

# Hvidbog om sikkerhed i Dropbox

En sikkerhedsrapport fra Dropbox

©2026 Dropbox. Alle rettigheder forbeholdes. V2026.03



# Indholdsfortegnelse

<b>Dropbox' tillidsprogram</b>	<b>5</b>
<b>Sikkerhed på enterprise-niveau</b>	<b>5</b>
Vores politikker	5
Engageret og erfarent sikkerhedsteam	7
Medarbejderpolitik, personalesikkerhed og adgang	7
Sikkerhedstræning og -kendskab	8
Koncernkontorer	8
Håndtering af sårbarheder	9
Fysisk sikkerhed	9
Reaktion på hændelser	9
<b>Sikkerhed for infrastruktur</b>	<b>10</b>
Netværkssikkerhed	10
Tilstedeværelsespunkter (PoP'er)	11
Peering	11
Sikkerhedsovervågning	11
Pålidelighed	12
Datacentre og leverandører af administrerede tjenester	12
Fortsat drift	12
Katastrofegenopretelse	13
<b>Programsikkerhed</b>	<b>14</b>
Scanning og penetrationstests af sikkerheden (internt og eksternt)	14
Sådan holdes skadeligt indhold væk fra Dropbox	15
Dusører for detektion af fejl	15
Databeskyttelse og kryptering	15
Certifikat-pinning	17
Beskyttelse af godkendelsesdata	17
Malware-scanning	17
<b>Produktsikkerhed</b>	<b>17</b>
Designennemgange	17
Sikker implementering	18
Ændringsstyring	18
<b>Beskyttelse af personlige data</b>	<b>18</b>
<b>Dropbox til teams</b>	<b>19</b>
<b>Bag kulisserne</b>	<b>19</b>
Infrastruktur for filer	20
Opbevaring af fildata	21
Infrastruktur for Paper	21
Opbevaring af Paper-dokumenter	23
<b>Pålidelighed</b>	<b>24</b>
<b>Dropbox' brugergrænseflader</b>	<b>27</b>
<b>Brugergrænseflader i Paper</b>	<b>28</b>
<b>Dropbox Replay</b>	<b>28</b>

# Indholdsfortegnelse

<b>Apps til Dropbox .....</b>	<b>28</b>
Færdigbyggede komponenter .....	29
API-integrationer til Dropbox til teams.....	29
API-partnerskaber .....	31
<b>Dropbox-integrationer .....</b>	<b>32</b>
<b>Produktsikkerhed .....</b>	<b>33</b>
Indholdskontrol .....	33
Indholdssynlighed .....	35
Team-kontroller.....	38
Administrerede enheder og login.....	41
<b>Integritetscertifikater, attestationer og lovgivningsmæssig overholdelse .....</b>	<b>51</b>
<b>Compliance .....</b>	<b>52</b>
<b>Resumé.....</b>	<b>57</b>
<b>Dropbox Dash .....</b>	<b>58</b>
<b>Dropbox Sign .....</b>	<b>59</b>
<b>Kryptering .....</b>	<b>59</b>
<b>Revisionsspor .....</b>	<b>59</b>
Dropbox Sign-produkt.....	59
Autenticitet .....	60
<b>Godkendelse .....</b>	<b>60</b>
<b>Tilladelser .....</b>	<b>61</b>
<b>Compliance-certifikater, attestationer og lovgivningsmæssig overholdelse .....</b>	<b>62</b>
<b>Dropbox DocSend .....</b>	<b>66</b>
<b>Produktinformation.....</b>	<b>66</b>
Sikker fildeling.....	66
Dynamiske vandmærker .....	66
Virtuelle datarum .....	67
E-signatur .....	67
Fortrolighedserklæringer .....	67
Brugerroller .....	67
Brugeradministration .....	67
Overfør brugerdata.....	67
Enkeltlogon.....	68
Underteams.....	68
<b>Kryptering .....</b>	<b>68</b>
<b>Revisionsspor .....</b>	<b>68</b>
<b>Godkendelse .....</b>	<b>68</b>
<b>Tilladelser .....</b>	<b>69</b>
<b>Compliance-certifikater, attestationer og lovgivningsmæssig overholdelse .....</b>	<b>69</b>
<b>Underleverandører .....</b>	<b>71</b>

# Indholdsfortegnelse

<a href="#">Reclaim.ai</a>	72
<a href="#">Kryptering fra start til slut</a>	73
<a href="#">Avanceret nøgleadministration</a>	87

Denne hvidbog er gældende fra datoen for den engelske version. Denne oversættelse stilles kun til rådighed som en service, og i tilfælde af uoverensstemmelser har den engelske variant forrang.

# Dropbox' tillidsprogram

Tillid er grundlaget for vores forhold til millioner af mennesker og virksomheder i hele verden. Vi værdsætter din tillid og tager ansvaret for at beskytte dine personlige oplysninger seriøst. For at gøre os værdige til din tillid har vi udviklet og fortsætter med at udvikle Dropbox med fokus på sikkerhed, persondata, gennemsigtighed og compliance.

Politikken for Dropbox' tillidsprogram etablerer en risikovurderingsproces, der er designet til at håndtere miljømæssige risici, fysiske risici, brugerrisici, tredjepartsrisici, risici ifm. gældende love og bestemmelser, risici ifm. kontraktmæssige forpligtelser og en lang række andre risici, der kan påvirke systemsikkerhed, fortrolighed, integritet, tilgængelighed og beskyttelsen af personlige oplysninger. Udviklingen på de forskellige områder evalueres mindst én gang om året. Få flere oplysninger om Dropbox' tillidsprogram på [www.dropbox.com/business/trust](http://www.dropbox.com/business/trust).

Dropbox har oprettet et Trust Center for at give selvbetjent adgang til information relateret til vores produkters sikkerhed, databeskyttelse, compliance og driftssikkerhed. Du kan gå til vores Trust Center på [trust.dropbox.com](http://trust.dropbox.com) for at få mere at vide.

## Sikkerhed på enterprise-niveau

Vi anvender en tilgang bestående af flere lag til at sikre virksomhed, infrastruktur, applikationer og produkter, der påvirker din organisation.

Dropbox har retningslinjer for håndtering af informationssikkerhed, som omfatter formål, målsætning, principper og grundlæggende regler for, hvordan vi sikrer kundernes tillid til os. Dette opnås ved at vurdere risici og hele tiden forbedre Dropbox til teams-systemernes sikkerhed, fortrolighed, integritet, tilgængelighed og beskyttelse af personlige oplysninger. Vi gennemgår og opdaterer regelmæssigt sikkerhedspolitikkerne, uddanner i sikkerhed, tester applikations- og netværkssikkerhed (herunder penetrationstests), overvåger overholdelse af sikkerhedspolitikker og udfører interne og eksterne risikovurderinger.

### Vores politikker

Vi har udarbejdet et omfattende sæt sikkerhedspolitikker, der håndhæves af sikkerheds- og misbrugsteamet hos Dropbox. Alle sikkerhedspolitikker gennemgås og godkendes mindst én gang om året. Ansatte, praktikanter og leverandører deltager i obligatoriske sikkerhedskurser, når de bliver en del af virksomheden og gennem løbende træning i sikkerhedskendskab.

- **Informationssikkerhed**

Bruger- og Dropbox-oplysninger holdes sikre.

- **Godkendelse**  
Beskriver, hvordan Dropbox-medarbejdere godkender sig selv for at få adgang til informationssystemer og data.
- **Sikkerhed for enheder**  
Minimum sikkerhedskrav for mobilenheder, der bruges til adgang til virksomhedsinformation.
- **Logisk adgangskontrol**  
Adgang til Dropbox-systemer, -brugere og -oplysninger holdes sikker. Dækker adgangskontrol til både virksomheds- og produktionsmiljøer.
- **Datasikkerhed**  
Beskriver, hvordan Dropbox beskytter data gennem specifikke krav til opbevaring, adgang og brug.
- **Rejsesikkerhed**  
Beskriver, hvad Dropbox-medarbejdere skal gøre før oversøiske rejser.
- **Sikkerhedsretningslinjer for salg og kundeoplevelse (CX)**  
Brugeroplysninger holdes sikre, vores medarbejdere beskyttes, og der ydes support til vores brugere.
- **Fysisk sikkerhed**  
Opretholdelse af et trygt og sikkert miljø for mennesker og ejendom hos Dropbox.
- **Retningslinjer for fysisk sikkerhed i produktion**  
Håndtering af fysisk adgang til produktionsfaciliteter.
- **Reaktion på hændelser**  
Skitserer, hvordan Dropbox håndterer rapporterede sikkerheds-, privatlivs- og webstedsbegivenheder, og dokumenterer handlingsplaner for dem hver især.
- **Uautoriseret ophavsretligt beskyttet materiale**  
Forhindrer medarbejdere i at bruge Dropbox eller Dropbox-systemer til at gemme eller dele uautoriseret indhold.
- **Ændringsstyring**  
Håndtering af ændringer i produktionssystemer. Beregnet til alle Dropbox-medarbejdere, -leverandører og -praktikanter med adgang til systemer.
- **Beskyttelse af brugeroplysninger**  
Beskyttelse og håndtering af brugeroplysninger og brugerdata hos Dropbox til overholdelse af vores politik om beskyttelse af personlige oplysninger.
- **Forretningskontinuitetspolitik og nødadministration**  
Beskriver bevaring, beskyttelse og sikkerheds for personer (Dropbox-medarbejdere), ejendom og (virksomheds-)processer.
- **Dropbox' program til beskyttelse af persondata**  
Formålet, principperne og ansvarligheden for Dropboxes persondataprogram.

- **Dropbox' tillidsprogram**  
Beskriver, hvordan Dropbox fungerer og er pålideligt.
- **Sikkerhed i betalingsmiljø**  
Sikring og vedligeholdelse af det dedikerede betalingsmiljø, der bruges i Dropbox til at acceptere kreditkortbetalinger.

## Engageret og erfarent sikkerhedsteam

Vores sikkerhedsprogram er beregnet til at vurdere risici og skabe en sikkerhedskultur hos Dropbox. Hver enkelt medarbejder hos Dropbox er engageret i sikkerhed og at beskytte vores kundedata i alt, hvad vi foretager os. Alle produkter og tjenester er i overensstemmelse med det gældende program for informationssikkerhed under Dropbox' Head of Security. Som en del af vores formelle program for risikovurdering gennemgås sikkerhedsrisici regelmæssigt, hvilket resulterer i sikkerhedsrelaterede initiativer på produkt-, infrastruktur- og virksomhedsniveau.

Teamet for beskyttelse af persondata er ansvarligt for driften af persondataprogrammet. De implementerer vores vigtigste initiativer for persondata og arbejder for planlagt beskyttelse af persondata i vores datalivscyklus.

For at sikre, at alle Dropbox-medarbejdere er i stand til at fremme beskyttelsen af kundedata, arbejder vi på at sikre, at sikkerhed og beskyttelse af persondata er indarbejdet i vores virksomhedskultur fra dag ét. Medarbejderne gennemgår omfattende baggrundstjek, underskriver og følger et adfærdskodeks og politikker for acceptabel brug og gennemgår årligt træning i sikkerhedskendskab og beskyttelse af persondata. Løbende kendskab til informationssikkerhed vedligeholdes gennem månedlige nyhedsbreve om informationssikkerhed og sikkerhedsrelevante meddelelser.

## Medarbejderpolitik, personalesikkerhed og adgang

Ved ansættelsen skal alle Dropbox-medarbejders baggrund kontrolleres, de skal underskrive en accept af sikkerhedspolitikken og en fortrolighedsaftale, og de skal gennemføre sikkerhedstræning. Kun personer, der har gennemført disse procedurer, får fysisk og logisk adgang til virksomheds- og produktionsmiljøerne, alt efter hvad der er nødvendigt for, at de kan udføre deres job. Desuden skal alle ansatte fuldføre årlig træning i sikkerhed og beskyttelse af persondata, og de trænes regelmæssigt i sikkerhedskendskab via informationsmails, seminarer og præsentationer samt ressourcer på vores intranet.

Medarbejders adgang til Dropbox-miljøet angives i et centralt register og godkendes ved hjælp af en kombination af stærke adgangskoder, SSH-nøgler, som er beskyttet med adgangssætninger, og totrinsbekræftelse. Fjernadgang kræver brug af VPN, der er beskyttet med totrinsbekræftelse, og alle særlige adgangshændelser gennemgås og vurderes af sikkerhedsteamet. Adgang til virksomheds- og produktionsnetværk er stærkt begrænset i henhold til definerede politikker. Adgang til produktionsnetværket er SSH-nøglebaseret og begrænset til ingeniørteams, der har brug for adgang for at udføre deres arbejdsopgaver. Konfiguration af firewalls kontrolleres omhyggeligt og er begrænset til et lille antal administratorer.

Desuden kræver vores interne politikker, at de medarbejdere, der får adgang til produktions- og virksomhedsmiljøer, skal overholde retningslinjer for oprettelse og opbevaring af private SSH-nøgler. Adgang til andre ressourcer, herunder datacentre, programmer til serverkonfigurering, produktionsservere og programmer til udvikling af kildekode, tildeles udelukkende efter specifik godkendelse af den relevante ledelse. Registrering af anmodningen om adgang, begrundelsen herfor og godkendelsen heraf udføres af ledelsen, og de relevante personer giver adgang.

Dropbox benytter teknisk adgangskontrol og interne politikker til at forhindre ansatte i at opnå vilkårlig adgang til brugerfiler og til at begrænse adgang til metadata og andre oplysninger om brugerkonti. For at beskytte slutbrugernes personlige oplysninger og sikkerhed er det kun et lille antal ingeniører, der er ansvarlige for at udvikle Dropbox' kerneydelser og har adgang til det miljø, hvor brugerfilerne opbevares. En medarbejders adgang fjernes med det samme, når medarbejderen forlader virksomheden.

Eftersom Dropbox-produkter og -tjenester bliver en forlængelse af vores kunders infrastruktur, garanterer vi dem, at vi er ansvarlige vogtere af deres data. Se afsnittet [Beskyttelse af personlige oplysninger](#) for at få flere oplysninger.

## Sikkerhedstræning og -kendskab

Vi udstyrer vores teams til softwareudvikling bedste praksis og teknikker til at udvikle sikre applikationer. I et digitalt landskab i konstant forandring er det afgørende at sørge for vores softwares sikkerhed, og vi forpligter os til at udruste vores teams med den viden og de færdigheder, der er nødvendige for at beskytte vores produkter og vores brugere.

## Koncernkontorer

- **Fysisk sikkerhed**

Dropbox' team for fysisk sikkerhed har ansvaret for at håndhæve politikken for fysisk sikkerhed og føre tilsyn med sikkerheden på vores kontorer.

- **Besøgs- og adgangspolitik**

Politik for besøgende og adgang. Fysisk adgang til virksomhedens faciliteter udover offentlige indgange og forhaller er begrænset til autoriseret Dropbox-personale og registrerede besøgende, som er ledsaget af Dropbox-personale. Et adgangssystem med adgangskort sørger for, at kun godkendte personer har adgang til områder i virksomhedens faciliteter, hvor der er adgang forbudt.

- **Serveradgang**

Adgang til områder, hvor virksomhedens servere befinder sig, såsom serverrum, er begrænset til autoriseret personale gennem ophøjede roller, der gives i systemet med adgangskort. Listerne over autoriserede personer, der er godkendt til fysisk adgang til virksomheds- og produktionsmiljøer, gennemgås som minimum hvert kvartal.

## Håndtering af sårbarheder

Vores sikkerhedsteam udfører regelmæssigt automatiserede og manuelle sikkerhedstest og patchadministration og samarbejder med eksterne specialister om at identificere og afhjælpe potentielle sikkerhedssårbarheder og fejl.

Som en nødvendig del af vores system til administration af informationssikkerhed rapporteres resultater og anbefalinger som følge af alle disse vurderingsaktiviteter til Dropbox-ledelsen, som vil evaluere dem og udføre de nødvendige handlinger, alt efter hvad der betragtes som nødvendigt. Alvorlige punkter dokumenteres, overvåges og håndteres af delegerede sikkerhedsingeniører.

## Fysisk sikkerhed

### Infrastruktur

Fysisk adgang til underleverandørers faciliteter, hvor produktionssystemerne findes, er begrænset til personale, som Dropbox har godkendt, i det omfang det er nødvendigt for at udføre deres jobfunktion. Alle personer, der skal have yderligere adgang til produktionsmiljøets faciliteter, opnår denne adgang ved hjælp af udtrykkelig godkendelse fra den relevante ledelse.

