# Beveiliging van Dropbox Business

Een whitepaper van Dropbox

Dropbox

# Inhoud

# Overzicht

In meerdere bedrijfstakken blijven digitale transformaties doorzetten en het is van vitaal belang dat gegevens, teams en apparaten overal worden beschermd. Organisaties die cloudoplossingen als Dropbox Business gebruiken om gedistribueerde workflows op afstand mogelijk te maken, moeten de samenwerking stroomlijnen, proactief risico's van de cloud beheren en effectieve controlemethoden implementeren om ervoor te zorgen dat intellectueel eigendom (IE), de integriteit van opgeslagen en gedeelde gegevens en de beschikbaarheid van gegevens via beheerde en robuuste cloudservices niet in het gedrang komt.

Meer dan 600.000 bedrijven en organisaties gebruiken Dropbox Business als dé oplossing waardoor gedistribueerde teams op afstand veilig kunnen samenwerken. De basisoplossing van Dropbox Business bestaat uit een smart workspace voor samenwerking en de mogelijkheid om bestanden te synchroniseren en delen. De ruggengraat van onze oplossingen? Een toonaangevende infrastructuur, functies voor geavanceerde beveiliging voor organisaties, beveiliging voor teams en content, elektronische handtekeningen, beveiligde overdracht en gegevensbeheer. Tenzij anders aangegeven, is de informatie in deze whitepaper van toepassing op alle producten van Dropbox Business (Standard, Advanced en Enterprise) en Dropbox Education. Paper is een functie van Dropbox Business en Dropbox Education.

Het Dropbox-vertrouwensprogramma, ons uitgebreide beveiligingsprogramma, vormt de basis van Dropbox Business. Bij dit programma wordt gebruikgemaakt van een gelaagde beveiliging, wat essentieel is in de ontwikkeling van op afstand werken.

In deze whitepaper lees je wat de beveiligingsmogelijkheden van Dropbox Business zijn, welke operationele beveiligingsmaatregelen Dropbox toepast, wat ons streven is op het gebied van privacy en transparantie, wat ons backendbeleid is en welke onafhankelijke certificeringen en maatregelen voor de naleving van richtlijnen Dropbox tot dé veilige oplossing maakt voor jouw organisatie.

***Tenzij anders aangegeven, is de informatie in deze whitepaper van toepassing op alle producten van Dropbox Business (Standard, Advanced en Enterprise) en Dropbox Education. Paper is een functie van Dropbox Business en Dropbox Education.***

# Onder de motorkap

Onze gebruiksvriendelijke interfaces worden ondersteund door een infrastructuur die achter de schermen zorgt voor snel en betrouwbaar synchroniseren, delen en samenwerken. Om dit voor elkaar te krijgen, zijn we voortdurend bezig ons product en onze architectuur zodanig te ontwikkelen dat de gegevensoverdracht sneller verloopt, de betrouwbaarheid steeds beter wordt en vlekkeloos kan worden gereageerd op veranderingen in de omgeving. In dit gedeelte leggen we uit hoe gegevens veilig worden verzonden, opgeslagen en verwerkt.

## Bestandsinfrastructuur

Dropbox-gebruikers kunnen op elk gewenst moment bestanden en mappen openen via onze desktop-, web- of mobiele client, of via toepassingen van derden die aan Dropbox zijn gekoppeld. Al deze clients zijn via beveiligde servers verbonden voor de toegang tot bestanden, het delen van bestanden met anderen en het bijwerken van gekoppelde apparaten wanneer bestanden worden toegevoegd, gewijzigd of verwijderd.

Het bestandsinfrastructuur van Dropbox bestaat uit de volgende componenten:

- ***Metadataservers***

  Bepaalde elementaire informatie over gebruikersgegevens die wordt aangeduid als metagegevens, wordt bewaard in een eigen afgezonderde opslagservice en fungeert als een index voor de gegevens in gebruikersaccounts. Metagegevens zijn onder meer basisgegevens over accounts en gebruikers, zoals e-mailadres, naam en namen van apparaten. Onder metagegevens vallen ook basisgegevens over bestanden, waaronder bestandsnamen en -typen, waarmee functies zoals versiegeschiedenis, herstel en synchronisatie worden ondersteund.

- ***Metagagevensdatabases***

  De metagegevens van bestanden worden opgeslagen in een transactionele sleutelwaardeopslag met multiversie gelijktijdigheidscontrole en worden naar behoefte gedeeld en gerepliceerd om aan de vereisten van prestatie en hoge beschikbaarheid te voldoen.

- ***Blokservers***

  Standaard biedt Dropbox een uniek beveiligingsmechanisme voor de bescherming van gebruikersgegevens dat verdergaat dan traditionele versleuteling. Blokservers verwerken bestanden uit de Dropbox-toepassingen door elk bestand op te splitsen in blokken, elk bestandsblok te versleutelen met een sterke coderingsmethode en alleen blokken te synchroniseren die tussen twee revisies in zijn aangepast. Wanneer een Dropbox-toepassing een nieuw bestand ontdekt of detecteert dat er iets aan een bestaand bestand is gewijzigd, brengt de toepassing de blokservers op de hoogte van die verandering en worden nieuwe of aangepaste bestandsblokken verwerkt en verzonden naar de blokopslagservers. Daarnaast worden blokservers gebruikt om bestanden en voorbeelden aan gebruikers te leveren. Zie het gedeelte Versleuteling hieronder voor meer informatie over de versleuteling die door deze services zowel tijdens verzending als in rust wordt gebruikt.

- ***Blokopslagservers***

  Het daadwerkelijke materiaal van bestanden van gebruikers wordt met deze blokopslagservers opgeslagen in versleutelde blokken.

  Voordat bestanden worden verzonden, worden ze door de Dropbox-client opgesplitst in bestandsblokken ter voorbereiding op opslag. De blokopslagservers fungeren als een CAS-systeem, wat staat voor Content-Addressable Storage, waarbij elk afzonderlijk versleuteld bestandsblok wordt opgehaald aan de hand van de hash-waarde.

- ***Voorbeeldservers***

  De voorbeeldservers produceren voorbeelden van bestanden. Voorbeelden geven het bestand van een gebruiker weer in een ander bestandsformaat dat meer geschikt is voor snelle weergave op het apparaat van een eindgebruiker. Voorbeeldservers halen bestandsblokken op uit de blokopslagservers om voorbeelden te genereren. Als er om een bestandsvoorbeeld wordt gevraagd, halen de voorbeeldservers het voorbeeld in de cache van de voorbeeldopslagservers op en sturen het naar de blokservers. Voorbeelden worden uiteindelijk door blokservers aan gebruikers getoond.

- ***Voorbeeldopslagservers***
  Voorbeelden in de cache worden in een versleuteld formaat opgeslagen in de voorbeeldopslagservers.

- ***Meldingsservice***
  Deze aparte service controleert of er al dan niet wijzigingen in Dropbox-accounts zijn aangebracht. Hier worden geen bestanden of metagegevens opgeslagen of verzonden. Elke client brengt een 'long poll'-verbinding tot stand met de meldingsservice en wacht. Bij een verandering aan een bestand in Dropbox geeft de meldingsservice een wijziging door aan de relevante client(s) door de long poll-verbinding te sluiten. Het sluiten van de verbinding is een signaal dat de client een veilige verbinding moet maken met de metagegevensservers om wijzigingen te synchroniseren.

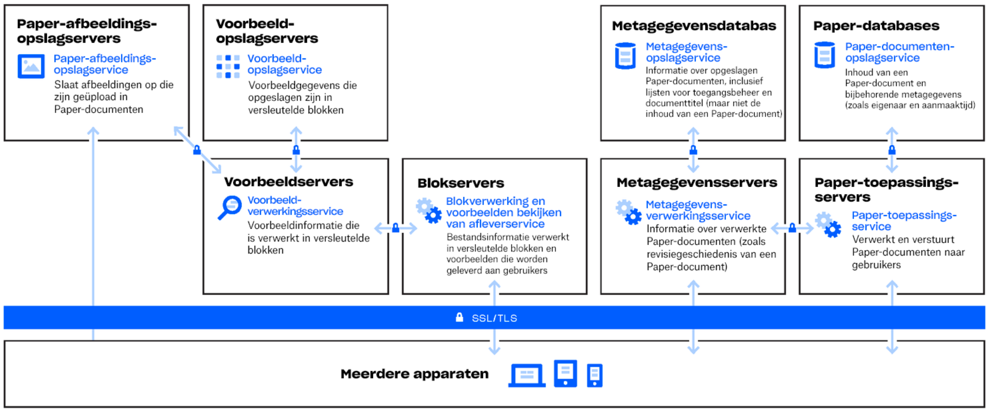
## Opslag van bestandsgegevens

Dropbox slaat voornamelijk twee soorten bestandsgegevens op: metagegevens over bestanden (zoals de datum en de tijd waarop een bestand voor het laatst is gewijzigd) en de daadwerkelijke inhoud van bestanden (bestandsblokken). De metagegevens van bestanden worden opgeslagen op de Dropbox-servers. De bestandsblokken worden in een van de volgende twee systemen opgeslagen: Amazon Web Services (AWS) of Magic Pocket, het eigen opslagsysteem van Dropbox. Magic Pocket bestaat uit bedrijfseigen software en hardware, en is vanaf de basis ontwikkeld om betrouwbaar en veilig te zijn. In zowel Magic Pocket als AWS zijn bestandsblokken versleuteld als er niets mee gebeurt, en beide systemen voldoen aan hoge betrouwbaarheidseisen. Zie het gedeelte Betrouwbaarheid hieronder voor meer informatie.

## Infrastructuur van Paper

Dropbox-gebruikers kunnen op elk gewenst moment Paper-documenten openen via onze desktop- of mobiele clients, of via toepassingen van derden die aan de Dropbox Paper-toepassing zijn gekoppeld. Al deze clients zijn via beveiligde servers verbonden voor de toegang tot Paper-documenten, het delen van documenten met anderen en het bijwerken van gekoppelde apparaten wanneer documenten worden toegevoegd, gewijzigd of verwijderd.

De infrastructuur van Dropbox Paper bestaat uit de volgende componenten:



- ***Paper-appservers***

  De Paper-toepassingsservers verwerken gebruikersverzoeken, retourneren de uitvoer van bewerkte Paper-documenten aan de gebruiker en voeren meldingsservices uit. Paper-toepassingsservers schrijven inkomende gebruikersbewerkingen naar de Paper-databases, waar ze in permanente opslag worden geplaatst. Communicatiesessies tussen de Paper-toepassingsservers en Paper-databases worden beveiligd met een Secure Hypertext Transfer Protocol (HTTPS).

- ***Paper-databases***

  De daadwerkelijke inhoud van Paper-documenten van gebruikers, evenals bepaalde metagegevens van deze Paper-documenten, worden gecodeerd in permanente opslag in de Paper-databases. Dit geldt voor informatie over een Paper-document (zoals de titel, eigenaar, aanmaaktijd en andere informatie) en de inhoud van het Paper-document zelf, waaronder opmerkingen en taken. De Paper-databases worden waar nodig opgesplitst en gerepliceerd om te kunnen voldoen aan de vereisten op het gebied van prestaties en hoge beschikbaarheid.

- ***Metadataservers***

  Voor Paper worden dezelfde metagegevensservers gebruikt als die worden beschreven in het diagram van de Dropbox-infrastructuur om informatie te verwerken over Paper-documenten, zoals de bestandsrevisiegeschiedenis van een Paper-document en wie er aan een gedeelde map kunnen werken. Dropbox beheert de metagegevensservers rechtstreeks. Deze staan in datacenters van derden.

- ***Metagagevensdatabases***

  Voor Paper worden dezelfde metagegevensservers gebruikt als die in het diagram van de Dropbox-infrastructuur om informatie te bewaren over Paper-documenten, zoals de bijbehorende deelrechten, machtigingen en mappen van een Paper-document en wie er aan een gedeelde map kunnen werken. Metagegevens van Paper-documenten worden opgeslagen in een MySQL-databaseservice en worden waar nodig opgesplitst en gerepliceerd om te kunnen voldoen aan de vereisten op het gebied van prestaties en hoge beschikbaarheid.

- ***Opslagservers voor Paper-afbeeldingen***

  Afbeeldingen geüpload naar Paper-documenten worden opgeslagen en in rust gecodeerd op de Paper-afbeeldingsopslagservers. Verzending van gegevens van afbeeldingen tussen de Paper-toepassing en de Paper-afbeeldingsopslagservers vindt plaats via een gecodeerde sessie.

- ***Voorbeeldservers***

  De voorbeeldservers produceren voorbeelden van afbeeldingen zowel voor afbeeldingen die naar Paper-documenten zijn geüpload als hyperlinks die in Paper-documenten zijn ingesloten. Voor afbeeldingen die naar Paper-documenten zijn geüpload, halen de voorbeeldservers via een gecodeerd kanaal afbeeldingsgegevens op die zijn opgeslagen in de Paper-afbeeldingsopslagservers. Voor hyperlinks die in Paper-documenten zijn ingesloten, halen voorbeeldservers de afbeeldingsgegevens op en geven een voorbeeld van de afbeelding weer met behulp van versleuteling zoals gespecificeerd door de bronlink. Voorbeelden worden uiteindelijk door blokservers aan gebruikers getoond.

- ***Voorbeeldopslagservers***

  Paper gebruikt dezelfde voorbeeldopslagservers als beschreven in het Dropbox-infrastructuurdiagram voor het opslaan van voorbeelden van afbeeldingen in de cache. Delen van voorbeelden in de cache worden in een versleuteld formaat opgeslagen in de voorbeeldopslagservers.

## Opslag van Paper-documenten

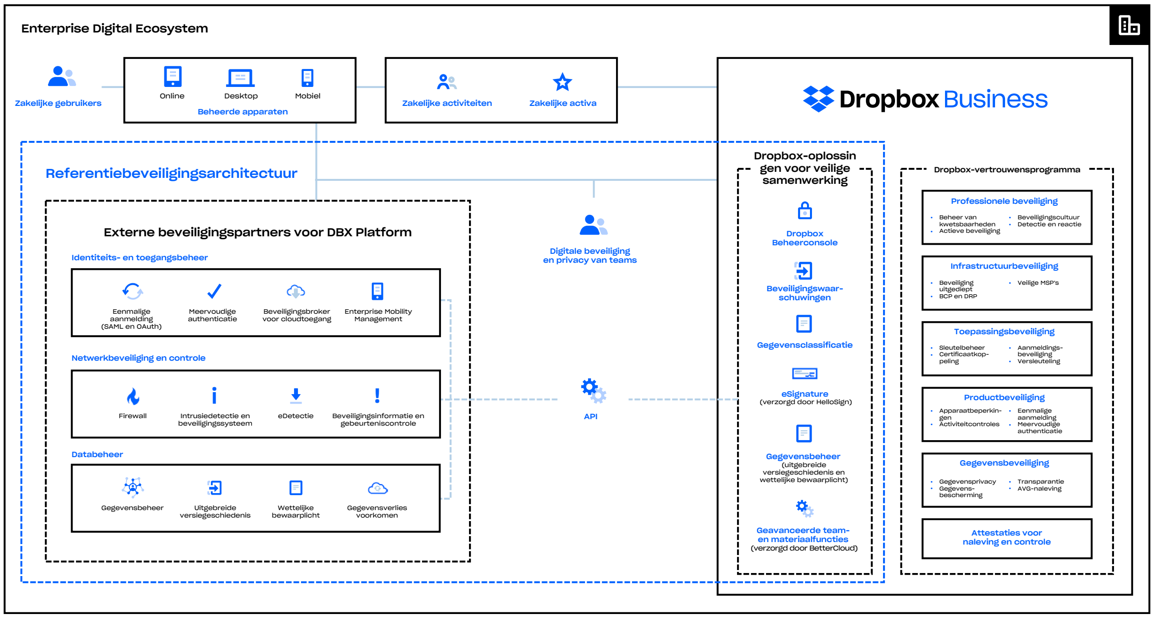
Dropbox bewaart voornamelijk de volgende gegevens in Paper-documenten: metagegevens over Paper-documenten (zoals gedeelde machtigingen van een document) en de daadwerkelijke inhoud van Paper-documenten die door de gebruiker zijn geüpload. Deze worden gezamenlijk Paper-documentgegevens genoemd en afbeeldingen die naar Paper-documenten zijn geüpload, worden Paper-afbeeldingsgegevens genoemd. Elk van deze gegevens wordt opgeslagen in Amazon Web Services (AWS). Paper-documenten worden in rust in AWS gecodeerd, wat voldoet aan hoge normen voor betrouwbaarheid. Raadpleeg het gedeelte Betrouwbaarheid hieronder voor meer informatie.

# Dropbox-vertrouwensprogramma

Vertrouwen is de basis van onze relatie met miljoenen mensen en bedrijven overal ter wereld. We waarderen het vertrouwen dat je in ons hebt en nemen de verantwoordelijkheid voor het beschermen van jouw informatie serieus. Om je vertrouwen te verdienen, hebben we Dropbox gebouwd met de nadruk op beveiliging, privacy, transparantie en naleving, en met dezelfde instelling blijven we eraan bouwen.

Het Dropbox-vertrouwensprogramma stelt een risicobeoordelingssysteem vast, dat is ontworpen om rekening te houden met milieurisico's, fysieke risico's, gebruikers, derden, toepasselijke wetten en regels, contractuele vereisten en diverse andere risico's die gevolgen kunnen hebben voor de veiligheid, vertrouwelijkheid, integriteit, beschikbaarheid of privacy van het systeem. Prestatiebeoordelingen vinden minimaal een keer per jaar plaats. Meer informatie over het Dropbox-vertrouwensprogramma vind je op: dropbox.com/business/trust.

We hanteren een meerlaagse aanpak om de handelingen, infrastructuur, toepassingen en producten die van invloed zijn op jouw organisatie te beveiligen.



# Professionele beveiliging

Dropbox heeft een kader voor informatiebeveiliging ontwikkeld waarin het doel, de richting, de beginselen en de basisregels zijn vastgelegd voor behoud van vertrouwen. Dit wordt gerealiseerd door een weging van de risico's en door de beveiliging, betrouwbaarheid, integriteit, beschikbaarheid en privacy van de Dropbox Business-systemen doorlopend te verbeteren. Op regelmatige basis evalueren en herzien we ons beveiligingsbeleid, bieden we beveiligingstrainingen, voeren we toepassings- en netwerkbeveiligingstests uit (inclusief penetratietests), controleren we de naleving van het beveiligingsbeleid, en voeren we interne en externe risicoanalyses uit.

## Ons beleid

We hebben een grondige reeks beveiligingsbeleidsregels opgesteld die worden afgedwongen door het beveiligings- en misbruikteam van Dropbox. Het beveiligingsbeleid wordt ten minste één keer per jaar geëvalueerd en goedgekeurd. Medewerkers, stagiair(e)s en ingehuurde krachten nemen deel aan een verplichte beveiligingstraining wanneer ze bij het bedrijf komen en daarna een doorlopende opleiding voor beveiligingsbewustwording ondergaan.

- ***Informatiebeveiliging***
  Gegevens van gebruikers en Dropbox veilig stellen en houden.
- ***Authenticatie***
  Hierin wordt beschreven hoe Dropbox-medewerkers zich authenticeren om toegang tot informatiesystemen en gegevens te krijgen.
- ***Apparaatbeveiliging***
  De minimale beveiligingsvereisten voor mobiele apparaten die worden gehanteerd voor toegang tot bedrijfsgegevens.
- ***Logisch toegangsbeheer***
  De toegang tot de Dropbox-systemen, -gebruikers en -gegevens beveiligd houden. Dit omvat de toegangscontrole tot zowel bedrijfs- als productieomgevingen.
- ***Gegevensbeveiliging***
  Hierin wordt beschreven hoe Dropbox de gegevens beschermt via specifieke vereisten voor opslag, toegang en gebruik.
- ***Reisbeveiliging***
  Hierin wordt beschreven wat Dropbox-medewerkers moeten doen voordat ze naar het buitenland reizen.
- ***Veiligheidsrichtlijnen voor verkoop- en klantervaring***
  Hiermee worden gebruikersgegevens veilig gehouden, worden onze medewerkers beschermd en bieden we onze gebruikers support.
- ***Fysieke beveiliging***
  Een veilige omgeving creëren voor mensen en eigendommen bij Dropbox.
- ***Fysieke veiligheidsrichtlijnen voor productie***
  Beheren van fysieke toegang tot productiefaciliteiten.

