, consistindo em código nativo (iOS ou Android) envolvido em um navegador web interno.

- ***API***

  A API do Dropbox já descrita acima contém pontos de extremidade e tipos de dados para gerenciar documentos e pastas no Dropbox Paper, inclusive atendimento por funcionalidade como gerenciamento de permissões, arquivamento e exclusão permanente.

Criptografia

Dados em trânsito

Para proteger os dados em trânsito entre os aplicativos do Dropbox e nossos servidores, o Dropbox usa criptografia Secure Sockets Layer (SSL)/Transport Layer Security (TLS) para transferência de dados, criando um túnel seguro protegido por padrões avançados de criptografia AES de 128 bits ou superior. Os dados do arquivo em trânsito entre um cliente do Dropbox (atualmente: desktop, dispositivos móveis, API ou web) e o serviço hospedado são criptografados via SSL/TLS. Do mesmo modo, os dados dos documentos do Paper em trânsito entre um cliente Paper (atualmente dispositivo móvel, API ou web) e os serviços hospedados são criptografados via SSL/TLS. Para os pontos de extremidade que controlamos (desktop e móvel) e navegadores modernos, usamos cifras fortes com suporte à criptografia PFS (Perfect Forward Secrecy) e atribuição de certificados. Além disso, na web, indicamos que todos os cookies de autenticação são seguros e habilitamos a opção HTTP Strict Transport Security (HSTS) com includeSubDomains ativo.

Observação: O Dropbox utiliza exclusivamente o TLS, e o uso do SSLV3 tornou-se obsoleto devido a vulnerabilidades conhecidas. Porém, "SSL/TLS" é a forma frequente como nos referimos ao TLS, por isso utilizamos essa designação aqui.

Para impedir ataques de terceiros (man-in-the-middle), a autenticação dos servidores front-end do Dropbox é realizada por meio de certificados públicos mantidos pelo cliente. Uma conexão criptografada é negociada antes da transferência de qualquer arquivo ou documento do Paper, garantindo a entrega segura para servidores front-end do Dropbox.

Dados em repouso

Os arquivos do Dropbox enviados pelos usuários são criptografados em repouso usando o Advanced Encryption Standard (AES) de 256 bits. Os arquivos são armazenados em vários centros de dados em blocos de arquivos independentes. Cada bloco é fragmentado e criptografado usando cifra forte. Apenas blocos que foram modificados entre as revisões são sincronizados. Os documentos do Paper também são criptografados usando o Advanced Encryption Standard (AES) de 256 bits. Os documentos do Paper são armazenados em várias zonas disponíveis usando sistemas de terceiros.

Gerenciamento de chave

A infraestrutura de gerenciamento de chave do Dropbox é projetada com controles de segurança, operacionais, técnicos e de procedimento, com acesso direto às chaves muito limitado. A geração, troca e o armazenamento de chave de criptografia é distribuído por processamento descentralizado.

- ***Chaves de criptografia de arquivos***

  O Dropbox foi desenvolvido de forma a gerenciar chaves de criptografia de arquivos em nome dos usuários para remover complexidade, habilitar recursos avançados de produtos e apresentar forte controle criptográfico. As chaves de criptografia de arquivos são criadas, armazenadas e protegidas por controles de segurança de infraestrutura do sistema de produção e políticas de segurança.

- ***Chaves SSH internas***

  O acesso a sistemas de produção é restrito a pares únicos de chaves SSH. Os procedimentos e as políticas de segurança requerem a proteção das chaves SSH. Um sistema interno gerencia o processo seguro de troca da chave pública, e as chaves privadas são armazenadas em segurança. As chaves internas SSH não podem ser utilizadas para acessar sistemas de produção sem um segundo fator separado de autenticação.

- ***Distribuição de chaves***

  O Dropbox automatiza o gerenciamento e a distribuição de chaves sigilosas apenas para os sistemas essenciais às operações.

Atribuição de certificados

O Dropbox executa a atribuição de certificados em navegadores modernos compatíveis com especificações de atribuição de chave pública HTTP e em nossos clientes para desktop e dispositivos móveis. A atribuição de certificado é uma verificação extra para garantir que o serviço ao qual você está se conectando é o esperado e não um impostor. Nós o utilizamos para nos resguardar contra outras medidas que hackers habilidosos podem tentar utilizar para espionar suas atividades.

Proteção de dados de autenticação

O Dropbox vai além do uso regular de hash para proteger as credenciais de acesso dos usuários. De acordo com as melhores práticas do setor, cada senha é "salgada" com um "salt" único, gerado de forma aleatória, e usamos hashing iterativo para retardar a computação. Essas práticas ajudam na proteção contra ataques de força bruta, de dicionário e rainbow. Como medida adicional de precaução, criptografamos as hashes com uma chave armazenada separadamente do banco de dados, o que ajuda a manter as senhas seguras no caso de um comprometimento somente do banco de dados.

Varredura de malware

Desenvolvemos um sistema automatizado que faz uma varredura de malware no momento em que um conteúdo é compartilhado fora da conta do usuário de origem. O sistema aproveita tanto a tecnologia patenteada quanto os mecanismos de detecção padrão do setor e é projetado para impedir a propagação do malware.

Segurança do produto

O Dropbox oferece recursos administrativos de controle e visibilidade que capacitam as equipes de TI e os usuários finais a gerenciarem e protegerem seus dados de forma eficaz. Com o Dropbox, você tem tudo o que precisa em um só lugar: ferramentas, conteúdo e colaboradores. O Dropbox é mais do que um armazenamento seguro, é uma maneira inteligente e contínua de otimizar seu fluxo de trabalho atual.

Segue os destaques dos recursos disponíveis a administradores e usuários, além de integrações de terceiros para gerenciar os principais processos de TI.

Observação: A disponibilidade de recursos varia de acordo com o plano de assinatura. Acesse dropbox.com/business/plans para mais detalhes.

Controles de conteúdo

Proteger ativos empresariais confidenciais, como propriedade intelectual e informações de identificação pessoal (PII), é crucial para as equipes de TI e segurança de dados. De permissões detalhadas de conteúdo a políticas de retenção de dados e retenções legais, o Dropbox oferece soluções líderes do setor para gerenciar, monitorar e proteger seu conteúdo. Abaixo estão os principais produtos e recursos do Dropbox que apoiam o controle de conteúdo.

Permissões detalhadas de conteúdo e permissões de arquivos e pastas compartilhados

- ***Permissões para arquivos compartilhados***

  Um membro da equipe, proprietário de um arquivo compartilhado, pode remover o acesso de usuários específicos e desabilitar comentários no arquivo.

- ***Permissões para arquivos compartilhados***

  Um membro da equipe que seja proprietário de uma pasta compartilhada pode remover o acesso de usuários específicos à pasta, alterar as permissões de visualização/edição para usuários específicos e transferir a propriedade da pasta. Dependendo das permissões de compartilhamento global da equipe, cada proprietário da pasta compartilhada poderá também controlar se ela poderá ser compartilhada com pessoas que não pertençam à equipe, se outras pessoas com permissões de edição poderão gerenciar a participação na equipe e se links poderão ser compartilhados com pessoas fora da pasta.

- ***Senhas para links compartilhados***

  Qualquer link compartilhado pode ser protegido por uma senha definida pelo proprietário. Antes que qualquer dado de arquivo ou pasta seja transmitido, uma camada de controle ao acesso verifica se a senha correta foi enviada e se todas as outras exigências (como equipe, grupo ou pasta ACL) foram cumpridas. Se estiver tudo certo, um cookie seguro será armazenado no navegador do usuário para lembrar que a senha foi verificada anteriormente. Com os controles de compartilhamento, os administradores também podem definir senhas padrão, em vez de tê-las como opcionais, para proteger melhor o conteúdo da equipe.

- ***Prazos de validade para links compartilhados***

  Usuários podem configurar um prazo de validade para qualquer link compartilhado, fornecendo acesso temporário a arquivos e pastas. Com os controles de compartilhamento, os administradores também podem definir prazos padrão, em vez de tê-los como opcionais, para proteger melhor o conteúdo da equipe.

Permissões de documentos do Paper e pastas compartilhadas do Paper

- ***Permissões para documentos do Paper e pastas compartilhadas do Paper***

  Um membro da equipe, proprietário de um documento do Paper ou pasta compartilhada do Paper, pode remover o acesso de usuários específicos e desabilitar a edição em documentos do Paper.

- ***Permissões para documentos do Paper***

  Um membro da equipe, proprietário de um documento do Paper, pode remover o acesso de usuários específicos que estão explicitamente listados no painel de compartilhamento. Tanto o proprietário quanto os editores de um documento do Paper podem alterar as permissões de visualização/edição

para usuários específicos bem como alterar a política de link do documento. A política de links controla quais usuários podem abrir o documento e as permissões que recebem. O administrador da equipe pode definir políticas em toda a equipe para links e compartilhamento de documentos.

- ***Permissões para pastas do Paper***

  Um membro da equipe que seja membro de uma pasta pode alterar a política de compartilhamento da pasta e remover o acesso de usuários específicos que foram explicitamente adicionados à pasta.

Ações de arquivo e pasta

- ***Pastas da equipe para arquivos***

  Administradores podem criar pastas da equipe que concedam automaticamente os níveis corretos de acesso (visualização e edição) ao conteúdo que grupos e outros colaboradores precisam.

- ***Controles de compartilhamento e acesso detalhado***

  Os controles de compartilhamento permitem que administradores gerenciem participações e permissões no nível superior ou no nível de subpastas para que pessoas e grupos dentro e fora da empresa tenham acesso somente a pastas específicas.

- ***Gerente da pasta da equipe***

  Administradores podem visualizar todas as pastas da equipe e personalizar políticas de compartilhamento a partir de um lugar central para ajudar a evitar o compartilhamento indevido de materiais confidenciais.

- ***Pastas compartilhadas para documentos do Paper***

  Administradores podem criar pastas compartilhadas do Paper que concedam automaticamente os níveis corretos de acesso, para comentar ou editar, ao conteúdo que outros colaboradores precisam.

- ***Exclusão remota***

  Quando algum funcionário sai da equipe ou quando ocorre a perda de algum dispositivo, os administradores podem excluir remotamente os dados do Dropbox e as cópias locais de arquivos. Os arquivos serão removidos tanto de computadores quanto de dispositivos móveis quando ficarem on-line e o aplicativo do Dropbox estiver em execução.

- ***Transferência de conta***

  Depois do desprovisionamento de um usuário (tanto manualmente quanto pelo diretório de serviços), os administradores podem transferir arquivos e propriedade de documentos do Paper criados pelo antigo membro da equipe da conta daquele usuário para a conta de outro membro da equipe. O recurso de transferência de conta pode ser usado ao remover um usuário ou a qualquer momento depois da exclusão da conta de um usuário.

Os recursos a seguir estão disponíveis como recursos de add-on (entre em contato com a equipe de vendas para mais informações).