Registrering af anmodningen om adgang, begrundelsen herfor og godkendelsen heraf udføres af ledelsen, og de relevante personer giver adgang. Når godkendelsen er modtaget, vil et godkendt medlem af infrastrukturteamet kontakte den relevante underleverandør for at anmode om, at den godkendte person får adgang. Underleverandøren angiver brugerens oplysninger i sit eget system og giver det godkendte Dropbox-personale adgang ved hjælp af et adgangskort og biometrisk scanning (hvis det er muligt). Når godkendte personer har fået adgang, er det datacenterets opgave at sørge for, at adgang begrænses til kun de godkendte personer.

### Bemærkninger:

Tjenesterne Dropbox til teams, Dropbox Sign og Dropbox DocSend bruger Amazon Web Services til SaaS og IaaS, som driver avancerede faciliteter, der evalueres uafhængigt ved eksterne sikkerhedsvurderinger (f.eks. SOC 1, SOC 2 og ISO 27001). Amazon forvalter løbende risici og foretager løbende vurderinger for at sikre overholdelse af branchestandarder. Derudover bliver PaaS gennem Heroku, som servicerer Dropbox DocSend, også uafhængigt evalueret ved eksterne sikkerhedsvurderinger (f.eks. SOC 1, SOC 2 og ISO 27001).

Du kan se flere oplysninger om AWS' complianceprogram [her](#).

## Reaktion på hændelser

Vi har politikker for reaktion på hændelser og procedurer for håndteringen af problemer med tjenestens tilgængelighed, integritet, sikkerhed, beskyttelse af persondata og fortrolighed. Som en del af vores procedurer for reaktion på hændelser har vi dedikerede teams, der er uddannet til at:

- Reagere hurtigt på advarsler om potentielle hændelser.
- Bestemme hændelsens alvorsgrad.
- Om nødvendigt udføre handlinger for at afhjælpe og begrænse problemer.
- Kommuniker med relevante interne og eksterne interessenter, f.eks. ved at sende meddelelser til berørte kunder, for at overholde kontraktmæssige forpligtelser samt relevante love og bestemmelser vedrørende underretning om misligholdelse eller andre hændelser.
- Indsamle og opbevare beviser som led i en efterforskning.
- Dokumentere det arbejde, der foretages efter en sikkerhedsbrist, og udarbejde en permanent prioriteringsplan.

Politikker og processer for reaktioner på hændelser revideres som en del af vores SOC 2, ISO/IEC 27001 og andre sikkerhedsvurderinger.

## Sikkerhed for infrastruktur

Dropbox bruger standard- og brugerdefinerede tjenester, der hostes på Dropbox- og AWS-infrastruktur. AWS drives under fælles ansvar delt mellem Dropbox og AWS. AWS-infrastrukturens logiske og netværkssikkerhed leveres af AWS.

**Bemærk:** I øjeblikket befinder al AWS-infrastruktur anvendt til Dash sig i USA og distribueres på tværs af flere tilgængelighedszoner. Efterhånden som produktudvikling skrider frem for Dash, og kundefølgelse vokser, kan der blive tilføjet yderligere globale regioner for at understøtte krav til dataresidens.

### Netværkssikkerhed

Hos Dropbox sørger vi altid for at opretholde sikkerheden til vores basale netværk. Vores teknikker til netværkssikkerhed og -overvågning er udviklet til at levere adskillige lag af beskyttelse og forsvar. Vi anvender branchens standardteknikker til beskyttelse, herunder firewalls, scanning efter netværkssårbarheder, overvågning af netværkssikkerhed og systemer til registrering af indtrængen, for at sikre, at kun berettiget trafik er i stand til at nå vores infrastruktur.

Vores interne private netværk er segmenteret efter brug og risikoniveau. De primære netværk er:

- Internet-DMZ
- Prioriteret infrastruktur for DMZ
- Produktionsnetværk
- Erhvervsnetværk
- Dropbox-tjenester og -applikationer er isoleret via containere, når det er muligt

Adgang til produktionsmiljøet er begrænset til autoriserede IP-adresser og kræver multifaktorgodkendelse for alle slutpunkter. IP-adresser med adgang er tilknyttet virksomhedsnetværket eller godkendt Dropbox-personale. Autoriserede IP-adresser gennemgås hvert kvartal for at sikre et sikkert produktionsmiljø. Adgang til ændring af listen over IP-adresser er begrænset til autoriserede personer.

Trafik fra internettet, der er rettet mod vores produktionsnetværk, beskyttes med flere lag, der består af firewalls og proxyer.

Der opretholdes en streng afgrænsning mellem det interne Dropbox-netværk og det offentlige internet. Internetrelateret trafik til og fra produktionsnetværket kontrolleres nøje gennem en særlig proxytjeneste, som på sin side beskyttes af restriktive firewallregler.

Dropbox anvender sofistikerede værktøjssæt til at overvåge både bærbare og stationære computere med Mac- og Windows-operativsystemer og produktionssystemer for ondsindede hændelser. Sikkerhedslogfiler samles ét centralt sted til undersøgelse og reaktion på hændelser iht. branchestandarden for opbevaringspolitik.

Dropbox identificerer og reducerer risici via regelmæssig afprøvning af netværkssikkerheden og kontroller, der foretages af dedikerede interne sikkerhedsteams og eksterne sikkerhedsekspertes.

## Tilstedeværelsespunkter (PoP'er)

For at give brugerne den bedst mulige oplevelse med webstedet benytter Dropbox tredjepartsnetværk til levering af indhold (CDN'er) og Dropbox-hostede tilstedeværelsespunkter (PoP'er) på 31 steder i verden. Ingen brugerdata cachelagres på disse steder, og alle brugerdata, der overføres, krypteres med TLS. Fysisk og logisk adgang til Dropbox-hostede PoP'er begrænses til kun at omfatte personale, der er godkendt af Dropbox. Dropbox optimerer både transportlaget (TCP) og applikationslaget (HTTP).

## Peering

Dropbox har en åben peering-politik, og alle kunder er velkomne til at udføre peering med os. Se flere oplysninger på [dropbox.com/peering](https://dropbox.com/peering).

## Sikkerhedsovervågning

Dropbox bruger cloudbaserede sikkerhedsplatforme til at overvåge sikkerheden i produktionsmiljøet og holder aktivt udkig efter mistænkelig brugeraktivitet. Det omfatter direkte advarselseskalering til Dropbox Security.

## Påidelighed

Når du arbejder, har du brug for, at vi er der for dig. Derfor bestræber vi os på at nå den højest mulige opetid. Vi udvikler Dropbox-produkter og -tjenester med adskillige sikkerhedslag for at beskytte mod tab af data og sikre tilgængelighed.

## Datacentre og leverandører af administrerede tjenester

Dropbox' erhvervs- og produktionssystemer drives fra eksterne underleverandørers datacentre og leverandører af administrerede tjenester med adresse forskellige steder i USA. SOC-rapporter for underleverandørers datacentre og/eller leverandørernes sikkerhedsspørgeskemaer og kontraktlige forpligtelser gennemgås mindst én gang om året for at sikre tilstrækkelig sikkerhedskontrol. Disse eksterne tjenesteudbydere er ansvarlige for de fysiske, omgivelsesmæssige og driftsmæssige sikkerhedskontroller ved Dropbox-infrastrukturens begrænsninger. Dropbox er ansvarlig for den logiske, netværksmæssige og applikationsmæssige sikkerhed i vores infrastruktur, der drives fra tredjeparters datacentre.

Vores leverandør af administrerede tjenester til behandling og lagring, Amazon Web Services (AWS), er ansvarlig for den logiske og netværksikkerhedsmæssige del af Dropbox' tjenester, som leveres via deres infrastruktur. Forbindelser beskyttes ved hjælp af deres firewall, der konfigureres i en standardtilstand, hvor alt afvises. Dropbox begrænser adgangen til miljøet til et begrænset antal IP-adresser og medarbejdere.

Dashs intelligente dataanalyse- og beslutningsfunktioner er drevet af AWS Managed OpenSearch-platform, som leverer en komplet administreret SaaS-løsning med sikkerhed, hvilket demonstreres gennem deres ISO-certificerings- og SOC-attesteringsrapporter.

### Infrastruktur i Den Europæiske Union, Australien, Japan og Storbritannien

Dropbox tilbyder kvalificerede kunder lagring af filblokke i regioner uden for USA.

Vores opbevaringsinfrastruktur i EU hostes af Dropbox og er underlagt de samme kontroller og bestemmelser som beskrevet ovenfor for vores USA-baserede infrastruktur. Vores opbevaringsinfrastruktur hostes af Amazon Web Services (AWS) i Australien, Japan og Storbritannien og kopieres i den respektive region for at sikre redundans og beskytte mod datatab.

Filmetadata lagres i USA på Dropbox' egne servere. Paper-dokumenter og previews lagres i USA for alle kunder.

**Bemærk:** I øjeblikket er al AWS-infrastruktur, der bruges til Dash, placeret i USA og er fordelt på tværs af flere tilgængelighedszoner.

## Fortsat drift

Dropbox har etableret et system til håndtering af virksomhedsdrift (BCMS), der skal løse problemet med at genoptage eller fortsætte med at tilbyde tjenester til brugere (og hvordan man kan fungere som en virksomhed), hvis virksomhedskritiske processer og aktiviteter afbrydes. Vi udfører en cyklisk proces, som består af følgende faser:

- **Forretningsmæssige konsekvenser og risikovurderinger**

Vi udfører en vurdering af virksomhedskonsekvenser (BIA) mindst én gang om året for at finde ud af, hvilke processer der er vigtige for Dropbox, vurdere de mulige konsekvenser ved afbrydelser, etablere prioriterede tidsfrister for gendannelse og identificere vigtige elementer, som vi er afhængige af, og leverandører. Vi udfører også risikovurdering i hele virksomheden mindst én gang årligt. Risikovurderingen hjælper os med systematisk at identificere, analysere og evaluere risikoen ved afbrydelser af Dropbox. Risikovurderingen og BIA er med til at fremhæve prioriteter i forbindelse med kontinuitet samt afhjælpnings- og gendannelsesstrategier for planer til at sikre virksomhedskontinuitet (BCP'er).

- **Planer for virksomhedskontinuitet**

Teams, der ifølge BIA er kritiske for Dropbox' kontinuitet, bruger denne platform til at udvikle BCP'er for deres kritiske processer. Disse planer viser teams, hvem der er ansvarlig for at genoptage processer i nødstilfælde, hvem der i en anden Dropbox-afdeling kan overtage deres processer i tilfælde af en afbrydelse, og hvilke kommunikationsmetoder der skal bruges i tilfælde af afbrudt kontinuitet. Disse planer hjælper os også med at forberede os på en afbrydelse ved at centralisere vores gendannelsesplaner og andre vigtige oplysninger, f.eks. hvornår og hvordan planen skal bruges, kontakt- og mødeoplysninger, vigtige apps og gendannelsesstrategier. Dropbox' kontinuitetsplaner er en del af vores krisehåndteringsplan for hele virksomheden (CMP), der angiver Dropbox' krisehåndterings- og problemløsningsteams.

- **Planlæg test/udøvelse**

Dropbox tester udvalgte elementer i sine virksomhedskontinuitetsplaner mindst én gang om året. Disse tests er i overensstemmelse med BCMS' omfang og målsætninger, de er baserede på relevante scenarier, og de er gennemtænkte med tydeligt definerede målsætninger. Omfanget for disse tests kan være alt lige fra gruppeøvelser til omfattende simuleringer af virkelige begivenheder. Ved hjælp af resultaterne af testen og erfaring fra virkelige hændelser kan teams opdatere og forbedre deres planer for at afhjælpe problemer og blive bedre til at reagere på hændelser.

- **Gennemgang og godkendelse af BCMS**

Mindst én gang om året gennemgår vores ledelse BCMS som en del af gennemgangen af Dropbox' tillidsprogram.

## Katastrofegenoprettelse

Virksomheden er opmærksom på, at katastrofer kan ske når som helst uanset region eller placering. Infrastrukturen er designet til robusthed, og der er udarbejdet beredskabsplaner i tilfælde af hændelser, der påvirker tjenesterne. Vi bruger Amazon Web Services (AWS), som er spredt ud over flere datacentre til data- og behandlingsredundans. Vigtige data relateret til systemet sikkerhedskopieres dagligt. Ingeniørteamet underrettes i tilfælde af fejl i sikkerhedskopiering, og problemer løses efter behov.

For at leve op til kravene om sikkerhed i tilfælde af en voldsom krise eller et nedbrud, der påvirker driften af Dropbox til teams, følger vi altid en plan for gendannelse efter nedbrud. Dropbox' ingeniørteam gennemgår denne plan årligt og tester udvalgte elementer mindst én gang om året. Relevante problemstillinger dokumenteres og følges nøje, indtil de er løst.

Vores plan for gendannelse efter nedbrud (DRP) omfatter både holdbarheds- og tilgængelighedsnedbrud, der er defineret på følgende måder:

- Et holdbarhedsnedbrud består af en eller flere af følgende:
  - Et fuldstændigt eller permanent tab af et primært datacenter, hvor metadata gemmes, eller af flere datacentre, hvor filblokke opbevares.
  - Mistet evne til at kommunikere eller hente data fra et datacenter, hvor metadata opbevares, eller fra flere datacentre, hvor filindhold opbevares.
- Et tilgængelighedsnedbrud omfatter et eller flere af følgende:
  - Et nedbrud, der varer mere end 10 dage.
  - Manglende evne til at kommunikere eller hente data fra en lagertjeneste eller et datacenter, hvor metadata opbevares, eller fra flere lagertjenester eller datacentre, hvor filindhold opbevares.

Vi definerer et Recovery Time Objective (RTO), som er den tid, det tager at genoprette forretningsprocesser og tjenester til et bestemt serviceniveau efter en katastrofe, og et Recovery Point Objective (RPO), som er den længste acceptable periode, hvor data kan være mistet efter en afbrydelse af tjenesten. Vi måler også Recovery Time Actual (RTA) under testen af katastrofegenoprettelsen, som udføres mindst en gang om året.

Dropbox' planer for reaktion på hændelser, virksomhedskontinuitet og genoprettelse efter nedbrud testes i planlagte intervaller og efter betydelige organisatoriske og miljømæssige ændringer.

## Programsikkerhed

### Scanning og penetrationstests af sikkerheden (internt og eksternt)

Vores sikkerhedsteam udfører regelmæssig automatiseret og manuel test af applikationssikkerheden for at identificere og reparere potentielle sikkerhedsmangler og -fejl i vores computer-, web- og mobilapplikationer.

Alle Dropbox-applikationer er fuldt integreret med Dropbox' applikationssikkerhedsprogram. Vi foretager design- og arkitekturgennemgange af nye funktioner via vores indtagelsesproces. Al Dropbox-kode scannes for sikkerhedsrelaterede problemer ved hjælp af statiske kodeanalyseværktøjer som Semgrep og CodeScan.

Derudover har Dropbox indgået samarbejde med tredjepartsudbydere om at udføre periodiske penetrations- og sårbarhedstests i produktionsmiljøet. Vi samarbejder med eksterne specialister, andre sikkerhedsteams i branchen og netværket for forskning i sikkerhed for at beskytte vores applikationer. Vi bruger også automatiske analysesystemer til at identificere sårbarheder. Denne proces omfatter internt udviklede systemer, open source-systemer, som vi tilpasser til vores behov, og eksterne udbydere, som vi hyrer til kontinuerlig, automatiseret analyse.

## Sådan holdes skadeligt indhold væk fra Dropbox

Vi har scanningsfunktioner, der sigter mod at forhindre lagring og distribution af skadeligt indhold i Dropbox. Vores scannere benytter vores egen teknologi såvel som avancerede kapaciteter fra partnere som Microsoft og Google for at gøre Dropbox til et sikkert sted for vores kunder.

## Dusører for detektion af fejl

Mens vi samarbejder med professionelle firmaer, når det drejer sig om penetrationstests, og udfører vores egne interne tests, trækker dusører for detektering af fejl (eller belønningsprogrammer for sårbarhedsdetektering) på ekspertisen hos det bredere sikkerhedsfællesskab. Vores dusørprogram for detektering af fejl tilskynder forskere til at identificere og videregive softwarefejl på en ansvarlig måde. Vores inddragelse af det eksterne fællesskab forsyner vores sikkerhedsteam med uafhængige granskninger af vores applikationer for at hjælpe med at holde brugere sikre. Vi bestræber os på at være blandt de førende i branchen, når det gælder dusørprogrammer samt reaktions- og afhjælpningstider.