- ***Calamiteitenplan***

  Hierin staat uitgestippeld hoe Dropbox omgaat met gemelde gebeurtenissen rondom beveiliging, privacy en locaties en hierin worden ook voor elke gebeurtenis calamiteitenplannen vastgelegd.

- ***Ongeoorloofd auteursrechtelijk beschermd materiaal***

  Hiermee wordt het medewerkers verboden om ongeautoriseerd materiaal te bewaren op of te delen via Dropbox of Dropbox-systemen.

- ***Wijzigingsbeheer***

  Wijzigingen aan productiesystemen beheren. Bedoeld voor alle Dropbox-medewerkers, -contractanten en -stagiairs met toegang tot systemen.

- ***Privacy van gebruikersgegevens***

  Gebruikersinformatie en gebruikersgegevens bij Dropbox in overeenstemming met ons privacybeleid verwerken en beschermen.

- ***Beleid voor bedrijfscontinuïteit en crisismanagement***

  Hierin wordt het behoud, de bescherming en de veiligheid van mensen (Dropbox-medewerkers), eigendommen en (bedrijfs)processen beschreven.

- ***Privacyprogramma van Dropbox***

  Het doel, de principes en de verantwoordelijkheid rondom het privacyprogramma van Dropbox.

- ***Dropbox-vertrouwensprogramma***

  Hierin staat beschreven hoe Dropbox als bedrijf werkt en waarom het bedrijf betrouwbaar is.

- ***Beveiliging van betaalomgevingen***

  Onderhoud en beveiliging van de speciale betaalomgeving van Dropbox zodat betalingen met creditcards kunnen worden geaccepteerd.

## Medewerkersbeleid en toegang

Wanneer een Dropbox-medewerker in dienst wordt genomen, moet deze een achtergrondonderzoek ondergaan, ons beveiligingsbeleid en een geheimhoudingsverklaring ondertekenen, en een beveiligingstraining doorlopen. Alleen personen die deze procedure hebben doorlopen, krijgen fysiek en digitaal toegang tot het bedrijfs- en productienetwerk, wanneer dat vereist is om hun functie uit te oefenen. Daarnaast moeten alle medewerkers jaarlijks een beveiligingstraining afronden en krijgen ze regelmatig training op het gebied van beveiligingsbewustzijn via informatieve e-mails, bijeenkomsten en presentaties, en bronnen die via ons intranet worden aangeboden.

De toegang van medewerkers tot de Dropbox-omgeving wordt beheerd vanuit een centrale directory en geverifieerd op basis van een combinatie van sterke wachtwoorden, met een wachtwoord beveiligde SSH-sleutels en tweefactorauthenticatie. Externe toegang vereist het gebruik van een VPN dat met behulp van tweefactorauthenticatie is beveiligd. Speciale toegang wordt beoordeeld en gecontroleerd door het beveiligingsteam. Toegang tot zakelijke en productienetwerken is strikt beperkt op basis van gedefinieerde bedrijfsregels. De toegang tot het productienetwerk bijvoorbeeld vindt plaats op basis van een SSH-sleutel en wordt beperkt tot engineeringteams die uit hoofde van hun functie toegang moeten hebben. Firewallconfiguratie wordt streng gecontroleerd en is beperkt tot een klein aantal beheerders.

Daarnaast vereist ons interne beleid dat medewerkers met toegang tot productie- en ondernemingsomgevingen de best practices voor het maken en opslaan van privé-SSH-sleutels in acht nemen. Toegang tot andere bedrijfsmiddelen, waaronder datacenters, serverconfiguratietools, productieservers en ontwikkelingstools voor broncode, wordt toegekend na expliciete goedkeuring door het relevante management. Een dossier met het toegangsverzoek, de onderbouwing en de goedkeuring wordt door het management bijgehouden, en de toegang wordt verleend door hiervoor bevoegde mensen.

Dropbox werkt met technisch toegangsbeheer en hanteert een intern beleid dat medewerkers verbiedt willekeurig gebruikersbestanden te openen en dat de toegang tot metagegevens en andere informatie over gebruikersaccounts beperkt. Ter bescherming van de privacy en beveiliging van eindgebruikers heeft slechts een klein aantal engineers dat verantwoordelijk is voor de ontwikkeling van de Dropbox-kernservices, toegang tot de omgeving waar gebruikersbestanden zijn opgeslagen. Toegang die een medewerker heeft, wordt direct verwijderd zodra hij of zij uit dienst gaat.

In de gevallen waarin Dropbox fungeert als verlengstuk van de infrastructuur van onze klanten, kunnen zij erop vertrouwen dat wij hun gegevens verantwoordelijk beheren. Zie het gedeelte Privacy hieronder voor meer informatie.

## Beheer van kwetsbaarheden

Ons beveiligingsteam voert regelmatig geautomatiseerde en handmatige veiligheidstest en patchbeheer uit. Ze werken samen met externe specialisten om potentiële beveiligingsproblemen en fouten op te sporen en te verhelpen.

Als noodzakelijk onderdeel van ons beheersysteem voor informatiebeveiliging worden de bevindingen en aanbevelingen die voortvloeien uit al deze beoordelingsactiviteiten gerapporteerd aan het management van Dropbox en geëvalueerd. Vervolgens worden de noodzakelijke maatregelen genomen. Urgente problemen worden vastgelegd, opgevolgd en opgelost door geselecteerde beveiligingsmedewerkers.

### Wijzigingsbeheer

Bij alle processen rondom ontwikkeling, probleemoplossing en patches wordt ons formele beleid voor wijzigingsbeheer gevolgd dat is opgesteld door het Dropbox-engineeringteam om te waarborgen dat wijzigingen van het systeem zijn getest en geautoriseerd voordat deze worden geïmplementeerd in de productieomgevingen. Wijzigingen in de broncode worden geïnitieerd door ontwikkelaars die een verbetering willen aanbrengen aan de Dropbox-toepassing of -service. Wijzigingen worden opgeslagen in een versiebeheersysteem en moeten geautomatiseerde QA-testprocedures (Quality Assurance, kwaliteitsborging) doorlopen om te verifiëren dat aan alle beveiligingseisen is voldaan. Wanneer de QA-procedures zijn voltooid, kan de wijziging worden geïmplementeerd. QA-goedgekeurde wijzigingen worden automatisch geïmplementeerd in de productieomgeving. Onze Software Development LifeCycle (SDLC) vereist inachtneming van de richtlijnen voor veilig programmeren, evenals het screenen van wijzigingen in de code op mogelijke beveiligingsrisico's middels onze QA- en handmatige beoordelingsprocessen. Wijzigingen die in productie worden vrijgegeven, worden vastgelegd en gearchiveerd. Daarnaast worden waarschuwingen automatisch naar het team voor techniekbeheer van Dropbox verzonden.

Wijzigingen in de Dropbox-infrastructuur mogen uitsluitend worden aangebracht door geautoriseerd personeel. Het Dropbox-beveiligingsteam is verantwoordelijk voor het handhaven van de beveiliging van de infrastructuur en moet ervoor zorgen dat de server-, firewall- en andere beveiligingsgerelateerde configuraties bijgewerkt en in overeenstemming blijven met de geldende normen in de branche. De sets met firewallregels en de personen met toegang tot productieservers worden periodiek geëvalueerd.

## Scans en penetratietests van de beveiliging (intern en extern)

Ons beveiligingsteam voert regelmatig automatische en handmatige toepassingsbeveiligingstests uit om mogelijke beveiligingsproblemen en -fouten in onze desktopclient, webapp (Dropbox en Paper) en mobiele apps (Dropbox en Paper) op te sporen en te verhelpen.

Daarnaast huurt Dropbox externe leveranciers in om periodiek penetratietests en kwetsbaarheidstests uit te voeren in productieomgevingen. We werken samen met externe specialisten, andere beveiligingsteams in de branche en de community van beveiligingsonderzoekers om onze toepassingen veilig te houden. We zoeken ook naar kwetsbaarheden via geautomatiseerde analysesystemen. Voor dit proces gebruiken we systemen die we intern ontwikkelen, opensourcesystemen die we aanpassen aan onze behoeften en geautomatiseerde analyse door externe leveranciers.

## Schadelijk materiaal uit Dropbox weren

Via onze scanmogelijkheden streven we ernaar om de opslag en distributie in Dropbox van schadelijk materiaal te voorkomen. Voor onze scanners wordt gebruikgemaakt van onze eigen technologie en geavanceerde oplossingen van partners zoals Microsoft en Google. Zo wordt Dropbox een nog veiligere plek voor onze klanten.

## Premies voor bugs

We werken samen met professionele bedrijven voor penetratietests en voeren intern tests uit, maar we maken ook gebruik van de expertise van de beveiligingscommunity in het algemeen door premies voor softwarefouten (oftewel beloningen voor het melden van kwetsbaarheden) uit te loven. Onze premies voor softwarefouten vormen een stimulans voor onderzoekers om fouten in software op een verantwoorde manier op te sporen en bekend te maken. Door de community buiten ons bedrijf erbij te betrekken, profiteert ons beveiligingsteam van onafhankelijk onderzoek naar onze toepassingen, om onze gebruikers veilig te houden. We streven ernaar om een marktleider te zijn in premies, evenals in respons- en reparatietijden.

We hebben uiteengezet welke bijdragen voor bepaalde Dropbox-toepassingen in aanmerking komen, en een beleid voor verantwoorde openbaarmaking opgesteld, waarmee het ontdekken en melden van kwetsbaarheden en het verbeteren van de veiligheid voor de gebruiker worden bevorderd. Dit beleid bestaat uit de volgende richtlijnen:

- Vertel ons in detail over het beveiligingsprobleem.
- Ga verantwoordelijk om met onze bestaande applicaties. Spam sturen via formulieren met behulp van geautomatiseerde kwetsbaarheidscanners levert geen premie of beloning op, want die vallen nadrukkelijk buiten het beleid.
- Geef ons redelijk de tijd om op het probleem te reageren voordat je informatie over het beveiligingsprobleem publiekelijk bekendmaakt.
- Open of wijzig geen gebruikersgegevens zonder toestemming van de accounteigenaar.
- Bekijk, wijzig, bewaar en verstuur de gegevens niet, sla ze niet op en open ze op geen enkele andere wijze, maar verwijder lokale informatie direct nadat de kwetsbaarheid aan Dropbox is gemeld.
- Handel naar eer en geweten om overtredingen rondom privacy en de vernietiging van gegevens te voorkomen en onze services niet nadelig te beïnvloeden (waaronder Denial of Service).

Problemen kunnen worden gemeld door een rapport in te dienen bij Bugcrowd op: bugcrowd.com/dropbox.

## Fysieke beveiliging

### Infrastructuur

De fysieke toegang tot de faciliteiten van subdienstverleners waar de productiesystemen zich bevinden, is beperkt tot door Dropbox geautoriseerd personeel zoals vereist voor de uitoefening van hun functie. Iedereen die aanvullende toegang nodig heeft tot faciliteiten van de productieomgeving, krijgt die toegang pas na expliciete goedkeuring door het betreffende management.

Een dossier met het toegangsverzoek, de onderbouwing en de goedkeuring wordt door het management bijgehouden, en de toegang wordt verleend door hiervoor bevoegde personen. Nadat de goedkeuring is verkregen, neemt een bevoegd lid van het infrastructuurteam contact op met de desbetreffende subdienstverlener om toegang te vragen voor de goedgekeurde persoon. De subdienstverlener voert de gebruikersgegevens in het eigen systeem in en verleent het bevoegde Dropbox-personeel toegang via een badge en, indien mogelijk, via een biometrische scan. Zodra de toegang is verleend aan de goedgekeurde personen, is het de verantwoordelijkheid van het datacenter ervoor te zorgen dat de toegang beperkt wordt tot alleen die geautoriseerde personen.

## Bedrijfsvestigingen

- ***Fysieke beveiliging***

  Het fysieke beveiligingsteam van Dropbox is verantwoordelijk voor het handhaven van het beleid voor fysieke beveiliging en het toezien op de beveiliging van het kantoor.

- ***Bezoekers en toegangsbeleid***

  Fysieke toegang tot faciliteiten van de onderneming (anders dan openbare ingangen en lobby's) is beperkt tot geautoriseerd Dropbox-personeel en geregistreerde bezoekers die worden vergezeld door Dropbox-personeel. Een toegangssysteem via badges garandeert dat alleen geautoriseerde personen toegang kunnen krijgen tot beperkte gebieden binnen faciliteiten van de onderneming.

- ***Servertoegang***

  Toegang tot plekken waar bedrijfsservers en netwerkapparatuur staan is beperkt tot geautoriseerd personeel via oplopende rollen die worden verleend middels het systeem voor badgetoegang. De lijst met mensen die zijn geautoriseerd voor fysieke toegang tot de productieomgevingen van de onderneming wordt minstens eenmaal per kwartaal beoordeeld.

## Calamiteitenplan

We hebben calamiteitenplannen en procedures om problemen met de beschikbaarheid, integriteit, beveiliging, privacy en vertrouwelijkheid van de service op te vangen. Als onderdeel van onze procedures voor incidentrespons hebben we toegewijde teams die zijn opgeleid om het volgende te doen:

- Snel reageren op waarschuwingen van mogelijke incidenten.
- De ernst van het incident bepalen.
- Waar nodig maatregelen voor risicobeperking en indamming uitvoeren.

- Communiceren met relevante interne en externe betrokkenen, inclusief een melding aan betrokken klanten, om te voldoen aan contractuele verplichtingen voor het melden van incidenten en om de wet- en regelgeving op dit gebied na te leven.
- Bewijs verzamelen en bewaren voor onderzoek.
- Een nabespreking documenteren en een permanent diagnoseplan ontwikkelen.

De regels en processen van ons calamiteitenplan zijn gecontroleerd in onze veiligheidsbeoordelingen voor onder meer SOC 2 en ISO/IEC 27001.

# Infrastructuurbeveiliging

## Netwerkbeveiliging

Dropbox handhaaft zorgvuldig de beveiliging van ons back-endnetwerk. Onze netwerkbeveiligings- en bewakingstechnieken zijn ontworpen om verschillende beveiligings- en verdedigingslagen te bieden. We maken gebruik van algemeen in de branche aanvaarde beschermingstechnieken, waaronder firewalls, scans van kwetsbaarheden in het netwerk, bewaking van de netwerkbeveiliging en indringingsdetectiesystemen om te garanderen dat alleen verkeer dat daarvoor in aanmerking komt onze infrastructuur kan bereiken.

Het interne privénetwerk van Dropbox is gesegmenteerd naar gebruik en risiconiveau. De belangrijkste netwerken zijn:

- DMZ voor het internet
- DMZ voor de prioriteitsinfrastructuur
- Productienetwerk
- Ondernemingsnetwerk

De productieomgeving is uitsluitend toegankelijk voor geautoriseerde IP-adressen en meervoudige authenticatie is vereist op alle eindpunten. IP-adressen met toegang worden gekoppeld aan het ondernemingsnetwerk of bevoegd Dropbox-personeel. Geautoriseerde IP-adressen worden ieder kwartaal geëvalueerd om een veilige productieomgeving te garanderen. Het aanpassen van de lijst met IP-adressen is beperkt tot geautoriseerde personen.

Verkeer van internet naar ons productienetwerk wordt beveiligd met meerdere lagen firewalls en proxy's.

Er wordt een strikte scheiding gehandhaafd tussen het interne Dropbox-netwerk en openbaar internet. Er wordt zorgvuldig toegezien op het internetverkeer van en naar het productienetwerk via een speciaal daarvoor ingerichte proxyservice, die op zijn beurt weer wordt beschermd door restrictieve firewallregels.

Dropbox gebruikt geavanceerde toolsets om laptops en desktops met Mac- en Windows-besturingssystemen en productiesystemen te bewaken en schadelijke gebeurtenissen te herkennen. Beveiligingslogboeken worden op een centrale locatie verzameld voor forensisch onderzoek en incidentenbestrijding, volgens het standaardbeleid in de branche voor het bewaren van gegevens.

Dropbox spoort risico's op en neemt die zoveel mogelijk weg door het regelmatig testen van de netwerkbeveiliging en het laten uitvoeren van audits door zowel speciale interne beveiligingsteams als externe beveiligingsdeskundigen.

### Aanwezigheidspunten (PoP's, Points of Presence)

Dropbox gebruikt externe content delivery networks (CDN's) en door Dropbox gehoste aanwezigheidspunten (PoP's) op 31 locaties verspreid over de wereld om de websiteprestaties voor gebruikers te optimaliseren. Op deze locaties worden geen gebruikersgegevens in het cachegeheugen gezet en alle overgedragen gebruikersgegevens worden versleuteld met SSL/TLS. De fysieke en logische toegang tot door Dropbox gehoste aanwezigheidspunten is beperkt tot uitsluitend geautoriseerd Dropbox-personeel. Dropbox voert optimalisaties uit voor zowel de transportlaag (TCP) als de toepassingslaag (HTTP).

### Peering

Dropbox beschikt over een open peeringbeleid en alle klanten kunnen als peer met ons samenwerken. Voor meer informatie, ga naar dropbox.com/peering

## Betrouwbaarheid

Een opslagsysteem is zo goed als de betrouwbaarheid ervan. Daarom hebben we Dropbox ontwikkeld met verschillende redundantielagen om gegevensverlies te voorkomen en de beschikbaarheid te waarborgen.

### Metagegevens van bestanden

Redundante exemplaren van metagegevens worden verspreid over onafhankelijke apparaten in een datacenter volgens ten minste één N+2-beschikbaarheidsmodel. Incrementele back-ups worden minstens elk uur uitgevoerd en er worden elke 36 uur volledige back-ups gemaakt. Metagegevens worden opgeslagen op servers die worden gehost en beheerd door Dropbox in de Verenigde Staten.

### Bestandsblokken

Redundante exemplaren van bestandsblokken worden onafhankelijk opgeslagen op ten minste twee afzonderlijke geografische locaties en binnen elke regio betrouwbaar gerepliceerd. (**Opmerking:** voor klanten die ervoor kiezen om hun bestanden in onze Duitse, Australische, Japanse of Britse infrastructuur op te slaan, worden bestandsblokken alleen binnen hun respectieve regio's gerepliceerd. Raadpleeg voor meer informatie Datacenters en beheerde dienstverleners hieronder.) Zowel Magic Pocket als AWS zijn ontworpen voor een jaarlijkse duurzaamheid van gegevens van ten minste 99.999999999%.

De architectuur, toepassingen en synchronisatiemechanismen van Dropbox werken samen om gebruikersgegevens te beschermen en altijd beschikbaar te maken. Ook als de service niet online is, wat zelden gebeurt, hebben Dropbox-gebruikers toegang tot de laatste exemplaren van bestanden die in de lokale Dropbox-map op gekoppelde computers gesynchroniseerd zijn. Kopieën van bestanden die zijn gesynchroniseerd met de Dropbox-desktopclient/lokale map zijn beschikbaar op de harde schijf van de gebruiker tijdens uitvaltijd, storingen of als ze offline zijn. Wijzigingen in bestanden en mappen worden naar Dropbox gesynchroniseerd, zodra de service of verbinding weer is hersteld.