- ***Digitalização de conteúdo***

  Com o add-on Controles avançados da equipe, os clientes do Dropbox Business Advanced e Enterprise podem escanear conteúdo novo e existente no Dropbox para localizar e evitar vulnerabilidades de dados.

- ***Configurar e acionar fluxos de trabalho personalizados***

  Com o add-on Controles avançados da equipe, os administradores podem realizar ações personalizáveis contra arquivos que violam as políticas da empresa.

- ***Configurar alertas***

  Os administradores podem monitorar preocupações de segurança em tempo real e evitar vulnerabilidades de dados. Receba alertas sobre arquivos compartilhados externamente e dados confidenciais escaneados.

Visibilidade de conteúdo

Alertas e notificações de segurança

Os administradores do Dropbox Enterprise recebem notificações em tempo real quando atividades abusivas, atividades arriscadas ou possíveis vazamentos de dados forem detectados em suas contas. Os seguintes eventos são monitorados:

- Exclusões em massa
- Transferência de dados em massa
- Conteúdo confidencial compartilhado externamente
- Malware compartilhado de fora da equipe
- Malware compartilhado dentro da equipe
- Muitas tentativas de login fracassadas
- Tentativa de entrada de um país de alto risco
- Detecção de ransomware

O Dropbox também possibilita a configuração de limites de alerta, o ajuste de destinatários de notificações e o acionamento de alertas quando pastas com arquivos confidenciais forem compartilhadas externamente. Também é possível para os administradores marcarem alertas como em revisão, resolvidos ou ignorados. Além disso, um widget de painel mostra estatísticas gerais de alerta da equipe e tendências da última semana.

Página e relatório de compartilhamento externo

O Dropbox fornece mais visibilidade com o relatório e a página de compartilhamento externo. Os administradores podem criar um relatório da página de estatísticas ou da página de compartilhamento externo. O relatório lista todos os arquivos e as pastas da equipe que são compartilhados fora da equipe e todos os links compartilhados. A página de compartilhamento externo é uma página adicional na seção de Administração que permite que os administradores vejam e filtrem (por tipo de arquivo, quem compartilhou, configurações de link e muito mais) os arquivos e as pastas compartilhados diretamente da equipe e os links compartilhados.

Controles de compartilhamento

As configurações fazem com que os administradores da equipe tenham mais controle sobre o compartilhamento e acesso ao conteúdo da equipe. Os administradores podem definir prazos padrão para as equipes, restrições de senha ou ambos. Essas restrições reduzem o risco de perda de dados ao remover a responsabilidade dos usuários de definir restrições.

Classificação de dados

As equipes no Dropbox Enterprise têm dados pessoais e confidenciais rotulados automaticamente para maior proteção contra exposição. Os administradores recebem alertas de prevenção à perda de dados (DLP) por e-mail e na seção de Administração quando arquivos ou pastas contendo informações confidenciais e salvos nas pastas da equipe forem compartilhados externamente. Os administradores têm a capacidade de identificar e classificar automaticamente dados confidenciais armazenados em pastas compartilhadas e em pastas pessoais de membros da equipe. Os administradores do Dropbox Enterprise podem ativar a classificação automática de dados na seção de Administração.

Add-on Governança de dados

Governança de dados é o conjunto geral de processos, tecnologias e equipes que se reúnem para gerenciar e proteger os ativos de dados de uma organização. Isso inclui a capacidade de armazenar, identificar, descobrir e recuperar dados corporativos conforme necessário.

O add-on Governança de dados do Dropbox agrupa um conjunto de recursos que permitem que as organizações controlem e protejam melhor seus dados, ao mesmo tempo que reduzem os riscos e os custos associados ao atendimento das necessidades regulamentares e de conformidade. Atualmente, esse add-on inclui quatro recursos principais para administradores de equipe e administradores de conformidade.

- ***Histórico de versões ampliado***

  Seu histórico de versões de arquivo padrão depende do tipo de conta do Dropbox que você tem. No entanto, as equipes do Dropbox Business podem comprar um add-on do Histórico de versões ampliado separadamente ou como parte do pacote do add-on Governança de dados, que permite recuperar qualquer arquivo excluído ou alterado nos últimos 10 anos.

- ***Retenções legais***

  Aplicar uma retenção legal a um membro da equipe permite que os administradores de equipe e de conformidade visualizem e exportem todo o conteúdo que foi criado ou modificado por esse membro. Os membros afetados por uma retenção legal não são notificados e ainda mantêm suas permissões para criar, editar e excluir arquivos.

- ***Retenção de dados***

  A retenção de dados permite que equipes e administradores de conformidade evitem a exclusão acidental dos conteúdos que precisam ser mantidos por determinado período para cumprir com os regulamentos. Esse recurso permite que os clientes retenham dados dos últimos 10 anos a partir da última data de “revisão”.

- ***Descarte de dados***

  O descarte de dados permite que os administradores de equipe e de conformidade excluam dados permanentemente em uma data específica para cumprir os requisitos de retenção e descarte de dados. Os administradores monitoram a atividade e recebem relatórios com alertas para as próximas exclusões de arquivos.

Recuperação e controle de versão

Os clientes do Dropbox Business têm a capacidade de restaurar arquivos excluídos e documentos do Paper, bem como recuperar versões anteriores de arquivos e documentos do Paper, garantindo que alterações em dados importantes possam ser controladas e recuperadas.

Segurança de dados em dispositivos móveis

- ***Excluir dados***

  Para segurança adicional, um usuário pode habilitar a opção de excluir todos os dados do Dropbox do dispositivo após 10 tentativas erradas de preenchimento da senha.

- ***Armazenamento interno e arquivos off-line***

  Por padrão, os arquivos não são salvos no armazenamento interno de dispositivos móveis. Clientes do Dropbox para dispositivos móveis podem salvar arquivos e pastas individuais no dispositivo para uso off-line. Quando um dispositivo for desvinculado de uma conta do Dropbox, tanto pela interface web quanto móvel, as pastas e os arquivos salvos serão automaticamente excluídos do armazenamento interno do dispositivo.

- ***Documentos off-line do Paper***

  Quando um dispositivo for desvinculado do Paper, pela página de segurança de conta do Dropbox, o usuário será desconectado e os documentos off-line do Paper serão automaticamente excluídos do armazenamento interno do dispositivo.

Controles da equipe

Como nenhuma empresa é exatamente igual a outra, desenvolvemos diversas ferramentas que possibilitam aos administradores personalizar o Dropbox Business para as necessidades particulares de suas próprias equipes. O Dropbox Business também inclui ferramentas que permitem aos usuários finais proteger ainda mais suas contas e dados. A autenticação, recuperação, registro e outros recursos de segurança listados a seguir estão disponíveis através das várias interfaces de usuário do Dropbox.

Seguem abaixo alguns dos controles e recursos de visibilidade disponíveis na seção de Administração do Dropbox Business.

Permissões de conteúdo detalhadas

- ***Funções administrativas em níveis***

  O Dropbox oferece funções de administração em níveis para habilitar gerenciamento de equipe mais eficaz. Pode-se atribuir aos administradores de conta um de três níveis de acesso. Não há limite para o número de administradores que uma equipe pode ter, e é possível atribuir a qualquer membro da equipe a função de administrador.

- ***Administrador de equipe***

  Pode definir permissões de segurança e compartilhamento válidas para toda a equipe, criar administradores e gerenciar membros. Um administrador de equipe tem todas as permissões administrativas disponíveis. Apenas os administradores de equipe podem conceder funções de administrador a outros membros da equipe e alterá-las. Cada conta do Dropbox Business deve ter sempre pelo menos um administrador de equipe.

- ***Administrador de gerenciamento de usuários***

  Pode lidar com a maioria das tarefas de gerenciamento da equipe, inclusive adicionar e remover membros, gerenciar grupos e acessar o feed de atividades da equipe.

- ***Administrador de atendimento***

  Lida com solicitações comuns de serviço feitas por membros da equipe, como restaurar arquivos excluídos ou ajudar membros da equipe bloqueados pela verificação em dois passos. Administradores de atendimento também podem restaurar senhas de não administradores e exportar um registro de atividade para um membro da equipe específico.

- ***Administrador de faturamento***

  Pode acessar páginas de pagamento na seção de Administração.

- ***Administrador de conteúdo***

  Pode criar e gerenciar pastas da equipe dentro do Gerenciador de conteúdo.

- ***Administrador de relatórios***

  Pode criar relatórios dentro da seção de Administração e tem acesso à página Atividade.

- ***Administrador de segurança***

  Pode gerenciar alertas de segurança, compartilhamento externo e riscos de segurança.

- ***Administrador de conformidade (disponível somente para equipes com o add-on Governança de dados)***

  Pode gerenciar páginas de Governança de dados (retenções legais, retenção de dados e descarte de dados) e acessar o Gerenciador de conteúdo.

- ***Grupos***

  Equipes podem criar e gerenciar listas de membros dentro do Dropbox e facilmente conceder acesso a pastas específicas. O Dropbox também pode sincronizar grupos do Active Directory usando o Conector do Active Directory.

- ***Grupos gerenciados pela empresa***

  Somente administradores podem criar, excluir e gerenciar participações desse tipo de grupo. Usuários não podem solicitar sua inclusão ou exclusão de um grupo gerenciado pela empresa.

- ***Grupos gerenciados por usuários***

  Os administradores podem escolher se os usuários podem criar e gerenciar seus próprios grupos. Os administradores também podem alterar de um grupo gerenciado por usuários para um grupo gerenciado por empresas a qualquer momento, para assumir o controle.

- ***Restrição de várias contas em computadores***

  Os administradores podem impedir que membros da equipe vinculem uma segunda conta do Dropbox a computadores que estejam vinculados à conta de trabalho do Dropbox deles.

- ***Estado de usuário suspenso***

  Os administradores conseguem desabilitar o acesso de um usuário a sua conta, ao mesmo tempo que

preservam seus dados e compartilham suas relações, para manter as informações da empresa seguras. Os administradores podem, em outro momento, reativar ou excluir a conta.

- ***Iniciar sessão como usuário***

  Os administradores da equipe podem acessar a conta como membros de suas equipes. Isso fornece aos administradores acesso direto aos arquivos, às pastas e aos documentos do Paper nas contas de membros da equipe, a fim de que eles possam fazer alterações, compartilhar em nome de membros da equipe ou conduzir auditorias de eventos no nível de arquivo. Situações do tipo "Acessar a conta como usuário" são gravadas no registro de atividade da equipe, e os administradores podem determinar se os membros serão notificados sobre essas situações.

- ***Permissões de compartilhamento***

  Os administradores de equipe têm controle abrangente das capacidades de compartilhamento de suas equipes usuárias do Dropbox, inclusive se:

  - Membros da equipe podem compartilhar arquivos e pastas com pessoas que não façam parte da equipe.
  - Membros de equipe podem editar pastas cujos proprietários não fazem parte da equipe.
  - Links compartilhados criados por membros da equipe funcionarão para pessoas que não fazem parte da equipe.
  - Membros da equipe podem criar solicitações de arquivo e coletar arquivos de membros da equipe e/ou de pessoas que não fazem parte da equipe.
  - Outras pessoas podem visualizar e fazer comentários nos arquivos de propriedade da equipe.
  - Membros da equipe podem compartilhar documentos do Paper e pastas do Paper fora da equipe.
  - Permissões de exclusão permanente são concedidas.