Vi har udarbejdet instrukser til, hvilke typer fejl der kan gøres opmærksom på i forbindelse med de enkelte Dropbox-applikationer, og vi har suppleret dem med en ansvarlig videregivelsespolitik, der opfordrer til detektering og rapportering af sikkerhedsårbarheder for at øge brugersikkerheden. Politikken indeholder følgende retningslinjer:

- Giv os en detaljeret beskrivelse af sikkerhedsproblemet.
- Vis respekt for vores eksisterende applikationer. Spamming af formularer gennem automatiserede sårbarhedsscannere vil ikke resultere i nogen form for belønning eller tildeling, da disse eksplicit er uden for anvendelsesområdet.
- Giv os rimelig tid til at reagere på problemet, før du videregiver oplysninger om sikkerhedsproblemet.
- Undlad at få adgang til eller ændre brugerdata uden tilladelse fra kontoens ejer.
- Dataene må ikke vises, ændres, gemmes, lagres, overføres eller på anden måde tilgås, og lokal information skal straks slettes, når du rapporterer sårbarheden til Dropbox.
- Foretag handlinger i god tro for at undgå at krænke beskyttelse af personlige oplysninger eller afbrydelse eller forringelse af vores tjenester (herunder denial of service-angreb).

Problemer kan rapporteres ved at indsende en rapport til Intigriti på:

<https://app.intigriti.com/programs/dropbox/dropbox>

## Databeskyttelse og kryptering

### Data under overførsel/dataoverførsler

Til beskyttelse af data under overførsel mellem Dropbox-apps og vores servere bruger Dropbox Transport Layer Security (TLS) til dataoverførsel, hvilket skaber en sikker kanal, som er beskyttet af 128-bit eller højere Advanced Encryption Standard-kryptering (AES). De fildata, der er under overførsel mellem en Dropbox til teams-klient (i øjeblikket computer, mobil, API eller web) og den

hostede tjeneste, krypteres altid ved hjælp af SSL/TLS. Til Dash-klienten og moderne browsere bruger vi robuste cifre, og på nettet markerer vi desuden alle godkendelsescookies som sikre og aktiverer HTTP Strict Transport Security (HSTS) med aktivering af inkludering af underdomæner. På samme måde krypteres Paper-dokumentdata, som overføres mellem en Paper-klient (i øjeblikket API eller web) og værtstjenesterne, vha. SSL/TLS.

Til Dropbox Sign og DocSend gemmes dokumenter bag en firewall og autentificeres mod afsenderens session, hver gang der afgives en anmodning om et dokument. Derudover er hvert dokument krypteret med en unik nøgle. Som en ekstra beskyttelse krypteres hver nøgle med en regelmæssigt udskiftet hovednøgle. Det betyder, at selv hvis nogen omgik fysisk sikkerhed og fjernede en harddisk, ville de ikke kunne dekryptere dine data.

På slutpunkter, der administreres af os (computer og mobil) og moderne browsere, bruger vi stærke koder og understøtter Perfect Forward Secrecy og certifikat-pinning. På nettet markerer vi desuden alle godkendelsescookies som sikre og aktiverer HTTP Strict Transport Security (HSTS) med aktivering af "includeSubDomains".

**Bemærk:** Dropbox benytter udelukkende TLS og har udfaset brugen af SSLv3 på grund af kendte sårbarheder. Men TLS kaldes ofte for "SSL/TLS", så vi bruger denne betegnelse her.

For at forhindre attacker-in-the-middle-angreb udføres der godkendelse af Dropbox' frontend-servere gennem offentlige certifikater, der er i klientens besiddelse. En krypteret forbindelse forhandles, før der overføres nogen filer eller Paper-dokumenter, og er med til at sørge for sikker levering til Dropbox' frontend-servere.

### **Data under opbevaring**

Dropbox-filer, som brugerne uploader, krypteres i hvile vha. 256-bit Advanced Encryption Standard-kryptering (AES). Filer gemmes på flere datacentre i diskrete filblokke. Hver blok fragmenteres og krypteres med en stærk kode. Kun de blokke, der er blevet ændret mellem versioner, synkroniseres. Paper-dokumenter i hvile krypteres også vha. 256-bit Advanced Encryption Standard-kryptering (AES). Paper-dokumenter gemmes på tværs af flere tilgængelighedszoner vha. tredjepartssystemer.

### **Nøgleadministration**

Dropbox' infrastruktur til nøgleadministration er udviklet med driftsmæssig, teknisk og proceduremæssig sikkerhedskontrol med meget begrænset direkte adgang til nøgler. Generering, udveksling og opbevaring af krypteringsnøgler fordeles med henblik på decentraliseret behandling. Tjenester til nøgleadministration er udviklet med driftsmæssig, teknisk og proceduremæssig sikkerhedskontrol.

- **Filkrypteringsnøgler**

Dropbox administrerer bevidst filkrypteringsnøgler på vegne af brugerne for at fjerne kompleksitet samt muliggøre avancerede produktfunktioner og robust kryptografisk kontrol. Filkrypteringsnøgler oprettes, lagres og beskyttes af sikkerhedskontroller og sikkerhedspolitikker i produktionssystemets infrastruktur.

- **Interne SSH-nøgler**

Adgang til produktionssystemer er begrænset med unikke SSH-nøglepar. Sikkerhedspolitikker og -procedurer kræver beskyttelse vha. SSH-nøgler. Et internt system administrerer den sikre offentlige nøgleudvekslingsproces, og private nøgler opbevares sikkert. Interne SSH-nøgler kan ikke bruges til at få adgang til produktionssystemer uden en separat anden godkendelsesfaktor.

- **Nøglefordeling**

Dropbox automatiserer administrationen og distributionen af følsomme nøgler til systemer, der er påkrævede for handlinger.

## Certifikat-pinning

Dropbox bruger certifikat-pinning på vores skrivebords- og mobilklienter. Certifikat-pinning er et ekstra tjek for at sikre, at vores klienter kun opretter forbindelse til servere med digitale certifikater fra en autoriseret liste over certifikatmyndigheder. Vi bruger det til at beskytte mod nationalstatsangribere, der har kontrol over en ondsindet certifikatmyndighed, samt til at beskytte dig mod lokal malware, der kan kapre dine forbindelser.

## Beskyttelse af godkendelsesdata

Dropbox bruger mere end almindelig hashing til at beskytte brugernes loginoplysninger. I henhold til retningslinjerne i branchen "saltes" hver enkelt adgangskode med tilfældigt genereret "salt", som er unikt for hver bruger, og vi bruger gentagen hashing til at gøre beregningen langsommere. Disse metoder er med til at beskytte mod voldsomme forsøg på indtrængen, ordbogs- og regnbueangreb. Som en ekstra foranstaltning krypterer vi hashene med en nøgle, der gemmes separat fra databasen, hvilket er med til at beskytte adgangskoder i tilfælde af, at kun databasen kompromitteres.

## Malware-scanning

Vi har udviklet et automatiseret system, der scanner efter malware på det tidspunkt, hvor indhold deles uden for den oprindelige brugers konto. Systemet benytter både patenteret teknologi og registreringsprogrammer, som er standard i branchen, og er designet til at standse malware i at blive spredt.

# Produktsikkerhed

## Designgennemgange

Sikkerhedsteamet hos Dropbox integrerer sikkerhedsgennemgang i produktkøreplanen, så alle større udgivelser har gennemgået trusselsmodeller og designgennemgange for at kunne levere en sikker oplevelse til vores brugere.

## Sikker implementering

Som en del af vores livscyklus for udvikling af software bliver koden først analyseret og scannet for kodekvalitet og sikkerhedsfejl, hver gang der tilføjes nye Dropbox-applikationsfunktioner til vores kodebase. Funktioner skal bestå denne gennemgang, herunder fagfællebedømmelse, før de anses for at være klar til udgivelse.

## Ændringsstyring

Alle udviklings-, problemrensings- og rettelserprocesser følger vores formelle politik til ændringsstyring, der er defineret af teknikerteamet hos Dropbox, for at sikre, at systemændringer er blevet testet og godkendt inden implementering i produktionsmiljøerne. Ændringer i kildekode påbegyndes af udviklere, der vil forbedre Dropbox-applikationen eller -tjenesten. Ændringer gemmes i et system til versionskontrol og skal gennemgå automatiserede testprocedurer for kvalitetssikring (QA) for at bekræfte, at sikkerhedskravene er opfyldt. En vellykket kvalitetskontrol betyder, at ændringen vil blive implementeret. QA-godkendte ændringer implementeres automatisk i produktionsmiljøet. Vores livscyklus for udvikling af software (SDLC) kræver, at sikre retningslinjer for kodning overholdes, og kodeændringer gennemgås for sikkerhedsproblemer via vores processer til kvalitetskontrol og manuel gennemgang. Ændringer, der er udgivet til produktion, bliver logget og arkiveret, og advarsler sendes automatisk til Dropbox' ingeniørteam.

Kun autoriseret personale kan lave ændringer i Dropbox' infrastruktur. Dropbox' sikkerhedsteam er ansvarlig for at vedligeholde infrastrukturens sikkerhed og sørge for, at serverne, firewalls og andre sikkerhedsrelaterede konfigurationer opdateres og overholder branchens standarder. Firewallregelsæt og enkeltpersoner med adgang til produktionsservere gennemgås regelmæssigt.

# Beskyttelse af personlige data

Enkeltpersoner og organisationer betror Dropbox med deres vigtigste arbejde, og det er vores ansvar at beskytte det. Hos Dropbox mener vi, at du ejer dine data, og vi lægger vægt på at beskytte dem. Vores [persondatapolitik](#) beskriver tydeligt, hvordan vi håndterer og beskytter dine oplysninger. På årlig basis tester uafhængige, eksterne inspektører vores kontrolforanstaltninger for persondata og aflægger deres rapporter og udtalelser, som vi derefter kan give dig efter anmodning. Du kan få mere information om vores praksisser og principper for beskyttelse af persondata i [hvidbogen om beskyttelse af personlige oplysninger og data](#).

Hvis du vil rapportere et problem relateret til databeskyttelse, skal du kontakte: [privacy@dropbox.com](mailto:privacy@dropbox.com).

# Dropbox til teams

Digitale transformationer vinder større og større indpas i flere brancher, og det er afgørende, at data, teams og enheder beskyttes, uanset hvor de er. Organisationer, der bruger cloudløsninger som Dropbox til teams til at muliggøre fjern- og distribuerede arbejdsgange, har brug for at strømline samarbejde, proaktivt styre cloudrisici og implementere effektive kontrolforanstaltninger, der sikrer fortroligheden af deres intellektuelle ejendom (IP), integriteten af lagrede og delte data, tilgængeligheden af data gennem administrerede og robuste cloudtjenester.

Mere end 575.000 virksomheder og organisationer bruger Dropbox til teams som løsningen til sikkert samarbejde mellem eksterne og distribuerede teams. Den centrale Dropbox til teams-løsning inkluderer et smart workspace til samarbejde samt filsynkronisering og delingsfunktioner. Vores løsninger understøttes af branchens førende infrastruktur samt funktioner til avanceret virksomhedssikkerhed, team- og indholdssikkerhed, elektronisk underskrift, sikker overførsel og dataforvaltning. Medmindre andet er angivet, gælder oplysningerne i denne hvidbog for alle Dropbox til teams-produkter. Paper er en funktion i Dropbox til teams.

Kernen i Dropbox til teams er vores omfattende sikkerhedsprogram – Dropbox' tillidsprogram – som har en sikkerhedstilgang med flere lag, hvilket er vigtigt, da globale tilgange til fjernarbejde udvikler sig.

Denne hvidbog beskriver produktsikkerhedsfunktioner for Dropbox til teams, Dropbox' operationelle sikkerhedsforanstaltninger, vores forpligtelse til beskyttelse af personlige oplysninger og gennemsigtighed samt backend-politikker, uafhængige certificeringer og lovgivningsmæssige compliance-foranstaltninger, der gør Dropbox til den sikre løsning for din organisation.

**Bemærk:** Medmindre andet er angivet, gælder oplysningerne i denne hvidbog for alle Dropbox til teams-produkter. Paper er en funktion i Dropbox til teams.

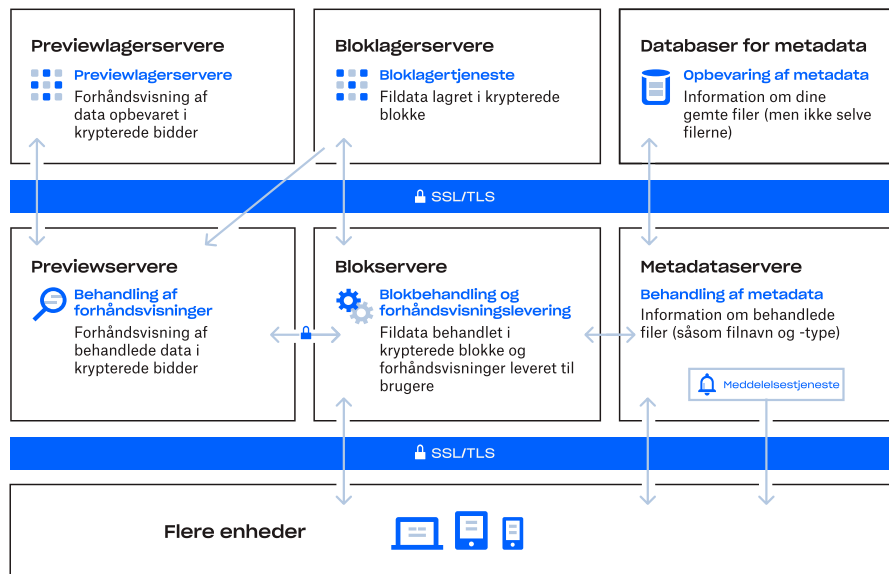
## Bag kulisserne

Vores brugervenlige grænseflader understøttes af en infrastruktur, som fungerer bag kulisserne for at sikre hurtig og pålidelig synkronisering, deling og samarbejde. Til det formål forbedrer vi hele tiden vores produkt og arkitektur for at gøre dataoverførsler hurtigere, forbedre driftsikkerheden og tilpasse os til ændringer i omgivelserne. I dette afsnit forklarer vi, hvordan data overføres, opbevares og behandles på sikker vis.

## Infrastruktur for filer

Dropbox-brugere kan få adgang til filer og mapper når som helst på stationære pc'er, internettet og mobilklienter eller via tredjepartsapplikationer, som er brugt til at oprette forbindelse til Dropbox. Alle disse klienter opretter forbindelse til krypterede servere, så brugerne kan få adgang til filer, dele filer med andre og opdatere tilknyttede enheder, når filerne tilføjes, ændres eller slettes.

Dropbox' filinfrastruktur består af følgende komponenter:



- **Metadataservere**

Vise grundlæggende oplysninger om brugerdata, der kaldes metadata, opbevares i deres egen særskilte lagertjeneste og fungerer som et indeks for dataene på brugernes konti. Metadataene indeholder grundlæggende konto- og brugeroplysninger, f.eks. e-mailadresse, navn og enhedsnavne. Metadataene indeholder også grundlæggende oplysninger om filer, f.eks. filnavne og -typer, hvilket understøtter funktioner som versionshistorik, gendannelse og synkronisering.

- **Databaser for metadata**

Filmetadata lagres i en transaktionel nøgleværdiopbevaring med multiversionkontrol af samtidighed og deles og kopieres efter behov for at opfylde kravene til ydeevne og høj tilgængelighed.

- **Blokserevere**

Dropbox er designet med en unik sikkerhedsmekanisme, som beskytter brugerdata med mere end blot traditionel kryptering. Blokserevere behandler filer fra Dropbox-applikationerne ved at dele hver enkelt fil op i blokke, kryptere hver enkelt fil ved hjælp af en stærk kode og kun synkronisere de blokke, som er ændret fra version til version. Når en Dropbox-applikation registrerer en ny fil eller ændringer af en eksisterende fil, underretter applikationen blokserevere om ændringen, og nye eller ændrede filblokke behandles og overføres til bloklagerserverne. Blokserevere bruges desuden til at levere filer og forhåndsvisninger til brugere. Du kan se detaljerede oplysninger om den kryptering, der bruges af disse tjenester både under overførsel og ved opbevaring, under [Kryptering](#).

- **Bloklagerservere**

Det faktiske indhold af brugerfiler lagres i krypterede blokke på bloklagerserverne. Før overførslen opdeler Dropbox-klienten filerne i filblokke som forberedelse til lagringen. Bloklagerserverne fungerer som et CAS-system (Content-Addressable Storage), hvor hver enkelt krypteret filblok hentes på baggrund af dens hash-værdi.

- **Previewservere**

Forhåndsvisningsserverne producerer forhåndsvisninger af filer. Forhåndsvisninger er en gengivelse af en brugers fil i et andet filformat, der er bedre egnet til hurtig visning på en slutbrugers enhed. Forhåndsvisningsservere henter filblokke fra bloklagerserverne for at generere forhåndsvisninger. Når der anmodes om forhåndsvisning af en fil, henter forhåndsvisningsserverne cache-forhåndsvisningen fra forhåndsvisningslagerserverne og overfører den til blokserverne. Til sidst vises forhåndsvisninger til brugere af blokservere.

