Dropbox Business

Responsabilidade compartilhada: trabalhando juntos para manter seus dados seguros

O Dropbox trabalha com seus clientes do Business e do Dropbox Education para manter os dados deles seguros. Tomamos medidas amplas para proteger nossa infraestrutura, rede e aplicativos; treinamos colaboradores com práticas de segurança e privacidade; construímos uma cultura em que ser digno de confiança é a maior prioridade; e implementamos nossos sistemas e práticas por meio de testes e auditorias feitos por terceiros.

Embora o Dropbox seja responsável por proteger cada aspecto do serviço que está sob nosso controle, os clientes desempenham um papel importante em garantir que suas equipes e seus dados estejam protegidos e seguros. Como administrador de uma equipe do Dropbox Business ou do Dropbox Education, você consegue configurar, usar e monitorar a sua conta de forma a atender às necessidades de segurança, privacidade e conformidade da sua empresa.

Elaboramos esse guia para ajudá-lo a entender o que o Dropbox faz para manter sua conta segura e o que você pode fazer para manter a visibilidade e o controle sobre os dados da sua equipe.

Responsabilidades do Dropbox

Desenvolver a segurança em nossa arquitetura

Milhares de empresas no mundo todo confiam em nós para proteger seus arquivos mais importantes. Para ganhar essa confiança, trabalhamos duro para construir produtos seguros, nos quais administradores como você podem confiar. Aqui estão algumas das formas como protegemos a nossa arquitetura e nossas redes.

Arquitetura distribuída

A arquitetura do Dropbox distribui níveis de informação diferentes entre vários serviços. Isso não só torna a sincronização mais rápida e confiável, mas também melhora a segurança. A natureza da arquitetura do Dropbox garante que o acesso a qualquer serviço individual não será usado para recriar arquivos ou documentos do Paper.

Redes seguras

Mantemos um limite rígido entre a rede interna do Dropbox e a Internet pública. O tráfego entre a Internet e a rede de produção (quer o tráfego esteja entrando ou saindo) é cuidadosamente controlado através de um serviço de proxy dedicado, protegido por regras rígidas de firewall. O acesso ao ambiente de produção é restrito apenas a endereços de IP autorizados e exige múltiplas autenticações em todos os endpoints.

Criptografar dados do usuário

Os clientes do Dropbox Business e do Dropbox Education interagem com os nossos sistemas por meio de aplicativos em dispositivos móveis, desktop e web e APIs. Independentemente de qual aplicativo você usa, protegemos seu arquivo e documento do Paper, tanto em trânsito quanto em repouso.

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.

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 em repouso são criptografados usando o padrão de criptografia Advanced Encryption Standard (AES) de 256 bits. Os arquivos são armazenados em vários centros de dados em blocos de dados discretos. 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.

Manter um serviço confiável

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. Cópias redundantes de metadados são distribuídas por dispositivos independentes dentro de uma central de dados em pelo menos um modelo de disponibilidade N+2. Backups incrementais de metadados são executados de hora em hora, e backups completos a cada três dias. Os metadados são armazenados em servidores hospedados e gerenciados pelo Dropbox. Para armazenamento de blocos de arquivos, o Dropbox usa sistemas internos e de terceiros, desenvolvidos para fornecer uma durabilidade anual de dados de pelo menos 99,999999999%.

No caso raro de uma indisponibilidade de serviço, os usuários do Dropbox ainda terão acesso às cópias sincronizadas mais recentes de seus arquivos na pasta local do Dropbox, nos computadores vinculados. As cópias de arquivos sincronizados na pasta local/do cliente do Dropbox para desktop estarão acessíveis na unidade de disco rígido do usuário durante quedas ou interrupções do serviço, ou quando você estiver off-line.

Da mesma forma, 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.