O administrador de equipe da conta do Dropbox Business pode limitar a capacidade de exclusão permanente de arquivos e documentos do Paper apenas a administradores de equipe.

Integração e provisionamento de usuários

Métodos de provisionamento de usuário e gerenciamento de identidade

- ***Convite por e-mail***

  Uma ferramenta na seção de Administração do Dropbox Business permite que administradores criem manualmente um convite por e-mail.

- ***Active Directory***

  Os administradores do Dropbox Business podem automatizar a criação e remoção de contas de um sistema Active Directory existente, usando nosso conector do Active Directory ou provedor de identidade de terceiros. Uma vez integrado, o Active Directory pode ser utilizado para gerenciar a participação dos membros.

- ***SSO (logon único)***

O Dropbox Business pode ser configurado para permitir que membros da equipe acessem suas contas fazendo login em um provedor de identidade central. Nossa implementação SSO (logon único), que usa o Security Assertion Markup Language 2.0 (SAML 2.0), padrão do setor, facilita o provisionamento e o deixa mais seguro, deixando um provedor de identidade confiável responsável pela autenticação e por fornecer aos membros da equipe acesso ao Dropbox sem a necessidade de gerenciar mais uma senha. O Dropbox

também firmou parcerias com provedores de gerenciamento de identidade líderes no setor, para que os usuários possam provisionar e desprovisionar de forma automática. Consulte a seção de Integrações à API do Dropbox Business abaixo.

- ***API***

  A API do Dropbox Business pode ser utilizada pelos clientes para criar soluções personalizadas em provisionamento de usuários e gerenciamento de identidade. Consulte a seção de Integrações à API do Dropbox Business neste documento.

Verificação em dois passos

Esse recurso de segurança altamente recomendado adiciona uma camada de proteção extra à conta do Dropbox do usuário. Quando a verificação em dois passos for habilitada, o Dropbox exigirá um código de segurança de seis dígitos, além de uma senha, após o logon ou ao vincular um novo computador, celular ou tablet.

- Administradores podem decidir exigir a verificação em dois passos para todos os membros da equipe ou apenas membros específicos.
- Os administradores de conta podem acompanhar quais membros da equipe têm a verificação em dois passos ativada.
- Os códigos da autenticação em dois passos do Dropbox podem ser recebidos por SMS ou aplicativos que estejam em conformidade com o padrão de algoritmo de Senhas de uso único com base em tempo (TOTP).
- Caso um usuário não possa receber os códigos de segurança por esses métodos, ele pode optar por utilizar um código de reserva de emergência de uso único com 16 dígitos. Como alternativa, esse usuário pode usar um número de telefone secundário para receber um código reserva por mensagem de texto.
- O Dropbox também é compatível com o padrão aberto FIDO Universal 2nd Factor (U2F), que habilita a autenticação de usuários não pelo código de seis dígitos, mas sim por uma chave de segurança USB.

Instalador corporativo

Os administradores que precisarem fazer provisionamento escalonado podem usar nosso instalador Enterprise para Windows, instalando o cliente do Dropbox para desktop remotamente por meio de soluções de software gerenciado e mecanismos de implementação.

Dispositivos gerenciados e login

- ***Gerenciamento de mobilidade corporativa (EMM)***

  O Dropbox se integra a provedores terceirizados de EMM para oferecer a administradores do Dropbox Business em um plano Enterprise mais controle sobre como os membros da equipe usam o Dropbox em dispositivos móveis. Os administradores podem restringir o uso de aplicativos móveis para contas do Dropbox Enterprise a apenas dispositivos gerenciados (dispositivos pessoais ou fornecidos pela empresa), obter visibilidade sobre o uso do aplicativo (incluindo o armazenamento disponível e os locais de acesso) e apagar remotamente um dispositivo perdido ou roubado. Observe que o aplicativo móvel do Paper não é gerenciável pelo EMM.

- ***Aprovações de dispositivo***

  O Dropbox permite que os administradores das equipes do Dropbox Education e do Dropbox Business

nos planos Advanced e Enterprise definam limites para o número de dispositivos que um usuário pode sincronizar com o Dropbox, e escolham entre aprovações gerenciadas pelo usuário ou pelo administrador. Os administradores também podem criar uma lista de exceções de usuários que não possuam um número restrito de dispositivos. Observe que o aplicativo móvel do Paper não está incluído nas aprovações de dispositivo.

- ***Requisitos de verificação em dois passos***

  Os administradores podem achar necessário exigir a verificação em dois passos para todos os membros de equipe ou apenas para membros específicos. Outros requisitos de autenticação multifatorial podem ser exigidos por meio de sua implementação SSO (logon único).

- ***Controle de senhas***

  Administradores de equipes do Education, Advanced e Enterprise podem exigir que os membros definam e mantenham senhas fortes e complexas para suas contas. Quando esse recurso é habilitado, os membros da equipe são desconectados de qualquer sessão da web e solicitados a criar novas senhas quando se conectarem novamente. Uma ferramenta interna analisa a complexidade das senhas comparando-as a um banco de dados de palavras, nomes, padrões e números comuns. Um usuário que inserir uma senha comum é solicitado a inserir outra mais exclusiva e difícil de se adivinhar. Os administradores também podem redefinir senhas para toda uma equipe ou por usuário.

- ***Gerenciamento de domínios***

  O Dropbox fornece um conjunto de ferramentas para empresas, a fim de simplificar e aumentar a velocidade de processos de integração de usuários e o controle de uso do Dropbox.

  - **Verificação de domínio**
    As empresas podem reivindicar propriedade de seus domínios e desbloquear as outras ferramentas de gerenciamento de domínio.

  - **Adesão obrigatória**
    Os administradores podem exigir que os usuários individuais do Dropbox que foram convidados para a equipe do Dropbox da empresa migrem para a equipe ou alterem o endereço de e-mail de suas contas pessoais.

  - **Informações de domínio**
    Os administradores podem ver informações-chave, como quantas contas individuais do Dropbox estão usando endereços de e-mail de empresa.

  - **Captura de contas**
    Os administradores podem impor a todos os usuários do Dropbox que estão usando um endereço de e-mail de empresa que entrem na equipe da empresa ou alterem o endereço de e-mail em sua conta pessoal.

- ***Controle de sessão da web***

  Os administradores podem controlar por quanto tempo os membros da equipe podem ficar conectados ao dropbox.com. Os administradores podem limitar a duração das sessões da web e/ou das sessões ociosas. As sessões que atingirem esse limite são automaticamente desconectadas. Os administradores também podem rastrear e terminar as sessões da web de usuários individuais.

- ***Acesso de aplicativos***

  Os administradores podem visualizar e revogar o acesso de aplicativos de terceiros às contas de usuários.

- ***Desvincular dispositivos***

  Computadores e dispositivos móveis conectados a contas de usuário podem ser desvinculados pelo

administrador através da seção de Administração ou pelo próprio usuário por meio das configurações individuais de segurança da conta. No caso de computadores, o cancelamento do vínculo remove os dados de autenticação e fornece a opção de excluir cópias locais de arquivos na próxima vez que o computador ficar on-line (consulte abaixo **Exclusão remota**). No caso de dispositivos móveis, o ato de desvincular remove arquivos marcados como favoritos, dados em cache e informações de acesso. A desvinculação também remove documentos off-line do Paper do aplicativo de dispositivo móvel do Paper. Se a verificação em dois passos estiver ativada, os usuários deverão fazer uma nova autenticação para qualquer dispositivo ao vincular novamente. Além disso, as configurações da conta dos usuários oferecem a opção de enviar um e-mail de notificação automaticamente quando algum dispositivo for vinculado.

- ***Controle de rede***

  Os administradores do Dropbox Business em um plano Enterprise podem restringir o uso do Dropbox na rede da empresa a apenas a conta da equipe Enterprise. Esse recurso se integra ao provedor de segurança de rede da empresa para bloquear qualquer tráfego que exista fora da conta sancionada em computadores. Observe que o Paper não está atualmente sendo gerenciado por controle de rede.

Segurança em dispositivos móveis

- ***Verificação de impressão digital***

  Os usuários podem habilitar o Touch ID ou Face ID nos dispositivos iOS e o Fingerprint unlock (caso compatível) nos dispositivos Android como um método de desbloqueio do aplicativo Dropbox para dispositivos móveis.

Visibilidade de acesso

- ***Verificação de identidade por parte do atendimento técnico***

  Antes que o atendimento do Dropbox forneça qualquer informação relacionada a contas ou à resolução de problemas, o administrador da conta deve fornecer um código de segurança de uso único, gerado aleatoriamente, para validar sua identidade. Esse PIN só está disponível pela seção de Administração.

Atividade de conta de usuário

Cada usuário pode visualizar as páginas a seguir a partir de suas configurações da conta para obter informações atualizadas sobre suas próprias atividades.

- ***Página de compartilhamento***

  Essa página mostra as pastas compartilhadas que estão atualmente no Dropbox do usuário, bem como pastas compartilhadas que o usuário pode adicionar. Um usuário pode cancelar o compartilhamento de pastas e arquivos e definir permissões de compartilhamento.

- ***Página de arquivos***

  Essa página mostra os arquivos que foram compartilhados com o usuário e a data em que cada arquivo foi compartilhado. O usuário tem a opção de remover seu acesso a esses arquivos. Para ver documentos do Paper que foram compartilhados com o usuário por outra pessoa, ele poderá navegar até a página “Compartilhados comigo” na interface de navegação de documentos do Paper.

- ***Página de links***

  Essa página mostra todos os links ativos compartilhados que o usuário criou e a data de criação de cada um. Ela também mostra todos os links compartilhados com o usuário por outras pessoas. O usuário pode desabilitar links ou alterar permissões.

- ***Notificação por e-mail***

  Um usuário poderá optar por receber uma notificação por e-mail sempre que um novo dispositivo ou aplicativo for vinculado à sua conta do Dropbox.

Permissões de conta do usuário

- ***Dispositivos vinculados***

  A seção **Dispositivos** das configurações de segurança da conta de um usuário exibe todos os computadores e dispositivos móveis vinculados à conta do usuário. Para cada computador, são exibidos o endereço IP, o país e o horário aproximado da atividade mais recente. Um usuário pode desvincular qualquer dispositivo, com a opção de que os arquivos nos computadores vinculados sejam excluídos na próxima vez que ficarem on-line.

- ***Sessões de web ativas***

  A seção **Sessões** mostra todos os navegadores da web atualmente conectados à na conta do usuário. Para cada um deles também são exibidos o endereço IP, o país e o horário de início da sessão mais recente, bem como o horário aproximado da atividade mais recente. Um usuário pode encerrar qualquer sessão remotamente a partir de configurações de segurança da sua conta.