- **Previewlagerservere**

Cachede previews lagres i et krypteret format på previewlagerserverne.

- **Meddelelsetjeneste**

Denne separate tjeneste overvåger, om der foretages ændringer af Dropbox-konti. Ingen filer eller metadata opbevares eller overføres her. Hver klient etablerer en lang forespørgselsforbindelse til meddelelsetjenesten og venter. Når der sker en ændring i en fil i Dropbox, giver meddelelsetjenesten besked om ændringen til de(n) pågældende klient(er) ved at lukke den lange forespørgselsforbindelse. Når forbindelsen lukkes, er det tegn til, at klienten skal oprette en sikker forbindelse til metadataserverne for at synkronisere eventuelle ændringer.

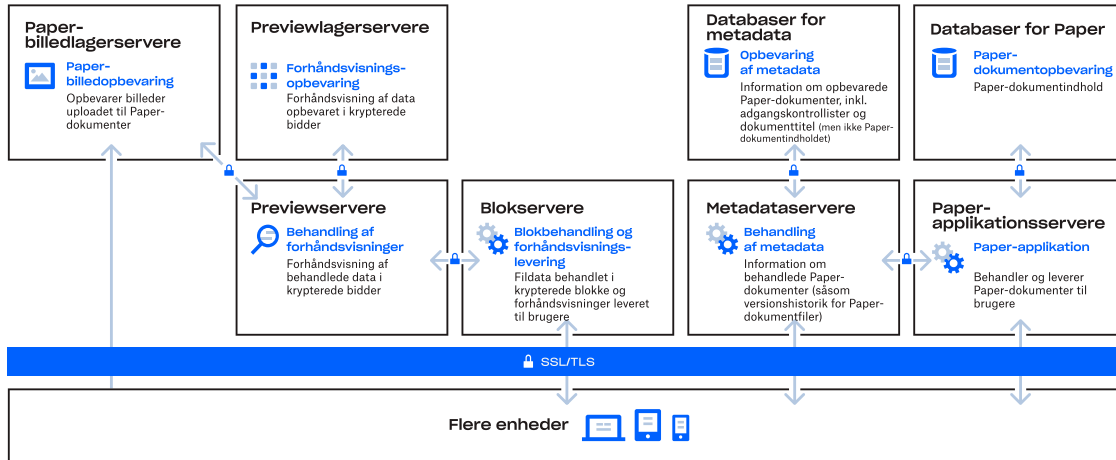
## Opbevaring af fildata

Dropbox opbevarer primært to typer fildata: metadata om filer (f.eks. datoen og tidspunktet, hvor en fil sidst blev ændret) og filernes egentlige indhold (filblokke). Filers metadata gemmes på Dropbox-servere. Filblokke gemmes i enten Amazon Web Services (AWS) eller Magic Pocket, som er Dropbox' interne lagersystem. Magic Pocket består af både patenteret software og hardware og er designet fra bunden til at være pålideligt og sikkert. I både Magic Pocket og AWS krypteres filblokke under opbevaring, og begge systemer overholder strenge standarder for driftssikkerhed. Få flere oplysninger under [Pålidelighed](#).

## Infrastruktur for Paper

Dropbox-brugere kan når som helst få adgang til Paper-dokumenter via internettet eller gennem eksterne applikationer, der er forbundet med Dropbox Paper-applikationen. Alle disse klienter er forbundet til sikre servere for at give adgang til Paper-dokumenter, gøre det muligt at dele dokumenter med andre og at opdatere forbundne enheder, når dokumenter tilføjes, ændres eller slettes.

Dropbox Papers infrastruktur består af følgende komponenter:



- **Paper-applikationsservere**

Paper-applikationsserverne behandler brugeranmodninger, gengiver output fra redigerede Paper-dokumenter tilbage til brugeren og kører meddelelsestjenester. Paper-applikationsservere skriver indgående brugerændringer til Paper-databaserne, hvor de gemmes i permanent lager. Kommunikationssessioner mellem Paper-applikationsservere og Paper-databaser er sikret med Transport Layer Security (TLS).

- **Paper-databaser**

Det faktiske indhold af brugernes Paper-dokumenter samt visse metadata om Paper-dokumenter krypteres i permanent lager i Paper-databaserne. Dette inkluderer oplysninger om et papirdokument (såsom titel, ejer, oprettelsestid og anden information) samt indhold i selve papirdokumentet, inklusive kommentarer og opgaver. Paper-databaserne opdeles og kopieres efter behov for at opfylde kravene til ydeevne og høj tilgængelighed.

- **Metadataservere**

Paper bruger de samme metadata-servere, der er beskrevet i Dropbox-infrastrukturdiagrammet til at behandle oplysninger om Paper-dokumenter, såsom revisionshistorik for Paper-dokumenter og medlemskab af delt mappe. Dropbox har direkte administration af metadata-servere, som er placeret i tredjeparts samlokaliserede datacentre.

- **Databaser for metadata**

Paper bruger de samme metadata-databaser, der er beskrevet i Dropbox-infrastrukturdiagrammet til at gemme oplysninger, der er relateret til Paper-dokumenter, såsom deling, tilladelser og mapeassociationer. Filmetadata lagres i en MySQL-understøttet databasetjeneste og deles og kopieres efter behov for at opfylde kravene til ydeevne og høj tilgængelighed.

- **Paper-billedlagerservere**

Billeder, der uploades til Paper-dokumenter, lagres og krypteres i hvile på Paper-billedlagerserverne. Overførsel af billeddata mellem Paper-applikationen og Paper-billedserverne foregår med en krypteret session.

- **Previewservere**

Previewserverne producerer previews for både billeder, som uploades til Paper-dokumenter, og for hyperlinks, som er indlejret i Paper-dokumenter. For billeder, der uploades til Paper-dokumenter, henter previewserverne billeddata, der er lagret på Paper-billedlagerserverne, gennem en krypteret kanal. For hyperlinks, der er indlejret i Paper-dokumenter, henter previewservere billeddataene og viser et preview af billedet ved hjælp af kryptering, der er specificeret i kildelinket. Til sidst vises previewet for brugere af blokserverne.

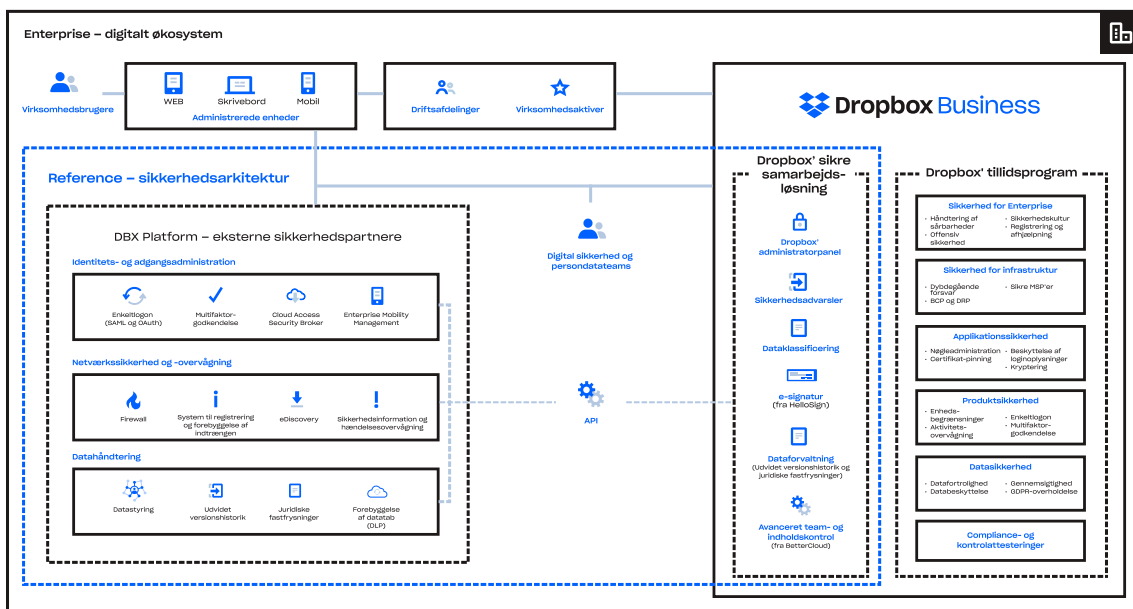
- **Previewlagerservere**

Paper bruger de samme previewlagerservere, der er beskrevet i diagrammet over Dropbox-infrastrukturen, til at lagre cachede billedpreviews. Bidder af cachede previews lagres i et krypteret format på previewlagerserverne.

## Opbevaring af Paper-dokumenter

Dropbox gemmer primært de følgende datatyper i Paper-dokumenter: metadata om Paper-dokumenter (for eksempel et dokumentes delte tilladelser) og det faktiske indhold af de Paper-dokumenter, som brugeren har uploadet. Disse kaldes under ét for Paper-dokumentdata, og billeder, der uploades til Paper-dokumenter, kaldes for Paper-billeddata. Hver af disse datatyper gemmes i Amazon Web Services (AWS). Paper-dokumenter er krypteret under opbevaring i AWS, og AWS overholder strenge standarder for driftssikkerhed. Du kan finde flere oplysninger under [Pålidelighed](#).

Vi anvender en tilgang bestående af flere lag til at sikre virksomhed, infrastruktur, applikationer og produkter, der påvirker din organisation.



# Pålidelighed

Et opbevaringssystem er kun godt, hvis det er driftssikkert, og vi har derfor udviklet Dropbox med adskillige sikkerhedslag for at beskytte mod tab af data og sikre, at disse data er tilgængelige.

## Metadata for filer

Ekstra kopier af metadata fordeles på tværs af uafhængige enheder i et datacenter i mindst en N+2-tilgængelighedsmodel. Delvise sikkerhedskopier oprettes som minimum på timebasis, og der oprettes komplette sikkerhedskopier for hver 36. time. Metadata gemmes på servere, der hostes og administreres af Dropbox i USA.

## Filblokke

Ekstra kopier af filblokke lagres uafhængigt i mindst to separate geografiske regioner og kopieres pålideligt inden for hver region. (Bemærk: For kunder, som vælger at have deres files lagret i vores tyske, australske, japanske eller britiske infrastruktur, kopieres filblokke kun inden for deres respektive regioner. Se yderligere oplysninger under [Datacentre og leverandører af administrerede tjenester](#).) Både Magic Pocket og AWS er beregnet til at levere en årlig datavarighed på mindst 99,999999999 %.

Dropbox' arkitektur, applikationer og synkroniseringsmekanismer arbejder sammen om at beskytte brugerdata og gøre dem vidt tilgængelige. I det sjældne tilfælde, at der skulle opstå problemer med tjenestens tilgængelighed, vil Dropbox-brugere stadig have adgang til de seneste kopier af filer, der er blevet synkroniseret til den lokale Dropbox-mappe på tilknyttede computere. De kopier af filer, der er synkroniseret i Dropbox-computerappen/den lokale mappe, er tilgængelige fra en brugers harddisk under nedetid eller driftsstop, eller i offline-tilstand. Ændringer af filer og mapper synkroniseres til Dropbox, når der igen er forbindelse til tjenesten eller netværket.

## Paper-dokumenter

Ekstra kopier af Paper-dokumentdata fordeles på tværs af uafhængige enheder i et datacenter i en N+1-tilgængelighedsmodel. Der tages også komplette sikkerhedskopier af Paper-dokumentdata hver dag. Til lagring af Paper-dokumenter bruger Dropbox AWS-infrastruktur i USA, som er designet til at give en årlig datastabilitet på mindst 99,999999999 %.

## Filsynkronisering

Dropbox har den bedste filsynkronisering, som er anerkendt i resten af branchen. Vores synkroniseringsmekanismer giver hurtige, responsive filoverførsler og mulighed for adgang til data på tværs af enheder overalt. Dropbox-synkronisering er også robust. Hvis forbindelsen til Dropbox-tjenesten afbrydes, genoptager en klient hurtigt handlingen, så snart forbindelsen genoprettes.

Filerne opdateres kun på den lokale klient, hvis de er synkroniseret fuldstændigt og valideret med Dropbox-tjenesten. Justering af belastningen på tværs af flere forskellige servere sikrer redundans og en konsekvent synkroniseringsoplevelse for slutbrugere.

### Deltasynkronisering

Hvis man bruger denne synkroniseringsmetode, bliver kun ændrede dele af filer downloadet eller uploadet. Dropbox gemmer hver fil i separate, krypterede blokke og opdaterer kun de blokke, der er ændret.

### Streamingsynkronisering

I stedet for at vente på at en filupload afsluttes, begynder streamingsynkroniseringen at downloade synkroniserede blokke til en anden enhed, før upload af alle blokkene fra den første enhed er afsluttet. Denne metode bruges automatisk, hvis separate computere forbindes til den samme Dropbox-konto eller når forskellige Dropbox-konti deler en mappe.

### Sparer plads på harddisken

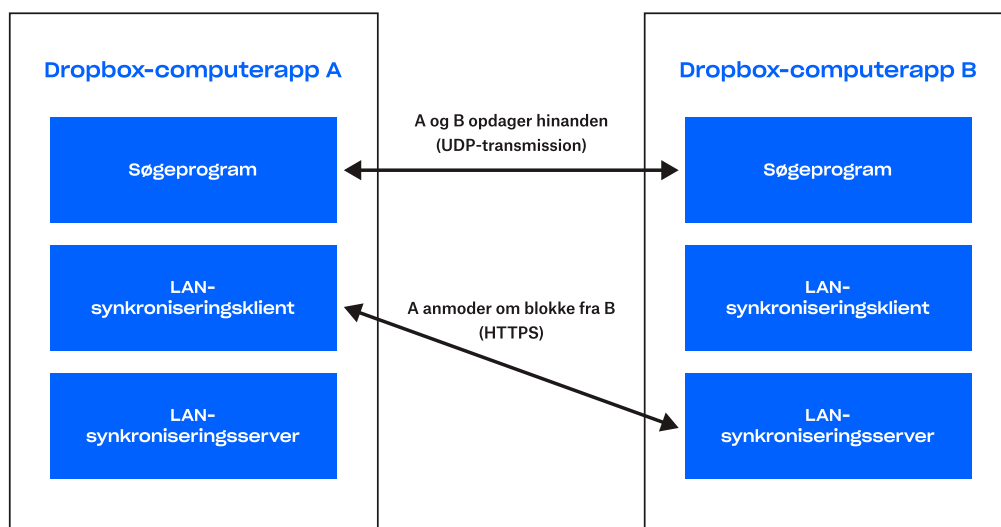
Brugere kan frigøre lagerplads på deres computere ved kun at gøre de filer, de vil have på deres harddisk, tilgængelige offline. Det frigør computerplads, ved at alt andet kun er online på [dropbox.com](https://dropbox.com).

### LAN-synkronisering

Når denne funktion aktiveres, henter den nye og opdaterede filer fra andre computere på det samme lokale netværk (LAN), hvilket sparer tid og båndbredde i forhold til at downloade filerne fra Dropbox-servere.

### Arkitektur

Der findes tre hovedkomponenter i LAN-synkroniseringssystemet, som kører på computerappen: søgeprogrammet, serveren og klienten. Søgeprogrammet finder maskiner på netværket, der skal synkroniseres med. Dette begrænses til maskiner, som har autoriseret adgang til samme personlige eller delte Dropbox-mappe(r). Serveren håndterer anmodninger fra andre maskiner på netværket og henter de filblokke, der anmodes om. Klienten anmoder om filblokke fra netværket.



## Søgeprogram

Hver enkelt maskine i det lokale netværk sender og lytter efter UDP-signalpakker via port 17500 (som reserveres af IANA til LAN-synkronisering). Disse pakker indeholder versionen af den protokol, der bruges af den pågældende computer, de personlige og delte Dropbox-mapper, der understøttes, den TCP-port, der bruges til at køre serveren (som kan være en anden end 17500, hvis den pågældende port ikke er tilgængelig) og en tilfældig identifikator til maskinen. Når en pakke opdages, føjes maskinens IP-adresse til en liste for hver personlige eller delte mappe for at angive en potentiel destination.

## Protokol

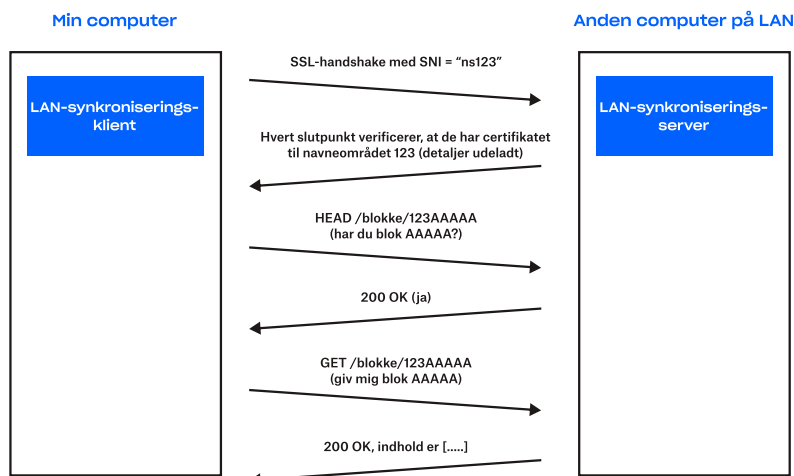
Selve overførslen af filblokke udføres via HTTPS. Hver enkelt computer kører en HTTPS-server med slutpunkter. En klient vil polle flere ligesindede for at se, om de har blokkene, men downloader kun blokke fra en enkelt server.