### Paper-documenten

Redundante exemplaren van Paper-documentgegevens worden verspreid over onafhankelijke apparaten in een datacenter volgens een N+1-beschikbaarheidsmodel. Daarnaast worden volledige back-ups van Paper-documentgegevens dagelijks uitgevoerd. Voor de opslag van Paper-documenten gebruikt Dropbox de AWS-infrastructuur in de Verenigde Staten die ontworpen is om een jaarlijkse duurzaamheid van gegevens van ten minste 99,999999999% te bieden. Mocht een service uitvallen, hebben gebruikers nog gewoon toegang tot de laatst gesynchroniseerde exemplaren van hun Paper-documenten in de offlinemodus in de mobiele toepassing.

### Bestandssynchronisatie

Dropbox biedt door de branche erkende, hoogwaardige bestandssynchronisatie. Onze synchronisatiemethoden zorgen voor snelle, responsieve bestandsoverdracht, zodat gegevens overal op allerlei apparaten beschikbaar zijn. Daarnaast is synchronisatie van Dropbox flexibel. In het geval van een storing in de verbinding met een Dropbox-service neemt een client de service ongemerkt over zodra de verbinding weer is hersteld. Bestanden worden alleen bijgewerkt op de lokale client als ze volledig zijn gesynchroniseerd en gevalideerd met de Dropbox-service. Door de verdeling van de belasting over verschillende servers wordt de redundantie en een consistente synchronisatie voor de eindgebruiker gegarandeerd.

### Delta-synchronisatie

Met deze synchronisatiemethode worden alleen de gewijzigde gedeelten van bestanden gedownload of geüpload. Dropbox slaat elk geüpload bestand op in aparte versleutelde blokken en werkt alleen de blokken bij die zijn gewijzigd.

### Streamingsynchronisatie

Bij streamingsynchronisatie wordt niet gewacht tot een bestand volledig is geüpload, maar wordt begonnen met het downloaden van gesynchroniseerde blokken naar een ander apparaat voordat alle blokken volledig naar het eerste apparaat zijn geüpload. Dit wordt automatisch toegepast wanneer aparte computers aan hetzelfde Dropbox-account zijn gekoppeld of als verschillende Dropbox-accounts een map delen.

### Ruimte op de harde schijf besparen

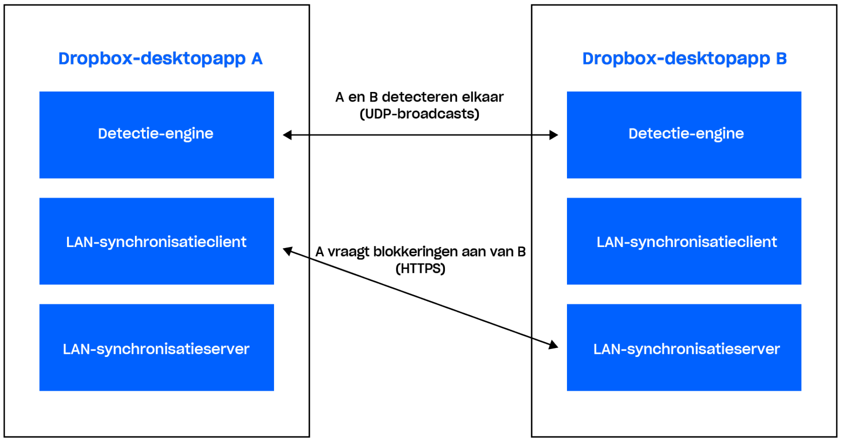
Gebruikers kunnen opslagruimte op hun computer vrijmaken door alleen de bestanden beschikbaar te maken waartoe ze op hun harde schijf of offline toegang willen hebben. Dit maakt opslagruimte op de computer vrij door alles alleen online te houden op dropbox.com.

### LAN-synchronisatie

Wanneer LAN-synchronisatie is ingeschakeld, downloadt deze functie nieuwe en bijgewerkte bestanden van andere computers die met hetzelfde LAN-netwerk (Local Area Network) zijn verbonden. Zo wordt er meer tijd en bandbreedte bespaard in vergelijking met het downloaden van de bestanden via de Dropbox-servers.

### Architectuur

Er zijn drie hoofdonderdelen van het LAN-synchronisatiesysteem die op de desktop-app draaien: de detectie-engine, de server en de client. Met de detectie-engine wordt naar systemen in het netwerk gezocht waarmee kan worden gesynchroniseerd. Dit is beperkt tot systemen die geautoriseerde toegang hebben tot dezelfde persoonlijke of gedeelde Dropbox-map(pen). De server verwerkt aanvragen van andere systemen in het netwerk en levert de aangevraagde bestandsblokken. De client vraagt bestandsblokken op van het netwerk.



## Detectie-engine

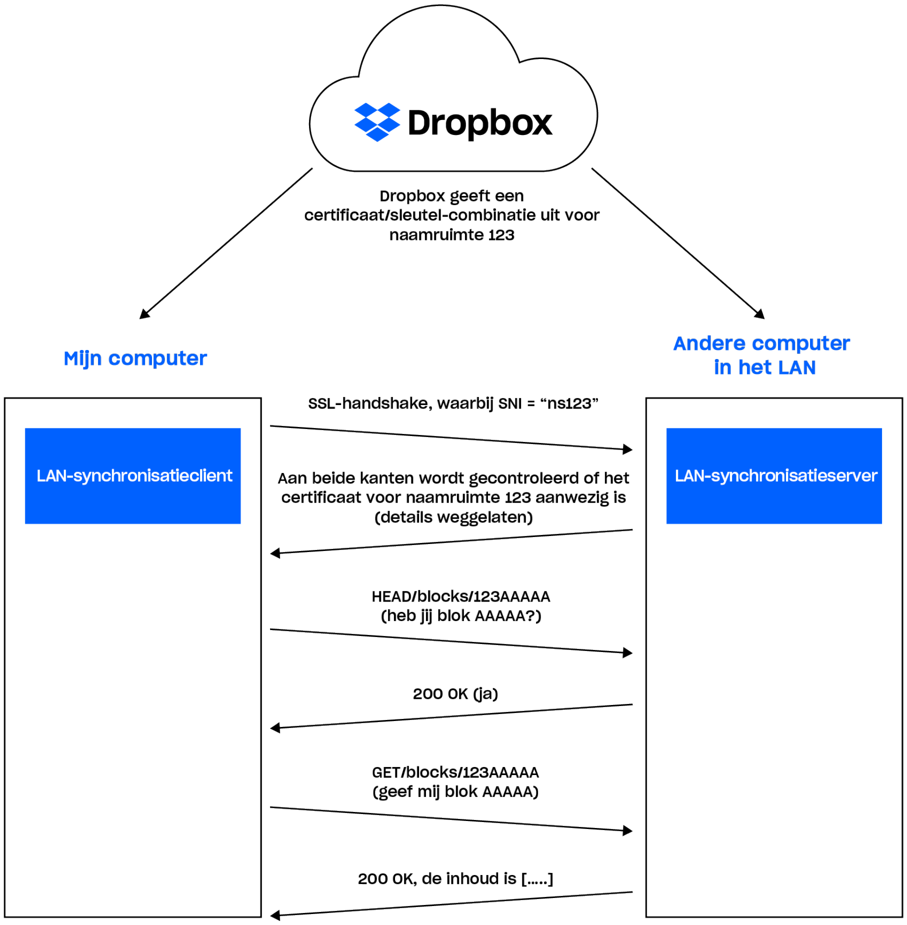
Elke machine binnen het LAN-netwerk verstuurt en ontvangt periodiek UDP-uitzendingspakketten via poort 17500 (deze poort is gereserveerd door IANA voor LAN-synchronisatie). Deze pakketten bevatten de versie van het protocol dat door de betreffende computer wordt gebruikt, de ondersteunde persoonlijke en gedeelde Dropbox-mappen, de TCP-poort die wordt gebruikt om de server uit te voeren (dit kan een andere poort zijn dan 17500 als deze niet beschikbaar is) en een willekeurige identificatie voor het systeem. Als een pakket wordt gedetecteerd, wordt het IP-adres van het systeem toegevoegd aan een lijst voor elke persoonlijke of gedeelde map, om zo een potentieel doel aan te geven.

## Protocol

De daadwerkelijke overdracht van bestandsblokken wordt via HTTPS gedaan. Elke computer voert een HTTPS-server met eindpunten uit. Een client controleert meerdere peers om te achterhalen of ze over de blokken beschikken, maar downloadt de blokken slechts via één server.

We zorgen ervoor dat alleen clients met de juiste machtigingen voor een specifieke map bestandsblokken kunnen aanvragen om zo al je gegevens veilig te houden. Daarnaast zorgen we ervoor dat computers zich niet kunnen voordoen als servers voor mappen die niet door deze computers worden beheerd. Als oplossing hiervoor genereren we SSL-sleutel/certificaatparen voor elke persoonlijke Dropbox of gedeelde map. Deze paren worden via de Dropbox-servers verzonden naar de computers van de gebruiker die zijn gemachtigd voor de map. De sleutel/certificaatparen rouleren wanneer het lidmaatschap wordt gewijzigd (bijvoorbeeld wanneer iemand uit een gedeelde map wordt verwijderd). Beide eindpunten van de HTTPS-verbinding moeten worden geverifieerd met hetzelfde certificaat (het certificaat voor de Dropbox-map of de gedeelde map). Zodoende kan worden aangetoond dat beide eindpunten van de verbinding zijn geverifieerd.

Bij het maken van een verbinding laten we de server weten met welke persoonlijke Dropbox of map we verbinding willen maken door gebruik te maken van servernaamindicatie (SNI), zodat de server het juiste certificaat gebruikt.



## Server/client

Aan de hand van het hierboven beschreven protocol hoeft de server alleen te weten welke blokken aanwezig zijn en waar deze te vinden zijn.

Op basis van de resultaten van de detectie-engine onderhoudt de client een lijst van peers voor elke persoonlijke Dropbox-map en gedeelde map. Wanneer het LAN-synchronisatiesysteem een aanvraag ontvangt om een bestandsblok te downloaden, stuurt dit systeem een aanvraag naar een willekeurig aantal peers dat is gedetecteerd voor de persoonlijke Dropbox of gedeelde map. Vervolgens wordt het blok aangevraagd via de eerste peer die laat weten dat deze over het blok beschikt.

Ter voorkoming van vertragingen gebruiken we verbindingspools om al actieve verbindingen opnieuw te gebruiken. Een verbinding wordt niet geopend tot deze nodig is en zodra een verbinding is geopend, houden we deze actief voor het geval we deze opnieuw nodig hebben. We beperken ook het aantal verbindingen met één peer.

Als een bestandsblok niet is gevonden of is gedownload, of als de verbinding te langzaam blijkt te zijn, valt het systeem terug op de Dropbox-servers om daar het blok op te halen.

## Datacenters en beheerde dienstverleners

De ondernemings- en productiesystemen van Dropbox bevinden zich in datacenters van externe subdienstverleners en providers van beheerde services op verschillende locaties in de Verenigde Staten. Minimaal eenmaal per jaar wordt geëvalueerd of de SOC-rapporten en/of beveiligingsvragenlijsten en contractuele verplichtingen van de datacenters van subdienstverleners voldoende beveiliging bieden. Deze externe serviceproviders zijn verantwoordelijk voor de fysieke, omgevings- en operationele beveiligingsmaatregelen aan de buitengrenzen van de Dropbox-infrastructuur. Dropbox is verantwoordelijk voor de logische, netwerk- en toepassingsbeveiliging van onze infrastructuur die zich in datacenters van derden bevindt.

Amazon Web Services (AWS) is onze provider van beheerde services voor verwerking en opslag en is verantwoordelijk voor de logische en netwerkbeveiliging van Dropbox-services die via de infrastructuur van deze provider worden geleverd. Verbindingen worden beschermd via de firewall van AWS, die is geconfigureerd in een standaard 'alles weigeren'-modus. Dropbox beperkt de toegang tot de omgeving tot een beperkt aantal IP-adressen en medewerkers.

### Infrastructuur in Duitsland, Australië, Japan en het Verenigd Koninkrijk

Dropbox biedt gekwalificeerde klanten opslag van bestandsblokken in regio's buiten de Verenigde Staten. Onze infrastructuur wordt gehost door Amazon Web Services (AWS) in Duitsland, Australië en Japan en wordt in de respectievelijke regio gerepliceerd om redundantie te garanderen en tegen gegevensverlies te beschermen. Metagegevens van bestanden worden in de Verenigde Staten opgeslagen op de eigen servers van Dropbox. Paper-documenten en voorbeelden worden altijd in de Verenigde Staten opgeslagen.

## Continuïteit van de bedrijfsvoering

Dropbox heeft een beheersysteem voor bedrijfscontinuïteit (BCMS, Business Continuity Management System) ontwikkeld om aan te geven hoe we de services aan gebruikers hervatten of voortzetten (en als bedrijf blijven functioneren) als bedrijfskritieke processen en activiteiten worden onderbroken. We voeren een cyclisch proces uit, bestaande uit de volgende fasen:

- ***Evaluaties van zakelijke impact en risico's***

  We voeren minstens één keer per jaar een evaluatie van de zakelijke impact (BIA, Business Impact Assessment) uit om voor Dropbox kritieke processen te identificeren, de potentiële impact van onderbrekingen te evalueren, prioriteitsperiodes voor herstel in te stellen, en onze kritieke afhankelijkheden en leveranciers te achterhalen. Daarnaast voeren we minstens één keer per jaar een bedrijfsbrede risico-evaluatie uit. Via de risico-evaluatie kunnen we op systematische wijze de risico's van verstorende incidenten voor Dropbox identificeren, analyseren en evalueren. Samen zorgen de risico-evaluatie en BIA ervoor dat er prioriteiten voor continuïteit kunnen worden gesteld, en strategieën voor risicobeperking en herstel kunnen worden ontwikkeld voor bedrijfscontinuïteitsplannen (BCP's).

- ***Bedrijfscontinuïteitsplannen***

  Teams die via de BIA worden geïdentificeerd als kritiek voor de continuïteit van Dropbox, gebruiken deze informatie om BCP's op te stellen voor hun kritieke processen. Deze plannen bieden de teams inzicht in wie er verantwoordelijk is voor het hervatten van processen in noodgevallen, wie in een ander Dropbox-kantoor of op een andere Dropbox-locatie de processen tijdens een onderbreking kan overnemen, en welke communicatiemethoden moeten worden gehanteerd tijdens een continuïteitsgebeurtenis. Deze plannen helpen ons ook voor te bereiden op verstorende incidenten via een centralisatie van onze herstelplannen en overige belangrijke informatie (zoals wanneer en hoe het plan moet worden ingezet, contact- en vergaderingsinformatie, belangrijke apps en herstelstrategieën). De continuïteitsplannen van Dropbox zijn gekoppeld aan ons bedrijfsbrede crisisbeheerplan (CMP, Crisis Management Plan), waarin de teams voor crisisbeheer en calamiteiten zijn vastgesteld.

- ***Plannen testen/uitvoeren***

  Dropbox test minstens één keer per jaar specifieke onderdelen van de bedrijfscontinuïteitsplannen. Deze tests sluiten aan op de reikwijdte en doelstellingen van de BCM's, zijn gebaseerd op toepasselijke scenario's, en zijn goed ontworpen met duidelijk gedefinieerde doelen. De tests kunnen variëren van oefeningen aan het bureau tot volledige simulaties van incidenten uit het echte leven. Op basis van de testresultaten en ervaringen die tijdens echte incidenten zijn opgedaan, worden de plannen door de teams bijgewerkt en verbeterd om problemen aan te pakken en de reactievaardigheden aan te scherpen.

- ***Beoordeling en goedkeuring van BCM's***

  De directie beoordeelt de BCM's minstens één keer per jaar als onderdeel van de beoordeling van het Dropbox-vertrouwensprogramma.

## Noodherstel

Er is een noodherstelplan aanwezig om de vereiste beveiliging van informatie te kunnen bieden tijdens een crisis of calamiteit die het functioneren van Dropbox Business bedreigt. Het technische team van Dropbox bekijkt dit plan jaarlijks en test geselecteerde elementen minstens elk jaar. Relevante bevindingen worden gedocumenteerd en opgevolgd tot er een oplossing is.

Ons noodherstelplan (DRP, Disaster Recovery Plan) betreft zowel noodgevallen gerelateerd aan duurzaamheid als noodgevallen gerelateerd aan beschikbaarheid. Deze noodgevallen worden als volgt gedefinieerd.

- Een noodgeval gerelateerd aan duurzaamheid bestaat uit een of meer van de volgende elementen:
  - Een volledig of permanent verlies van een primair datacenter waar metagegevens zijn opgeslagen of van meerdere datacenters waar bestandsblokken zijn opgeslagen.
  - Geen mogelijkheid meer om te communiceren of gegevens te leveren via een datacenter waar metagegevens zijn opgeslagen, of via meerdere datacenters waar bestandsinhoud is opgeslagen.
- Een noodgeval gerelateerd aan beschikbaarheid bestaat uit een of meer van de volgende elementen:
  - Uitval van langer dan tien dagen.
  - Geen mogelijkheid meer om te communiceren of gegevens te leveren via een opslagservice-/datacenter waar metagegevens zijn opgeslagen, of via meerdere opslagservice-/datacenters waar bestandsblokken zijn opgeslagen.

We definiëren een beoogde hersteltijd (RTO, Recovery Time Objective), de tijdsduur en het serviceniveau waarmee een bedrijfsproces of service moet worden hersteld na een noodgeval, en een beoogd herstelpunt (RPO, Recovery Point Objective), de maximale toegestane periode waarin gegevens verloren kunnen gaan tijdens een onderbreking van de service. Verder meten we ten minste eenmaal per jaar de werkelijke hersteltijd (RTA, Recovery Time Actual) tijdens het testen van noodherstel.

Het calamiteitenplan, het bedrijfscontinuïteitsplan en het noodherstelplan van Dropbox worden periodiek en na ingrijpende wijzigingen van de organisatie of de omgeving getest.

# Toepassingsbeveiliging

## Dropbox-gebruikersinterfaces

De Dropbox-service kan worden gebruikt en geopend via een aantal interfaces. Elk van deze interfaces is voorzien van beveiligingsinstellingen en -functies die de gebruikersgegevens beschermen, maar er tegelijkertijd voor zorgen dat ze gemakkelijk toegankelijk blijven.

- ***Web***

  Deze interface is toegankelijk via elke moderne webbrowser. Via de webinterface kunnen gebruikers bestanden uploaden, downloaden, weergeven en delen. Via de webinterface kunnen gebruikers ook bestaande lokale versies van bestanden openen via de standaardtoepassing van hun computer.

- ***Desktop***

  De Dropbox-desktopclient is een krachtige synchronisatieclient die bestanden lokaal opslaat voor offline toegang. Met de desktopclient krijgen gebruikers volledige toegang tot hun Dropbox-accounts. De client werkt op Windows- en Mac-besturingssystemen. Bestanden worden bekeken en kunnen direct worden gedeeld in de bestandsbrowsers van het besturingssysteem.

- ***Mobiel***

  De Dropbox-app is beschikbaar voor iOS- en Android-apparaten, zodat gebruikers ook onderweg toegang hebben tot al hun bestanden. Met de mobiele app kunnen gebruikers ook bestanden beschikbaar maken voor offline toegang.

- ***API***

  De Dropbox-API's bieden een flexibele manier om inhoud te lezen en te schrijven naar Dropbox-gebruikersaccounts. Ook bieden ze toegang tot geavanceerde functies zoals zoeken, revisies en herstel van bestanden. De API's kunnen worden gebruikt om de levenscyclus van een gebruiker te beheren voor een Dropbox Business-account, acties uit te voeren voor alle leden van een team, en toegang te verlenen tot de Dropbox Business-beheerfunctie.