- ***Aplicativos vinculados***

  A seção **Aplicativos vinculados** fornece uma lista de todos os aplicativos de terceiros que tenham acesso a uma conta de usuário e o tipo de acesso que cada aplicativo detém. Um usuário pode revogar a permissão de qualquer aplicativo para acessar seu Dropbox.

Feed de atividades

O Dropbox Business registra ações em arquivos no feed de atividades da equipe, que pode ser acessado na seção de Administração. O feed de atividades oferece opções flexíveis de filtragem, que permitem que administradores conduzam investigações direcionadas sobre atividades em contas, arquivos ou documentos do Paper. Por exemplo, eles podem visualizar o histórico completo de um arquivo ou documento do Paper e como os usuários interagiram com ele, ou até mesmo visualizar todas as atividades de uma equipe durante um período de tempo específico. O feed de atividades pode ser exportado como um relatório baixado em formato CSV e também pode ser diretamente integrado a um produto de SIEM (gerenciamento de informações de segurança e eventos) ou a outra ferramenta de análise por meio de soluções de parceiros. Os seguintes eventos de conteúdo são registrados no feed de atividades:

- ***Compartilhamento de arquivos, pastas e links***

  Quando aplicável, os relatórios especificam se as ações envolveram pessoas de fora da equipe.

  Compartilhamento de arquivos

  - Adição ou remoção de um membro da equipe, ou de pessoas que não pertencem à equipe.
  - Alteração das permissões para um membro da equipe ou pessoas que não pertencem à equipe.
  - Adição ou remoção de um grupo.
  - Adição de um arquivo compartilhado ao Dropbox do usuário.
  - Visualização do conteúdo de um arquivo que foi compartilhado através de um convite de pasta ou arquivo.
  - Cópia de conteúdo compartilhado para os usuários do Dropbox.
  - Download de conteúdo compartilhado.
  - Comentários em arquivos.

- Comentários solucionados ou não solucionados.
- Comentários excluídos.
- Assinatura ou cancelamento de assinatura para notificações de comentários.
- Exigência de um convite para um arquivo cujo proprietário é a equipe.
- Solicitação de acesso a um arquivo cujo proprietário é a equipe.
- Cancelamento do compartilhamento de um arquivo.

Pastas compartilhadas

- Criação de uma nova pasta compartilhada.
- Adição ou remoção de um membro da equipe, pessoas que não pertencem à equipe ou grupo.
- Adição de uma pasta compartilhada ao Dropbox dos usuários ou remoção do próprio acesso pelo usuário à pasta compartilhada.
- Adição de uma pasta compartilhada por meio de um link.
- Alteração das permissões de um membro da equipe ou de pessoas que não pertencem à equipe.
- Transferência da propriedade da pasta para outro usuário.
- Cancelamento do compartilhamento de uma pasta.
- Exigência de participação na equipe para uma pasta compartilhada.
- Solicitação de acesso a uma pasta compartilhada.
- Adição de usuário solicitado a uma pasta compartilhada.
- Bloqueio ou desbloqueio de pessoas que não pertencem à equipe por meio da adição delas à pasta.
- Permissão para qualquer membro da equipe adicionar pessoas a uma pasta ou apenas o proprietário.
- Alteração do acesso do grupo a uma pasta compartilhada.

Links compartilhados

- Criação ou remoção de um link.
- Conteúdo de um link visível para qualquer pessoa que tenha o link ou somente membros da equipe.
- Conteúdo de um link protegido por senha.
- Definição ou remoção da data de validade de um link.
- Visualização de link.
- Download do conteúdo de um link.
- Cópia do conteúdo de um link para a conta do Dropbox do usuário.
- Criação de um link para um arquivo por meio de um aplicativo API.
- Compartilhamento de um link com um membro da equipe, pessoas que não pertencem à equipe ou grupo.
- Bloqueio ou desbloqueio de pessoas que não pertencem à equipe por meio de visualização de links para arquivos em uma pasta compartilhada.
- Compartilhamento de álbum.

Solicitações de arquivo

- Criação, alteração, fechamento ou exclusão de uma solicitação de arquivo.
- Adição de usuários à solicitação de arquivo.
- Adição ou remoção do prazo para solicitação de arquivo.
- Alteração de uma pasta de solicitação de arquivo.
- Recebimento de arquivos por meio de solicitação de arquivo.
- Arquivos recebidos por e-mail para o Dropbox.

Eventos individuais de arquivos e pastas.

- Adição de arquivos ao Dropbox.
- Pasta criada.
- Visualização de arquivo.
- Edição de um arquivo.
- Download de arquivos.
- Cópia de arquivo ou pasta.
- Transferência de arquivo ou pasta.
- Pasta ou arquivo renomeado.
- Reversão de um arquivo para uma versão anterior.
- Remoção de alterações em arquivos.
- Restauração ou exclusão de arquivos.
- Exclusão de um arquivo ou pasta.
- Exclusão permanente de um arquivo ou de uma pasta.

Acessos bem-sucedidos e malsucedidos.

- Tentativa de acesso bem-sucedida ou malsucedida.
- Tentativa de acesso malsucedida ou erro por meio de SSO (logon único).
- Tentativa de acesso malsucedida ou erro pelo EMM.
- Saída da conta.
- Alteração de endereço IP para sessão web.

Senhas

Alterações em senhas ou configurações da verificação em dois passos. Os administradores não podem ver as senhas dos usuários.

- Alteração ou redefinição de senha.
- Habilitação, recuperação ou desabilitação da verificação em dois passos.
- Configuração ou alteração da verificação em dois passos para usar SMS ou aplicativo móvel.

- Adição, edição ou remoção de um backup de celular para verificação em dois passos.
- Adição ou remoção de uma chave de segurança para verificação em dois passos.

Participação na equipe

Inclusões e exclusões de membros da equipe.

- Convite a alguém para a equipe.
- Participação na equipe.
- Remoção de um membro da equipe.
- Suspensão ou não de um membro da equipe.
- Recuperação de um membro da equipe removido.
- Solicitação para juntar-se à equipe com base no domínio de conta.
- Aprovação ou recusa de uma solicitação para juntar-se à equipe com base no domínio de conta.
- Envio de convites de domínio para contas de domínio existentes.
- Usuário entrou na equipe em resposta à captura de contas.
- Usuário saiu do domínio em resposta à captura de contas.
- Membros da equipe bloqueados ou desbloqueados pela sugestão de novos membros da equipe.
- Sugestão de um novo membro da equipe.

Aplicativos

Aplicativos de terceiros vinculados a contas do Dropbox.

- Autorização ou remoção de um aplicativo.
- Autorização ou remoção de um aplicativo da equipe.

Dispositivos

Computadores ou dispositivos móveis vinculados a contas do Dropbox.

- Vinculação ou desvinculação de um dispositivo.
- Uso de exclusão remota e exclusão com sucesso de todos os arquivos ou falha na exclusão de alguns arquivos.
- Alteração de endereço IP para computador desktop ou dispositivo móvel.

Ações do administrador

Alterações em configurações na seção de Administração, como permissões de pastas compartilhadas.

- ***Autenticação e SSO (logon único)***
  - Redefinição da senha de membro da equipe.
  - Redefinição das senhas de todos os membros da equipe.
  - Bloqueio ou desbloqueio de membros da equipe por meio da desabilitação da verificação em dois passos.
  - Habilitação ou desabilitação do SSO (logon único).

- Transformação do acesso à conta por meio de SSO (logon único) obrigatório.
- Alteração ou remoção da URL do SSO (logon único).
- Atualização do certificado SSO (logon único).
- Alteração do modo de identidade SSO (logon único).

- ***Participação na equipe***
  - Bloqueio ou desbloqueio de usuários por meio de solicitação para juntar-se à equipe baseada em domínio de conta.
  - Definição de que solicitações de participação na equipe sejam automaticamente aprovadas ou exijam aprovação do administrador.

- ***Gerenciamento de conta de membro***
  - Alteração do nome do membro da equipe.
  - Alteração do endereço de e-mail de um membro da equipe.
  - Geração ou remoção de status de administrador, ou alteração da função de administrador.
  - Conexão ou desconexão como membro da equipe.
  - Transferência ou exclusão dos conteúdos de uma conta de membro removida.
  - Exclusão permanente do conteúdo de uma conta de membro removida.

- ***Configurações de compartilhamento globais***
  - Bloqueio ou desbloqueio de membros da equipe por meio de adição de pastas compartilhadas cujos proprietários são pessoas que não pertencem à equipe.
  - Bloqueio ou desbloqueio de membros da equipe por meio de pastas compartilhadas com pessoas que não pertencem à equipe.
  - Ativação dos avisos exibidos aos usuários antes que eles compartilhem pastas com pessoas que não pertencem à equipe.
  - Bloqueio ou desbloqueio de pessoas que não pertencem à equipe por meio de visualização de links compartilhados.
  - Definição de links compartilhados para ser somente equipe por padrão.
  - Bloqueio ou desbloqueio de pessoas por meio de comentários em arquivos.
  - Bloqueio ou desbloqueio de membros da equipe por meio da criação de solicitações de arquivo.
  - Adição, alteração ou remoção de um logo para páginas de link compartilhado.
  - Bloqueio ou desbloqueio de membros da equipe por compartilhar documentos do Paper e pastas do Paper com pessoas que não pertencem à equipe.

- ***Gerenciamento da pasta da equipe de arquivos***
  - Criação de pasta da equipe.
  - Renomeação de pasta da equipe.
  - Arquivamento ou desarquivamento de uma pasta da equipe.
  - Exclusão permanente de uma pasta da equipe.
  - Downgrade de uma pasta da equipe para uma pasta compartilhada.

- ***Gerenciamento de domínio***
  - Tentativa de verificação ou verificação de um domínio com sucesso, ou remoção de um domínio.
  - Verificação ou remoção de um domínio pelo Atendimento Dropbox.
  - Habilitação ou desabilitação de envio de convites de domínio.
  - Ativação ou desativação de "Convidar automaticamente novos usuários".
  - Alteração de modo de captura de contas.
  - O Atendimento do Dropbox concedeu ou revogou a captura de contas.
- ***Gerenciamento de mobilidade corporativa (EMM)***
  - Habilitação do EMM para o modo de teste (opcional) ou para o modo de implementação (obrigatório).
  - Renovação de token EMM.
  - Adição ou remoção de membros da equipe da lista de usuários EMM excluídos.
  - EMM desativado.
  - Criação de um relatório de lista de exceções EMM.
  - Criação de um relatório de uso do aplicativo móvel EMM.
- ***Alterações em outras configurações de equipe***
  - Equipes mescladas.
  - Upgrade da equipe para o Dropbox Business ou downgrade para uma equipe gratuita.
  - Alteração do nome da equipe.
  - Criação do relatório de atividade da equipe.
  - Bloqueio ou desbloqueio de membros da equipe que tenham mais de uma conta vinculada a um computador.
  - Permissão para criar grupos concedida a todos os membros da equipe ou apenas aos administradores.
  - Bloqueio ou desbloqueio de membros da equipe por meio de arquivos excluídos permanentemente.
  - Início ou conclusão de uma sessão de Atendimento Dropbox para um revendedor.