For at beskytte alle dine data sørger vi for, at det kun er de klienter, som har adgang til en bestemt mappe, der kan anmode om filblokke. Vi sørger også for, at computere ikke kan udgive sig for at være servere til mapper, som de ikke har kontrol over. For at løse dette genererer vi TLS-/certifikatpar for hver enkelt personlige Dropbox-mappe eller delte mappe. Disse fordeles fra Dropbox-servere til de af brugerens computere, som har adgang til mappen. Nøgle-/certifikatparrene udskiftes, hver gang et medlemskab ændres (f.eks. når en person fjernes fra en delt mappe). Vi bruger begge ender af HTTPS-forbindelsen til at godkende ved hjælp af det samme certifikat (certifikatet for Dropbox-mappen eller den delte mappe). Dette beviser, at begge ender af forbindelsen har tilladelse.

Når der skal etableres en forbindelse, fortæller vi serveren, hvilken personlig Dropbox eller mappe vi forsøger at oprette forbindelse til, ved at bruge Server Name Indication (SNI), så serveren bruger det korrekte certifikat.



Dropbox distribuerer cert/nøglepar til navneområdet 123



## Server/klient

Med den førnævnte protokol skal serveren kun vide, hvilke blokke der er til stede, og hvor de findes.

Ved hjælp af søgeprogrammets resultater opretholder klienten en liste over peers for hver enkelt personlige Dropbox-mappe eller delte mappe. Når LAN-synkroniseringssystemet modtager en anmodning om at hente en filblok, sender det en anmodning til et tilfældigt eksempel på de peers, som det har søgt efter for den personlige Dropbox-mappe eller delte mappe, og derefter anmoder det om blokken fra den første, der svarer, at den har blokken.

For at undgå forsinkelser benytter vi forbindelsespuljer, der gør det muligt at genanvende forbindelser, som allerede er oprettet. Vi åbner først en forbindelse, når det er nødvendigt, og når den er åbnet, holder vi den aktiv, hvis vi skulle få brug for at benytte den igen. Vi begrænser også antallet af forbindelser til en enkelt peer.

Hvis en filblok ikke kan findes eller hentes, eller hvis forbindelsen er for langsom, henter systemet i stedet blokken fra Dropbox-servere.

## Dropbox' brugergrænseflader

Dropbox-tjenesten kan udnyttes og tilgås via en række grænseflader. Hver enkelt grænseflade har sikkerhedsindstillinger og funktioner, der behandler og beskytter brugerdata og samtidig gør det let at få adgang.

- **WEB**

Denne grænseflade kan åbnes i alle moderne webbrowsere. Den giver brugere mulighed for at uploade, downloade, se og dele deres filer. Webgrænsefladen giver også brugere mulighed for at åbne eksisterende lokale versioner af filer via deres computers standardprogram.

- **Skrivebord**

Dropbox' computerapp er en effektiv synkroniseringsklient, som opbevarer filer lokalt med henblik på offlineadgang. Den giver brugere fuld adgang til deres Dropbox-konti og kører på operativsystemerne Windows og Mac. Filer kan ses og deles direkte i operativsystemernes filbrowsere.

- **Mobil**

Dropbox-appen kan fås til iOS- og Android-enheder og giver brugere adgang til alle deres filer, når de er på farten. Mobilappen giver også brugerne mulighed for at gøre filer tilgængelige til offlineadgang.

- **API**

Dropbox-API'er giver en fleksibel metode til at læse og skrive til Dropbox-brugerkonti og til at få adgang til avancerede funktioner såsom søgning, revideringer og gendannelse af filer. API'erne kan bruges til at administrere brugerlivscyklussen for en Dropbox til teams-konto, udføre handlinger for alle medlemmer af teamet og give adgang til administratorfunktioner i Dropbox til teams.

# Brugergænseflader i Paper

Du kan bruge og få adgang til Paper-tjenesten via en række grænseflader. Hver enkelt grænseflade har sikkerhedsindstillinger og funktioner, der behandler og beskytter brugerdata og samtidig gør det let at få adgang.

- **WEB**

Denne grænseflade kan åbnes i alle moderne webbrowsere. Den giver brugerne mulighed for at oprette, se, redigere, downloade og dele deres Paper-dokumenter.

- **API**

Dropbox API'en, som er beskrevet ovenfor, omfatter slutpunkter og datatyper til administration af dokumenter og mapper i Dropbox Paper, herunder understøttelse af funktioner som f.eks. administration af tilladelser, arkivering og permanent sletning.

## Dropbox Replay

Dropbox Replay er et værktøj til medie gennemgang og -godkendelse, der giver brugerne mulighed for at samarbejde om at markere, kommentere og færdiggøre video-, billed- og lydfiler. Det understøtter feedback i realtid, nem deling, uden at samarbejdspartnere behøver have Dropbox-konti, og funktioner som live gennemgang, versionssammenligning og avancerede kommentarer.

Replay indeholder flere sikkerhedsforanstaltninger for at beskytte medieindhold og brugerdata. Det integreres med Dropbox' administratorpanel til adgangskontrol, delingsbegrænsninger og brugeradministration, herunder overvågningslog og brugerfjernelsesfunktioner. Replay udfører også godkendelseskontroller af søgeresultater for at sikre, at brugerne kun ser indhold, de har adgang til, og anvender inputvalidering og rensning for at forebygge sikkerhedsrisici som Cross-Site Scripting (XSS). Derudover understøtter Replay sikker håndtering af filer, herunder PDF'er og PSD'er, med forholdsregler for at afbøde JavaScript-baserede angreb.

## Apps til Dropbox

Dropbox-plattformen omfatter et solidt økosystem af udviklere, der udarbejder vores fleksible Application Programming Interfaces (API'er). Mere end 750.000 udviklere har oprettet applikationer og tjenester på platformen til produktivitet, samarbejde, sikkerhed, administration med mere.

## Færdigbyggede komponenter

Chooser, Saver, and Embedder er forudbyggede web- og mobilkomponenter, der giver nem adgang til Dropbox i tredjeparts apps/websteder på bare et par kodelinjer.

- Vælgeren aktiverer valg af filer fra Dropbox.
- Gemmeren gør det muligt for brugerne at gemme filer direkte i Dropbox.
- Indlejrerer giver brugerne mulighed for at se filer og mapper fra Dropbox.

Autorisationen til disse komponenter er udelukkende via Dropbox. Apps får adgang til filer, der er valgt af Chooser via Dropbox-delte links eller kortvarige download-links. Disse færdigbyggede komponenter kan bruges uafhængigt eller i forbindelse med API'en som beskrevet nedenfor.

## Dropbox til teams-API-integrationer

Den offentlige Dropbox API giver tredjepartsudviklere mulighed for at få adgang til og interagere med Dropbox i deres applikationer. Dette inkluderer fil- og metadata-interaktion, deling og teamfunktionalitet.

### Bemyndigelse

Dropbox bruger protokollen OAuth, som er standard i branchen, til godkendelse, så brugerne får mulighed for at give apps adgang til konti uden at afsløre deres loginoplysninger til disse konti. Vi understøtter OAuth 2.0 til godkendelse af API-anmodninger. Anmodninger godkendes via Dropbox' website eller mobilapp. Dropbox understøtter OAuth-bedste praksis, bla. kortvarige adgangstokener og PKCE til distribueere apps.

### Brugertilladelser

Apps, der bruger Dropbox API, kan bygges med følgende niveau af indholdsadgang til en slutbrugers Dropbox:

- **App-mappe**

Der oprettes en dedikeret mappe med samme navn som appen i mappen Apps i en brugers Dropbox. Appen får kun læse- og skriveadgang til denne mappe, og brugere kan stille indhold til rådighed for appen ved at flytte filer til denne mappe. Appen kan desuden anmode om fil-/mappeadgang via Chooser eller Saver.

- **Fuld Dropbox**

Appen får fuld adgang til alle filer og mapper i en brugers Dropbox og kan også anmode om fil-/mappeadgang via Vælgeren eller Gemmeren.

Ansøgninger kan også anmode om specifikke anvendelsesområder, som begrænser deres adfærd ved adgang til undergrupper af API-slutpunkter. F.eks. kan applikationer være begrænset til skrivebeskyttet adgang til filer – eller mulighed for at uploade indhold, men ikke til at oprette delinger.

## Teamtilladelser

Administratorer for Dropbox til teams kan godkende applikationer til administrationsfunktionalitet, som er i teamets administratorpanel. De handlinger, som teamforbundne apps kan udføre, er begrænset gennem tilladelser, der specificerer, hvilke teamindstillinger appen kan læse eller administrere.

*Almindelige kombinationer af omfangs-kombinationer inkluderer:*

- **Teaminformationer**  
Skrivebeskyttet information om teamet og høj anvendelse.
- **Teamrevision**  
Skrivebeskyttet adgang til teaminfo og den detaljerede hændelseslog.
- **Filadgang for teammedlemmer**  
Muligheden for at udføre handlinger på vegne af brugere i teamet, f.eks. administration af deres filer og mapper.
- **Administration af teammedlemmer**  
Tilføjelse og fjernelse af medlemmer til og fra teamet.

## Webhooks

Webhooks er en måde, hvorpå webapps kan modtage meddelelser i realtid om ændringer i en brugers Dropbox. Når en URI registreres til at modtage webhooks, sendes der en HTTP-anmodning til den pågældende URI, hver gang der sker en ændring for en af appens registrerede brugere. Med API'en for Dropbox til teams kan webhooks også bruges til at generere meddelelser om ændringer i teammedlemskab. Mange sikkerhedsapps bruger webhooks til at hjælpe administratorer med at spore og administrere teamaktiviteter.

## Udvidelser

Apps kan registrere udvidelses-URI'er, så aktiveringer kan vises i menuerne "Del" og "Åbn" i Dropbox' brugergrænseflade. Udvidelser giver brugerne mulighed for at starte tilpassede arbejdsgange fra tredjepart direkte fra en fil i en Dropbox-overflade. Når en handling udløses, vil Dropbox omdirigere brugere til den specificerede URI og sende en filidentifikation, der kan bruges med API'en til at udføre enhver filoperation. En app skal autoriseres, før en registreret udvidelse er synlig for brugeren. Vi kan promovere et udvalgt sæt udvidelsesintegrationer i menuerne "Del" og "Åbn", selvom disse apps ikke har adgang til indhold, før brugeren godkender det.

## Retningslinjer for Dropbox-udviklere

Vi har udarbejdet en række retningslinjer og fremgangsmåder til at hjælpe udviklere med at oprette API-apps, der respekterer og beskytter brugernes personlige oplysninger og forbedrer brugernes Dropbox-oplevelse.

- **App-nøgler**  
Til hver enkelt app, som en udvikler opretter, skal der bruges en unik Dropbox-appnøgle. Hvis en app leverer tjenester eller software, der indkapsler Dropbox-plattformen, således at andre udviklere kan bruge den, skal hver enkelt udvikler desuden anskaffe en individuel Dropbox-appnøgle.

- **App-tilladelser**

Udviklere får besked om, at en app skal bruge tilladelsen med færrest mulige privilegier. Når en udvikler indsender en app til produktionsstatusgodkendelse, kontrollerer vi den for at sikre, at appen ikke anmoder om en unødvendig bred tilladelse baseret på den funktionalitet, som appen udfører.

- **Proces til gennemgang af apps**

- **Udviklingsstatus**

Når en Dropbox API-app udvikles, får den udviklingsstatus. Appen fungerer på samme måde som enhver produktionsstatus-app bortset fra, at den kun kan knyttes til maks. 500 Dropbox-brugere. Når en app tilknytter 50 Dropbox-brugere, har udvikleren to uger til at ansøge om og få produktionsstatusgodkendelse, før appens mulighed for at tilknytte yderligere Dropbox-brugere suspenderes.

- **Produktionsstatus og godkendelse**

For at opnå godkendelse til produktionsstatus skal alle API-apps overholde vores retningslinjer for branding samt vilkår og betingelser for udviklere, som indeholder eksempler på ulovlig anvendelse af DBX-plattformen. Disse anvendelser omfatter: Opfordring til krænkelse af intellektuel ejendomsret eller ophavsret, oprettelse af fildelingsnetværk og ulovligt download af indhold. Udviklere bliver først bedt om at give yderligere oplysninger om deres apps funktionalitet, og hvordan den bruger Dropbox API'en, før den indsendes til gennemgang. Når appen er godkendt til produktionsstatus, kan et hvilket som helst antal Dropbox-brugere oprette forbindelse til appen.

## **Administration af teamapps**

I et teams administratorpanel kan administratorer for Dropbox til teams [administrere](#) forbundne apps og integrationer for deres team.

## **API-partnerskaber**

Dropbox har arbejdet tæt sammen med sine teknologipartnere for at gøre det muligt for dem at udvikle integrationer med deres populære softwarepakker. Disse partnere bygger applikationer med Dropbox API'er og arbejder tæt sammen med Dropbox-arkitekter for at følge bedste praksis for sikkerhed og UX. Disse inkluderer en række produktivitetsapps for slutbrugere samt sikkerheds- og administrationsværktøjer såsom:

- **Sikkerhedsoplysninger og begivenhedsstyring (SIEM) og analyse**

Forbind din Dropbox til teams-konto til SIEM- og analyseværktøjer, så du kan overvåge og evaluere brugerdeling, forsøg på logon, administratorhandlinger med mere. Få adgang til og administrer logfiler for medarbejderaktivitet og sikkerhedsrelevante data via dit centrale administrationsværktøj for logfiler.

- **Forebyggelse af datatab (DLP)**

Scan automatisk metadata og indhold af filer, så der udløses advarsler, rapportering og handlinger, når der foretages vigtige ændringer på din Dropbox til teams-konto. Integrer virksomhedens politikker i din implementering af Dropbox til teams, så du hjælper med til at overholde alle krav og regler.

- **eDiscovery og fastfrysning af data**

Besvar søgsmål, voldgifter og lovmæssige høringer med data fra din Dropbox til teams-konto. Søg efter og indsamle relevante elektronisk gemte oplysninger, og bevar dine data gennem hele eDiscovery-processen, så du kan spare din virksomhed tid og penge.

- **Administration af digitale rettigheder (DRM)**

Tilføj tredjepartsprogrammer som beskyttelse af følsomme og ophavsretligt beskyttede data, der er gemt på medarbejderkonti. Få adgang til effektive DRM-funktioner, inklusive klientbaseret kryptering, vandmærkning, revisionsspor, tilbagekaldelse af adgangsrettigheder og blokering af brugere/enheder.

- **Dataoverførsel og sikkerhedskopiering på stedet**

Overførsel af data til Dropbox fra eksisterende servere eller andre cloudbaserede løsninger, så du sparer tid, penge og besvær. Automatisering af sikkerhedskopier fra din Dropbox til teams-konto til lokale servere.

- **Identitetsadministration og Single Sign-On (SSO)**

Automatisering af processen for klargøring og fjernelse af brugere og hurtigere onboarding af nye medarbejdere. Strømlining af administrationen, og styrkelse af sikkerheden ved at integrere Dropbox til teams med et eksisterende identitetssystem.

- **Brugerdefinerede arbejdsgange**

Udvikl interne apps, der integrerer Dropbox i eksisterende forretningsprocesser, for at forbedre virksomhedens interne arbejdsgange.

På siden for [Dropbox-appintegrationer](#) kan ses en liste over disse teknologipartnere. Slutbrugere kan finde udvalgte apps og integrationer fra første- og tredjepart i [App Center](#).

## Dropbox-integrationer

Vi har også samarbejdet med nogle af vores bedste teknologipartnere om at opbygge integrationer i Dropbox-overflader. Disse dybere integrationer er udviklet i fællesskab af Dropbox og partneren. Disse omfatter:

### Dropbox Extensions

Med disse integrationer kan du bruge forskellige typer appudvidelser til problemfrit at udføre handlinger såsom at offentliggøre en video, tilføje filer til e-mails og chats, sende en fil til e-signatur med mere – direkte fra Dropbox. Disse applikationer er bygget af partneren, mens Dropbox fremmer opdagelsen af udvalgte udvidelsespartnere gennem menuerne "Åbn med" og "Del med".