## Paper-gebruikersinterfaces

De Paper-service kan worden gebruikt en benaderd via een aantal interfaces. Elk van deze interfaces is voorzien van beveiligingsinstellingen en -functies die de gebruikersgegevens beschermen, maar er tegelijkertijd voor zorgen dat ze gemakkelijk toegankelijk blijven.

- ***Web***

  Deze interface is toegankelijk via elke moderne webbrowser. Via de webinterface kunnen gebruikers Paper-documenten maken, weergeven, bewerken, downloaden en delen.

- ***Mobiel***

  De mobiele applicatie van Paper is beschikbaar voor mobiele iOS- en Android-apparaten en -tablets, waardoor gebruikers onderweg bij al hun Paper-documenten kunnen. De mobiele applicatie is gebouwd als een hybride applicatie die bestaat uit systeemeigen code (iOS of Android) in combinatie met een interne webviewbrowser.

- ***API***

  De hierboven beschreven Dropbox API bevat eindpunten en gegevenstypen voor het beheren van documenten en mappen in Dropbox Paper, inclusief ondersteuning voor functies zoals management van machtigingen, archivering en permanente verwijdering.

## Versleuteling

### Gegevens tijdens verzending

Voor de bescherming van gegevens tijdens verzending tussen Dropbox-apps en onze servers, gebruikt Dropbox SSL/TLS (Secure Sockets Layer / Transport Layer Security). Hiermee wordt een veilige tunnel tot stand gebracht die wordt beschermd door 128-bits AES-versleuteling (Advanced Encryption Standard) of hoger. Bestandsgegevens tijdens verzending tussen een Dropbox-client (momenteel desktop, mobiel, API of web) en de gehoste service worden versleuteld via SSL/TLS. Op dezelfde manier worden gegevens van Paper-documenten op doorvoer tussen een Paper-client (mobiel, API of web) en de gehoste services versleuteld via SSL/TLS. Voor de eindpunten die we beheren (desktop en mobiel) en moderne browsers, gebruiken we een sterke coderingsmethode en ondersteunen we Perfect Forward Secrecy en certificate pinning. Bovendien markeren we op internet alle authenticatiecookies als veilig en activeren we HTTP Strict Transport Security (HSTS) met includeSubDomains ingeschakeld.

**Opmerking:** Dropbox maakt uitsluitend gebruik van TLS en heeft het gebruik van SSLv3 omwille van bekende kwetsbaarheden gestaakt. Er wordt echter vaak met 'SSL/TLS' verwezen naar TLS en om die reden gebruiken we deze verwijzing ook in deze whitepaper.

Om zogenaamde attacker-in-the-middle-aanvallen te voorkomen, wordt de authenticatie van front-endservers van Dropbox uitgevoerd via openbare certificaten die door de client worden beheerd. Er wordt een versleutelde verbinding tot stand gebracht vóór de overdracht van bestanden of Paper-documenten, zodat ze gegarandeerd veilig worden afgeleverd bij de front-endservers van Dropbox.

### Gegevens in rust

Dropbox-bestanden geupload door gebruikers worden in rust versleuteld met de 256-bits Advanced Encryption Standard (AES). Bestanden worden in meerdere datacenters opgeslagen in afzonderlijke bestandsblokken. Elk blok wordt gefragmenteerd en versleuteld met een sterke coderingsmethode. Alleen blokken die tussen twee revisies in zijn aangepast, worden gesynchroniseerd. Paper-documenten in rust worden ook versleuteld met de 256-bits Advanced Encryption Standard (AES). Paper-documenten worden opgeslagen in meerdere beschikbaarheidszones met behulp van systemen van derden.

### Sleutelbeheer

De Dropbox-infrastructuur voor sleutelbeheer is ontworpen met operationele, technische en procedurele beveiligingstechnieken met zeer beperkte directe toegang tot sleutels. Het genereren, uitwisselen en opslaan van sleutels wordt verspreid uitgevoerd voor een gedecentraliseerde verwerking.

- ***Bestandsversleutelingssleutels***

  Standaard beheert Dropbox de bestandsversleutelingssleutels namens gebruikers om complexiteit tegen te gaan, geavanceerde productfuncties en een sterk cryptografisch beheer mogelijk te maken. Bestandsversleutelingssleutels worden gemaakt, opgeslagen en beschermd door de beveiligingsinstrumenten van de productiesysteeminfrastructuur en ons beveiligingsbeleid.

- ***Interne SSH-sleutels***

  De toegang tot productiesystemen wordt beperkt met unieke SSH-sleutelparen. Volgens de beveiligingsbeleidsregels en -procedures is bescherming van SSH-sleutels vereist. Een intern systeem beheert het uitwisselingsproces van openbare sleutels, en privésleutels worden veilig opgeslagen. Interne SSH-sleutels kunnen niet worden gebruikt om toegang te krijgen tot productiesystemen zonder een afzonderlijke tweede authenticatiefactor.

- ***Sleuteldistributie***

  Dropbox automatiseert het beheer en de distributie van vertrouwelijke sleutels naar systemen die zijn vereist voor de bedrijfsvoering.

## Certificate pinning

Dropbox biedt certificaatkoppeling in moderne browsers die de specificatie HTTP Public Key Pinning ondersteunen, en op onze desktop- en mobiele clients. Certificaatkoppeling is een extra controle om er zeker van te zijn dat de service waarmee je verbinding maakt, inderdaad de service is die je verwacht en niet van bedriegers is. We gebruiken dit om je te beschermen tegen andere manieren die handige hackers kunnen inzetten om je activiteiten te bespioneren.

## Bescherming van authenticatiegegevens

Dropbox gaat verder dan standaardhashing om de aanmeldgegevens van gebruikers te beschermen. Elk wachtwoord wordt conform de best practices uit de branche voorzien van een willekeurig gegenereerd, voor elke gebruiker uniek salt. Daarnaast gebruiken we iterative hashing om berekeningen te vertragen. Deze benaderingen vergroten de beveiliging tegen beveiligingsaanvallen, woordenboekaanvallen en rainbowaanvallen. Als extra beveiliging versleutelen we de hashes met een sleutel die buiten de database wordt opgeslagen om wachtwoorden veilig te houden in het geval van inbreuk op uitsluitend de database.

## Scannen op malware

We hebben een geautomatiseerd systeem ontwikkeld dat op malware scant op het moment dat materiaal buiten het account van de oorspronkelijke gebruiker wordt gedeeld. Het systeem maakt gebruik van zowel bedrijfseigen technologie als industriestandaard detectie-engines en is ontworpen om de verspreiding van malware tegen te houden.

# Productbeveiliging

Dropbox biedt beheerfuncties waarmee zowel de IT-afdeling als de eindgebruikers controle hebben en het inzicht krijgen, zodat ze hun bedrijf en gegevens effectief kunnen beheren. Met Dropbox heb je alles wat je nodig hebt voor je werk, je tools, inhoud en bijdragers, allemaal op één plek. Dropbox is meer dan veilige opslag: het is een slimme, naadloze manier om je bestaande workflow te optimaliseren.

Hieronder vind je een overzicht van functies die beschikbaar zijn voor beheerders en gebruikers, en integraties met andere software voor het beheer van essentiële IT-processen.

**Opmerking:** de beschikbaarheid van de functies verschilt per abonnement. Ga naar dropbox.com/business/plans voor meer informatie.

## Controle van de inhoud

Het beschermen van gevoelige bedrijfsmiddelen, zoals intellectueel eigendom en persoonlijk identificeerbare informatie (PII), is cruciaal voor IT- en gegevensbeveiligingsteams. Of het nu om aangepaste materiaalmachtigingen, gegevensretentiebeleid of wettelijke bewaarplicht gaat, Dropbox biedt toonaangevende oplossingen waarmee jij je materiaal kunt beheren, bewaken en beschermen. Hieronder vind je de belangrijkste producten en functies van Dropbox waarmee je materiaal kunt beheren.

### Aangepaste machtigingen voor materiaal en gedeelde bestanden en mappen

- ***Machtigingen voor gedeelde bestanden***

  Een teamlid dat eigenaar is van een gedeeld bestand kan de toegang voor specifieke gebruikers verwijderen en opmerkingen voor het bestand uitschakelen.

- ***Rechten voor gedeelde bestanden***

  Een teamlid dat eigenaar is van een gedeelde map kan de maptoegang voor specifieke gebruikers verwijderen, machtigingen voor bekijken/bewerken voor specifieke gebruikers wijzigen, en het eigendom van de map overdragen. Afhankelijk van de algemene machtigingen voor delen van het team, kan elke eigenaar van een gedeelde map ook bepalen of de map kan worden gedeeld met mensen buiten het team, of anderen met machtigingen voor bewerken lidmaatschappen kunnen beheren, en of links kunnen worden gedeeld met mensen buiten de map.

- ***Wachtwoorden voor gedeelde links***

  Elke gedeelde link kan via een door de gebruiker ingesteld wachtwoord worden beveiligd. Voordat een bestand of mapgegevens worden overgedragen, verifieert een toegangsbeheerlaag of het juiste wachtwoord is opgegeven en of er is voldaan aan alle andere vereisten (zoals een team-, groeps- of map-ACL). Als dit het geval is, wordt er een veilig cookie opgeslagen in de browser van de gebruiker om zo te onthouden dat het wachtwoord eerder is geverifieerd. Met besturingselementen voor delen kunnen beheerders ook standaardwachtwoorden instellen, in plaats van ze als optioneel te gebruiken, om de inhoud van hun team beter te beschermen.

- ***Vervaldatums voor gedeelde links***

  Gebruikers kunnen een vervaldatum instellen voor elke gedeelde link om tijdelijk toegang tot bestanden of mappen te verlenen. Met besturingselementen voor delen kunnen beheerders ook standaardverlooptijden instellen, in plaats van deze als optioneel te gebruiken, om de inhoud van hun team beter te beschermen.

### Paper-document en machtigingen voor delen van Paper-map

- ***Machtigingen voor Paper-documenten en gedeelde Paper-mappen***

  Een teamlid dat eigenaar is van een Paper-document of een gedeelde Paper-map kan de toegang voor specifieke gebruikers verwijderen en het bewerken van het Paper-document uitschakelen.

- ***Machtigingen voor Paper-documenten***

  Een teamlid dat eigenaar is van een Paper-document kan de toegang voor specifieke gebruikers die expliciet in het deelvenster verschijnen verwijderen. Zowel de eigenaar als de bewerkers van een Paper-document kunnen de machtigingen voor weergeven/bewerken voor specifieke gebruikers wijzigen en het koppelingsbeleid van het document wijzigen. Het koppelingsbeleid bepaalt welke gebruikers het document mogen openen en de machtiging die aan hen is verleend. De teambeheerder kan een teambrede beleidsinstelling voor koppelen en het delen van documenten instellen.

- ***Machtigingen voor Paper-mappen***

  Een teamlid dat lid is van de map kan het deelbeleid van de map wijzigen en de toegang voor specifieke gebruikers die expliciet aan de map zijn toegevoegd verwijderen.

## Handelingen rondom bestanden en mappen

- ***Teammappen voor bestanden***

  Beheerders kunnen teammappen maken waarin groepen en andere collega's automatisch het juiste toegangsniveau voor het benodigde materiaal hebben (alleen-lezen of bewerken).

- ***Aangepaste functies voor toegang en delen***

  Met functies voor delen kunnen beheerders lidmaatschappen en machtigingen op het hoogste niveau of op submapniveau beheren. Zo krijgen individuen en groepen binnen en buiten het bedrijf alleen toegang tot specifieke mappen.

- ***Teammapbeheerder***

  Beheerders kunnen vanuit een centraal punt al hun teammappen bekijken en beleidsregels voor delen aanpassen om te voorkomen dat vertrouwelijk materiaal onterecht wordt gedeeld.

- ***Gedeelde mappen voor Paper-documenten***

  Beheerders kunnen gedeelde Paper-mappen maken waarin andere collega's automatisch het juiste toegangsniveau voor het benodigde materiaal hebben (opmerkingen of bewerken).

- ***Extern verwijderen***

  Wanneer werknemers het team verlaten of een apparaat kwijtraken, kunnen beheerders Dropbox-gegevens en lokale exemplaren van bestanden op afstand wissen. Bestanden worden zowel van computers als van mobiele apparaten verwijderd zodra ze online komen terwijl de Dropbox-app of -toepassing actief is.

- ***Accountoverdracht***

  Als de bevoegdheden van een gebruiker worden ingetrokken (hetzij handmatig hetzij via directoryservices), kunnen beheerders bestanden en eigendom van Paper-documenten gemaakt door een voormalig teamlid uit die gebruikersaccount overzetten naar een andere gebruiker in het team. De functie accountoverdracht kan worden gebruikt tijdens het verwijderen van een gebruiker of op elk moment na het verwijderen van het account van een gebruiker.

De volgende add-on functies zijn ook beschikbaar (neem contact op met Sales voor meer informatie).

- ***Materiaal scannen***

  Met de add-on Geavanceerde team- en materiaalfuncties kunnen gebruikers van Dropbox Business Advanced en Enterprise scannen op nieuw en bestaand materiaal in Dropbox om zo kwetsbaarheden in de gegevens op te sporen en te voorkomen.

- ***Aangepaste workflows instellen en activeren***
  Met de add-on Geavanceerde team- en materiaalfuncties kunnen beheerders aanpasbare acties ondernemen tegen bestanden die het bedrijfsbeleid schenden.

- ***Waarschuwingen instellen***
  Beheerders kunnen beveiligingsproblemen in realtime volgen en kwetsbaarheden in gegevens voorkomen. Ze ontvangen ook waarschuwingen wanneer de bestanden met externen worden gedeeld en als gevoelige gegevens worden gescand.

## Zichtbaarheid van het materiaal

### Beveiligingswaarschuwingen en -meldingen

Beheerders van Dropbox Enterprise kunnen realtimemeldingen ontvangen wanneer misbruik, risicovolle activiteiten of mogelijke gegevenslekken op hun accounts worden gedetecteerd. De volgende gebeurtenissen kunnen worden gecontroleerd:

- Massaverwijderingen
- Massale verplaatsing van gegevens
- Gevoelig materiaal extern gedeeld
- Malware gedeeld van buiten je team
- Malware gedeeld binnen uw team
- Te veel mislukte aanmeldingspogingen
- Aanmelden vanuit een hoog risico land
- Detectie van ransomware

Dropbox heeft ook de mogelijkheid toegevoegd om waarschuwingsdrempels te configureren, ontvangers van meldingen aan te passen en waarschuwingen te activeren wanneer mappen met gevoelige bestanden extern worden gedeeld. Beheerders kunnen waarschuwingen ook markeren als controleren, opgelost of afgewezen. Bovendien toont een dashboardwidget de algemene inzichten en trends van teamwaarschuwingen van de afgelopen week.

### Rapport en pagina voor extern delen

Dropbox biedt extra zichtbaarheid met een rapport en pagina voor extern delen. Beheerders kunnen een rapport maken vanaf de inzichtenpagina of de pagina voor extern delen. In het rapport worden alle bestanden en mappen van het team vermeld die buiten hun team zijn gedeeld en alle gedeelde links. De pagina voor extern delen is een extra pagina in de Beheerconsole, waarmee beheerders de bestanden en mappen kunnen zien en filteren (bestandstype, wie gedeeld, linkinstellingen en nog veel meer) door de bestanden en mappen die rechtstreeks vanuit team- en gedeelde links worden gedeeld.

## Functies voor delen

Instellingen voor delen geven teambeheerders meer controle over het delen van en toegang tot de inhoud van hun team. Beheerders kunnen standaard vervaldatums, wachtwoordbeperkingen of beide op teamniveau instellen. Deze beperkingen verminderen het risico op gegevensverlies door de verantwoordelijkheid van de gebruikers om beperkingen in te stellen, weg te nemen.

## Gegevensclassificatie

Teams op Dropbox Enterprise kunnen persoonlijke en gevoelige gegevens automatisch laten labelen om ze beter te beschermen tegen blootstelling. Beheerders ontvangen waarschuwingen voor preventie van gegevensverlies (DLP) via e-mail en in de beheerconsole wanneer bestanden of mappen die zijn opgeslagen in teammappen met gevoelige informatie, buiten hun team worden gedeeld. Beheerders kunnen automatisch gevoelige gegevens identificeren en classificeren die zijn opgeslagen in gedeelde mappen en persoonlijke mappen van teamleden. Dropbox Enterprise-beheerders kunnen automatische gegevensclassificatie activeren vanuit de Beheerconsole.

## Add-on voor gegevensbeheer

Gegevensbeheer is het geheel van processen, technologieën en teams waarmee gegevensbestanden van een organisatie worden beheerd en beschermd. Dit omvat de mogelijkheid om bedrijfsgegevens indien nodig op te slaan, te identificeren, te ontdekken en op te halen.

De add-on Gegevensbeheer van Dropbox bundelt een reeks functies waarmee organisaties hun gegevens beter kunnen beheren en beveiligen, terwijl de risico's en kosten die gepaard gaan met het voldoen aan regelgeving en nalevingsbehoeften worden verminderd. Momenteel bevat deze add-on vier belangrijke functies voor teambeheerders en nalevingsbeheerders.

- ***Uitgebreide versiegeschiedenis***

  De standaard versiegeschiedenis van een bestand hangt af van jouw Dropbox-account. Teams die gebruikmaken van Dropbox Business kunnen de add-on Uitgebreide versiegeschiedenis (UVG) apart aanschaffen of als onder deel van de bundel voor de add-on Gegevensbeheer. Daarmee kunnen ze bestanden die in de afgelopen tien jaar zijn gewijzigd of verwijderd weer terugzetten.

- ***Wettelijke bewaarplicht***

  Team- en nalevingsbeheerders kunnen wettelijke bewaarplicht inschakelen voor een teamlid. Een beheerder kan daardoor het materiaal dat het lid heeft gemaakt of gewijzigd, bekijken en exporteren. Leden die een wettelijke bewaarplicht krijgen, krijgen geen melding van de bewaarplicht en blijven gemachtigd om bestanden aan te maken, te bewerken en te verwijderen.

- ***Bewaring van gegevens***

  Dankzij het bewaren van gegevens kunnen teams en nalevingsbeheerders voorkomen dat per ongeluk inhoud wordt verwijderd die volgens de regelgeving voor een bepaalde tijd moet worden bewaard. Met deze functie kunnen klanten gegevens bewaren tot 10 jaar vanaf de laatste 'revisie'-datum.

- ***Gegevensverwijdering***

  Met gegevensverwijdering kunnen team- en nalevingsbeheerders op een bepaalde datum permanent gegevens verwijderen om aan de vereisten voor het bewaren en verwijderen van gegevens te voldoen. Beheerders kunnen activiteiten controleren door rapporten te ontvangen die ze op de hoogte te brengen van toekomstige bestandsverwijderingen.

### Bestandsherstel en versiebeheer

Alle klanten van Dropbox Business kunnen verwijderde bestanden en Paper-documenten en vorige versies van bestanden en Paper-documenten terugzetten, zodat wijzigingen van belangrijke gegevens kunnen worden bijgehouden en teruggehaald.

### Gegevensbeveiliging op mobiele apparaten

- ***Gegevens wissen***

  Voor extra beveiliging kan een gebruiker de optie inschakelen om alle Dropbox-gegevens van het apparaat te wissen na 10 mislukte pogingen om de toegangscode in te voeren.

- ***Interne opslag en offline bestanden***

  Standaard worden bestanden niet bewaard in de interne opslag van mobiele apparaten. De mobiele clients van Dropbox zijn voorzien van de mogelijkheid om individuele bestanden en mappen op het apparaat op te slaan voor offline weergave. Wanneer een apparaat wordt ontkoppeld van een Dropbox-account, hetzij via de mobiele, hetzij via de webinterface, worden die bestanden en mappen automatisch verwijderd uit de interne opslag van het apparaat.

- ***Offline Paper-documenten***

  Wanneer een apparaat wordt ontkoppeld van Paper via de beveiligingspagina van het Dropbox-account, wordt de gebruiker afgemeld en worden offline Paper-documenten automatisch verwijderd uit de interne opslag van het apparaat.