Grupos

Criação, exclusão e informações de associação a grupos.

- Criação, renomeação, movimentação ou exclusão de um grupo.
- Adição ou remoção de membro.
- Alteração do tipo de acesso a membros de um grupo.
- Alteração de grupo para gerenciado pela equipe ou pelo administrador.
- Alteração do ID externo de um grupo.

Registro de atividades do Paper

Administradores podem selecionar um tipo de atividade no Paper no feed da atividade ou baixar um relatório completo da atividade. Os eventos do Paper são registrados para:

- Habilitação ou desabilitação do Paper.
- Criação, edição, exportação, arquivamento, exclusão permanente e restauração de documento do Paper.
- Comentários e resolução de comentários do documento do Paper.
- Documento do Paper compartilhado e não compartilhado com membros da equipe e pessoas que não pertencem à equipe.
- Solicitações de acesso a documentos do Paper de membros da equipe e pessoas que não pertencem à equipe.
- Menções em documentos do Paper a membros da equipe e pessoas que não pertencem à equipe.
- Visualizações de documentos do Paper por membros da equipe e pessoas que não pertencem à equipe.
- Seguimento do documento do Paper.
- Alterações de permissão de membro de documentos do Paper (editar, comentar ou somente visualizar).
- Alterações na política de compartilhamento externo de documento do Paper.
- Criação, arquivamento e exclusão permanente de pastas do Paper.
- Documento do Paper adicionado ou removido de uma pasta.
- Renomeação da pasta do Paper.
- Transferências de documento e pasta do Paper.

Dropbox Passwords

O Dropbox Passwords é uma maneira simples e segura de armazenar, sincronizar e preencher automaticamente nomes de usuário, senhas e cartões de crédito e débito em vários dispositivos para proteção de suas credenciais on-line. O Dropbox Passwords protege seus nomes de usuário, senhas e cartões de crédito e débito de contas on-line confidenciais com criptografia de conhecimento zero na nuvem e em seus dispositivos. Nossos produtos são desenvolvidos para uso diário e são nativamente seguros.

Criptografia de conhecimento zero

O Dropbox Passwords armazena seus dados criptografados na nuvem, mas as chaves para descriptografá-los são armazenadas somente em seus dispositivos. **O Dropbox nunca tem acesso a essas chaves.** Elas são longas, aleatórias e geradas no seu dispositivo. Elas nunca saem do seu dispositivo, exceto quando você decide emparelhar ou registrar um novo dispositivo. Essa transferência usa criptografia de chave pública para assinar criptograficamente e proteger as chaves durante a transferência, para que você possa ter certeza de que ninguém mais poderá descriptografá-las, além de verificar que elas são autênticas. Essa propriedade é frequentemente chamada de criptografia de conhecimento zero porque os dados criptografados são inúteis para quem não tem as chaves, incluindo o Dropbox. Isso significa que **apenas você pode ver suas informações** e, no caso improvável de o Dropbox ser invadido, suas informações ainda estarão seguras. Os dados criptografados não ficam nas pastas visíveis do Dropbox e não podem ser acessados usando clientes ou APIs do Dropbox.

Detalhes da criptografia

O Dropbox criptografa seus dados usando XChaCha20-Poly1305 no modo combinado para autenticação implícita. Todas as nossas extensões de navegador e aplicativos móveis usam implementações de criptografia respaldadas pela biblioteca libsodium, que é uma derivação auditada e amplamente distribuída da biblioteca NaCl.

Cada operação de criptografia gera um nonce (número utilizado apenas uma vez) aleatório de 192 bits, que é armazenado com a carga criptografada para posterior descriptografia. Diferente do AES-GCM, o XChaCha20-Poly1305 tem compatibilidade com nonces aleatórios. Durante a descriptografia, o nonce de 192 bits é lido da carga e usado para descriptografar a carga criptografada. Qualquer criptografia subsequente gera um nonce aleatório de 192 bits independente do nonce anterior. O Dropbox Passwords gera números aleatórios usando a biblioteca libsodium, cujo padrão é um gerador de números aleatórios criptograficamente seguro em cada uma das plataformas compatíveis.

Chaves e palavras de recuperação

Geramos uma chave simétrica de 256 bits (a chave de criptografia) a partir de 128 bits de entropia (a chave do usuário) através do hash Blake2. Essa chave de criptografia permanece apenas nos dispositivos de seu proprietário e, sempre que possível, é armazenada no local mais seguro a que temos acesso nesses dispositivos. Por exemplo, em iPhones, a chave de criptografia é armazenada nas Chaves do iOS.

Usamos 128 bits de entropia como fonte porque oferece segurança suficiente enquanto exige apenas 12 palavras de recuperação usando o padrão BIP-39 para backup. O BIP-39 fornece uma maneira simples de representar chaves aleatórias grandes, transformando-as em uma lista de 12 palavras. Qualquer chave de 128 bits tem uma lista correspondente de palavras e cada lista de 12 palavras identifica exclusivamente 128 bits. A única ressalva é que as 12 palavras correspondem a 132 bits, então os quatro bits extras são usados como uma verificação de integridade para identificar erros. As palavras de recuperação fornecem uma maneira de recuperar sua chave de criptografia caso seu dispositivo seja perdido ou roubado. É recomendável imprimi-las e armazená-las em local seguro. Você também pode considerar entregá-las a um amigo ou familiar de confiança ou armazená-las em um pendrive.

Registro de dispositivo

Quando um usuário acessa o Dropbox Passwords em um novo dispositivo, esse dispositivo deve concluir um procedimento de registro seguro para ter acesso os dados do usuário no Passwords. Esse procedimento garante que a chave secreta do usuário e aos dados do Passwords sejam acessíveis apenas entre os dispositivos registrados do usuário. Garante também que um usuário só possa registrar dispositivos adicionais se tiver acesso a um dispositivo registrado existente ou a suas palavras de recuperação. O procedimento de registro do dispositivo ocorre da maneira a seguir.

Um novo dispositivo para registro gera aleatoriamente um par de chaves de dispositivo público/privado de 256 bits e envia a chave pública no servidor do Dropbox. Então, ocorre o cenário **A**, **B** ou **C**.

A: Se o usuário não tiver registrado um dispositivo, o dispositivo de registro vai gerar aleatoriamente uma chave secreta de usuário de 128 bits. Tanto a chave de usuário quanto o par de chaves do dispositivo são armazenados em um local seguro específico do sistema operacional, como descrito na seção Armazenamento de chaves a seguir. O dispositivo inicializa os dados do Passwords do usuário, os criptografa e envia a carga criptografada para o servidor do Dropbox.

B: Se o usuário tiver algum dispositivo registrado, uma solicitação de aprovação de registro será enviada para cada um desses dispositivos. A chave pública do dispositivo de registro é anexada à solicitação. O usuário deve então aprovar a solicitação em um de seus dispositivos registrados. Se aprovado, o dispositivo registrado criptografa a chave do usuário usando sua chave privada e a chave pública do dispositivo de registro via X25519 ECDH com XSalsa20-Poly1305. O dispositivo registrado envia a chave de usuário criptografada para o servidor do Dropbox para enviar ao dispositivo de registro. O dispositivo de registro baixa e descriptografa a chave do usuário usando sua chave privada e a chave pública do dispositivo registrado. O dispositivo de registro baixa os dados de carga criptografados do Passwords e os descriptografa com a chave do usuário.

C: Se o usuário tiver registrado um dispositivo, mas não conseguir mais acessá-lo, poderá inserir suas 12 palavras de recuperação para reconstruir localmente a chave do usuário. O dispositivo de registro baixa os dados de carga criptografados do Passwords e os descriptografa com a chave do usuário.

Armazenamento de chaves

Extensões do navegador

Nos navegadores da web, a chave do usuário é armazenada na área de armazenamento local da extensão do navegador. Os valores de armazenamento local da extensão do navegador são acessíveis somente pela própria extensão. Nenhum código em execução em sites visitados pelo usuário pode ler a área de armazenamento local da extensão do navegador. Além disso, as extensões do navegador não permitem a execução de nenhum código que não faça parte do pacote de extensão assinado, eliminando o risco de uma vulnerabilidade XSS que poderia acessar os valores de armazenamento local.

Um invasor com acesso irrestrito ao dispositivo do usuário pode acessar a chave do usuário lendo o arquivo de armazenamento local no disco. Exemplos dessas ameaças incluem: um invasor com acesso físico ao dispositivo ou um invasor executando malware mal-intencionado no dispositivo. Para se proteger contra esses cenários, o usuário pode configurar uma frase-senha do dispositivo local.

Quando uma frase-senha é configurada, a chave do usuário é criptografada em repouso no armazenamento local da extensão do navegador. A chave de criptografia deriva da frase-senha por meio do hash de senha Argon2 e o método de criptografia usado é o XChaCha20-Poly1305. Cada vez que a extensão do navegador é reiniciada, o usuário precisa fornecer sua frase-senha para descriptografar a chave do usuário e desbloquear seus dados. Com isso, um invasor sem a frase-senha não pode descriptografar a chave do usuário armazenada no arquivo de armazenamento local em disco.

iOS

No iOS, a chave do usuário é armazenada nas Chaves do iOS, que é um arquivo de banco de dados criptografado em disco. Este arquivo é criptografado com uma chave secreta que é armazenada no módulo de hardware Secure Enclave, usando o método de criptografia AES256-GCM. Somente o aplicativo assinado do Dropbox Passwords para iOS pode acessar os itens armazenados nas Chaves. Isso impede que outro código em execução no dispositivo do usuário acesse a chave do usuário.

Android

No Android, a chave do usuário é armazenada em um objeto EncryptedSharedPreferences, que é um arquivo de preferência criptografado no disco. Este arquivo é criptografado com uma chave mestra que é armazenada no hardware seguro Android Keystore, usando o método de criptografia AES256-GCM. Somente o aplicativo assinado do Dropbox Passwords para iOS pode acessar a chave mestra usada para descriptografar o arquivo de preferências.

Autenticação local

O Dropbox Passwords fornece medidas opcionais de autenticação local para restringir ainda mais o acesso aos dados do Passwords de um usuário em seu dispositivo físico. Para aplicativos móveis, o gesto de autenticação do sistema operacional local pode ser reutilizado (ou seja: um código com autenticação biométrica complementar). Para extensões de navegador, pode ser configurada uma frase-senha opcional. Esses mecanismos fornecem uma camada extra de segurança do aplicativo quando o sistema operacional do dispositivo do usuário é desbloqueado. Com isso, o usuário protege seus dados do Passwords quando outro usuário acessar seu dispositivo, como um membro da família ou colega de trabalho.