### Slack

Denne integration er bygget af Dropbox som førstepart, så brugere kan starte Slack-samtaler fra Dropbox. Slutbrugere godkender Slack via OAuth.

## Microsoft Office til mobilenheder og web

Vores Microsoft Office-integrationer giver brugere mulighed for at åbne Word-, Excel- og PowerPoint-filer, der er gemt i deres Dropbox, foretage ændringer i Office-mobilapps eller -webapps og gemme disse ændringer direkte i Dropbox. Brugere skal give adgang den første gang, hvor en Dropbox-fil åbnes i en Office-mobilapp eller -webapp. Når de senere åbnes igen, bevares disse links.

## Adobe Acrobat og Acrobat Reader

Vores integrationer med versioner af disse apps til computer og mobil (Android og iOS) giver brugere mulighed for at se, redigere og dele PDF-filer, som er gemt i deres Dropbox. Brugere bliver bedt om at give adgang ved første forsøg på at åbne en Dropbox-fil i hver enkelt app. Ændringer i PDF-filer gemmes automatisk i Dropbox.

# Produktsikkerhed

Dropbox indeholder funktioner til administrativ kontrol og synlighed, som gør det muligt for både it-teams og slutbrugere at administrere og sikre data på en effektiv måde. Med Dropbox får du alt, hvad du har brug for til arbejdet – dine værktøjer, indhold og samarbejdspartnere – alt på ét sted. Dropbox er mere end sikker opbevaring – det er en smart, problemfri måde at optimere din eksisterende arbejdsgang på.

Nedenfor kan du se fremhævede funktioner, der er tilgængelige for administratorer og brugere, samt tredjepartsintegrationer til administration af vigtige it-processer.

**Bemærk:** Tilgængeligheden af funktioner afhænger af abonnement. Se [dropbox.com/business/plans](https://dropbox.com/business/plans) for yderligere information.

## Indholdskontrol

Beskyttelse af følsomme virksomhedsaktiver – såsom intellektuel ejendom og personlig identificerbar information (PII) – er afgørende for it- og datasikkerhedsteams. Fra niveauinddelte indholdstilladelser til politikker for opbevaring af data og juridisk fastfrysning har Dropbox brancheførende løsninger til at administrere, overvåge og beskytte dit indhold. Nedenfor er de vigtigste Dropbox-produkter og -funktioner, der understøtter indholdskontrol.

### Niveauinddelte indholdstilladelser og delte fil- og mappetilladelser

- **Tilladelser til delte filer**

Et teammedlem, der ejer en delt fil, kan fjerne bestemte brugeres adgang og deaktivere kommentarer til filen.

- **Tilladelser til delte mapper**

Et teammedlem, der ejer en delt mappe, kan fjerne bestemte brugeres adgang til mappen, ændre visnings-/redigeringsstilladelser for bestemte brugere og overføre mappeejerskab. Alt efter teamets globale delingsstilladelser kan hver enkelt delt mappes ejer også bestemme, om den kan deles med personer uden for teamet, om andre med tilladelse til redigering kan administrere medlemskab, og om links kan deles med personer uden tilknytning til mappen.

- **Adgangskoder til delte links**

Ethvert delt link kan beskyttes med en adgangskode, som vælges af ejeren. Før filer eller data overføres, bekræfter et lag til adgangskontrol, at den rigtige adgangskode er indtastet, og at alle øvrige krav (f.eks. team, gruppe eller mappe-ACL) er overholdt. Hvis dette er tilfældet, gemmes en sikker cookie i brugerens browser. Denne cookie husker, at adgangskoden tidligere er bekræftet. Med delingsfunktioner kan administratorer også indstille standardadgangskoder i stedet for at have dem som valgfri for bedre at beskytte deres teams indhold.

- **Udløbsdatoer til delte links**

Brugere kan angive en udløbsdato til alle delte links for at give midlertidig adgang til filer eller mapper. Med delingsfunktioner kan administratorer også indstille standardudløbsdatoer i stedet for at have dem som valgfri for bedre at beskytte deres teams indhold.

## **Tilladelser til Paper-dokument og delt Paper-mappe**

- **Tilladelser til Paper-dokumenter og delte Paper-mapper**

Et teammedlem, der ejer et Paper-dokument eller en delt Paper-mappe, kan fjerne bestemte brugeres adgang og deaktivere redigering af Paper-dokumentet.

- **Tilladelser for Paper-dokumenter**

Et teammedlem, der ejer et Paper-dokument, kan fjerne adgangen for bestemte brugere, som eksplicit er angivet i delingspanelet. Både ejeren og redaktørerne for et Paper-dokument kan ændre visnings- og redigeringsstilladelser for bestemte brugere samt ændre dokumentets linkpolitik. Linkpolitikken bestemmer, hvilke brugere der kan åbne dokumentet, samt deres tilladelser. Teamadministratoren kan angive politikker for dokumentdeling, der gælder for hele teamet.

- **Tilladelser for Paper-mapper**

Et teammedlem, der er medlem af mappen, kan ændre mappens delingspolitik og fjerne adgangen for bestemte brugere, som er blevet tilføjet eksplicit til mappen.

## **Fil- og mappehandlinger**

- **Teammapper for filer**

Administratorer kan oprette teammapper, der automatisk giver grupper og andre kollegaer det rette adgangsniveau (se eller redigere) til det relevante indhold.

- **Detaljerede adgangs- og delingskontroller**

Med delingsfunktioner kan administratorer styre medlemskaber og tilladelser på øverste niveau eller undermappeniveau, så personer i og uden for virksomheden udelukkende har adgang til specifikke mapper.

- **Teammappe-leder**  
Administratorer kan få vist alle deres teammapper og tilpasse delingspolitikker fra en central placering for at forhindre deling af fortroligt materiale ved en fejltagelse.
- **Delte mapper til Paper-dokumenter**  
Administratorer kan oprette delte Paper-mapper, der automatisk giver andre samarbejdspartnere det rette adgangsniveau – kommentering eller redigering – til det indhold, de har brug for.
- **Fjernsletning**  
Når medarbejdere forlader teamet, eller hvis en enhed går tabt, kan administratorer fjernslette Dropbox-data og lokale kopier af filer. Filerne fjernes både fra computere og mobilenheder, næste gang de er online, og Dropbox-programmet kører.
- **Kontooverførsel**  
Efter at have fjernet en bruger (enten manuelt eller via mappetjenester) kan administratorer overføre filer og ejerskab af Paper-dokumenter, som det tidligere teammedlem har oprettet, fra brugerens konto til en anden bruger på teamet. Funktionen til kontooverførsel kan bruges, når en bruger fjernes, eller på ethvert tidspunkt efter sletningen af en brugers konto.

De følgende funktioner fås som tilføjelsesprogrammer (kontakt [salg](#) for at få mere information).

- **Scan indhold**  
Med tilføjelsesprogrammet Avancerede team- og indholdskontroller kan kunder med Dropbox til teams Advanced og Enterprise scanne efter nyt og eksisterende indhold i Dropbox for at lokalisere og undgå datasårbarheder.
- **Konfigurer og udløs tilpassede arbejdsgange**  
Med tilføjelsen Advanced Team og Content Controls kan administratorer foretage handlinger, der kan tilpasses mod filer, der overtræder virksomhedens politikker.
- **Konfigurér advarsler**  
Administratorer kan overvåge sikkerhedsproblemer i realtid og undgå datasårbarheder. Få advarsler om filer, der deles eksternt, og få følsomme data scannet.

## Indholdssynlighed

### Sikkerhedsadvarsler og meddelelser

Administratorer på Dropbox Enterprise kan modtage meddelelser i realtid, når mistænkelige aktiviteter, risikabel aktivitet eller potentielle datalækager registreres på deres konti. Følgende hændelser kan overvåges:

- Massesletninger
- Masseflytninger af data
- Følsomt indhold, der deles eksternt

- Malware delt uden for dit team
- Malware, der deles i dit team
- For mange fejlslagne loginforsøg
- Login fra et højrisikoland
- Registrering af ransomware

Dropbox giver også mulighed for at konfigurere advarselsgrænser, justere meddelelsesmodtagere og udløse advarsler, når mapper med følsomme filer deles eksternt. Administratorer kan også markere advarsler som under gennemgang, løst eller afvist. Derudover viser en dashboard-widjet overordnet indsigt og tendenser for teamadvarsler for den sidste uge.

### **Rapport og side om eksternt deling**

Dropbox giver ekstra synlighed med eksternt delingsrapport og -side. Administratorer kan oprette en rapport enten fra indsigtssiden eller den eksterne delingsside. Rapporten viser alle teamets filer og mapper, der deles uden for deres team, og alle delte links. Den eksterne delingsside er en ekstra side i administratorpanelet, der tillader administratorer at se og filtrere (filtype, hvem der delte, linkindstillinger og mange flere) gennem de filer og mapper, der blev delt direkte ud af teamet, og delte links.

### **Delingsfunktioner**

Delingsindstillinger giver teamadministratorer mere kontrol over delingen og adgang til deres teams indhold. Administratorer kan angive standardudløb på teamniveau, adgangsbegrænsninger eller begge dele. Disse begrænsninger reducerer risikoen for datatab ved at fjerne brugerens ansvar for at angive begrænsninger.

### **Dataklassificering**

Teams på Dropbox Enterprise kan have personlige og følsomme data automatisk mærket for bedre at beskytte dem. Administratorer modtager advarsler om forebyggelse af datatab (DLP) via e-mail og i administrationskonsollen, når filer eller mapper, der er gemt i teammapper, der indeholder følsomme oplysninger, deles uden for deres team. Administratorer har mulighed for automatisk at identificere og klassificere følsomme data, der er gemt i delte mapper og teammedlemmers personlige mapper. Dropbox Enterprise-administratorer kan aktivere automatisk dataklassificering fra administrationskonsollen.

### **Tilføjesprogram til dataforvaltning**

Dataforvaltning er det overordnede sæt processer, teknologier og teams, der går sammen om at styre og beskytte en organisations dataaktiver. Dette inkluderer muligheden for at gemme, identificere, opdage og hente virksomhedsdata efter behov.

Dropbox' tilføjesprogram til dataforvaltning samler et sæt funktioner, der giver organisationer mulighed for bedre at kontrollere og sikre deres data, samtidig med at de reducerer risici og omkostninger forbundet med at opfylde lovmæssige og compliance-behov. I øjeblikket indeholder dette tilføjesprogram fire nøglefunktioner til teamadministratorer og compliance-administratorer.

- **Udvidet versionshistorik**

Din standardmæssige filversionshistorik afhænger af den type Dropbox-konto, du har. Men med Dropbox til teams kan du købe et tilføjelsesprogram med udvidet versionshistorik (EVH) separat eller som en del af pakken med tilføjelsesprogrammet til dataforvaltning, der gør det muligt at genskabe filer, der er blevet slettet eller ændret i de seneste 10 år.

- **Juridiske fastfrysninger**

Ved at placere en juridisk fastfrysning på et teammedlem kan team- og compliance-administratorer se og eksportere alt det indhold, der er oprettet eller ændret af det pågældende medlem. Medlemmer, der er berørt af en juridisk fastfrysning, får ikke besked om tilbageholdelsen og bevarer deres tilladelser til at oprette, redigere og slette filer.

- **Dataopbevaring**

Dataopbevaring gør det muligt for teams og compliance-administratorer at forhindre utilsigtet sletning af indhold, der i henhold til reglerne skal bevares i et bestemt tidsrum. Denne funktion gør det muligt for kunder at bevare data i de sidste 10 år fra datoen for den seneste "revision".

- **Dataforældelse**

Dataforældelse gør det muligt for team- og compliance-administratorer at slette data permanent på en bestemt dato for at overholde krav til dataopbevaring og forældelse. Administratorer kan overvåge aktivitet ved at modtage rapporter, der advarer dem om kommende sletninger af filer.

## **Gendannelse og versionskontrol**

Dropbox til teams-kunder kan gendanne slettede filer og Paper-dokumenter og gendanne tidligere versioner af filer og Paper-dokumenter, så ændringer i vigtige data kan spores og genfindes.

## **Datasikkerhed på mobile enheder**

- **Slet data**

For at styrke sikkerheden har brugeren mulighed for at slette alle Dropbox-data fra enheden efter 10 mislykkede forsøg på at indtaste adgangskoden.

- **Internt lager og offlinefiler**

Som standard gemmes filer ikke i mobilenheders interne lagerplads. I Dropbox' mobilklienter er det muligt at gemme individuelle filer og mapper på enheden, så de kan ses offline. Når en enheds forbindelse til en Dropbox-konto afbrydes, enten via mobil- eller webgrænsefladen, slettes disse filer og mapper automatisk fra enhedens interne lagerplads.

- **Offline Paper-dokumenter**

Når en enheds forbindelse til Paper afbrydes via Dropbox-kontoens sikkerhedsside, bliver brugeren logget ud, og offline Paper-dokumenter bliver automatisk slettet fra enhedens interne lagerplads.

## Team-kontroller

Ikke to organisationer er ens, og derfor har vi udviklet en række værktøjer, der giver administratorer mulighed for at tilpasse Dropbox til teams til deres teams specifikke behov. Dropbox til teams indeholder værktøjer, der giver slutbrugere mulighed for at beskytte deres konti og data yderligere. Godkendelses-, gendannelses-, logførings- og de øvrige sikkerhedsfunktioner nedenfor er tilgængelige via de forskellige Dropbox-brugergrænseflader.

Nedenfor ses flere af de kontrol- og synlighedsfunktioner, som kan benyttes via administratorpanelet til Dropbox til teams.

### Tilladelser for detaljeret indhold

- **Administratorroller**

Dropbox tilbyder opdeltede administratorroller for at muliggøre mere effektiv teamadministration. Kontoadministratorer kan tildeles et af tre adgangs niveauer. Der er ingen grænse for, hvor mange administratorer et team kan have, og ethvert teammedlem kan tildeles en administratorrolle.

- **Teamadministrator**

Kan angive sikkerheds- og delingstilladelser for hele teamet, oprette administratorer og administrere medlemmer. Teamadministratoren har alle tilgængelige administratortilladelser. Kun teamadministratorer kan tildele eller ændre administratorroller, og der skal altid være mindst én teamadministrator på en Dropbox til teams-konto.

- **Brugeradministrator**

Kan håndtere de fleste teamadministrationsopgaver, herunder at tilføje og fjerne teammedlemmer, administrere grupper og få vist et teams aktivitetsfeed.

- **Supportadministrator**

Kan håndtere almindelige serviceanmodninger fra teammedlemmer, såsom at gendanne slettede filer eller hjælpe teammedlemmer, som ikke længere har adgang til tottrinsbekræftelse. Supportadministratorer kan også nulstille ikke-administratoradgangskoder og eksportere en logfil over aktiviteter for et bestemt teammedlem.

- **Faktureringsadministrator**

Kan få adgang til faktureringssider i administratorpanelet.

- **Indhold**

Kan oprette og administrere teammapper i medlemsadministrator.

- **Rapporteringsadministrator**

Kan oprette rapporter i administratorpanel og har adgang til aktivitetssiden.

- **Sikkerhedsadministrator**

Kan administrere sikkerhedsadvarsler, ekstern deling og sikkerhedsrisici.

- **Compliance-administrator (kun for teams med tilføjelsesprogrammet til dataforvaltning)**

Kan administrere dataforvaltningssider (juridiske fastfrysninger, dataopbevaring og datadisponering) og også få adgang til medlemsadministrator.

- **Grupper**  
Teams kan oprette og administrere medlemslister i Dropbox og nemt give dem adgang til bestemte mapper. Dropbox kan også synkronisere Active Directory-grupper ved hjælp af Active Directory-konnektoren.
- **Virksomhedsstyrede grupper**  
Kun administratorer kan oprette, slette og administrere medlemskabet for denne type gruppe. Brugere kan ikke anmode om at deltage i eller forlade en virksomhedsstyret gruppe.
- **Brugerstyrede grupper**  
Administratorer kan vælge, om brugere kan oprette og administrere deres egne grupper. Administratorer kan også til enhver tid ændre en brugerstyret gruppe til en virksomhedsadministreret gruppe for at tage kontrol over den.
- **Begrænsning af flere konti på computere**  
Administratorer kan forhindre teammedlemmer i at knytte en sekundær Dropbox-konto til computere, som er knyttet til deres arbejdsrelaterede Dropbox-konto.
- **Brugertilstanden Suspenderet**  
Administratorer kan deaktivere en brugers adgang til vedkommendes konto, samtidig med at vedkommende beholder sine data- og delingsforhold, så virksomhedsoplysningerne beskyttes. Administratorer kan reaktivere eller slette kontoen senere.
- **Log på som bruger**  
Teamadministratorer kan logge ind som medlemmer af deres teams. Dette giver administratorer direkte adgang til filer, mapper og Paper-dokumenter på teammedlemmers konti, så de kan ændre, dele på vegne af teammedlemmer eller kontrollere hændelser på filniveau. "Log ind som bruger"-hændelser registreres i teamets aktivitets-logfil, og administratorer kan vælge, om medlemmer skal underrettes om disse hændelser.
- **Delingstilladelser**  
Teamadministratorer har omfattende kontrol over deres teams muligheder for at dele ved hjælp af Dropbox, herunder om:
  - Teammedlemmer kan dele filer og mapper med personer uden for teamet.
  - Teammedlemmer kan redigere mapper, der ejes af personer uden for teamet.
  - Delte links oprettet af teammedlemmer kan bruges af personer uden for teamet.
  - Teammedlemmer kan oprette filanmodninger og indsamle filer fra teammedlemmer og/eller personer uden for teamet.
  - Andre kan se og kommentere filer, der ejes af teamet.
  - Teammedlemmer kan dele Paper-dokumenter og Paper-mapper uden for teamet.
  - Der gives tilladelser til permanent sletning.