## Teamcontroles

Geen enkele organisatie is hetzelfde. We hebben daarom een aantal tools ontwikkeld waarmee beheerders Dropbox Business kunnen afstemmen op de specifieke behoeften van hun team. Dropbox Business bevat ook tools waarmee eindgebruikers hun account en gegevens nog beter kunnen beschermen. De onderstaande functies voor authenticatie, herstel, registratie en andere beveiligingsopties zijn beschikbaar via de diverse gebruikersinterfaces van Dropbox.

Hieronder worden een aantal functies voor inzicht en beheer uiteengezet die beschikbaar zijn via de Beheerconsole van Dropbox Business.

### Aangepaste materiaalmachtigingen

- ***Beheerdersrollen op meerdere niveaus***

  Dropbox biedt gelaagde beheerdersrollen om effectiever teambeheer mogelijk te maken. Accountbeheerders kunnen een van de drie toegangsniveaus toegewezen krijgen. Er is geen limiet voor het aantal beheerders dat een team kan hebben en aan elk teamlid kan een beheerdersrol worden toegewezen.

- ***Teambeheer***

  Deze beheerder kan machtigingen voor beveiligen en delen instellen voor het hele team, beheerders maken en leden beheren. De teambeheerder beschikt over alle beschikbare beheerdersmachtigingen. Alleen teambeheerders kunnen beheerdersrollen toewijzen of wijzigen. Er moet altijd ten minste één teambeheerder aan een Dropbox Business-account zijn gekoppeld.

- ***Beheerder van gebruikersbeheer***

  Deze kan de meeste teambeheertaken uitvoeren, waaronder het toevoegen en verwijderen van teamleden, het beheren van groepen en het bekijken van de activiteitenfeed van een team.

- ***Supportbeheer***

  Deze beheerder kan veelvoorkomende serviceaanvragen van teamleden verwerken, zoals herstel van verwijderde bestanden of hulp bij een blokkering van tweestapsverificatie voor teamleden. Supportbeheerders kunnen daarnaast wachtwoorden van niet-beheerders opnieuw instellen en een activiteitenlogboek voor een specifiek teamlid exporteren.

- ***Factureringsbeheerder***

  Heeft toegang tot factureringspagina's in de beheerconsole.

- ***Inhoudsbeheerder***

  Kan teammappen maken en beheren binnen de Content Manager.

- ***Rapportbeheerder***

  Kan rapporten maken in de Beheerconsole en heeft toegang tot de pagina Activiteit.

- ***Beveiligingsbeheerder***

  Kan beveiligingswaarschuwingen, extern delen en beveiligingsrisico's beheren.

- ***Nalevingsbeheerder (alleen beschikbaar voor teams met de add-on Gegevensbeheer)***

  Kan pagina's voor gegevensbeheer beheren (wettelijke bewaarplichten, gegevensbewaring en gegevensverwijdering) en toegang krijgen tot Content Manager.

- ***Groepen***

  Teams kunnen in Dropbox lijsten met leden maken en beheren, en hen eenvoudig toegang geven tot specifieke mappen. Dropbox kan daarnaast Active Directory-groepen synchroniseren die gebruikmaken van de Active Directory-connector.

- ***Door bedrijf beheerde groepen***

  Alleen beheerders kunnen het lidmaatschap instellen, verwijderen en beheren voor dit type groep. Gebruikers kunnen geen aanvraag indienen om aan een door het bedrijf beheerde groep te worden toegevoegd of hieruit te worden verwijderd.

- ***Door gebruikers beheerde groepen***

  Beheerders kunnen kiezen of gebruikers hun eigen groepen kunnen maken en beheren. Admins kunnen ook op elk moment een door gebruikers beheerde groep wijzigen in een door het bedrijf beheerde groepen als ze het beheer ervan willen overnemen.

- ***Meerdere accounts op computers beperken.***

  Beheerders kunnen teamleden blokkeren voor het koppelen van een tweede Dropbox-account aan computers die aan hun zakelijke Dropbox-account zijn gekoppeld.

- ***Gebruikers schorsen***

  Beheerders hebben de mogelijkheid een gebruiker de toegang tot zijn of haar account te ontzeggen, waarbij de gegevens en instellingen voor delen worden behouden om zo bedrijfsinformatie veilig te houden. Beheerders kunnen het account op een later tijdstip opnieuw activeren of verwijderen.

- ***Aanmelden als gebruiker***

  Teambeheerders kunnen zich aanmelden als lid van hun team. Zo hebben beheerders direct toegang tot de bestanden, mappen en Paper-documenten in accounts van teamleden, zodat ze wijzigingen kunnen aanbrengen, namens teamleden kunnen delen of audits kunnen uitvoeren voor gebeurtenissen op bestandsniveau. Gebeurtenissen voor 'Aanmelden als gebruiker' worden geregistreerd in het activiteitenlogboek van het team. Beheerders kunnen bepalen of leden een melding krijgen over deze gebeurtenissen.

- ***Machtigingen voor delen***

  Teambeheerders hebben uitgebreide controle over de deelmogelijkheden van hun team via Dropbox, waaronder:

  - De mogelijkheid voor teamleden om bestanden en mappen met mensen buiten het team te kunnen delen.
  - De mogelijkheid voor teamleden om mappen te bewerken die eigendom zijn van mensen buiten het team.
  - De mogelijkheid voor gedeelde links die door teamleden zijn gemaakt voor mensen buiten het team.
  - De mogelijkheid voor teamleden om bestandsaanvragen te maken en bestanden te verzamelen bij teamleden en/of mensen buiten het team.
  - De mogelijkheid voor mensen om bestanden die eigendom zijn van het team te bekijken en er opmerkingen bij te plaatsen.
  - De mogelijkheid voor teamleden om Paper-documenten en -mappen buiten het team te delen.
  - Machtigingen voor permanent verwijderen worden toegekend.

De teambeheerder van een Dropbox Business-account kan de mogelijkheid om bestanden en Paper-documenten permanent te verwijderen beperken tot uitsluitend teambeheerders.

## Onboarding en het inrichten van gebruikers

***Methoden voor het toekennen van gebruikersbevoegdheden en identiteitsmanagement***

- ***E-mailuitnodiging***

  Met een tool in de beheerconsole van Dropbox Business kunnen beheerders handmatig een e-mailuitnodiging genereren.

- ***Active Directory***

  Beheerders van Dropbox Business kunnen het maken en verwijderen van accounts van een bestaand Active Directory-systeem automatiseren via onze Active Directory-connector of een externe identiteitsprovider. Nadat Active Directory is geïntegreerd, kunnen hiermee lidmaatschappen worden beheerd.

- ***Eenmalige aanmelding (SSO)***

Dropbox Business kan zo worden geconfigureerd dat teamleden toegang krijgen wanneer zij zich aanmelden bij een centrale identiteitsprovider. Met onze SSO-implementatie, waarbij gebruik wordt gemaakt van de in de branche algemeen erkende Security Assertion Markup Language 2.0 (SAML 2.0), wordt gebruikers inrichten een stuk gemakkelijker en veiliger, doordat de authenticatie wordt uitbesteed aan een vertrouwde identiteitsprovider en teamleden toegang krijgen tot Dropbox zonder dat ze nog meer wachtwoorden hoeven te beheren. Daarnaast werkt Dropbox samen met toonaangevende providers van identiteitsbeheer voor automatische inrichting van gebruikers en het ongedaan maken daarvan. Zie het gedeelte Integratie via de Dropbox Business-API hieronder voor meer informatie.

- ***API***

  Klanten kunnen de Dropbox Business-API gebruiken om aangepaste oplossingen voor het inrichten van gebruikers en identiteitsbeheer te ontwikkelen. Zie het gedeelte Integratie via de Dropbox Business-API hieronder voor meer informatie.

## Tweestapsverificatie

Met deze sterk aanbevolen beveiligingsfunctie wordt een extra beschermingslaag toegevoegd aan het Dropbox-account van de gebruiker. Als de tweestapsverificatie is ingeschakeld, vraagt Dropbox bij het koppelen van een nieuwe computer, telefoon of tablet, om bij het aanmelden naast het wachtwoord ook een beveiligingscode van zes cijfers op te geven.

- Beheerders kunnen tweestapsverificatie verplicht stellen voor alle teamleden of alleen voor bepaalde leden.

- Accountbeheerders kunnen bijhouden voor welke teamleden tweestapsverificatie is ingeschakeld.

- De tweestapsverificatiecodes van Dropbox kunnen worden opgevraagd via een sms-bericht of via apps die voldoen aan de TOTP-algoritmestandaard (Time-based One-Time Password).

- Als het een gebruiker niet lukt de beveiligingscodes via deze methoden op te vragen, kan er worden gekozen voor een back-upcode voor noodgevallen van 16 cijfers voor eenmalig gebruik. Ook kan een ander telefoonnummer worden gebruikt voor ontvangst van een sms-bericht met een back-upcode.

- Dropbox biedt daarnaast ondersteuning voor de open standaard FIDO Universal 2nd Factor (U2F), waarmee gebruikers kunnen worden geverifieerd via een USB-beveiligingssleutel die ze hebben ingesteld, in plaats van via een zescijferige code.

## Installatieprogramma voor ondernemingen

Beheerders die op grote schaal gebruikersaccounts willen toewijzen, kunnen ons Windows-installatieprogramma voor ondernemingen gebruiken om de Dropbox-desktopclient op de achtergrond en op afstand te installeren via oplossingen voor beheerde software en implementatieprocessen.

## Beheerde apparaten en aanmelden

- ***Enterprise Mobiliteitsbeheer (EMM)***

  Dropbox kan worden geïntegreerd met externe EMM-providers om beheerders van Dropbox Business met een Enterprise-abonnement meer controle te geven over hoe teamleden Dropbox gebruiken op mobiele apparaten. Beheerders kunnen het gebruik van mobiele apps met Dropbox Enterprise-accounts beperken tot alleen beheerde apparaten (zowel door het bedrijf verstrekte als persoonlijke apparaten), inzicht krijgen in appgebruik (inclusief beschikbare opslagruimte en toegangslocaties) en een verloren of gestolen apparaat extern verwijderen. Houd er rekening mee dat de mobiele app van Paper niet door EMM kan worden beheerd.

- ***Goedkeuringen van apparaten***

  Dropbox stelt beheerders van Dropbox Education en Dropbox Business met een Advanced- of Enterprise-abonnement in staat limieten in te stellen voor het aantal apparaten dat een gebruiker met Dropbox kan synchroniseren en bepalen of goedkeuringen door gebruikers of beheerders worden beheerd. Beheerders kunnen ook een lijst met uitgezonderde gebruikers maken voor wie de apparatenlimiet niet geldt. Houd er rekening mee dat de mobiele app van Paper niet is opgenomen in apparaatgoedkeuringen.

- ***Tweestapsverificatie verplichten***

  Beheerders kunnen tweestapsverificatie verplichten voor alle teamleden of alleen voor bepaalde leden. Andere vereisten voor meervoudige verificatie kunnen worden afgedwongen via de implementatie voor eenmalige aanmelding (SSO) van het team.

- ***Wachtwoordbeheer***

  Beheerders van Education-, Advanced- en Enterprise-teams kunnen van leden vereisen dat ze sterke, complexe wachtwoorden voor hun accounts instellen. Wanneer deze functie is ingeschakeld, worden teamleden uit alle websessies afgemeld en moeten nieuwe wachtwoorden worden gemaakt wanneer ze inloggen. Een ingebouwde tool analyseert de sterkte van wachtwoorden door ze te vergelijken met een database van veelgebruikte woorden, namen, patronen en getallen. Een gebruiker die een gemeenschappelijk wachtwoord invoert, wordt gevraagd iets uniekers te bedenken dat moeilijk te raden is. Beheerders kunnen wachtwoorden ook voor het hele team of per gebruiker opnieuw instellen.

- ***Domeinbeheer***

  Dropbox biedt bedrijven een aantal tools om het onboardingproces van gebruikers en het beheer van Dropbox-gebruik te vereenvoudigen en te versnellen.

  - **Domeinverificatie** Bedrijven kunnen het eigendom van hun domeinen claimen en de overige tools voor domeinbeheer ontgrendelen.

  - **Uitnodiging afdwingen**
    Beheerders kunnen van individuele Dropbox-gebruikers die zijn uitgenodigd voor het Dropbox-team van het bedrijf vereisen dat ze naar het team migreren of het e-mailadres van hun persoonlijke accounts wijzigen.

  - **Domeininzichten**
    Beheerders kunnen belangrijke informatie zien, zoals het aantal individuele Dropbox-accounts dat een e-mailadres van het bedrijf gebruikt.

  - **Accountovername**
    Beheerders kunnen afdwingen dat alle Dropbox-gebruikers die een e-mailadres van het bedrijf gebruiken, lid worden van het bedrijfsteam of het e-mailadres van hun persoonlijke accounts wijzigen.

- ***Websessiebeheer***

  Beheerders kunnen bepalen hoelang teamleden bij dropbox.com aangemeld kunnen blijven. Beheerders kunnen de duur van alle websessies en/of inactieve sessies beperken. Sessies die deze limieten bereiken, worden automatisch uitgelogd. Beheerders kunnen ook de websessies van individuele gebruikers volgen en beëindigen.

- ***Apptoegang***

  Beheerders hebben de mogelijkheid om de toegang van apps van derden tot gebruikersaccounts te bekijken en in te trekken.

- ***Apparaten ontkoppelen***

  Computers en mobiele apparaten die aan gebruikersaccounts zijn gekoppeld, kunnen door de beheerder via de beheerconsole of door de gebruiker via de individuele instellingen voor accountbeveiliging worden ontkoppeld. Op computers worden door het ontkoppelen authenticatiegegevens verwijderd en kunnen lokale exemplaren van bestanden worden verwijderd zodra de computer weer online komt (zie **Extern verwijderen** hieronder). Op mobiele apparaten worden door het ontkoppelen bestanden die zijn gemarkeerd als favoriet, cachegegevens en aanmeldingsinformatie verwijderd. Als tweestapsverificatie is ingeschakeld, moeten gebruikers de authenticatie opnieuw uitvoeren voor elk apparaat dat ze opnieuw willen koppelen. Verder is het via de accountinstellingen van de gebruiker mogelijk om automatisch een e-mailbericht te verzenden zodra er een apparaat wordt gekoppeld.

- ***Netwerkbeheer***

  Beheerders van Dropbox Business met een Enterprise-abonnement kunnen het gebruik van Dropbox op het bedrijfsnetwerk beperken tot alleen het teamaccount van Enterprise. Deze functie wordt geïntegreerd met de netwerkbeveiligingsprovider van het bedrijf om verkeer te blokkeren dat plaatsvindt buiten het gesanctioneerde account op computers. Houd er rekening mee dat Paper momenteel niet via netwerkbeheer wordt beheerd.

### Mobiele beveiliging

- ***Vingerafdrukscans***

  Gebruikers kunnen op iOS-apparaten Touch ID of Face ID en op Android-apparaten vergrendeling middels een vingerafdruk (wanneer ondersteund) inschakelen als een manier om de mobiele Dropbox-app te ontgrendelen.

### Zicht op de toegang

- ***Identiteitsverificatie voor technische support***

  Voordat er gegevens ten behoeve van het oplossen van problemen of accountgegevens door Dropbox Support worden verstrekt, moet de accountbeheerder een willekeurig gegenereerde beveiligingscode voor eenmalig gebruik opgeven om zijn of haar identiteit te valideren. Deze pincode is uitsluitend beschikbaar via de beheerconsole.

### Activiteit van gebruikersaccounts

Iedere gebruiker kan via zijn of haar accountinstellingen de volgende pagina's bekijken om bijgewerkte informatie op te vragen over de eigen accountactiviteit.

- ***Pagina delen***

  Op deze pagina staan de gedeelde mappen die momenteel in de Dropbox van de gebruiker aanwezig zijn en gedeelde mappen die de gebruiker kan toevoegen. Een gebruiker kan het delen van mappen en bestanden opheffen en machtigingen voor delen instellen.

- ***Pagina Bestanden***

  Deze pagina toont de bestanden die met de gebruiker zijn gedeeld en de datum waarop elk bestand gedeeld werd. De gebruiker heeft de mogelijkheid om hun toegang tot deze bestanden te verwijderen. Om Paper-documenten te zien die door anderen met de gebruiker zijn gedeeld, kan de gebruiker navigeren naar de pagina 'Met mij gedeeld' in de navigatie-interface van het Paper-document.

- ***Pagina Links***

  Op deze pagina staan alle actieve gedeelde links die de gebruiker heeft gemaakt en de creatiedatum van elke link. Ook worden alle links weergegeven die door anderen met de gebruiker zijn gedeeld. De gebruiker kan links uitschakelen of machtigingen wijzigen.

- ***E-mailmeldingen***

  Gebruikers kunnen aangeven dat ze een e-mailmelding willen ontvangen zodra een nieuw apparaat of nieuwe app wordt gekoppeld aan hun Dropbox-account.

## Machtigingen voor gebruikersaccounts

- ***Gekoppelde apparaten***

  In het gedeelte **Apparaten** in de accountbeveiligingsinstellingen van een gebruiker staan alle computers en mobiele apparaten die aan het gebruikersaccount zijn gekoppeld. Voor elke computer worden het IP-adres, het land en een benadering van de tijd van de meest recente activiteit weergegeven. Een gebruiker kan elk apparaat ontkoppelen en heeft de mogelijkheid om bestanden op een gekoppelde computer te verwijderen zodra deze online komt.

- ***Actieve websessies***

  In het gedeelte **Sessies** staan alle webbrowsers die momenteel bij een gebruikersaccount zijn aangemeld. Voor elke browser worden het IP-adres, het land en de aanmeldtijd van de meest recente sessie weergegeven, evenals een benadering van de tijd van de meest recente activiteit. Een gebruiker kan elke sessie op afstand beëindigen vanuit de accountbeveiligingsinstellingen.

- ***Gekoppelde apps***

  In het gedeelte **Gekoppelde apps** staat een lijst met alle apps van derden die toegang hebben tot het account van een gebruiker, evenals het type toegang van elke app. Een gebruiker kan de machtigingen voor elke app voor toegang tot zijn of haar Dropbox intrekken.

## Activiteitenfeed

Dropbox Business registreert de acties rondom een bestand in de activiteitenfeed van het team. Deze feed is toegankelijk via de beheerconsole. Met de flexibele filteropties in de activiteitenfeed kunnen beheerders activiteiten van accounts, bestanden of Paper-documenten gericht onderzoeken. Beheerders kunnen bijvoorbeeld de volledige geschiedenis van een bestand bekijken en zien wat gebruikers ermee hebben gedaan, of alle teamactiviteit binnen een bepaalde periode bekijken. De activiteitenfeed kan als downloadbaar rapport in CSV-indeling worden geëxporteerd en ook direct in een SIEM-product (Security Information and Event Management) of andere analysetool worden geïntegreerd via oplossingen van derden. De volgende gebeurtenissen worden in de activiteitenfeed geregistreerd:

- ***Delen voor bestanden, mappen en links***

  Indien van toepassing wordt in rapporten aangegeven of acties zijn gekoppeld aan mensen buiten het team.

  **Gedeelde bestanden**

  - Heeft een teamlid of niet-teamlid toegevoegd of verwijderd.
  - Heeft de machtigingen van een teamlid of niet-teamlid gewijzigd.
  - Heeft een groep toegevoegd of verwijderd.
  - Heeft een gedeeld bestand toegevoegd aan de Dropbox van de gebruiker.
  - Heeft de inhoud bekeken van een bestand dat via een uitnodiging voor een bestand of een map is gedeeld.
  - Heeft gedeeld materiaal gekopieerd naar de Dropbox van de gebruiker.
  - Heeft gedeeld materiaal gedownload.
  - Heeft een opmerking aan een bestand toegevoegd.