Sugestão de força de senha

O Dropbox construiu a ferramenta zxcvbn de código aberto que é usada por vários gerenciadores de senhas para avaliar a força de uma senha. A ferramenta compara senhas com um banco de dados de 30.000 senhas comuns, nomes e sobrenomes comuns de acordo com os dados do censo dos EUA, palavras em inglês populares na Wikipedia e em programas da televisão e filmes dos EUA e outros padrões comuns como datas, repetições (aaa), sequências (abcd), padrões de teclado (qwertyuiop) e Leet (1337) Speak (linguagem da internet). Se a senha que um usuário tentar inserir for comum, a ferramenta solicitará que ele insira algo mais exclusivo e difícil de adivinhar. Usar a configuração **Muito forte** garante o mais alto nível de segurança de conta para os usuários.

Segurança de dados, privacidade e transparência

Pessoas e organizações confiam seus trabalhos mais importantes ao Dropbox diariamente, e é nossa responsabilidade proteger e manter essas informações privadas.

Política de privacidade

Nossa política de privacidade está disponível em dropbox.com/privacy. A Política de privacidade do Dropbox, o Contrato de serviços, os Termos de serviço e a Política de uso aceitável incluem os seguintes termos:

- Que tipo de dados coletamos e o porquê.
- Com quem podemos compartilhar informações.

- Como protegemos esses dados e por quanto tempo os mantemos.
- Onde mantemos e transmitimos seus dados.
- O que acontecerá se houver alterações nas políticas ou se você tiver dúvidas.

Transparência

O Dropbox tem compromisso com a transparência ao lidar com solicitações judiciais de informações de usuários, assim como ao divulgar a quantidade e o tipo dessas solicitações. Examinamos todas as solicitações de dados para garantir que estejam em conformidade com a lei e temos o compromisso de notificar usuários quando suas contas são identificadas em uma solicitação legal, exceto quando proibido por lei.

Esses esforços ressaltam nosso compromisso de resguardar a privacidade de nossos usuários e seus dados. Para tanto, mantemos um relatório de transparência e estabelecemos um conjunto de Princípios de solicitação de dados pelo Governo. Os seguintes princípios regem nossas ações ao receber, examinar e responder a solicitações de dados de nossos usuários por parte do governo:

- ***Ser transparente***

  Para nós, os serviços on-line devem ter permissão para publicar o número e os tipos de solicitações recebidas do governo e para notificar as pessoas quando informações sobre elas forem solicitadas. Esse tipo de transparência capacita os usuários ajudando-os a entender melhor instâncias e padrões de alcance do governo. Continuaremos a publicar informações detalhadas sobre essas solicitações e defender o direito de fornecer mais dessas importantes informações.

- ***Recusar solicitações excessivamente abrangentes***

  As solicitações de dados por parte do governo devem ser limitadas a pessoas específicas e investigações legítimas. Recusaremos solicitações excessivamente abrangentes.

- ***Proteger todos os usuários***

  Leis que dão às pessoas proteções diferentes com base em onde elas vivem ou sua cidadania são antiquadas e não refletem a natureza global dos serviços on-line. Continuaremos a defender a reforma dessas leis.

- ***Oferecer serviços confiáveis***

  Os governos nunca deveriam instalar backdoors em serviços on-line ou comprometer a infraestrutura desses serviços para obter dados de usuários. Continuaremos nos esforçando para proteger nossos sistemas e mudar as leis a fim de deixar clara a ilegalidade desse tipo de atividade.

Nossos relatórios de transparência podem ser consultados em dropbox.com/transparency.

Certificações e atestados de privacidade e conformidade regulamentar

Todos os dias, pessoas e organizações confiam no Dropbox seus arquivos de trabalho mais importantes. Por causa disso, é nossa responsabilidade proteger esses arquivos e mantê-los privados. Nosso compromisso com a sua privacidade está no centro de todas as decisões que tomamos.

ISO/IEC 27018 (Código de práticas para proteção de dados pessoais na nuvem) e ISO/IEC 27701 (extensão para ISO/IEC 27001 e ISO/IEC 27002 para Gerenciamento de informações de privacidade)

O Dropbox Business foi um dos primeiros grandes provedores de serviço em nuvem a conseguir a certificação ISO/IEC 27018 e ISO/IEC 27701.

A ISO/IEC 27018 é uma norma global para privacidade e proteção de dados na nuvem e foi publicada em agosto de 2014 para abordar especificamente a privacidade do usuário e a proteção de dados.

A ISO/IEC 27701 é a primeira norma global certificável para gerenciamento de informações de privacidade e foi publicada em 2019 para fornecer uma estrutura para ampliar o sistema de gerenciamento de segurança da informação (ISMS) da ISO/IEC 27001 para um sistema de gerenciamento de informações de privacidade (PIMS), incluindo considerações de privacidade de dados.

A norma estabelece vários requisitos que dizem respeito ao modo como o Dropbox utilizará ou não os dados da sua empresa:

- ***Sua empresa está em controle de seus dados***

  Apenas utilizamos as informações pessoais que você nos fornece para lhe oferecer os serviços que assinou. Você pode adicionar, modificar ou excluir arquivos e documentos do Paper do Dropbox sempre que precisar.

- ***Trataremos seus dados com transparência***

  Trataremos seus dados com transparência. Vamos informar você sobre onde estão seus dados em nossos servidores. Também vamos lhe dizer quem são nossos parceiros de confiança. Vamos lhe contar o que acontece quando você encerra uma conta ou exclui um arquivo ou documento do Paper. Por fim, informaremos se qualquer um dos itens acima mudar.

- ***Seus dados estão seguros e protegidos***

  ISO/IEC 27018 e ISO/IEC 27701 foram desenvolvidas como aprimoramentos e extensões para ISO/IEC 27001, uma das normas de segurança de informações mais aceitas no mundo. Recebemos renovação da certificação ISO/IEC 27001 em outubro de 2021.

- ***Nossas práticas são revisadas regularmente***

  Como parte de nossa aderência às normas ISO/IEC 27018, ISO/IEC 27701 e ISO/IEC 27001, passaremos por auditorias anuais conduzidas por empresas independentes para manter essas certificações. Você pode ver nossas certificações ISO aqui.

Transferências de dados

Ao transferir dados da União Europeia, do Espaço Econômico Europeu, do Reino Unido e da Suíça, o Dropbox depende de uma variedade de mecanismos legais, como contratos com nossos clientes e afiliados, Cláusulas contratuais padrão e decisões de adequação da Comissão Europeia sobre determinados países, conforme aplicável.

O Dropbox está em conformidade com as Estruturas do Privacy Shield entre a União Europeia e os Estados Unidos e entre a Suíça e os Estados Unidos, conforme estabelecido pelo Departamento de

Comércio dos EUA em relação à coleta, uso e retenção de dados pessoais transferidos da União Europeia, do Espaço Econômico Europeu, do Reino Unido e da Suíça para os Estados Unidos, embora o Dropbox não utilize as Estruturas do Privacy Shield entre União Europeia e os Estados Unidos e entre a Suíça e os Estados Unidos como base legal para transferências de dados pessoais. O Dropbox assegurou ao Departamento de Comércio que está em conformidade com os Princípios do Privacy Shield no que diz respeito a tais dados. Para saber mais sobre o Privacy Shield, acesse https://www.privacyshield.gov.

Reclamações e disputas relacionadas à nossa conformidade com o Privacy Shield são investigadas e resolvidas através da JAMS, uma empresa terceira independente. Para saber mais, consulte nossa Política de privacidade (dropbox.com/privacy).

Regulamento Geral de Proteção de Dados (GDPR) da UE

O GDPR é um regulamento da União Europeia de 2018 que estabelece uma estrutura abrangente para o tratamento e proteção de dados pessoais.

O Dropbox está sempre comprometido com a segurança e proteção dos dados dos usuários, de acordo com as exigências legais e melhores práticas. De acordo com o nosso comprometimento com usuários, trabalhamos duro para garantir que o Dropbox está em conformidade com o GDPR, incluindo a nomeação de uma pessoa responsável pela proteção de dados, rearquitetando nosso programa de privacidade de forma a garantir que usuários possam exercer seus direitos de titulares de dados, documentando nossas atividades de processamento de dados e reforçando nossos processos internos no caso de violação de segurança. Continuamos fazendo ajustes para garantir que, à medida que novas orientações continuem a surgir por parte das autoridades de proteção de dados, nossos processos e práticas se adaptem ou excedam elementos específicos das novas regras.

Código de conduta da nuvem UE

O Código de conduta da nuvem (EU Cloud of Conduct) da UE é um instrumento voluntário que permite a um provedor de serviços em nuvem como o Dropbox demonstrar seu compromisso em relação à conformidade com o GDPR. Foi constatada a adesão do Dropbox Business, que é composto pelos planos para equipes Standard, Advanced, Enterprise e Education, ao Código de conduta na nuvem da UE e o Dropbox recebeu uma Marca de conformidade de "Nível 2", o que significa que esses serviços implementaram medidas técnicas, organizacionais e contratuais alinhadas aos requisitos do Código. Para mais informações sobre o Código de conduta da nuvem da UE e a conformidade do Dropbox com o código, visite o site oficial do Código.

Para mais informações sobre nossas práticas e políticas de privacidade, veja o whitepaper Privacidade de proteção de dados do Dropbox.

Conformidade

Existem vários requisitos regulatórios e específicos do setor para segurança e privacidade que sua organização pode ser obrigada a cumprir. Nossa abordagem é combinar as normas mais aceitas com medidas de conformidade voltadas para as necessidades específicas dos setores ou empresas dos nossos clientes.

ISO

A Organização Internacional para Padronização (ISO) desenvolveu uma série de padrões de classe mundial para segurança social e de informações para ajudar organizações a desenvolver produtos e serviços confiáveis e inovadores. O Dropbox certificou seus centros de processamento de dados, seus sistemas, seus aplicativos, suas equipes e seus processos por meio de uma série de auditorias conduzidas por uma empresa independente, a EY CertifyPoint, baseada nos Países Baixos. A EY CertifyPoint mantém suas certificações ISO a partir do Raad voor Accreditatie Comitê de Certificação Holandês).

ISO/IEC 27001 (Segurança da informação)

A certificação ISO/IEC 27001 é reconhecida como a principal norma de sistema de gerenciamento de segurança da informação (SGSI) no mundo. A norma também segue as melhores práticas de segurança detalhadas na certificação ISO/IEC 27002. Para que você continue a confiar em nosso trabalho, estamos contínua e amplamente gerenciando nossos controles físicos, técnicos e jurídicos na Dropbox.

Visualize o certificado ISO/ICE 27001 do Dropbox Business e do Dropbox Education.

ISO/IEC 27017 (Segurança na nuvem)

A certificação ISO/IEC 27017 é uma norma internacional para segurança da nuvem que fornece as diretrizes para controles de segurança aplicáveis à provisão e ao uso de serviços de nuvem. Os requisitos de segurança, privacidade e conformidade que o Dropbox e seus clientes podem solucionar juntos estão explicados em nosso Guia de Responsabilidade Compartilhada.

Visualize o certificado ISO/IEC 27017 do Dropbox Business e do Dropbox Education.