Teamadministratoren for en Dropbox til teams-konto kan begrænse muligheden for at slette filer og Paper-dokumenter permanent, så kun teamadministratorer kan gøre dette.

## Onboarding og klargøring af brugere

### Metoder til klargøring af brugere og identitetsstyring

- **E-mailinvitation**

Et værktøj i administratorpanelet til Dropbox til teams giver administratorer mulighed for manuelt at generere en invitation pr. e-mail.

- **Active Directory**

Dropbox til teams-administratorer kan automatisere oprettelsen og fjernelsen af konti fra et nuværende Active Directory-system via vores Active Directory-konnektor eller eksternt identitetsudbyder. Når Active Directory er integreret, kan det bruges til at administrere medlemskaber.

- **Enkeltlogon (SSO)**

Dropbox til teams kan konfigureres til at give teammedlemmer adgang ved at logge ind på en central identitetsudbyder. Vores SSO-implementering, der benytter branchestandarden Security Assertion Markup Language 2.0 (SAML 2.0), gør klargøring mere enkelt og sikkert ved at gøre en pålidelig identitetsudbyder ansvarlig for godkendelse og give teammedlemmer adgang til Dropbox uden behov for at administrere endnu en adgangskode. Dropbox har også indgået et samarbejde med førende udbydere af identitetsadministration, så brugere automatisk kan klargøres og fjernes. Se [API-integrationer til Dropbox til teams](#).

- **Adgangsnøgler**

Adgangsnøgler bruger offentlig nøglekryptering til at muliggøre sikker godkendelse uden at være afhængig af adgangskoder eller sms-koder. De er i øjeblikket tilgængelige som loginmetode på Dropbox-web, der bruger en godkender, en pinkode eller biometri. Den private nøgle forlader aldrig din enhed – Dropbox gemmer kun den offentlige nøgle.

- **SCIM (System for Cross-domain Identity Management)**

Dropbox understøtter SCIM-integration, hvilket gør det nemmere at administrere brugeridentiteter i cloudbaserede applikationer – herunder at tilføje brugere, opdatere brugere, fjerne brugere, oprette grupper og tilføje eller fjerne brugere fra grupper. I stedet for at kræve, at tredjeparter implementerer brugerdefineret logik via APIv2-slutpunkter, definerer SCIM en fælles grænseflade, som leverandører kan anvende til at klargøre brugere og grupper med alle de tjenester, der understøtter det, herunder Dropbox.

- **API**

Dropbox til teams API kan bruges af kunder til at oprette tilpassede løsninger til klargøring af brugere og administration af identitet. Se [API-integrationer til Dropbox til teams](#).

### 2-trins-bekræftelse

Denne yderst anbefalede sikkerhedsfunktion fjører et ekstra beskyttelseslag til en brugers Dropbox-konto. Når totrinsbekræftelse er aktiveret, kræver Dropbox en sekscifret sikkerhedskode ud over en adgangskode, hver gang der logges på eller forbindes en ny computer, telefon eller tablet.

- Administratorer kan vælge at kræve totrinsbekræftelse for alle eller kun for bestemte teammedlemmer.
- Kontoadministratorer kan kontrollere, hvilke teammedlemmer der har aktiveret totrinsbekræftelse.

- Koder til Dropbox-totrinsgodkendelse kan modtages via SMS eller i apps, der overholder algoritmestandarden TOTP (Time-based One-Time Password (tidsbaseret éngangs-adgangskode)).
- Hvis en bruger ikke kan modtage sikkerhedskoder ved hjælp af disse metoder, kan vedkommende vælge at bruge en 16-cifret éngangs-reservekode til nødstilfælde. Brugeren kan også vælge at bruge et sekundært telefonnummer til at modtage en reservekode som SMS.
- Dropbox understøtter desuden den åbne standard FIDO Universal 2nd Factor (U2F), der giver brugere mulighed for at godkende med en USB-sikkerhedsnøgle, som de har konfigureret, i stedet for en 6-cifret kode.

## Installationsprogram til store virksomheder

Administratorer med behov for skaleret klargøring kan bruge vores Enterprise-installationsprogram til Windows til at installere Dropbox-computerappen diskret og via fjernadgang ved hjælp af administrerede softwareløsninger og implementeringsmekanismer.

## Administrerede enheder og login

- **EMM (Enterprise Mobility Management)**

Dropbox integrerer med tredjepartsudbydere af EMM, så administratorer af Dropbox til teams-konti med en Enterprise-plan får mere kontrol over, hvordan teammedlemmer bruger Dropbox på mobilenheder. Administratorer kan begrænse brugen af mobilapps for Dropbox Enterprise-konti til kun administrerede enheder (uanset om de er til arbejde eller personlig brug), få indblik i brug af apps (herunder ledig lagerplads og adgangssteder) og benytte fjernsletning, hvis en enhed mistes eller bliver stjålet.

- **Enhedsgodkendelser**

Dropbox gør det muligt for administratorer af Dropbox til teams på Advanced- og Enterprise-planer at begrænse antallet af enheder, som en bruger kan synkronisere med Dropbox, og at vælge, om godkendelser er brugerstyrede eller administratorstyrede. Administratorer kan også oprette en undtagelsesliste over brugere, der ikke er begrænset til et bestemt antal enheder.

- **Krav om totrinsbekræftelse**

Administratorer kan vælge at kræve totrinsbekræftelse for alle teammedlemmer eller kun for bestemte medlemmer. Andre krav til multifaktorgodkendelse kan håndhæves gennem teamets SSO-implementering.

- **Adgangskodestyling**

Administratorer af Education-, Advanced- og Enterprise-teams kan kræve, at medlemmerne angiver og opretholder stærke, komplekse adgangskoder til deres konti. Når denne funktion er aktiveret, bliver teammedlemmerne logget ud fra alle websessioner og bedt om at oprette nye adgangskoder, når de logger på. Et indbygget værktøj analyserer styrken af adgangskoder ved at sammenligne dem med en database over ofte benyttede ord, navne, mønstre og tal. En bruger, der indtaster en almindelig adgangskode, bliver bedt om at finde på noget mere særegent, der er svært at gætte. Administratorer kan også nulstille adgangskoder for hele teamet eller for enkelte brugere.

- **Domæneadministration**

Dropbox kan tilbyde virksomheder en række værktøjer til at forenkle og fremskynde onboarding af brugere og kontrollere brug af Dropbox.

- **Domænebekræftelse**

Virksomheder kan kræve ejerskab over deres domæner og få adgang til andre værktøjer til domæneadministration.

- **Tvungne invitationer**

Administratorer kan kræve, at individuelle Dropbox-brugere, som er inviteret med på virksomhedens Dropbox-team, skal migrere til teamet eller ændre e-mailadressen på deres private konto.

- **Domæneindsigt**

Administratorer kan se vigtig information, for eksempel hvor mange individuelle Dropbox-konti der bruger virksomhedens e-mailadresser.

- **Kontoopsamling**

Administratorer kan tvinge alle Dropbox-brugere, der benytter virksomhedens mailadresse, til at blive medlem af virksomhedens team eller ændre e-mailadressen på deres private konto.

- **Kontrol af websessioner**

Administratorer kan styre, hvor længe teammedlemmer kan være logget på dropbox.com. Administratorer kan begrænse varigheden af alle websessioner og/eller inaktive sessioner. Sessioner, der overskrider disse grænser, bliver automatisk logget ud. Administratorer kan også holde øje med og afbryde enkelte brugeres websessioner.

- **Programadgang**

Administratorer kan se og tilbagekalde adgang til brugerkonti for tredjepartsapps.

- **Fjern forbindelsen mellem enheder**

Administratorer kan i administratorpanelet afbryde forbindelsen fra computere og mobilenheder til brugerkonti. Brugeren kan også afbryde forbindelsen i indstillingerne for kontosikkerhed. Når forbindelsen afbrydes på en computer, fjernes godkendelsesdata, og det er muligt at slette lokale kopier af filer, næste gang computeren er online (se [Fjernelsletning](#)). Når forbindelsen afbrydes på mobilenheder, fjernes de filer, der er markeret som favoritter, cachelagrede data og logoplysninger. Hvis totrinsbekræftelse er aktiveret, skal brugerne godkende enhederne igen, når forbindelsen genoprettes. Desuden er det muligt at angive i brugerens kontoindstillinger, at der automatisk skal sendes en e-mail til brugeren, hvis en ny enhed tilknyttes.

- **Netværksstyring**

Administratorer af Dropbox til teams på en Enterprise-plan kan begrænse brugen af Dropbox på virksomhedens netværk til kun at ske via Enterprise-teamkontoen. Denne funktion integreres med virksomhedens netværkssikkerhedsudbyder for at blokere al trafik, der eksisterer uden for den tilladte konto på computerne. Bemærk, at Paper i øjeblikket ikke administreres via netværksstyring.

## Mobilsikkerhed

- **Fingeraftryksscanning**

Brugere kan aktivere Touch ID eller Face ID på iOS-enheder og oplåsning med fingeraftryk (hvis dette understøttes) på Android-enheder som en metode til at låse op for Dropbox-mobilappen.

## Få adgang til synlighed

- **Identitetsbekræftelse af teknisk support**

Før Dropbox-support kan udlevere oplysninger om fejlfinding eller konti, skal kontoens administrator oplyse en tilfældigt genereret sikkerhedskode, der kun kan bruges én gang, for at bekræfte vedkommendes identitet. Denne kode kan kun ses i administratorpanelet.

## Aktivitet på brugerkonto

Hver bruger kan se følgende sider fra sine kontoindstillinger for at få de mest opdaterede oplysninger om vedkommendes egen kontoaktivitet.

- **Deling af side**

Denne side viser de delte mapper, der i øjeblikket findes i brugerens Dropbox, og delte mapper, som brugeren kan tilføje. En bruger kan afbryde deling af mapper og filer og vælge delingstilladelser.

- **Filside**

Denne side viser de filer, der er delt med brugeren, og datoen for delingen af hver fil. Brugeren kan fjerne sin adgang til disse filer. Hvis brugeren vil se Paper-dokumenter, som andre har delt med brugeren, kan vedkommende navigere til siden "Delt med mig" i navigationsgrænsefladen til Paper-dokumenter.

- **Linkside**

Denne side viser alle aktive delte links, som brugeren har oprettet, samt oprettelsesdatoen for dem hver især. Den viser desuden alle de links, som deles med brugeren af andre. Brugeren kan deaktivere links eller ændre tilladelser.

- **E-mailmeddelelser**

En bruger kan vælge at modtage en e-mailmeddelelse, så snart en ny enhed eller app forbindes til vedkommendes Dropbox-konto.

## Brugerkontotilladelser

- **Forbundne enheder**

I afsnittet Enheder i en brugers indstillinger for kontosikkerhed kan du se alle de computere og mobilenheder, der er forbundet til brugerens konto. For hver computer vises IP-adresse, land og det anslåede tidspunkt for seneste aktivitet. En bruger kan afbryde forbindelsen til enhver enhed, med mulighed for at slette filer på forbundne computere, næste gang de er online.

- **Aktive websessioner**

I afsnittet Sessioner kan du se alle de webbrowsere, der i øjeblikket er logget på en brugers konto. For hver af disse vises IP-adresse, land og logintidspunkt for den seneste session samt det anslåede tidspunkt for den seneste aktivitet. En bruger kan fjernafslutte enhver session fra vedkommendes indstillinger for kontosikkerhed.

- **Forbundne apps**

Afsnittet Forbundne apps indeholder en liste over alle apps fra tredjeparter med adgang til en brugers konto og den type adgang, hver app har. En bruger kan tilbagekalde en hvilken som helst apps tilladelse til at få adgang til brugerens Dropbox.

## Aktivitetsfeed

Dropbox til teams registrerer filhandlinger i teamets aktivitetsfeed, som kan tilgås fra administratorpanelet. Aktivitetsfeedet har fleksible filtreringsindstillinger, der gør det muligt for administratorer at udføre målrettede undersøgelser af konto-, fil- og Paper-dokumentaktivitet. De kan f.eks. se den komplette historik for en fil eller et Paper-dokument, og hvordan brugere har interageret med filen, eller se al aktivitet for teamet i løbet af en bestemt tidsperiode. Aktivitetsfeedet kan eksporteres som en rapport, der kan downloades i CSV-format, og også integreres direkte i et SIEM-produkt (Security Information and Event Management) eller et andet analyseværktøj via eksterne partnerløsninger. Følgende indholdshændelser registreres i aktivitetsfeedet:

- **Deling for filer, mapper og links**

Rapporterer, hvis det er relevant, om handlinger har vedrørt personer, som ikke er teammedlemmer.

### Delte filer

- Tilføjede eller fjernede et teammedlem eller et ikke-teammedlem.
- Ændrede tilladelser for et teammedlem eller ikke-teammedlem.
- Tilføjede eller fjernede en gruppe.
- Føjede en delt fil til brugerens Dropbox.
- Så indholdet i en fil, som blev delt via en fil- eller mappeinvitation.
- Kopierede delt indhold til brugerens Dropbox.
- Downloadede delt indhold.
- Kommenterede på en fil.
- Løste eller løste ikke en kommentar.
- Slettede en kommentar.
- Tilvalgte eller fravalgte kommentarmeddelelser.
- Godkendte en invitation til en fil, som ejes af teamet.
- Anmodede om adgang til en fil, der ejes af teamet.
- Afbrød deling af en fil.

### Delte mapper

- Oprettede en ny delt mappe.
- Tilføjede eller fjernede teammedlem, ikke-teammedlem eller gruppe.
- Føjede en delt mappe til brugerens Dropbox, eller brugeren fjernede sin egen adgang til en delt mappe.
- Tilføjede en delt mappe fra et link.
- Ændrede et teammedlems eller ikke-teammedlems tilladelser.
- Overførte mappeejerskab til en anden bruger.

- Afbrød deling af en mappe.
- Godkendte medlemskab til en delt mappe.
- Anmodede om adgang til en delt mappe.
- Føjede en bruger, der har anmodet om det, til en delt mappe.
- Blokerede eller fjernede blokering af ikke-teammedlemmer mulighed for at blive føjet til en mappe.
- Gav alle teammedlemmer eller kun ejeren mulighed for at føje personer til en mappe.
- Ændrede gruppeadgang til en delt mappe.

### **Delte links**

- Oprettede eller fjernede et link.
- Gjorde indholdet fra et link synligt for alle med linket eller kun for teammedlemmer.
- Beskyttede et links indhold med en adgangskode.
- Angav eller fjernede et udløb for et link.
- Så et link.
- Downloadede indholdet fra et link.
- Kopierede indholdet fra et link til brugerens Dropbox.
- Oprettede et link til en fil via en API-app.
- Delte et link med teammedlem, ikke-teammedlem eller gruppe.
- Blokerede eller fjernede blokering af ikke-teammedlemmers mulighed for at se links til filer i en delt mappe.
- Delte et album.

### **Filanmodninger**

- Oprettede, ændrede, lukkede eller slettede en filanmodning.
- Føjede brugere til en filanmodning.
- Tilføjede eller fjernede en tidsfrist for en filanmodning.
- Ændrede en filanmodningsmappe.
- Modtog filer via en filanmodning.
- Modtog filer via Email to Dropbox.

### **Individuelle fil- og mappehændelser**

- Føjede en fil til Dropbox.
- Oprettede en mappe.

- Så en fil.
- Redigerede en fil.
- Downloadede en fil.
- Kopierede en fil eller mappe.
- Flyttede en fil eller mappe.
- Omdøbte en fil eller mappe.
- Gendannede en fil til en tidligere version.
- Tilbageførte ændringer i filer.
- Gendannede en slettet fil.
- Slettede en fil eller mappe.
- Slettede en fil eller mappe permanent.