- Heeft een opmerking opgelost of niet opgelost.
- Heeft een opmerking verwijderd.
- Heeft zich aangemeld of afgemeld voor meldingen over opmerkingen.
- Heeft een uitnodiging geclaimd voor een bestand dat eigendom is van het team.
- Heeft toegang aangevraagd tot een bestand dat eigendom is van het team.
- Heeft het delen van een bestand stopgezet.

**Gedeelde mappen**

- Heeft een nieuwe gedeelde map gemaakt.
- Heeft een teamlid, niet-teamlid of groep toegevoegd of verwijderd.
- Heeft een gedeelde map toegevoegd aan de Dropbox van de gebruiker of de gebruiker heeft zijn eigen toegang tot een gedeelde map verwijderd.
- Heeft een gedeelde map toegevoegd via een link.
- Heeft de machtigingen van een teamlid of niet-teamlid gewijzigd.
- Heeft de eigendom van een map overgedragen naar een andere gebruiker.
- Heeft het delen van een map opgeheven.
- Heeft het lidmaatschap voor een gedeelde map geclaimd.
- Heeft toegang aangevraagd tot een gedeelde map.
- Heeft de gebruiker van de aanvraag toegevoegd aan een gedeelde map.
- Heeft de toevoeging van niet-teamleden aan een map geblokkeerd of gedeblokkeerd.
- Heeft alle teamleden of alleen de eigenaar toestemming gegeven om mensen toe te voegen aan een map.
- Heeft de groepstoegang tot een gedeelde map gewijzigd.

**Gedeelde links**

- Heeft een link gemaakt of verwijderd.
- Heeft de inhoud van een link zichtbaar gemaakt voor iedereen die de link heeft of alleen voor teamleden.
- Heeft de inhoud van een link beveiligd met een wachtwoord.
- Heeft een vervaldatum van een link ingesteld of verwijderd.
- Heeft een link bekeken.
- Heeft de inhoud van een link gedownload.
- Heeft de inhoud van een link gekopieerd naar de Dropbox van een gebruiker.
- Heeft een link naar een bestand gemaakt via een API-app.
- Heeft een link gedeeld met een teamlid, niet-teamlid of groep.
- Heeft het bekijken van links naar bestanden in een gedeelde map geblokkeerd of gedeblokkeerd voor niet-teamleden.
- Heeft een album gedeeld.

**Bestandsaanvragen**

- Heeft een bestandsaanvraag gemaakt, gewijzigd, gesloten of verwijderd.
- Heeft gebruikers toegevoegd aan een bestandsaanvraag.
- Heeft een deadline voor een bestandsaanvraag toegevoegd of verwijderd.
- Heeft de map van een bestandsaanvraag gewijzigd.
- Heeft bestanden ontvangen via een bestandsaanvraag.
- Heeft via Email to Dropbox bestanden ontvangen.

**Gebeurtenissen die betrekking hebben op afzonderlijke bestanden en mappen**

- Heeft een bestand toegevoegd aan Dropbox.
- Een map gemaakt.
- Heeft een bestand bekeken.
- Heeft een bestand bewerkt.
- Heeft een bestand gedownload.
- Heeft een bestand of map gekopieerd.
- Heeft een bestand of map verplaatst.
- Naam van bestand of map gewijzigd.
- Heeft een bestand teruggezet naar een vorige versie.
- Heeft wijzigingen in bestanden teruggedraaid.
- Heeft een verwijderd bestand hersteld.
- Heeft een bestand of map verwijderd.
- Heeft een bestand of map permanent verwijderd.

**Geslaagde en mislukte aanmeldingen**

- Geslaagde of mislukte aanmelding.
- Mislukte aanmeldpoging of fout via eenmalige aanmelding (SSO).
- Mislukte aanmeldpoging of fout via EMM.
- Heeft zich afgemeld.
- Wijziging van IP-adres voor websessie.

### Wachtwoorden

Wijzigingen in de instellingen voor wachtwoorden of tweestapsverificatie. Beheerders kunnen de wachtwoorden van gebruikers niet zien.

- Heeft een wachtwoord gewijzigd of opnieuw ingesteld.
- Heeft tweestapsverificatie ingeschakeld, opnieuw ingesteld of uitgeschakeld.

- Heeft tweestapsverificatie ingesteld of gewijzigd voor gebruik met sms of een mobiele app.
- Heeft een back-uptelefoon voor tweestapsverificatie toegevoegd, bewerkt of verwijderd.
- Heeft een beveiligingssleutel voor tweestapsverificatie toegevoegd of verwijderd.

### Lidmaatschap

Toevoegingen aan en verwijderingen uit het team.

- Heeft een teamlid uitgenodigd.
- Is lid van het team geworden.
- Heeft een teamlid verwijderd.
- Heeft een teamlid geblokkeerd of een blokkering opgeheven.
- Heeft een verwijderd teamlid teruggeplaatst.
- Heeft een aanvraag ingediend om lid te worden van het team op basis van accountdomein.
- Heeft een aanvraag om lid te worden van een team op basis van accountdomein goedgekeurd of afgewezen.
- Heeft domeinuitnodigingen verstuurd naar bestaande domeinaccounts.
- Gebruiker is lid geworden van het team als reactie op accountovername.
- Gebruiker heeft het domein verlaten als reactie op accountovername.
- Heeft het voorstellen van nieuwe teamleden door bestaande teamleden geblokkeerd of gedeblokkeerd.
- Heeft een nieuw teamlid voorgesteld.

### Apps

Koppeling van apps van derden aan Dropbox-accounts.

- Heeft een toepassing goedgekeurd of verwijderd.
- Heeft een toepassing van het team goedgekeurd of verwijderd.

### Apparaten

Koppeling van computers of mobiele apparaten aan Dropbox-accounts.

- Heeft een apparaat gekoppeld of ontkoppeld.
- Heeft de functie Extern verwijderen gebruikt en alle bestanden met succes verwijderd of een aantal bestanden niet verwijderd.
- Wijziging van IP-adres voor desktopcomputer of mobiel apparaat.

### Beheerdersacties

Wijzigingen aan instellingen in de beheerconsole, zoals machtigingen voor gedeelde mappen.

- ***Authenticatie en eenmalige aanmelding (SSO)***
    - Heeft het wachtwoord van een teamlid gereset.
    - Heeft de wachtwoorden van alle teamleden gereset.

  - Heeft het uitschakelen van tweestapsverificatie door teamleden geblokkeerd of gedeblokkeerd.
  - Heeft SSO in- of uitgeschakeld.
  - Heeft aanmelding via SSO verplicht.
  - Heeft de SSO-URL gewijzigd of verwijderd.
  - Heeft het SSO-certificaat bijgewerkt.
  - Heeft de SSO-identiteitsmodus gewijzigd.

- ***Lidmaatschap***
  - Heeft het indienen van een aanvraag door gebruikers om lid te worden van het team op basis van accountdomein geblokkeerd of gedeblokkeerd.
  - Heeft lidmaatschapsaanvragen voor het team ingesteld op automatische goedkeuring of vereiste handmatige goedkeuring door een beheerder.

- ***Beheer van ledenaccounts***
  - Heeft de naam van een teamlid gewijzigd.
  - Heeft het e-mailadres van een teamlid gewijzigd.
  - Heeft de beheerstatus toegewezen of verwijderd, of de beheerdersrol gewijzigd.
  - Heeft zich aangemeld of afgemeld als teamlid.
  - Heeft het materiaal van het account van een verwijderd lid overgezet of verwijderd.
  - Heeft het materiaal van het account van een verwijderd lid permanent verwijderd.

- ***Algemene instellingen voor delen***
  - Heeft het toevoegen van gedeelde mappen die eigendom zijn van niet-teamleden door teamleden geblokkeerd of gedeblokkeerd.
  - Heeft het delen van mappen met niet-teamleden door teamleden geblokkeerd of gedeblokkeerd.
  - Heeft waarschuwingen ingeschakeld die aan gebruikers worden getoond voordat ze mappen delen met niet-teamleden.
  - Heeft het bekijken van gedeelde links door niet-teamleden geblokkeerd of gedeblokkeerd.
  - Heeft gedeelde links standaard ingesteld op uitsluitend voor het team.
  - Heeft het plaatsen van opmerkingen bij bestanden geblokkeerd of gedeblokkeerd.
  - Heeft het maken van bestandsaanvragen door teamleden geblokkeerd of gedeblokkeerd.
  - Heeft een logo voor gedeelde linkpagina's toegevoegd, gewijzigd of verwijderd.
  - Heeft teamleden geblokkeerd of gedeblokkeerd voor het delen van Paper-documenten en Paper-mappen met niet-teamleden.

- ***Beheer van teammappen voor bestanden***
  - Heeft een teammap gemaakt.
  - Heeft een teammap hernoemd.
  - Heeft een teammap gearchiveerd of uit het archief gehaald.
  - Heeft een teammap permanent verwijderd.
  - Heeft een teammap gedowngraded naar een gedeelde map.

- ***Domeinbeheer***
  - Heeft geprobeerd een domein te verifiëren of een domein met succes geverifieerd, of een domein verwijderd.
  - Dropbox-support heeft een domein geverifieerd of verwijderd.
  - Heeft het versturen van domeinuitnodigingen in- of uitgeschakeld.
  - Heeft Nieuwe gebruikers automatisch uitnodigen in- of uitgeschakeld.
  - Heeft de accountovernamemodus gewijzigd.
  - Dropbox Support heeft accountovername verleend of ingetrokken.
- ***Enterprise Mobiliteitsbeheer (EMM)***
  - Heeft EMM ingeschakeld voor testmodus (optioneel) of implementatiemodus (verplicht).
  - Heeft het EMM-token vernieuwd.
  - Heeft teamleden aan de EMM-lijst met uitgesloten gebruikers toegevoegd of daaruit verwijderd.
  - Heeft EMM uitgeschakeld.
  - Heeft een rapport met de lijst met uitzonderingen voor EMM gemaakt.
  - Heeft een EMM-rapport over het gebruik van een mobiele app gemaakt.
- ***Wijzigingen in andere teaminstellingen***
  - Heeft teams samengevoegd.
  - Heeft het team geüpgraded naar Dropbox Business of gedowngraded naar een gratis team.
  - Heeft de teamnaam gewijzigd.
  - Heeft een activiteitenrapport voor het team gemaakt.
  - Heeft het koppelen van meer dan één account aan een computer door teamleden geblokkeerd of gedeblokkeerd.
  - Heeft alle teamleden of alleen beheerders toegestaan om groepen te maken.
  - Heeft het permanent verwijderen van bestanden door teamleden geblokkeerd of gedeblokkeerd.
  - Heeft een Dropbox Support-sessie voor een reseller gestart of beëindigd.

## Groepen

Informatie over het aanmaken, verwijderen en lidmaatschap van groepen.

- Heeft een groep gemaakt, hernoemd, verplaatst of verwijderd.
- Heeft een lid toegevoegd of verwijderd.
- Heeft het toegangstype van een groepslid gewijzigd.
- Heeft de groep gewijzigd naar door team beheerde of door beheerder beheerde groep.
- Heeft de externe ID van een groep gewijzigd.

## Paper-activiteitenlogboek

Beheerders kunnen een type Paper-activiteit op de activiteitenfeed selecteren of een volledig activiteitenverslag downloaden. Paper-gebeurtenissen worden opgeslagen voor:

- Paper is ingeschakeld of uitgeschakeld.
- Paper-document maken, bewerken, exporteren, archiveren, permanent verwijderen en herstellen.
- Opmerkingen op Paper-document en het oplossen daarvan.
- Heeft Paper-document dat is gedeeld met teamleden en niet-teamleden of het delen ervan opgeheven.
- Toegangsverzoeken voor Paper-document van teamleden en niet-teamleden.
- Vermeldingen in Paper-document van teamleden en niet-teamleden.
- Paper-document bekeken door teamleden en niet-teamleden.
- Paper-document gevolgd.
- Machtigingswijzigingen van lid voor Paper-document (bewerken, opmerking of alleen-lezen).
- Beleidswijzigingen voor extern delen van Paper-document.
- Maken, archiveren en permanent verwijderen van Paper-mappen.
- Paper-document in map toegevoegd of verwijderd.
- Paper-map hernoemd.
- Overdrachten van Paper-documenten en -mappen.

# Dropbox Passwords

Dropbox Passwords is een veilige, eenvoudige manier voor het opslaan, synchroniseren en automatisch invullen van gebruikersnamen, wachtwoorden, creditcards en betaalkaarten op verschillende apparaten, zodat je je online gegevens kunt beschermen. Dropbox Passwords beschermt je gevoelige online accountgebruikersnamen, wachtwoorden, creditcards en betaalkaarten met zero-knowledge-versleuteling in de cloud en op je apparaten. Onze producten zijn gemaakt voor dagelijks gebruik en met het oog op beveiliging.

## Zero-knowledge-versleuteling

Dropbox Passwords slaat je versleutelde gegevens op in de cloud, maar de sleutels om deze gegevens te ontsleutelen worden alleen op je apparaten opgeslagen. **Dropbox heeft er nooit toegang toe.** Deze sleutels zijn lang, willekeurig en worden op je apparaat gegenereerd. Ze verlaten je apparaat nooit, behalve wanneer je besluit een nieuw apparaat te koppelen of te registreren. Deze overdracht maakt gebruik van cryptografie met openbare sleutels om de sleutels tijdens de overdracht zowel cryptografisch te ondertekenen als te beschermen. Zo kun je erop vertrouwen dat niemand anders ze kan ontsleutelen en verifieer je tegelijkertijd dat ze authentiek zijn. Deze eigenschap wordt vaak zero-knowledge-versleuteling genoemd, omdat de versleutelde gegevens nutteloos zijn voor iedereen die de sleutels niet heeft, inclusief Dropbox. Dit betekent dat **alleen jij je gegevens kunt inzien** en dat in het onwaarschijnlijke geval dat Dropbox wordt gehackt, je gegevens nog steeds veilig zijn. De versleutelde gegevens zijn gescheiden van zichtbare Dropbox-mappen en kunnen niet worden gepasseerd met behulp van Dropbox-clients of -API's.

## Versleutelingsdetails

Dropbox versleutelt je gegevens met XChaCha20-Poly1305 in gecombineerde modus voor impliciete authenticatie. Onze browserextensies en mobiele toepassingen maken allemaal gebruik van versleutelingsimplementaties die worden ondersteund door libsodium, een gecontroleerde en wijdverspreide fork van NaCl.

Elke versleutelingsbewerking genereert een willekeurige nonce van 192 bits, die bij de versleutelde lading wordt opgeslagen voor latere ontsleuteling. In tegenstelling tot AES-GCM, ondersteunt XChaCha20-Poly1305 willekeurige nonces. Bij de ontsleuteling wordt de 192-bit nonce uit de lading gelezen en gebruikt om de versleutelde lading te ontsleutelen. Elke volgende versleuteling genereert een willekeurige nonce van 192 bits, die onafhankelijk is van de voorgaande nonce. Dropbox Passwords genereert willekeurige getallen met behulp van libsodium dat standaard een cryptografisch veilige willekeurige getallengenerator gebruikt op elk platform dat we ondersteunen.

## Sleutels en herstelwoorden

We genereren een 256-bits symmetrische sleutel (de versleutelingssleutel) uit 128-bits entropie (de gebruikerssleutel) via Blake2-hashing. Deze versleutelingsleutel blijft alleen beschikbaar op de apparaten van de eigenaar en, waar mogelijk, in de meest veilige opslag waartoe we op de betreffende apparaten toegang hebben. Op iPhones slaan we de versleutelingsleutel bijvoorbeeld op in de iOS-sleutelhanger.

We gebruiken 128-bits entropie als onze bron, omdat deze voldoende beveiliging biedt, terwijl er slechts 12 herstelwoorden nodig zijn bij gebruik van de BIP-39-standaard voor back-ups. BIP-39 biedt een mensvriendelijke manier om grote willekeurige sleutels weer te geven door deze sleutels om te zetten in een lijst van twaalf woorden. Elke 128-bits sleutel heeft een overeenkomstige lijst van woorden en elke lijst van 12 woorden identificeert 128 bits op unieke wijze. Het enige voorbehoud is dat deze twaalf woorden eigenlijk overeenkomen met 132 bits. De extra vier bits kunnen dus als controlesom worden gebruikt om fouten op te sporen. De herstelwoorden bieden je een manier om je versleutelingsleutel te herstellen in het geval je apparaat is verloren of gestolen. We raden je aan ze af te drukken en op een veilige plek te bewaren. Je kunt ook overwegen ze aan een betrouwbare vriend of familielid te geven of ze op een USB-stick te bewaren.

## Apparaatregistratie

Wanneer een gebruiker zich op een nieuw apparaat bij Dropbox Passwords aanmeldt, moet dat apparaat een veilige registratieprocedure doorlopen om toegang tot de wachtwoordgegevens van de gebruiker te krijgen. Deze procedure helpt ervoor te zorgen dat de geheime sleutel en Passwords-gegevens van een gebruiker alleen toegankelijk zijn op de geregistreerde apparaten van de gebruiker. Het zorgt er ook voor dat een gebruiker alleen extra apparaten kan registreren als hij of zij toegang heeft tot een bestaand geregistreerd apparaat of zijn of haar herstelwoorden. De registratieprocedure voor het apparaat verloopt als volgt.

Een nieuw geregistreerd apparaat genereert willekeurig een 256-bits openbaar/persoonlijk apparaatsleutelpaar en uploadt de openbare sleutel naar de Dropbox-server. Vervolgens treedt scenario **A**, **B** of **C** op.

**A:** als de gebruiker nog niet eerder een apparaat heeft geregistreerd, genereert het geregistreerde apparaat willekeurig een geheime gebruikerssleutel van 128 bits. Zowel de gebruikerssleutel als het apparaatsleutelpaar worden opgeslagen op een veilige OS-specifieke locatie, zoals beschreven in het volgende gedeelte over sleutelopslag. Het apparaat initialiseert de Passwords-gegevens van de gebruiker, versleutelt deze en uploadt de versleutelde lading naar de Dropbox-server.

**B:** als de gebruiker eerder geregistreerde apparaten heeft, wordt een goedkeuringsverzoek voor registratie naar elk van deze apparaten verzonden. De openbare sleutel van het geregistreerde apparaat wordt bij het verzoek gevoegd. De gebruiker moet het verzoek vervolgens op een van zijn of haar geregistreerde apparaten goedkeuren. Na deze goedkeuring versleutelt het geregistreerde apparaat de gebruikerssleutel met behulp van de persoonlijke sleutel en de openbare sleutel van het geregistreerde apparaat via X25519 ECDH met XSalsa20-Poly1305. Het geregistreerde apparaat uploadt de versleutelde gebruikerssleutel naar de Dropbox-server om naar het geregistreerde apparaat te verzenden. Het geregistreerde apparaat downloadt en ontsleutelt de gebruikerssleutel met behulp van de persoonlijke sleutel en de openbare sleutel van het geregistreerde apparaat. Het inschrijvende apparaat downloadt vervolgens de versleutelde ladinggegevens van Passwords en ontsleutelt deze met de gebruikerssleutel.

**C:** als de gebruiker eerder een apparaat heeft geregistreerd, maar er geen toegang meer toe heeft, kan hij of zij de twaalf herstelwoorden invoeren om de gebruikerssleutel lokaal te reconstrueren. Het geregistreerde apparaat downloadt vervolgens de versleutelde ladinggegevens van Passwords en ontsleutelt deze met de gebruikerssleutel.