ISO/IEC 27018 (Privacidade da nuvem e proteção de dados)

A ISO/IEC 27018 é uma norma internacional para privacidade e proteção de dados que se aplica a prestadores de serviços em nuvem, como o Dropbox, que processam informações pessoais em nome de seus clientes e serve de base para nossos clientes lidarem com requisitos ou questões comuns de natureza regulatória e contratual.

Visualize o certificado ISO/IEC 27018 do Dropbox Business e do Dropbox Education.

ISO/IEC 22301 (Continuidade dos negócios)

A ISO/IEC 22301 é a norma internacional para a continuidade de negócios que orienta organizações sobre como diminuir a probabilidade de eventos disruptivos e solucioná-los de maneira adequada se eles ocorrerem, minimizando possíveis danos. O sistema de continuidade de negócios (BCMS) do Dropbox Business faz parte de nossa estratégia geral de gerenciamento de riscos que visa proteger pessoas e operações durante tempos de crise.

Visualize o certificado ISO/IEC 22301 do Dropbox Business e do Dropbox Education.

ISO/IEC 27701 (Gerenciamento de informações de privacidade)

A ISO 27701 é uma norma internacional para o gerenciamento de informações de privacidade. A norma fornece uma estrutura para melhorar e ampliar o sistema de gerenciamento da segurança da informação segundo a norma ISO 27001 a um PIMS (sistema de gerenciamento de informação de privacidade). O Dropbox Business e o Dropbox Education receberam essa certificação como Processador de PII.

Visualize o certificado ISO 27701 do Dropbox Business e do Dropbox Education.

SOC

Os Relatórios de Controles de Organização de Serviço (SOC), conhecidos como SOC 1, SOC 2 ou SOC 3, são modelos estabelecidos pelo Instituto Americano de Contadores Públicos Certificados (AICPA) para a geração de relatórios sobre os controles internos implementados dentro de uma organização. O Dropbox validou seus sistemas, seus aplicativos, suas equipes e seus processos por meio de uma série de auditorias conduzidas por uma empresa independente, a Ernst & Young LLP.

SOC 3 para Segurança, Confidencialidade, Integridade, Disponibilidade e Privacidade

O relatório de certificação SOC 3 abrange os cinco critérios de serviços de confiança: segurança, confidencialidade, integridade, disponibilidade e privacidade (TSP Seção 100). O relatório de uso geral do Dropbox é um resumo executivo do relatório SOC 2 e inclui a opinião do auditor independente sobre o design e sobre a operação eficaz de nossos controles.

Visualize a verificação do SOC 3 do Dropbox Business e o Dropbox Education.

SOC 2 para Segurança, Confidencialidade, Integridade, Disponibilidade e Privacidade

O relatório SOC 2 oferece aos clientes um nível detalhado de certificações baseadas em controles, abrangendo os cinco critérios de serviços de confiança: segurança, disponibilidade, integridade de processos, confidencialidade e privacidade (TSP Seção 100). O relatório SOC 2 inclui uma descrição detalhada dos processos do Dropbox e mais de 100 controles que temos preparados para proteger seus dados. Além da opinião de nosso auditor independente sobre o design e a operação eficaz de nossos controles, o relatório inclui os procedimentos e resultados de teste do auditor para cada controle. O relatório SOC 2 (às vezes denominado como relatório SOC2+) também inclui um mapeamento auditorado de nossos controles para as normas ISO mencionadas acima, fornecendo mais transparência a nossos clientes. A verificação do SOC 2 do Dropbox Business e do Dropbox Education está disponível mediante solicitação.

SOC 1/SSAE 18/ISAE 3402 (antigo SSAE 16 ou SAS 70)

O relatório SOC 1 oferece certificações específicas aos clientes que apontaram o Dropbox Business, Enterprise ou Education como um elemento chave do seu programa de controles internos na geração de relatórios financeiros (ICFR). Essas certificações específicas são usadas, primeiramente, para a conformidade Sarbanes-Oxley (SOX) de nossos clientes. A auditoria terceirizada é conduzida de acordo com o número 16 das Declarações de Participações de Certificações (SSAE 16) e a Norma Internacional sobre Participações de Certificação número 3402 (ISAE 3402). Essas normas substituíram a obsoleta Declaração sobre Normas de Auditoria número 70 (SAS 70). A verificação do SOC 1 para o Dropbox Business e Education está disponível mediante solicitação.

CSA

Aliança de Segurança da Nuvem: registro de segurança, confiança e certificação (CSA STAR)

O Registro de Segurança, Confiança e Certificação (STAR) do CSA é um registro gratuito acessível publicamente que oferece um programa de certificação de segurança para serviços de nuvem, assim ajudando usuários a avaliar a postura de segurança dos provedores de nuvem que eles atualmente usam ou estão pensando em contratar.

Tanto o Dropbox Business como o Dropbox Education receberam a certificação CSA STAR de nível 2 e a conformidade de nível 2. O nível 2 do CSA STAR exige uma avaliação independente terceirizada dos nossos controles de segurança pela EY CertifyPoint (para certificação) e da Ernst & Young LLP (para atestado), com base nos requisitos da norma ISO/IEC 27001, dos Critérios de Segurança de Serviços de Confiança SOC 2 e da Matriz de Controles da Nuvem CSA (CCM) versão 4.0.2.

Veja nossa certificação e conformidade CSA STAR de nível 2 no site da CSA

HIPAA/HITECH

O Dropbox assinará acordos de parceria comercial (BAAs) com clientes do Dropbox Business ou do Dropbox Education, que precisem deles para cumprir com a Health Insurance Portability and Portability Act (HIPAA - lei de Portabilidade e Responsabilidade de Seguros de Saúde) e a Health Information Technology for Economic and Clinical Health Act (HITECH - lei da Tecnologia de Informação da Economia e da Saúde Clínica). Consulte Dropbox e HIPAA/HITECH para mais informações.

O Dropbox disponibiliza um relatório de garantia terceirizado avaliando nossos controles das regras de segurança, privacidade e notificação de violação do HIPAA/HITECH, bem como um mapeamento de nossas práticas e recomendações internas para clientes que querem atender aos requisitos da Regra de privacidade e segurança do HIPAA/HITECH com o Dropbox Business ou o Dropbox Education.

Os clientes interessados em solicitar esses documentos ou saber mais sobre como adquirir o Dropbox Business ou o Dropbox Education podem entrar em contato com nossa equipe de vendas. Se você, no momento, é um administrador de equipe do Dropbox Business ou do Dropbox Education, é possível assinar eletronicamente um BAA por meio da página Conta, na seção de Administração.

Observe que o recurso de assinar um BAA eletrônico por meio da seção de Administração está disponível apenas aos clientes baseados nos EUA.

NIST 800-171

O NIST (National Institute of Standards and Technology, Instituto Nacional de Normas e Tecnologia) dos EUA promove e mantém normas e diretrizes para ajudar a proteger os sistemas de informação. A Publicação especial do NIST (SP) 800171 Revisão 2 (R2) fornece diretrizes sobre a proteção de CUI (Controlled Unclassified Information, informações não classificadas controladas) em sistemas e organizações de informações não federais. Qualquer entidade que processe ou armazene CUI do governo dos EUA, como instituições de pesquisa e o setor educacional, deve cumprir com o NIST SP 800-171 R2. Os sistemas, processos e controles de CUI do Dropbox foram validados por um auditor independente terceiro, Ernst & Young LLP.

O relatório NIST SP 800-171 R2 para o Dropbox Business e o Dropbox Education está disponível mediante solicitação por meio de nossa equipe de vendas ou atendimento (para clientes existentes do Dropbox Business).

Observe que o Dropbox Paper não está incluído neste escopo do relatório NIST SP 800-171 R2.

FERPA e COPPA (Estudantes e Crianças)

O Dropbox Business e o Dropbox Education permitem que clientes usem serviços em conformidade com as obrigações do fornecedor impostas pela Lei de Privacidade e Direitos de Educação da Família dos EUA (FERPA). As instituições educacionais com estudantes menores de 13 anos também podem usar o Dropbox Business ou o Dropbox Education consistente com a Lei de Proteção da Privacidade On-line de Crianças (COPPA), contanto que eles concordem com cláusulas contratuais específicas que exigem que a instituição obtenha a autorização dos pais em relação ao uso de nossos serviços.

FDA 21 CFR Parte 11

O Título 21 do CFR (Code of Federal Regulations, Código de Regulamentos Federais) rege alimentos e medicamentos nos Estados Unidos para o FDA (Food and Drug Administration), o DEA (Drug Enforcement Administration) e o Office of National Drug Control Policy. A Parte 11 do Título 21 estabelece os critérios segundo os quais o FDA considera os registros e assinaturas eletrônicas como confiáveis e, geralmente, equivalentes a registros em papel e assinaturas manuscritas executadas em papel.

Consulte nosso whitepaper do Dropbox e do FDA 21 CFR Parte 11 e o artigo da Central de ajuda para obter mais informações sobre como o Dropbox pode ajudar em seus esforços de conformidade com a 21 CFR Parte 11.

PCI DSS

O Dropbox está em conformidade com a Payment Card Industry Data Security Standard (PCI DSS). No entanto, o Dropbox Business, o Dropbox Education e o Dropbox Paper não podem ser usados para processar ou armazenar transações de cartão de crédito. O Atestado de Conformidade (AoC) do PCI para nosso status de comerciante está disponível mediante solicitação.

Para mais informações sobre a conformidade do Dropbox Business e o Dropbox Education, visite dropbox.com/business/trust/compliance.

Aplicativos para o Dropbox

A DBX Platform é composta por um ecossistema robusto de desenvolvedores que tomam como base nossa API flexível (Interface de programação de aplicativo). Mais de 750 mil desenvolvedores criaram aplicativos de serviços na plataforma para produtividade, colaboração, segurança, administração e muito mais.

Componentes pré-construídos

O Chooser, Saver e Embedder são componentes da web e de dispositivos móveis pré-construídos que permitem acesso fácil ao Dropbox em aplicativos/sites de terceiros com apenas algumas linhas de código.

- O Chooser permite a seleção de arquivos do Dropbox.
- O Saver permite que usuários salvem arquivos diretamente no Dropbox.
- O Embedder permite que os usuários visualizem arquivos e pastas do Dropbox.

A autorização para esses componentes é inteiramente por meio do Dropbox. Os aplicativos têm acesso a arquivos selecionados por meio de links compartilhados do Dropbox ou links de download de curta duração. Esses componentes pré-construídos podem ser usados de forma independente ou em conjunto com a API, como descrito abaixo.

Integrações à API do Dropbox Business

A API pública do Dropbox permite que desenvolvedores terceiros acessem e interajam com o Dropbox em seus aplicativos. Isso inclui interação de arquivos e metadados, compartilhamento e funcionalidade de equipe.

Autorização

O Dropbox usa o OAuth, protocolo padrão da indústria para autorização, para permitir que os usuários concedam aos aplicativos acesso à conta, sem expor suas credenciais. Temos compatibilidade com o OAuth 2.0 para autenticar as solicitações de API por meio do site ou dispositivo móvel do Dropbox. O Dropbox oferece suporte às melhores práticas do OAuth, incluindo tokens de acesso de curta duração e PKCE para aplicativos distribuídos.