Limitar o acesso do funcionário a sistemas de backend

Sabemos que quando você, como cliente do Dropbox Business ou do Dropbox Education, armazena seus arquivos e documentos do Paper no Dropbox, espera que nós nos responsabilizemos totalmente pelos seus dados. Como parte dessa responsabilidade, garantimos que o acesso do colaborador ao sistema interno do Dropbox seja controlado de forma rígida. Para iniciar, o acesso entre as nossas redes corporativa e de produção é extremamente limitado. 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. 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 gerente correspondente. A gerência manterá registro da solicitação de acesso, da justificativa e da aprovação, e o acesso será concedido pelas pessoas competentes.

Manter a atenção sobre a privacidade e a segurança do colaborador

Parte de manter nosso serviço seguro é garantir que as pessoas que trabalham com o Dropbox entendam como prestar atenção na segurança e reconhecer atividades suspeitas. Para isso, os colaboradores do Dropbox precisam adquirir políticas de segurança antes de receber o acesso aos sistemas. Os colaboradores também participam de treinamentos de segurança e privacidade obrigatórios para os novos contratados, treinamento de acompanhamento anual, e recebem treinamento regular de conscientização de segurança via e-mails informativos, palestras/apresentações e recursos disponíveis em nossa intranet.

Validar nossas práticas

Para ajudar a assegurar que nossas práticas de segurança estão funcionando como planejado, usamos terceiros para avaliar sua eficácia. Especialistas realizam testes periódicos de vulnerabilidade e penetração nos ambientes corporativo e de produção do Dropbox. Os problemas identificados são priorizados e corrigidos pela nossa equipe de engenharia de segurança. Além disso, auditores terceirizados avaliam nossas práticas de segurança em relação aos padrões internacionais e do setor. Para ajudá-lo a entender melhor as práticas do Dropbox e avaliá-las, disponibilizamos nosso relatório SOC 3 e os certificados ISO 27001, ISO 27017, ISO 27018 e ISO 22301 disponíveis on-line. Você também pode solicitar nosso relatório SOC 2, um relatório de avaliação e mapeamento dos requisitos HIPAA, uma avaliação BSI C5 e mapeamento (disponíveis em inglês e alemão), além de resumos dos resultados de testes de penetração, nos termos de um acordo de confidencialidade (NDA).

Comunicar problemas

Status do serviço

O Dropbox disponibiliza um site de terceiros que comunica o status do nosso serviço aos clientes do Dropbox Business e do Dropbox Education. Como cliente atual, você pode visitar status.dropbox.com a qualquer momento para visualizar o status do site atual, bem como interrupções e manutenção anteriores.

Notificação de violação

O Dropbox notificará você caso haja uma violação de dados, conforme exigido pela legislação aplicável. Nós mantemos políticas e procedimentos de resposta a incidentes, inclusive um processo de notificação de violação, que nos permitem notificar os clientes afetados conforme necessário. Se você celebrou um Acordo de parceiro comercial (Business Associate Agreement) HIPAA ou um Acordo de processamento de dados (Data Processing Agreement) da União Europeia, você será notificado conforme especificado nesses acordos.

Dar a você as ferramentas de que precisa para ficar em segurança

Queremos que você e outros administradores do Dropbox Business e do Dropbox Education tenham as ferramentas necessárias para tomar decisões responsáveis e esclarecidas sobre a segurança da sua equipe. Para ajudá-lo a configurar, usar e monitorar sua conta de forma que ela atenda às suas necessidades, seu Painel de controle de administração vem equipado com recursos de segurança para você habilitar em nome da sua equipe. Por meio de guias como este, nosso Whitepaper de Segurança do Dropbox Business, a Central de ajuda e nossa equipe de atendimento, fornecemos informações para que você possa entender como essas configurações podem ajudá-lo a configurar sua conta de maneira responsável.