## Sleutelopslag

### Browserextensies

Bij webbrowsers wordt de gebruikerssleutel opgeslagen in de lokale opslagruimte van de browserextensie. De lokale opslagwaarden van de browserextensie zijn alleen toegankelijk vanuit de extensie. Elke code die op de door de gebruiker bezochte websites draait, kan niet uit de lokale opslagruimte van de browserextensie worden gelezen. Bovendien verbieden browserextensies de uitvoering van code die niet in het ondertekende extensiepakket zit. Zo wordt het risico geëlimineerd van een XSS-kwetsbaarheid die toegang tot lokale opslagwaarden kan geven.

Een aanvaller met onbeperkte toegang tot het apparaat van de gebruiker kan toegang krijgen tot de gebruikerssleutel door het lokale opslagbestand op schijf te lezen. Voorbeelden van dergelijke dreigingen zijn: een aanvaller met fysieke toegang tot het apparaat of een aanvaller die kwaadaardige malware op het apparaat laat draaien. Om je tegen deze scenario's te beschermen, kunnen gebruikers een lokale wachtwoordzin instellen.

Als er een wachtwoordzin is ingesteld, wordt de gebruikerssleutel in rust versleuteld in de lokale opslag van de browserextensie. De versleutelingssleutel is afgeleid van de wachtwoordzin via Argon2-wachtwoordhashing en de gebruikte versleutelingsmethode is XChaCha20-Poly1305. Elke keer dat de browserextensie opnieuw opstart, moet de gebruiker de wachtwoordzin opgeven om de gebruikerssleutel te ontsleutelen en de gegevens te ontgrendelen. Hierdoor kan een aanvaller de gebruikerssleutel die in het lokale opslagbestand op schijf staat, niet ontsleutelen zonder de wachtwoordzin.

### iOS

Op iOS wordt de gebruikerssleutel opgeslagen in de iOS-sleutelhanger, een versleuteld databasebestand op schijf. Dit bestand wordt versleuteld met een geheime sleutel die is opgeslagen in de Secure Enclave-hardwaremodule, waarbij AES256-GCM als versleutelingsmethode wordt gebruikt. Alleen de ondertekende Dropbox Passwords-app voor iOS heeft toegang tot de items die in de sleutelhanger zijn opgeslagen. Dit voorkomt dat andere code die op het apparaat van de gebruiker draait, toegang heeft tot de gebruikerssleutel.

### Android

Op Android wordt de gebruikerssleutel opgeslagen in een EncryptedSharedPreferences-object, een versleuteld voorkeurenbestand op schijf. Dit bestand wordt versleuteld met een hoofdsleutel die is opgeslagen in de beveiligde Android-keystore, waarbij AES256-GCM als versleutelingsmethode wordt gebruikt. Alleen de ondertekende Dropbox Passwords-app voor Android heeft toegang tot de hoofdsleutel die wordt gebruikt om het voorkeursbestand te ontsleutelen.

## Lokale authenticatie

Dropbox Passwords biedt optionele lokale authenticatiemaatregelen om de toegang tot de Passwords-gegevens van een gebruiker op zijn of haar fysieke apparaat verder te beperken. Voor mobiele toepassingen kan het authenticatiegebaar van het lokale besturingssysteem worden hergebruikt (oftewel: een toegangscode met aanvullende biometrische authenticatie). Voor browserextensies kan een optionele wachtwoordzin worden ingesteld. Deze mechanismen bieden een extra beveiligingslaag voor toepassingen wanneer het besturingssysteem van het apparaat van de gebruiker wordt ontgrendeld. Hiermee kan de gebruiker zijn of haar Passwords-gegevens beveiligen als een andere gebruiker toegang tot het apparaat heeft, zoals een familielid of collega.

## Suggestie voor wachtwoordsterkte

Dropbox heeft de open source tool zxcvbn ontwikkeld, die door verschillende wachtwoordbeheerders wordt gebruikt om de sterkte van wachtwoorden in te schatten. De tool vergelijkt wachtwoorden met een database van 30.000 veelvoorkomende wachtwoorden, veelvoorkomende namen en achternamen volgens Amerikaanse volkstellingsgegevens, populaire Engelse woorden van Wikipedia en Amerikaanse televisie en films, en andere veel voorkomende patronen zoals datums, herhalingen (aaa), reeksen (abcd), toetsenbordpatronen (qwertyuiop), en Leet (1337) Speak. Als het wachtwoord dat een gebruiker probeert in te voeren algemeen is, vraagt de tool om iets unieks en moeilijk te raden in te voeren. Met behulp van de instelling **Zeer sterk** kan het hoogste niveau van accountbeveiliging voor gebruikers worden behaald.

# Gegevensbeveiliging, -privacy en -transparantie

Mensen en organisaties vertrouwen Dropbox dagelijks met hun belangrijkste werk. Het is onze verantwoordelijkheid om deze informatie te beschermen en privé te houden.

## Privacybeleid

Ons privacybeleid kan worden bekeken op dropbox.com/privacy. In het Privacybeleid, de Serviceovereenkomst, de Servicevoorwaarden en het Beleid voor acceptabel gebruik van Dropbox worden de volgende voorwaarden meegedeeld:

- Welk soort gegevens we verzamelen en waarom.

- Met wie we mogelijk gegevens delen.
- Hoe we deze gegevens beschermen en hoelang we ze bewaren.
- Waar we je gegevens bewaren en verzenden.
- Wat er gebeurt als het beleid verandert of als je vragen hebt.

### Transparantie

Dropbox streeft naar transparantie rond de verwerking van verzoeken door politie en justitie om gebruikersgegevens, evenals rond het aantal en de aard van dergelijke verzoeken. Alle informatieverzoeken worden door ons tot in detail geëvalueerd om na te gaan of deze wettelijk zijn toegestaan. Verder stellen wij gebruikers op de hoogte, voor zover wettelijk toegestaan, wanneer hun accounts worden genoemd in een gerechtelijk verzoek om informatie.

Deze inspanningen onderstrepen hoezeer wij ernaar streven de privacy van onze gebruikers en hun gegevens te bewaken. Hiertoe houden wij een transparantierapport bij en hebben we de grondbeginselen voor verzoeken om informatie door de overheid opgesteld. De volgende beginselen beheersen ons handelen bij het ontvangen, beoordelen en reageren op overheidsverzoeken om gegevens van onze gebruikers:

- ***Transparant zijn***

  Wij vinden dat online services het aantal en het type overheidsverzoeken die worden ontvangen, moeten kunnen publiceren en dat personen geïnformeerd moeten worden wanneer informatie over hen is aangevraagd. Zulke transparantie stelt gebruikers in staat om instanties en patronen van overmacht van de overheid beter te begrijpen. We blijven gedetailleerde informatie over deze verzoeken publiceren en pleiten voor het recht om meer van deze belangrijke informatie te verstrekken.

- ***Strijden tegen zeer brede verzoeken***

  Gegevensverzoeken van overheden moeten worden beperkt tot specifieke personen en legitieme onderzoeken. We strijden tegen bulkverzoeken en brede verzoeken.

- ***Alle gebruikers beschermen***

  Wetten die mensen verschillende bescherming bieden op basis van waar ze wonen of hun burgerschap zijn verouderd en weerspiegelen niet het wereldwijde karakter van online diensten. We zullen blijven pleiten voor de hervorming van deze wetten.

- ***Vertrouwde diensten aanbieden***

  Overheden mogen nooit in het geheim installaties uitvoeren in online services of de infrastructuur misbruiken om gebruikersgegevens te verkrijgen. We werken voortdurend aan de beveiliging van onze systemen en blijven ons inzetten voor wetswijzigingen om duidelijk te maken dat dit soort activiteiten illegaal is.

Onze transparantierapporten kunnen worden bekeken via dropbox.com/transparency.

## Privacycertificeringen, attestaties en naleving van regelgeving.

Mensen en organisaties vertrouwen Dropbox dagelijks met de belangrijkste bestanden voor hun werk. Daarom is het onze verantwoordelijkheid om die bestanden te beschermen en ze privé te houden. Jouw privacy staat centraal bij elke beslissing die we nemen.

### ISO/IEC 27018 (praktijkcode voor de bescherming van persoonsgegevens in de cloud) en ISO/IEC 27701 (uitbreiding van ISO/IEC 27001 en ISO/IEC 27002 voor het beheer van privacygegevens).

Dropbox Business was een van de eerste grote aanbieders van cloudservices die een certificering met ISO/IEC 27018 en ISO/IEC 27701 wist te behalen.

ISO/IEC 27018 is een wereldwijde norm voor privacy- en gegevensbescherming in de cloud en werd in augustus 2014 gepubliceerd en is bedoeld om een kader te bieden voor specifiek de privacy van gebruikers en gegevensbescherming.

ISO/IEC 27701 is de eerste wereldwijde norm voor het beheer van privacygevoelige informatie waarvoor bedrijven gecertificeerd kunnen worden. Deze norm werd in 2019 gepubliceerd en is bedoeld om een kader te bieden voor het uitbreiden van het managementsysteem voor informatiebeveiliging (ISMS) uit ISO/IEC 27001 naar een managementsysteem voor privacygevoelige informatie (PIMS). Hiervoor moesten er overwegingen op het gebied van gegevensbescherming in worden opgenomen.

Deze normen omvatten allerlei vereisten voor hoe Dropbox de gegevens van jouw organisatie al dan niet gebruikt:

- ***Jouw organisatie is de baas over jouw gegevens***

  We gebruiken de persoonlijke gegevens die je ons verstrekt alleen om je de services te bieden waarvoor je je hebt geregistreerd. Je kunt wanneer je maar wilt bestanden en Paper-documenten toevoegen aan, bewerken in of verwijderen uit Dropbox.

- ***We zijn transparant over jouw gegevens***

  We zijn transparant over waar je gegevens op onze servers staan. We laten je ook weten wie onze vertrouwde partners zijn. We vertellen je wat er gebeurt wanneer je een account sluit of een bestand of Paper-document verwijdert. En ten slotte laten we je het meteen weten als er iets verandert.

- ***Jouw gegevens zijn veilig***

  ISO/IEC 27018 en ISO/IEC 27701 zijn ontworpen als verbetering en uitbreiding van ISO/IEC 27001, een van de meest geaccepteerde normen voor informatiebeveiliging ter wereld. In oktober 2021 is onze ISO/IEC 27001-certificering verlengd.

- ***Onze praktijken worden regelmatig geëvalueerd***

  Als onderdeel van de naleving van ISO/IEC 27018, ISO/IEC 27701 en ISO/IEC 27001 ondergaan we jaarlijkse audits door een onafhankelijke externe partij om deze certificaten te behouden. Je kunt al onze ISO-certificaten hier bekijken.

## Gegevensoverdrachten

Wanneer er gegevens worden overgedragen vanuit de Europese Unie, de Europese Economische Ruimte, het Verenigd Koninkrijk en Zwitserland, hanteert Dropbox diverse juridische mechanismen, zoals contracten met onze klanten en gelieerde ondernemingen, standaard contractbepalingen en adequaatheidsbesluiten van de Europese Commissie over bepaalde landen, voor zover van toepassing.

Dropbox voldoet aan de Amerikaans-Europese en Amerikaans-Zwitserse Privacy Shield Frameworks zoals omschreven door het Amerikaanse Department of Commerce, inzake het verzamelen, gebruiken en bewaren van persoonsgegevens die vanuit de Europese Unie, de Europese Economische Ruimte, het Verenigd

Koninkrijk en Zwitserland worden overgebracht naar de Verenigde Staten. Dropbox gebruikt de Amerikaans-Europese en Zwitsers-Amerikaanse Privacy Shields echter niet als juridische grondslag voor de overdracht van persoonsgegevens. Dropbox heeft aan de Department of Commerce verklaard dat het zich houdt aan de Privacy Shield Principles met betrekking tot dergelijke gegevens. Ga voor meer informatie over het Privacy Shield naarhttps://www.privacyshield.gov.

Klachten en geschillen met betrekking tot onze naleving van de Privacy Shield-principes worden onderzocht en opgelost door JAMS, een onafhankelijke externe partij. Lees ons privacybeleid voor meer informatie (dropbox.com/privacy).

### De algemene verordening gegevensbescherming van EU (AVG)

De AVG (Algemene verordening gegevensbescherming) is een verordening van de Europese Unie uit 2018 die een alomvattend kader vastlegt voor de verwerking en bescherming van persoonsgegevens.

Dropbox zet zich in voor de beveiliging en bescherming van de gegevens van onze gebruikers, in overeenstemming met de wettelijke vereisten en best practices. In lijn met onze betrokkenheid bij onze gebruikers hebben we hard gewerkt om ervoor te zorgen dat Dropbox voldoet aan de AVG-normen, waaronder het aanstellen van een Data Protection Officer, het herontwerpen van ons privacyprogramma om ervoor te zorgen dat gebruikers de betreffende rechten kunnen uitoefenen, het documenteren van onze activiteiten op het gebied van de verwerking van gegevens en het versterken van onze interne processen in het geval van een Schending van de Veiligheid. We gaan door met het doorvoeren van aanpassingen om ervoor te zorgen dat onze processen en praktijken in overeenstemming zijn met of verder gaan dan de specifieke elementen van de nieuwe regels, nu de gegevensbeschermingsautoriteiten verdere richtlijnen blijven geven.

### EU Cloud Code of Conduct

De EU-gedragscode voor de cloud is een vrijwillig instrument, waarmee een aanbieder van cloudservices als Dropbox kan aantonen dat we ons inzetten voor de naleving van de AVG. Dropbox Business dat uit de abonnementen Standard, Advanced, Enterprise en Education for Teams bestaat, is verklaard zich aan de EU-gedragscode voor de cloud te houden en heeft een nalevingsmerk van 'Niveau 2' ontvangen, wat betekent dat deze services technische, organisatorische en contractuele maatregelen hebben geïmplementeerd in overeenstemming met de vereisten van de code. Ga voor meer informatie over de EU-gedragscode voor de cloud en de naleving van de code door Dropbox naar de officiële website van de code.

Voor meer informatie over onze privacypraktijken en ons privacybeleid, kun je de whitepaper Privacy en gegevensbescherming van Dropbox raadplegen.

## Naleving

Er zijn veel verschillende voorschriften vanuit de regelgeving of de branche rondom beveiliging en privacy waar jouw organisatie zich mogelijk aan moet houden. Onze benadering omvat een combinatie van de meest geaccepteerde normen met nalevingsmaatregelen die zijn afgestemd op de specifieke behoeften van het bedrijf of de branche van onze klanten.

## ISO

De Internationale Organisatie voor Standaardisatie (ISO) heeft een reeks toonaangevende normen voor informatie- en maatschappelijke veiligheid ontwikkeld om organisaties te helpen betrouwbare en innovatieve producten en services te ontwikkelen. De datacenters, systemen, toepassingen, mensen en processen van Dropbox zijn gecertificeerd door middel van een reeks audits door een onafhankelijke derde partij, het Nederlandse EY CertifyPoint. EY CertifyPoint verkrijgt zijn ISO-accreditaties van de Nederlandse Raad voor Accreditatie.

### ISO/IEC 27001 (informatiebeveiliging)

ISO/IEC 27001 wordt over de hele wereld erkend als de belangrijkste ISMS-norm (Information Security Management System). De norm neemt ook de best practices voor beveiliging mee die worden beschreven in ISO/IEC 27002. We vinden het belangrijk dat je op ons kunt vertrouwen en houden ons daarom continu intensief bezig met de fysieke, technische en juridische beheerfuncties bij Dropbox.

Het ISO/IEC 27001-certificaat voor Dropbox Business en Dropbox Education bekijken.

### ISO/IEC 27017 (cloudbeveiliging)

ISO/IEC 27017 is een internationale norm voor cloudbeveiliging. Deze norm biedt richtlijnen voor de beveiligingsfuncties die van toepassing zijn op het inrichten en het gebruik van cloudservices. In onze Handleiding voor gedeelde verantwoordelijkheid worden de beveiligings-, privacy- en nalevingsvereisten toegelicht die Dropbox en klanten samen kunnen nakomen.

Het ISO/IEC 27017-certificaat voor Dropbox Business en Dropbox Education bekijken.

### ISO/IEC 27018 (bescherming van privacy en gegevens in de cloud)

ISO/IEC 27018 is een nieuwe internationale kwaliteitsnorm voor privacy- en gegevensbescherming toegespitst op cloudserviceproviders zoals Dropbox die persoonlijke gegevens verwerken namens hun klanten. Deze norm vormt een richtlijn voor situaties waarin onze klanten meer informatie willen of vragen hebben over veelvoorkomende wettelijke en contractuele kwesties.

Het ISO/IEC 27018-certificaat voor Dropbox Business en Dropbox Education bekijken.

### ISO/IEC 22301 (continuïteit van de bedrijfsvoering)

ISO/IEC 22301 is een internationale norm voor bedrijfscontinuïteit. Deze norm biedt organisaties een richtlijn waarmee ze het risico op verstorende gebeurtenissen kunnen verkleinen en adequaat kunnen reageren om potentiële schade te minimaliseren als dergelijke gebeurtenissen toch plaatsvinden. Het BCMS (beheersysteem voor bedrijfscontinuïteit) van Dropbox is onderdeel van onze algemene risicobeheerstrategie voor het beschermen van mensen en werkzaamheden in crisissituaties.

Het ISO/IEC 22301-certificaat voor Dropbox Business en Dropbox Education bekijken.

### ISO/IEC 27701 (Beheer van privacygevoelige informatie)

ISO 27701 is een nieuwe internationale norm voor het beheren van privacygevoelige informatie. De norm biedt een raamwerk voor het verbeteren en uitbreiden van het managementsysteem voor informatiebeveiliging onder ISO 27001 naar een managementsysteem voor privacygevoelige informatie (PIMS). Dropbox Business en Dropbox Education hebben deze certificering gekregen als PII-verwerker.

Bekijk het ISO 27701-certificaat voor Dropbox Business en Dropbox Education.

## SOC

SOC-rapporten (Service Organization Controls), beter bekend als SOC 1, 2 of 3, zijn kaders die door AICPA (American Institute of Certified Public Accountants) zijn opgesteld voor het rapporteren over de interne beheerfuncties die in een organisatie zijn geïmplementeerd. De systemen, toepassingen, mensen en processen van Dropbox zijn gevalideerd door middel van een reeks audits door Ernst & Young LLP, een onafhankelijke externe controle-instantie.

### SOC 3 voor beveiliging, vertrouwelijkheid, integriteit, beschikbaarheid en privacy

In het SOC 3-rapport worden alle vijf principes behandeld die van toepassing zijn op vertrouwensservices: beveiliging, vertrouwelijkheid, integriteit, beschikbaarheid en privacy (TSP sectie 100). Het rapport over het algemene gebruik van Dropbox is een managementssamenvatting van het SOC 2-rapport en bevat de mening van de onafhankelijke externe controle-instantie over het effectieve ontwerp en de werking van onze beheerfuncties.

De SOC 3-beoordeling van Dropbox Business en Dropbox Education bekijken.

### SOC 2 voor beveiliging, vertrouwelijkheid, integriteit, beschikbaarheid en privacy

Het SOC 2-rapport biedt klanten uitgebreide zekerheidsgaranties omtrent beheerfuncties en behandelt alle vijf principes die van toepassing zijn op vertrouwensservices: beveiliging, vertrouwelijkheid, verwerkingsintegriteit, beschikbaarheid en privacy (TSP sectie 100). Het SOC 2-rapport bevat een gedetailleerde beschrijving van de processen van Dropbox en meer dan 100 beheerfuncties om jouw spullen te beschermen. Naast de mening van de onafhankelijke externe controle-instantie over het effectieve ontwerp en de werking van onze beheerfuncties, bevat het rapport ook de testprocedures van de controle-instantie en de resultaten voor elke beheerfunctie. Ons SOC 2-rapport (soms ook wel SOC 2+ genoemd) omvat ook een gecontroleerde kaart van onze beheerfuncties aan de bovengenoemde ISO-normen, waardoor onze klanten extra transparantie hebben. De SOC 2-beoordeling van Dropbox Business en Dropbox Education is op verzoek verkrijgbaar.