Permissões de usuários

Os aplicativos que usam a API do Dropbox podem ser projetados com os seguintes níveis de acesso a conteúdo pelos usuário finais do Dropbox:

- ***Pasta de aplicativo.***
  Uma pasta exclusiva nomeada a partir do aplicativo é criada dentro da pasta de aplicativos do Dropbox de um usuário. O aplicativo recebe acesso de leitura e gravação apenas a essa pasta, e os usuários podem fornecer conteúdo ao aplicativo movendo arquivos para a pasta. Além disso, o aplicativo pode solicitar acesso a arquivo/pasta via Chooser ou Saver.

- ***Todo o Dropbox.***
  O aplicativo recebe acesso completo a todos os arquivos e pastas do Dropbox de um usuário, e também pode solicitar o acesso a um arquivo ou a uma pasta via Chooser ou Saver.

Os aplicativos também podem solicitar escopos específicos, restringindo seus comportamentos pelo acesso a subconjuntos de pontos de extremidade de API. Por exemplo, os aplicativos podem estar limitados ao acesso somente leitura de arquivos ou à capacidade de enviar conteúdo, mas não de criar compartilhamentos.

Permissões da equipe

Os administradores do Dropbox Business podem autorizar aplicativos para a funcionalidade de administração encontrada na seção de Administração da equipe. As ações que os aplicativos vinculados pela equipe podem executar são limitadas por meio de escopos, especificando quais configurações de equipe o aplicativo pode ler ou gerenciar.

Combinações comuns de escopos incluem:

- ***Informações da equipe***
  Informações somente leitura sobre a equipe e uso geral.

- ***Auditoria da equipe***
  Acesso somente leitura às informações da equipe e o registro de eventos detalhado.

- ***Acesso a arquivos de membros da equipe***
  A capacidade de executar ações em nome dos usuários da equipe, como gerenciar seus arquivos e suas pastas.

- ***Gerenciamento de membros da equipe***
  Adicionar e remover membros da equipe.

Webhooks

Os Webhooks são uma maneira para os aplicativos web obterem notificações em tempo real sobre alterações no Dropbox de um usuário. Depois que um URI é registrado para receber webhooks, uma solicitação HTTP é enviada para esse URI todas as vezes que ocorrer uma alteração em qualquer aplicativo registrado do usuário. Com o uso da API do Dropbox Business, os webhooks também podem ser usados para gerar notificações sobre alterações para membros da equipe. Muitos aplicativos de segurança usam webhooks para ajudar os administradores a controlar e gerenciar atividades da equipe.

Extensões

Os aplicativos podem registrar URIs de extensão, permitindo que as ações apareçam nos menus "Compartilhar" e "Abrir" na interface do usuário do Dropbox. As extensões permitem que os usuários iniciem fluxos de trabalho personalizados de terceiros diretamente de um arquivo em uma superfície do Dropbox. Quando uma ação é acionada, o Dropbox redireciona os usuários para o URI especificado, passando um identificador de arquivo que pode ser usado com a API para executar qualquer operação de arquivo. Um aplicativo precisa ser autorizado antes que uma extensão registrada seja visível ao usuário. Podemos promover um conjunto seleto de integrações de extensão nos menus "Compartilhar" e "Abrir", apesar de que esses aplicativos não terão acesso ao conteúdo até que o usuário autorize.

Diretrizes para desenvolvedor do Dropbox

Fornecemos uma série de orientações e práticas para ajudar os desenvolvedores a criar aplicativos API que respeitem e protejam a privacidade do usuário, ao mesmo tempo que melhoram a experiência dos usuários Dropbox.

- ***Chaves de aplicativos***

  Para cada aplicativo diferente que um desenvolvedor escreve, uma única chave de aplicativo do Dropbox deve ser usada. Além disso, caso um aplicativo forneça serviços ou software que envolvam a DBX Platform e outros desenvolvedores a usem, cada desenvolvedor deve registrar sua própria chave de aplicativo do Dropbox.

- ***Permissões do aplicativo***

  Os desenvolvedores recebem instruções para criar um aplicativo que use a permissão menos privilegiada possível. Quando um desenvolvedor envia um aplicativo para aprovação do status de produção, nós analisamos para garantir que o aplicativo não solicite permissões desnecessariamente amplas, com base na funcionalidade fornecida pelo aplicativo.

- ***Processo de revisão do aplicativo***

  - **Status de desenvolvimento**

    Quando um aplicativo da API do Dropbox é criado pela primeira vez, ele recebe o status de desenvolvimento. O aplicativo funciona da mesma maneira que qualquer aplicativo com status de produção, exceto pelo fato de que ele pode ser vinculado a no máximo 500 usuários do Dropbox. Assim que o aplicativo vincula 50 usuários do Dropbox, o desenvolvedor tem duas semanas para solicitar e receber a aprovação do status de produção, antes que a capacidade do aplicativo de vincular usuários adicionais do Dropbox seja congelada.

  - **Status de produção e aprovação**

    Para receber a aprovação do status de produção, todas as APIs de aplicativos devem aderir ao nosso manual de identidade visual para desenvolvedores e aos nossos Termos e condições, que incluem os usos proibidos da DBX Platform. Estes usos incluem: promover violação de IP ou de copyright, criar redes de compartilhamento de arquivos e fazer download de conteúdo ilegal. Em primeiro lugar, solicitamos dos desenvolvedores informações adicionais relacionadas à funcionalidade de seu aplicativo, e como o aplicativo usa a API do Dropbox, antes de enviar para revisão. Uma vez que o aplicativo é aprovado para status de produção, qualquer usuário do Dropbox pode se vincular a ele.

Administração de aplicativo de equipe

Dentro da seção de Administração da equipe, os administradores das equipes do Dropbox Business podem gerenciar os aplicativos vinculados e as integrações para sua equipe.

Parcerias de API

O Dropbox tem trabalhado em estreita colaboração com seus parceiros de tecnologia para permitir que desenvolvam integrações com seus pacotes de software mais conhecidos. Esses parceiros criam aplicativos usando APIs do Dropbox, trabalhando em conjunto com arquitetos do Dropbox para seguir as melhores práticas de segurança e experiência do usuário. Eles incluem uma variedade de aplicativos de produtividade do usuário final, bem como ferramentas de gerenciamento e segurança, como:

- ***Informações de segurança e gerenciamento de eventos (SIEM) e análise***

  Conecte sua conta do Dropbox Business ao SIEM e às ferramentas de análise para monitorar e avaliar o compartilhamento entre usuários, as tentativas de login, as ações administrativas e muito mais. Acesse e gerencie registros de atividade do funcionário e dados relevantes para a segurança por meio de sua ferramenta central de gerenciamento de registros.

- ***Prevenção de perda de dados (data loss prevention - DLP)***

  Varredura automática dos metadados e conteúdo de arquivos para acionar alertas, relatórios e ações quando houver mudanças importantes na sua conta do Dropbox Business. Aplique as políticas empresariais à implementação do seu Dropbox Business e atenda a requisitos regulatórios de conformidade.

- ***eDiscovery e Retenção legal***

  Responda a litígios, arbitragens e investigações regulatórias com dados de sua conta do Dropbox Business. Procure e reúna informações relevantes armazenadas eletronicamente e conserve seus dados por meio do processo de eDiscovery, poupando tempo e dinheiro.

- ***Gerenciamento de direitos digitais (digital rights management - DRM)***

  Adicione proteção de conteúdo de terceiros para dados confidenciais ou protegidos por copyright armazenados em contas de funcionários. Tenha acesso a recursos de DRM eficientes, incluindo criptografia do lado do cliente, impressão de marca d'água, trilhas de auditoria, revogação de acesso e bloqueio de usuário/dispositivo.

- ***Migração de dados e backup no local***

  Migre dados para o Dropbox de servidores existentes ou outras soluções baseadas na nuvem, economizando tempo, dinheiro e esforço. Faça backups automáticos de sua conta do Dropbox Business para servidores locais.

- ***Gerenciamento de identidade e SSO (logon único)***

  Automatize o processo de provisionamento e desprovisionamento e acelere a integração de novos funcionários. Agilize o gerenciamento e reforce a segurança integrando o Dropbox Business a um sistema de identidade existente.

- ***Fluxos de trabalho personalizados***

  Desenvolva aplicativos internamente que integrem o Dropbox em processos corporativos existentes para aprimorar os fluxos de trabalho.

Consulte a página Integrações do aplicativo Dropbox para uma lista desses parceiros de tecnologia. Usuários finais podem descobrir aplicativos e integrações de terceiros na Central de aplicativos.

Integrações do Dropbox

Também trabalhamos com alguns de nossos principais parceiros de tecnologia para criar integrações nas superfícies do Dropbox. Essas integrações mais profundas são desenvolvidas em conjunto pelo Dropbox e o parceiro. Incluindo:

Extensões do Dropbox

Essas integrações permitem que você use vários tipos de extensões de aplicativo para executar ações automaticamente, como publicar um vídeo, adicionar arquivos a e-mails e chats, enviar um arquivo para assinatura eletrônica e muito mais, diretamente do Dropbox. Esses aplicativos são criados pelo parceiro, enquanto o Dropbox facilita a descoberta de parceiros selecionados do Extension por meio dos menus "Abrir com" e "Compartilhar com".

Slack, Zoom e Trello

Essas integrações são criadas por equipes do Dropbox e permitem que os usuários iniciem conversas pelo Slack, comecem reuniões e criem tarefas tudo dentro do Dropbox. Usuários finais usam OAuth para acessar essas ferramentas.

Microsoft Office para dispositivos móveis e web

Com nossas integrações com o Microsoft Office, os usuários podem abrir arquivos do Word, do Excel e do PowerPoint armazenados no seu Dropbox, fazer alterações nos aplicativos Office para dispositivos móveis ou web e salvar essas alterações diretamente no Dropbox. Os usuários devem autorizar o acesso na primeira tentativa de abertura de um arquivo do Dropbox em cada aplicativo para dispositivos móveis ou web do Office. As inicializações subsequentes conservarão esses vínculos.

Adobe Acrobat e Acrobat Reader

Nossas integrações a versões móveis (Android e iOS) e de desktop desses aplicativos habilitam os usuários a visualizar, editar e compartilhar PDFs armazenados no Dropbox deles. Os usuários devem conceder acesso na primeira vez que tentam abrir um arquivo do Dropbox em cada aplicativo. Alterações nos arquivos PDF são salvas novamente de forma automática no Dropbox.

Resumo

O Dropbox Business oferece ferramentas fáceis de usar para ajudar equipes a colaborar efetivamente, fornecendo as medidas de segurança e certificações de conformidade que as empresas exigem. Com uma abordagem multicamadas que combina uma infraestrutura robusta de back-end com um conjunto personalizável de políticas, fornecemos às empresas uma solução poderosa que pode ser adaptada às suas necessidades específicas. Para saber mais sobre o Dropbox Business, entre em contato com nossa equipe de vendas em sales@dropbox.com.