Responsabilidades do cliente

Conhecer nossas práticas

Determinar se o Dropbox Business ou o Dropbox Education é a solução certa para as necessidades da sua empresa é um processo importante. Recomendamos que você reserve um tempo para validar nossas práticas, assim como faria com outro aplicativo. Para fornecer as ferramentas necessárias para que você verifique nossas práticas de segurança, nossos certificados ISO 27001, 27017, 27018 e 22301; o relatório de garantia SOC 3 e a Autoavaliação de nível 1 e a Certificação de Nível 2 CSA STAR estão disponíveis on-line. Também podemos fornecer acesso a documentação adicional nos termos de um acordo de confidencialidade, para ajudá-lo a tomar uma decisão embasada. Isso inclui nossos relatórios de avaliação SOC 1 e SOC 2, nosso relatório de avaliação C5 (disponíveis em inglês e alemão), um mapeamento de nossas práticas e recomendações internas para clientes que buscam atender aos requisitos da Regra de Segurança, Privacidade e Notificação de Violação HIPAA/HITECH, além de resumos de nossos testes de penetração mais recentes. Nossos Termos de serviços, nossa Política de uso aceitável e o Acordo comercial padrão estão disponíveis on-line para que você os analise e se certifique de que o Dropbox Business ou o Dropbox Education seja uma boa escolha para a sua equipe.

Configurar o compartilhamento e as permissões de visualização

O Dropbox Business e o Dropbox Education proporcionam flexibilidade para que você configure sua conta para respaldar suas necessidades de segurança, colaboração e privacidade. Os administradores podem revisar e modificar essas configurações por meio do Painel de controle de administração para refletir seu ambiente regulador ou de compartilhamento. Por exemplo, contas podem ser configuradas para que arquivos, pastas, links e documentos do Paper não possam ser compartilhados com pessoas fora da sua equipe. Quando os membros da equipe criam pastas compartilhadas para arquivos do Dropbox, eles podem personalizar ainda mais as configurações das pastas e escolher o nível de acesso adequado — edição ou somente visualização.

Reforçar a autenticação

Práticas de autenticação fortes ajudam a manter os dados da sua equipe seguros. Os administradores devem revisar as configurações de autenticação e permitir aquelas que sejam mais adequadas para proteger suas contas. As contas do Dropbox Business e do Dropbox Education incluem as seguintes opções:

Verificação em dois passos

Os administradores de equipe podem exigir que os membros usem a verificação em duas etapas para acessar suas contas. Esse recurso de segurança altamente recomendado adiciona uma camada de proteção extra às contas Dropbox dos usuários. Quando habilitado, o Dropbox exigirá um código de segurança de seis dígitos ou uma chave de segurança, além de uma senha durante o registro ou ao vincular um novo computador, telefone ou tablet.

SSO (logon único)

Se sua empresa já gerencia políticas e autenticação de senhas com um provedor de identidade central, configure o logon único para sua equipe do Dropbox Business e do Dropbox Education. Ao usar seu provedor SSO existente, os membros da sua equipe não precisam se lembrar de outra senha. Mais importante, a autenticação do acesso ao Dropbox será gerenciada por meio das mesmas políticas de senha de outros serviços na sua empresa.

Realizar revisões de acesso regulares

O acesso à conta da sua equipe deve evoluir à medida que a participação na equipe, funções internas e dispositivos mudem. Você deve verificar frequentemente para se certificar de que somente as pessoas, dispositivos e aplicativos devidos tenham acesso à sua conta para ajudar a manter suas informações nas mãos certas. Por meio do Painel de controle de administração, é fácil modificar ou remover o acesso.

Membros da equipe

Os membros da equipe podem ser facilmente adicionados, removidos e revisados no Painel de controle de administração. Para garantir que os dados confidenciais em sua conta do Dropbox Business ou do Dropbox Education só possam ser acessados pelas pessoas certas, recomendamos revisar esta lista com frequência. Você pode remover o acesso quando alguém sai da sua organização ou não precisa mais do acesso devido a uma alteração no cargo. De maneira semelhante, você pode modificar as funções dos membros da equipe no Painel de controle de administração para que cada conta de usuário tenha o nível de acesso adequado.