### SOC 1 / SSAE 18 / ISAE 3402 (voorheen SSAE 16 of SAS 70)

Het SOC 1-rapport biedt specifieke garanties aan klanten voor wie Dropbox Business of Dropbox Education een belangrijk intern controle-instrument voor programma's voor financiële rapportage (ICFR) is. Deze specifieke garanties worden voornamelijk gebruikt voor de naleving van Sarbanes-Oxley (SOX) door de klant. De onafhankelijke externe audit voor dit rapport wordt uitgevoerd in overeenstemming met de Standards for Attestation Engagements No. 18 (SSAE 18) en de International Standard on Assurance Engagements No. 3402 (ISAE 3402), die in de plaats zijn gekomen van de verouderde norm van het Standards for Attestation Engagement No. 16 (SSAE 16) en het Statement on Auditing Standards No. 70 (SAS 70). De SOC 1-beoordeling van Dropbox Business en Education is op verzoek verkrijgbaar.

## CSA

### Cloud Security Alliance: Security, Trust & Assurance Registry (CSA STAR)

De CSA Security, Trust & Assurance Registry (STAR) is een gratis, openbaar toegankelijk register waarmee de beveiliging van cloudservices kan worden gecontroleerd. Gebruikers kunnen hiermee de beveiligingsstatus nagaan van cloudaanbieders die ze momenteel gebruiken of overwegen te gaan gebruiken.

Dropbox Business en Dropbox Education hebben de CSA STAR Level 2-certificering en het Level 2-attest. CSA STAR van niveau 2 vereist een onafhankelijke, externe beoordeling van onze beveiligingsfuncties door EY CertifyPoint (voor certificatie) en Ernst & Young LLP (voor attestatie) op basis van de vereisten van ISO 27001, SOC 2 Trust Services Criteria en de CSA Cloud Controls Matrix (CCM) v.3.0.1.

Onze CSA STAR Level 1- en Level 2-certificering en -attestatie op de website van CSA bekijken.

## HIPAA/HITECH

Dropbox zal Business Associate Agreements (BAA's) ondertekenen voor klanten van Dropbox Business of Dropbox Education die deze nodig hebben om te voldoen aan de Health Insurance Portability and Accountability Act (HIPAA) en de Health Information Technology for Economic and Clinical Health Act (HITECH). Zie Dropbox en HIPAA/HITECH voor meer informatie.

Dropbox stelt een extern garantierapport beschikbaar met een evaluatie van onze beheersfuncties voor de regels van HIPAA/HITECH Security, Privacy en Breach Notification. Daarnaast wordt een kaart van onze interne methoden en aanbevelingen beschikbaar gesteld voor klanten die met Dropbox Business en Dropbox Education willen voldoen aan de vereisten van de HIPAA/HITECH Security and Privacy Rule.

Klanten die deze documenten willen aanvragen of meer informatie willen over de aanschaf van Dropbox Business of Dropbox Education, kunnen contact opnemen met ons verkoopteam. Als je op dit moment een Dropbox Business-teambeheerder bent, kun je een BAA elektronisch ondertekenen via de pagina Account in de beheerconsole.

Houd er rekening mee dat de mogelijkheid om een elektronische BAA te ondertekenen via de beheerconsole alleen beschikbaar is voor klanten in de VS.

## NIST 800-171

Het National Institute of Standards and Technology (NIST) in de VS bevordert en onderhoudt normen en richtlijnen die organisaties helpen om hun informatiesystemen te beschermen. De NIST Special Publication (SP) 800171 Revision 2 (R2) voorziet in richtlijnen over het beschermen van Controlled Unclassified Informatie (CUI, gecontroleerde niet-gerubriceerde gegevens) binnen niet-federale informatiesystemen en organisaties. Entiteiten die CUI van de Amerikaanse overheid verwerken of opslaan, zoals onderzoeksintituten en de onderwijssector, moeten voldoen aan NIST SP 800-171 R2. De CUI-systemen, -processen en -beheersingsmaatregelen van Dropbox zijn gecertificeerd door Ernst & Young LLP, een onafhankelijke, externe auditor.

Je kunt het NIST SP 800-171 R2-rapport voor Dropbox Business en Dropbox Education opvragen bij ons verkoopteam of (voor bestaande Dropbox Business-klanten) via de ondersteuningsafdeling.

Dropbox Paper is niet opgenomen in het bereik van het NIST SP 800-171 R2-rapport.

## FERPA en COPPA (leerlingen en kinderen)

Klanten kunnen de services van Dropbox Business en Dropbox Education gebruiken in overeenstemming met de leveranciersverplichtingen die zijn opgelegd door de Family Education Rights and Privacy Act (FERPA). Onderwijsinstellingen met leerlingen onder de 13 jaar mogen Dropbox Business en Dropbox Education ook gebruiken in navolging van de wet COPPA (Children's Online Privacy Protection Act), mits ze akkoord gaan met specifieke clausules die vereisen dat de instelling toestemming van ouders verkrijgt voor het gebruik van onze services.

### FDA 21 CFR Deel 11

Titel 21 van de Code of Federal Regulations (CFR) reglementeert voedingsmiddelen en geneesmiddelen in de Verenigde Staten voor de Food and Drug Administration (FDA), de Drug Enforcement Administration en de Office of National Drug Control Policy. In Deel 11 van Titel 21 worden de criteria uiteengezet waaraan elektronische documenten en handtekeningen moeten voldoen om als betrouwbaar te worden beschouwd door de FDA. Deze criteria gelden doorgaans ook voor papieren documenten en handtekeningen die met de hand op papier zijn gezet.

Lees het whitepaper van Dropbox over 21 CFR Deel 11 van de FDA en het artikel in ons helpcentrum als je meer wilt weten hoe Dropbox jou kan helpen om 21 CFR Deel 11 correct na te leven.

### PCI DSS

Dropbox voldoet als bedrijf aan de Payment Card Industry Data Security Standard (PCI DSS). Dropbox Business, Dropbox Education en Dropbox Paper zijn er echter niet voor bedoeld om creditcardtransacties te verwerken of op te slaan. De PCI Attestation of Compliance (AoC) voor onze bedrijfsstatus is op verzoek verkrijgbaar.

Ga voor meer informatie over de naleving van Dropbox Business en Dropbox Education naar dropbox.com/business/trust/compliance.

## Apps voor Dropbox

Het DBX Platform is samengesteld uit een robuust ecosysteem van ontwikkelaars die onze flexibele API (Application Programming Interface) als fundament voor hun werk gebruiken. Meer dan 750.000 ontwikkelaars hebben toepassingen en services op het platform gebouwd voor productiviteit, samenwerking, beveiliging, administratie en meer.

### Kant-en-klare onderdelen

De Chooser, Saver en Embedder zijn vooraf gebouwde componenten voor het web en mobiele apparaten waarmee met slechts enkele regels code makkelijk toegang tot Dropbox in apps of op websites van externen kan worden gegeven.

- Via de Chooser kunnen bestanden in Dropbox worden geselecteerd.
- Via de Saver kunnen gebruikers bestanden rechtstreeks opslaan in Dropbox.
- Via de Embedder kunnen gebruikers bestanden en mappen in Dropbox bekijken.

De autorisatie voor deze onderdelen loopt volledig via Dropbox. De apps krijgen via gedeelde Dropbox-links of tijdelijk beschikbare downloadlinks toegang tot de bestanden die door de Chooser zijn geselecteerd. Deze vooraf gebouwde onderdelen kunnen los of samen worden gebruikt met de API die hieronder wordt omschreven.

## Dropbox Business API-integraties

Met de openbare Dropbox-API hebben externe ontwikkelaars de mogelijkheid voor toegang tot en interactie met Dropbox binnen hun applicaties. Dat omvat ook interactie met bestanden en metagegevens, delen en teamfunctionaliteit.

### Autorisatie

Dropbox maakt gebruik van OAuth, een standaardautorisatieprotocol in de branche, waarmee gebruikers accounttoegang kunnen toekennen aan apps zonder hun accountgegevens te hoeven prijsgeven. We ondersteunen OAuth 2.0 voor de authenticatie van alle API-aanvragen, via de Dropbox-website of de mobiele app. Dropbox ondersteunt de best practices van OAuth, waaronder tijdelijke toegangstokens en PKCE voor gedistribueerde apps.

### Gebruikersmachtigingen

Apps die gebruikmaken van de Dropbox-API kunnen worden ontwikkeld met het volgende machtigingsniveau voor toegang tot materiaal in de Dropbox van een eindgebruiker:

- ***Appmap.***

  Een speciale map met de naam van de app wordt gemaakt in de map Apps in de Dropbox van een gebruiker. De app mag alleen in deze map lezen en schrijven, en gebruikers kunnen materiaal in de appmap zetten door bestanden ernaartoe te slepen. Daarnaast kan de app ook toegang tot bestanden of mappen vragen via de Chooser of Saver.

- ***Volledige Dropbox.***

  De app krijgt volledige toegang tot alle bestanden en mappen in de Dropbox van een gebruiker, plus machtigingen om toegang tot bestanden of mappen te vragen via de Chooser of Saver.

Toepassingen kunnen ook een bepaalde reikwijdte vragen, waarbij het gedrag wordt beperkt door toegang tot subsets van API-eindpunten. Toepassingen kunnen bijvoorbeeld worden beperkt tot alleen-lezen toegang van bestanden, of wel materiaal kunnen uploaden, maar delen niet kunnen instellen.

### Teammachtigingen

Beheerders van Dropbox Business kunnen applicaties voor beheerfunctionaliteit autoriseren in de Beheerconsole van het team. De acties die aan het team gekoppelde apps kunnen uitvoeren worden beperkt door de machtigingen waarmee is vastgesteld welke teaminstellingen de app mag lezen of beheren.

Veelvoorkomende combinaties van machtigingen zijn onder andere:

- ***Teaminformatie***

  Alleen-lezen van informatie over het team en algemeen gebruik.

- ***Team-auditing***

  Alleen-lezen toegang tot informatie over het team en het gedetailleerde gebeurtenissenlogboek.

- ***Toegang tot bestanden als teamlid***

  Het vermogen om actie te ondernemen namens de gebruikers in het team, zoals het beheren van hun bestanden en mappen.

- ***Teamledenbeheer***

  Het toevoegen en verwijderen van leden aan en uit het team.

## Webhooks

Met webhooks kunnen webapps meldingen in real time ontvangen over wijzigingen in de Dropbox van een gebruiker. Zodra een URI is geregistreerd voor het ontvangen van webhooks, wordt telkens wanneer er een wijziging is voor de geregistreerde gebruikers van de app een HTTP-aanvraag naar die URI verzonden. Met behulp van de Dropbox Business-API kunnen webhooks ook worden gebruikt om meldingen te genereren over wijzigingen in het teamlidmaatschap. Veel beveiligingsapps gebruiken webhooks om beheerders te helpen bij het volgen en beheren van teamactiviteiten.

## Extensies

Apps mogen extensie-URI's registreren en zo zorgen dat acties in de menu's Delen en Openen in de gebruikersinterface van Dropbox verschijnen. Met extensies kunnen gebruikers workflows van derden rechtstreeks vanuit een bestand in de gebruikersinterface van Dropbox starten. Als een actie wordt geactiveerd, stuurt Dropbox de gebruikers door naar de aangegeven URI, waarbij een bestands-ID wordt doorgegeven die kan worden gebruikt bij de API om een bestandsbewerking uit te voeren. Een app moet worden geautoriseerd voordat een geregistreerde extensie zichtbaar is voor de gebruiker. We kunnen een select aantal extensie-integraties in de menu's 'Delen' en 'Openen' promoten, hoewel deze apps geen toegang tot materiaal hebben, totdat de gebruiker daarvoor toestemming geeft.

## Richtlijnen voor Dropbox-ontwikkelaars

We bieden een aantal richtlijnen en gebruikstips waarmee ontwikkelaars API-apps kunnen maken die de privacy van de gebruiker respecteren en beschermen, terwijl de manier waarop de gebruiker met Dropbox kan werken, alleen maar beter wordt.

- ***Appsleutels***

  Voor elke afzonderlijke app die een ontwikkelaar schrijft, moet een unieke Dropbox-appsleutel worden gebruikt. Als een app services of software aanbiedt waarin het Dropbox-platform is opgenomen zodat andere ontwikkelaars het kunnen gebruiken, moet elke ontwikkelaar zich daarnaast ook aanmelden voor een eigen Dropbox-appsleutel.

- ***Appmachtigingen***

  Ontwikkelaars worden geïnstrueerd dat een app de machtiging met de minste privileges moet hanteren. Wanneer een ontwikkelaar een app indient ter goedkeuring voor productiestatus, controleren we of de app geen onnodig ruime machtigingen aanvraagt op basis van de functionaliteit die door de app wordt geboden.

- ***Beoordelingsprocedure voor apps***

  - **Ontwikkelingsstatus**
    Net gemaakte Dropbox-API-apps krijgen de ontwikkelingsstatus. De app werkt op dezelfde wijze als apps met de productiestatus, met als uitzondering dat deze app alleen kan worden gekoppeld aan maximaal 500 Dropbox-gebruikers. Zodra een app aan 50 Dropbox-gebruikers is gekoppeld, heeft de ontwikkelaar twee weken de tijd om goedkeuring voor productiestatus aan te vragen en te verkrijgen voordat de mogelijkheid van de app om extra Dropbox-gebruikers te koppelen wordt uitgeschakeld.

  - **Productiestatus en goedkeuring**
    Goedkeuring voor de productiestatus is alleen mogelijk als alle API-apps voldoen aan onze richtlijnen voor merkgebruik voor ontwikkelaars en aan onze voorwaarden, waarin wordt beschreven onder welke omstandigheden het gebruik van het DBX Platform verboden is. Verboden gebruik omvat onder meer: het bevorderen van inbreuk op IP-adressen of copyright, het maken van netwerken voor het delen van bestanden en het illegaal downloaden van materiaal. Ontwikkelaars wordt eerst gevraagd aanvullende informatie te verschaffen omtrent de functionaliteit van hun app en hoe die gebruikmaakt van de Dropbox-API, voordat de aanvraag ter beoordeling wordt ingediend. Zodra de app is goedgekeurd voor de productiestatus, kunnen alle Dropbox-gebruikers een koppeling maken met deze app.

### Beheer van de Team-app

In de teambeheerderconsole kunnen beheerders van Dropbox Business de gekoppelde apps en integraties voor hun team beheren.

## API-partnerschappen

Dropbox heeft nauw met technologiepartners samengewerkt om hen in staat te stellen integraties te ontwikkelen voor hun populaire softwarepakketten. Deze partners ontwikkelen toepassingen met behulp van Dropbox-API's en werken nauw samen met Dropbox-architecten om de best practices op het gebied van beveiliging en gebruikerservaringen te implementeren. Deze omvatten diverse productiviteitsapps voor eindgebruikers en beveiligings- en beheertools, zoals

- ***Beveiligingsinformatie en gebeurtenissenbeheer (SIEM) en analyse***

  Koppel je Dropbox Business-account aan SIEM- en analysetools om onder meer delen door gebruikers, aanmeldingspogingen en beheerdersacties te bewaken en te beoordelen. Open en beheer activiteitenlogboeken en beveiligingsgegevens van medewerkers via je centrale tool voor logboekbeheer.

- ***Preventie van gegevensverlies (DLP)***

  Scan automatisch metagegevens en inhoud van bestanden om meldingen, rapportages en acties te activeren wanneer belangrijke wijzigingen worden aangebracht in je Dropbox Business-account. Pas bedrijfsbeleid toe op je Dropbox Business-implementatie en voldoe aan nalevingsvereisten.

- ***eDiscovery en wettelijke bewaarplicht***

  Reageer op rechtszaken, arbitrage en onderzoeken van toezichthouders met gegevens uit je Dropbox Business-account. Zoek en verzamel relevante, elektronisch opgeslagen informatie en behoud je gegevens tijdens het eDiscovery-proces, zodat je bedrijf tijd en geld bespaart.

- ***Beheer van digitale rechten (DRM)***

  Bescherm vertrouwelijk of auteursrechtelijk beschermd materiaal van derden dat is opgeslagen in accounts van medewerkers. Gebruik krachtige DRM-functies, waaronder versleuteling aan clientzijde, watermerken, controlelogboeken, intrekking van toegang en blokkering van gebruikers of apparaten.

- ***Gegevensmigratie en back-up op locatie***

  Bespaar tijd, geld en moeite door gegevens van bestaande servers of andere cloudoplossingen te migreren naar Dropbox. Automatiseer back-ups van jouw Dropbox Business-account naar servers op locatie.

- ***Identiteitsbeheer en eenmalige aanmelding (SSO)***

  Automatiseer het inrichten van accounts en het ongedaan maken daarvan, en versnel de onboarding van nieuwe medewerkers. Stroomlijn het beheer en versterk de beveiliging door Dropbox Business te integreren met een bestaand identiteitssysteem.

- ***Aangepaste workflows***

  Maak interne apps waarmee Dropbox wordt geïntegreerd in bestaande bedrijfsprocessen, om interne workflows te verbeteren.

Op de pagina Dropbox-appintegraties staat een lijst met deze technologiepartners. Eindgebruikers kunnen in het App Center geselecteerde eigen en externe apps en integraties vinden.

# Integratie met Dropbox

We hebben daarnaast samen met onze beste technologiepartners integraties gebouwd die in Dropbox voor eindgebruikers zichtbaar zijn. Deze diepere integraties worden door Dropbox en de externe partner samen ontwikkeld. Deze integraties omvatten:

## Dropbox-extensies

Met deze integraties kun je diverse app-extensies gebruiken, zodat je rechtstreeks vanuit Dropbox vlekkeloos dingen kunt uitvoeren als een video publiceren, bestanden aan e-mails en chatgesprekken toevoegen, een bestand verzenden voor eSignature en nog meer. Deze applicaties worden door de partner gebouwd. Dropbox faciliteert dan weer de kennismaking met geselecteerde extensiepartners via de menu's Openen met en Delen met.

## Slack, Zoom en Trello

Deze integraties worden door Dropbox zelf gebouwd. Hiermee hebben gebruikers binnen Dropbox de mogelijkheid om Slack-gesprekken en vergaderingen te beginnen en taken aan te maken. Eindgebruikers authenticeren zich bij deze tools via OAuth.

## Microsoft Office voor mobiele apparaten en het web

Dankzij onze integratie met Microsoft Office kunnen gebruikers Word-, Excel- en PowerPoint-bestanden openen die zijn opgeslagen in hun Dropbox, wijzigingen opslaan in de mobiele of webapps voor Office en die wijzigingen weer opslaan in Dropbox. Gebruikers wordt gevraagd toegang te verlenen wanneer ze een Dropbox-bestand voor het eerst openen in een mobiele Office-app of een Office-webapp. Deze links blijven behouden wanneer de app later opnieuw wordt geopend.

## Adobe Acrobat en Acrobat Reader

Dankzij onze integraties met de versies voor desktops en mobiele apparaten (Android en iOS) van deze apps kunnen gebruikers de in hun Dropbox opgeslagen PDF-bestanden bekijken, bewerken en delen. Gebruikers worden gevraagd om toegang te verlenen wanneer ze voor het eerst een Dropbox-bestand proberen te openen in de apps. Wijzigingen in PDF-bestanden worden automatisch in Dropbox opgeslagen.

# Samenvatting

Dropbox Business biedt gebruiksvriendelijke tools waarmee teams doelgericht kunnen samenwerken, met de beveiligingsmaatregelen en nalevingscertificaten die organisaties vereisen. Met een gelaagde benadering waarbij een robuuste back-endinfrastructuur wordt gecombineerd met een aanpasbare set beleidsregels, voorzien wij bedrijven van een krachtige oplossing die volledig kan worden afgestemd op hun unieke behoeften. Voor meer informatie over Dropbox Business kun je contact met ons opnemen via sales@dropbox.com.