Dispositivos

Você e os membros da sua equipe devem revisar com frequência os dispositivos vinculados à sua conta e remover os que não são usados ou não estão autorizados. Os dispositivos podem ser desvinculados tanto por membros quanto por administradores da sua equipe. Você ou um membro da sua equipe também tem a opção de excluir remotamente o conteúdo do Dropbox do dispositivo ao desvinculá-lo. A desvinculação e exclusão de dispositivos podem manter seus dados seguros em caso de perda ou roubo ou caso alguém esteja saindo da sua equipe.

Aplicativos de terceiros

Há um robusto ecossistema de aplicativos de terceiros que você pode vincular à sua conta Dropbox Business ou do Dropbox Education para obter funcionalidade agregada. As integrações que oferecem serviços como SIEM, DLP e gerenciamento de identidade podem ser poderosas ferramentas para fortalecer suas práticas de segurança existentes. Embora essas integrações e aplicativos de terceiros possam ser ótimos complementos para a sua conta, é importante lembrar que eles não fazem parte dos nossos serviços. Portanto, eles não são abrangidos pelos Termos de Uso ou pelo Acordo Comercial do Dropbox, incluindo um Acordo de Parceiro Comercial (Business Associate Agreement - BAA) ou Acordo de Processamento de Dados, que você possa ter assinado com o Dropbox. Os aplicativos podem solicitar diversos níveis de acesso às suas informações dependendo da oferta de serviço deles. Como administrador, você pode vincular ou remover os aplicativos da equipe — aplicáveis a toda a sua conta — e remover aplicativos individuais que os membros da equipe possam ter adicionado à própria conta. O acesso e os aplicativos de terceiros podem ser revisados e modificados por meio do painel de controle de administração.

Monitorar atividades estranhas

Como administrador da equipe, você pode ver e exportar relatórios que detalham as atividades do administrador e os eventos, compartilhamento e autenticação de arquivos da sua equipe. Os administradores devem revisar esses relatórios de atividades regularmente para prestar atenção em qualquer atividade estranha e ajudar a manter sua equipe segura. Considere também usar um SIEM de terceiro ou outra integração de monitoramento para aprimorar seus recursos.

Determinar as necessidades de criptografia

Por padrão, o Dropbox armazena uma cópia local dos seus arquivos em seu computador para garantir que você tenha os arquivos necessários na ponta dos seus dedos. As cópias locais dos seus arquivos ficam tão protegidas quanto outros arquivos em seu computador. Para ajudar a mantê-las seguras, recomendamos que você habilite a criptografia de disco em seus dispositivos sempre que possível e exija uma senha forte para acessar seu laptop, telefone, tablet ou qualquer dispositivo que ofereça acesso à sua conta do Dropbox. Recomendamos o uso de senhas fortes e únicas nos seus dispositivos para proteger o acesso aos seus documentos no Paper.

O Dropbox protege os arquivos que você carrega em sua conta dividindo automaticamente esses arquivos em blocos discretos e criptografando cada bloco usando o padrão de criptografia Advanced Encryption Standard (AES) de 256 bits. Da mesma forma, o Dropbox protege documentos do Paper criptografando-os e deixando-os em repouso, no armazenamento persistente usando o padrão de criptografia Advanced Encryption Standard (AES) de 256 bits. O Dropbox gerencia as chaves de criptografia em nome dos nossos clientes para manter esse processo simples para usuários e para habilitar determinados recursos.

Os membros do Dropbox Business e do Dropbox Education também podem optar por criptografar arquivos antes de carregá-los no Dropbox por conta própria ou por meio de uma integração de terceiros. Contudo, os usuários que criptografam dados antes de carregá-los no Dropbox são responsáveis por gerenciar essas chaves de criptografia. Criptografar arquivos antes de carregá-los no Dropbox também pode reduzir a funcionalidade de alguns recursos.

Os clientes interessados em saber mais sobre como o Dropbox trata da segurança são convidados a analisar o Whitepaper de Segurança ou revisar nosso site: dropbox.com/business/trust. Para saber mais sobre o Dropbox Business ou o Dropbox Education e para solicitar relatórios de auditoria de terceiros nos termos de um acordo de confidencialidade, entre em contato com sales@dropbox.com.