#### **Vellykkede eller mislykkede logins**

- Vellykkede eller mislykkede loginforsøg.
- Mislykket loginforsøg eller fejl via enkeltlogon (SSO).
- Mislykket loginforsøg eller fejl via EMM.
- Loggede af.
- Ændring af IP-adresse for websession.

#### **Adgangskoder**

Ændring af indstillinger for adgangskoder eller totrinsbekræftelse. Administratorer kan ikke se brugernes faktiske adgangskoder.

- Ændrede eller nulstillede adgangskode.
- Aktiverede, nulstillede eller deaktiverede totrinsbekræftelse.
- Konfigurerede eller ændrede totrinsbekræftelse til at bruge sms eller en mobilapp.
- Tilføjede, redigerede eller fjernede en reservetelefon til totrinsbekræftelse.
- Tilføjede eller fjernede en sikkerhedsnøgle til totrinsbekræftelse.

#### **Medlemskab**

Tilføjelser til og fjernet fra teamet.

- Inviterede et teammedlem.

- Tilmeldte sig teamet.
- Fjernede et teammedlem.
- Suspenderede eller fjernede suspendering af et teammedlem.
- Genoprettede et fjernet teammedlem.
- Anmodede om at tilmelde sig teamet ud fra kontodomæne.
- Godkendte eller afviste en anmodning om at tilmelde sig teamet ud fra kontodomæne.
- Sendte domæneinvitationer til nuværende domænekonti.
- Bruger blev en del af teamet som følge af kontoopsamling.
- Bruger forlod domænet som følge af kontoopsamling.
- Blokerede eller fjernede blokering af teammedlemmers mulighed for at foreslå nye teammedlemmer.
- Foreslog et nyt teammedlem.

### **Apps**

Forbindelser mellem apps fra tredjeparter og Dropbox-konti.

- Godkendte eller fjernede en applikation.
- Godkendte eller fjernede en teamapplikation.

### **Enheder**

Forbindelser mellem computere eller mobilenheder og Dropbox-konti.

- Forbandt eller afbrød forbindelsen til en enhed.
- Brugte fjernsletning og slettede alle filer eller kunne ikke slette visse filer.
- Ændring af IP-adresse for computer eller mobilenhed.

### **Administratorhandlinger**

Ændring af indstillinger i administratorpanelet, såsom tilladelser for delte mapper.

- **Godkendelse og enkeltlogon (SSO)**
  - Nulstillede teammedlems adgangskode.
  - Nulstillede alle teammedlemmers adgangskoder.
  - Blokerede eller fjernede blokering af teammedlemmers mulighed for at deaktivere totrinsbekræftelse.

- Aktiverede eller deaktiverede SSO.
- Gjorde logon via SSO påkrævet.
- Ændrede eller fjernede webadresse til SSO.
- Opdaterede SSO-certifikatet.
- Ændrede SSO-identitetstilstanden.
- **Medlemskab**
  - Blokerede eller fjernede blokering af brugeres mulighed for at anmode om at blive en del af teamet ud fra kontodomæne.
  - Satte anmodninger om medlemskab af team til automatisk godkendelse eller at kræve manuel administratorgodkendelse.
- **Administration af medlemskonto**
  - Ændrede et teammedlems navn.
  - Ændrede et teammedlems e-mailadresse.
  - Tildelte eller fjernede administratorstatus eller ændrede administratorrollen.
  - Loggede ind eller loggede ud som et teammedlem.
  - Overførte eller slettede indholdet på et fjernet medlems konto.
  - Slettede permanent indholdet på et fjernet medlems konto.
- **Indstillinger for global deling**
  - Blokerede eller fjernede blokering af teammedlemmers mulighed for at tilføje delte mapper, som ejes af ikke-teammedlemmer.
  - Blokerede eller fjernede blokering af teammedlemmers mulighed for at dele mapper med ikke-teammedlemmer.
  - Aktiverede advarsler, der vises til brugere, før de deler mapper med ikke-teammedlemmer.
  - Blokerede eller fjernede blokering af ikke-teammedlemmers mulighed for at se delte links.
  - Satte delte links til kun at være for team som standard.
  - Blokerede eller fjernede blokering af personers mulighed for at kommentere filer.
  - Blokerede eller fjernede blokering af teammedlemmers mulighed for at oprette filanmodninger.
  - Tilføjede, ændrede eller fjernede et logo for sider med delt link.
  - Blokerede eller fjernede blokering af teammedlemmers mulighed for at dele Paper-dokumenter og Paper-mapper med ikke-teammedlemmer.
- **Administration af teammapper for filer**
  - Oprettede en teammappe.
  - Omdøbte en teammappe.

- Arkiverede eller fjernede arkivering af en teammappe.
- Slettede en teammappe permanent.
- Nedgraderede en teammappe til en delt mappe.
- **Domæneadministration**
  - Forsøgte at bekræfte eller bekræftede et domæne eller fjernede et domæne.
  - Dropbox-support bekræftede eller fjernede et domæne.
  - Aktiverede eller deaktiverede muligheden for at sende domæneinvitationer.
  - Aktiverede eller deaktiverede "Inviter automatisk nye brugere".
  - Ændrede kontoopsamlingstilstand.
  - Dropbox-support gav eller tilbagekaldte adgang til kontoopsamling.
- **EMM (Enterprise Mobility Management)**
  - Aktiverede EMM for testtilstand (valgfrit) eller implementeringstilstand (påkrævet).
  - Opdaterede EMM-token.
  - Tilføjede eller fjernede teammedlemmer fra liste over brugere, der er ekskluderet fra EMM.
  - Deaktiverede EMM.
  - Oprettede en rapport med en EMM-undtagelsesliste.
  - Oprettede en forbrugsrapport for EMM-mobilapp.
- **Ændringer af andre teamindstillinger**
  - Sammenflettede teams.
  - Opgraderede teamet til Dropbox til teams eller nedgraderede til et gratis team.
  - Ændrede teamnavnet.
  - Oprettede en rapport over teamaktivitet.
  - Blokerede eller fjernede en blokering af teammedlemmers mulighed for at have mere end én konto knyttet til en computer.
  - Gav alle teammedlemmer eller kun administratorer mulighed for at oprette grupper.
  - Blokerede eller fjernede blokering af teammedlemmers muligheder for at slette filer permanent.
  - Påbegyndte eller afsluttede en Dropbox-supportsession for en forhandler.

## Grupper

Oprettelse, sletning og oplysninger om medlemmer for grupper.

- Oprettede, omdøbte, flyttede eller slettede en gruppe.
- Tilføjede eller fjernede et medlem.
- Ændrede et gruppemedlems adgangstype.
- Ændrede gruppe til teamadministreret eller administratorstyret.
- Ændrede en gruppes eksterne id.

## Paper-aktivitetslog.

Administratorer kan vælge en Paper-aktivitetstype på aktivitetsfeeden eller downloade en komplet aktivitetsrapport Paper-hændelser registreres for:

- Paper aktiveret eller deaktiveret.
- Oprettelse, redigering, eksport, arkivering, permanent sletning og gendannelse af Paper-dokument.
- Kommentering af Paper-dokument og løsning af kommentarer.
- Deling og ophævelse af deling af Paper-dokument med teammedlemmer og ikke-teammedlemmer.
- Anmodninger om adgang til Paper-dokument fra teammedlemmer og ikke-teammedlemmer.
- Omtaler af Paper-dokument for teammedlemmer og ikke-teammedlemmer.
- Paper-dokument set af teammedlemmer og ikke-teammedlemmer.
- Paper-dokument fulgt.
- Ændringer af medlemstilladelser for Paper-dokument (rediger, kommenter eller skrivebeskyttet).
- Ændringer til politik for ekstern deling af Paper-dokument.
- Oprettelse, arkivering og permanent sletning af Paper-mappe.
- Paper-dokument tilføjet i eller fjernet fra en mappe.
- Paper-mappe omdøbt.
- Overførsler af Paper-dokument og -mappe.

# Integritetscertifikater, attestationer og lovgivningsmæssig overholdelse

Følgende standarder indeholder vores krav til, hvordan Dropbox bruger og ikke bruger din organisations oplysninger:

- **Din organisation kontrollerer dine data**

Vi bruger kun de personlige oplysninger, som du giver os, til at levere den tjeneste, du er tilmeldt. Du kan tilføje, ændre eller slette filer og Paper-dokumenter fra Dropbox, når du har brug for det.

- **Fuld åbenhed om dine data**

Vi er fuldt åbne om, hvor dine data befinder sig på vores servere. Vi fortæller også, hvem der er vores betroede partnere. Vi giver dig besked om, hvad der sker, hvis du lukker en konto eller sletter en fil eller et Paper-dokument, og vi underretter dig, hvis der sker ændringer på nogen af områderne.

- **Dine data er i sikre hænder**

ISO/IEC 27018 og ISO/IEC 27701 blev designet som supplement til og udvidelser af ISO/IEC 27001, som er en af verdens mest accepterede standarder for informationssikkerhed. Vi modtog ISO/IEC 27001 certificeringsfornyelse i oktober 2021.

- **Vores praksis gennemgås regelmæssigt**

Som en del af vores overholdelse af ISO/IEC 27018, ISO/IEC 27701 og ISO/IEC 27001 kontrolleres vi hvert år af en uafhængig tredjepart, så vi fortsat er kvalificerede til disse certificeringer. Du kan se alle vores ISO-certificeringer i vores [Trust Center](#).

## Dataoverførsler

Når Dropbox overfører data fra Den Europæiske Union, Det Europæiske Økonomiske Samarbejdsområde, Storbritannien og Schweiz, er vi afhængige af en række juridiske mekanismer, såsom kontrakter med vores kunder og tilknyttede virksomheder, [standardkontraktbestemmelser](#), programmet til værn om privatlivets fred mellem EU og USA, den britiske udvidelse af programmet til værn om privatlivets fred mellem EU og USA samt programmet til værn om privatlivets fred mellem Schweiz og USA og Europa-Kommissionens [afgørelse om tilstrækkeligt beskyttelsesniveau](#) for visse lande, hvor det er relevant.

Dropbox overholder programmet til værn om privatlivets fred mellem EU og USA, programmet til værn om privatlivets fred mellem Schweiz og USA samt den britiske udvidelse af programmet til værn om privatlivets fred mellem EU og USA som fastsat af det amerikanske handelsministerium vedrørende behandling af persondata, der overføres fra EU, det Europæiske Økonomiske Samarbejdsområde, Storbritannien og Schweiz til USA. Dropbox har certificeret over for det amerikanske handelsministerium, at det overholder principperne i databeskyttelsesrammer med hensyn til sådanne data, men dette omfatter ikke DocSend- eller Formswift-delene af tjenesterne. Hvis der er nogen konflikt mellem denne persondatapolitik og principperne i databeskyttelsesrammerne, har principperne forrang. I overensstemmelse med principperne forbliver Dropbox ansvarlig for videre overførsel, hvis en databehandler behandler persondata på en måde, der er uforenelig med principperne. Hvis du vil vide mere om databeskyttelsesrammerne og se vores certificering, kan du besøge <https://www.dataprivacyframework.gov>.

Klager og tvister i relation til vores overholdelse af databeskyttelsesrammerne undersøges og løses gennem JAMS, en uafhængig tredjepart. Du kan finde flere oplysninger i vores persondatapolitik ([dropbox.com/privacy](https://dropbox.com/privacy)).

## EU's generelle forordning om databeskyttelse (GDPR)

Dropbox har en permanent forpligtelse, når det drejer sig om sikkerheden og beskyttelsen af vores brugeres data i overensstemmelse med lovkrav og bedste praksis. I overensstemmelse med vores forpligtelse over for vores brugere har vi arbejdet hårdt for at sikre, at Dropbox er kompatibel med GDPR, herunder udnævnelse af en databeskyttelsesansvarlig, omstrukturering af vores privatlivsprogram for at sikre, at brugere kan udøve deres rettigheder som dataemner, dokumentation af vores databehandlingsaktiviteter og styrkelse af vores interne processer i tilfælde af et brud på sikkerheden. Efterhånden som databeskyttelsesmyndigheder giver yderligere vejledning, fortsætter vi med at foretage justeringer for at sikre, at vores proces og praksis opfylder eller mere end opfylder specifikke elementer af de nye regler.

Du kan finde flere oplysninger om vores praksisser og politikker for beskyttelse af personlige oplysninger i Dropbox' [hvidbog om beskyttelse af personlige oplysninger og data](#).

## EU Cloud Code of Conduct

EU Cloud Code of Conduct er et frivilligt redskab, der giver leverandører af cloudtjenester, som f.eks. Dropbox, mulighed for at vise, at vi forpligter os til at overholde GDPR. Dropbox til teams, som består af planerne Standard, Advanced, Enterprise, Education, Business og Business Plus til teams, er blevet erklæret i overensstemmelse med EU Cloud Code of Conduct og har modtaget en compliance-karakter på "niveau 2", som betyder, at disse tjenester har implementeret tekniske, organisatoriske og kontraktmæssige foranstaltninger i overensstemmelse med kravene i EU Cloud Code of Conduct. Du kan få mere at vide om EU Cloud Code of Conduct og Dropbox' overholdelse af den på [det officielle websted for EU Cloud Code of Conduct](#).

Du kan få mere information om vores praksisser og politikker for beskyttelse af personlige oplysninger i Dropbox' [hvidbog om beskyttelse af personlige oplysninger og data](#).

# Compliance

Der er forskellige lovgivningsmæssige og branche-specifikke krav til sikkerhed og beskyttelse af persondata, som organisationer kan være påkrævet at overholde. Vores tilgang er at kombinere de bredest anerkendte standarder med foranstaltninger, der er skræddersyet til de specifikke behov i vores kunders virksomheder eller brancher. Dropbox til teams, herunder planerne Dropbox Standard, Advanced, Enterprise, Education, Dropbox Business og Dropbox Business Plus, overholder følgende rammer, standarder og lovgivninger:

## ISO

International Organization for Standardization (ISO) har udviklet en række standarder for informations- og samfundsmæssig sikkerhed for at hjælpe virksomheder med at udvikle pålidelige og innovative produkter og tjenester. Dropbox har certificeret sine datacentre, systemer, programmer, medarbejdere og processer via en række revisioner udført af en uafhængig tredjepart, EY CertifyPoint i Holland. EY CertifyPoint opretholder sine ISO-akkrediteringer fra [Raad voor Accreditatie](#) (det hollandske akkrediteringsråd).

### **ISO/IEC 27001 (Informationssikkerhed)**

ISO/IEC 27001 er anerkendt som verdens førende ISMS-standard (Information Security Management System). Standarden anvender også den bedste praksis for sikkerhed, der er beskrevet i ISO/IEC 27002. For at gøre os fortjent til din tillid har vi fokus på løbende og omfattende administration af vores fysiske, tekniske og juridiske kontrol hos Dropbox.

[Se ISO/IEC 27001-certifikatet for Dropbox til teams.](#)

### **ISO/IEC 27017 (Cloud-sikkerhed)**

ISO/IEC 27017 er en international standard for cloudbaseret sikkerhed, der giver retningslinjer for sikkerhedskontroller, der gælder for levering og brug af cloudtjenester. Vores [Vejledning til fælles ansvar](#) forklarer en række af de krav til sikkerhed, beskyttelse af personlige oplysninger og krav til regler og standarder, som Dropbox og dets kunder kan løse i fællesskab.

[Se ISO/IEC 27017-certifikatet for Dropbox til teams.](#)

### **ISO/IEC 27018 (cloudbaseret beskyttelse af personlige oplysninger og data)**

ISO/IEC 27018 er en international standard for beskyttelse af data og personlige oplysninger. Standarden finder anvendelse for udbydere af cloudtjenester som Dropbox, der behandler personlige oplysninger på vegne af deres kunder, og udgør grundlaget for vores kunders almindelige krav eller spørgsmål i forbindelse med lovgivningsmæssige og kontraktmæssige forhold.

[Se ISO/IEC 27018-certifikatet for Dropbox til teams.](#)

### **ISO/IEC 22301(Kontinuitet i virksomheden)**

ISO/IEC 22301 er en international standard for kontinuitet i virksomheden, der vejleder virksomheder i at reducere risikoen for forstyrrende hændelser og reagere korrekt på dem, hvis de opstår, ved at minimere den potentielle skade. Dropbox Business continuity management system (BCMS) er en del af vores overordnede risikostyringsstrategi til beskyttelse af personer og driften under nedbrud.

[Se ISO/IEC 22301-certifikatet for Dropbox til teams.](#)

## **ISO/IEC 27701 (Administration af beskyttelse af persondata)**

ISO 27701 er en international standard for administration af persondata. Standarden giver en ramme til forbedring og udvidelse af systemet til sikkerhedsadministration under ISO 27001 til et system til administration af persondata (PIMS). Dropbox til teams har modtaget denne certificering som PII-behandler.

[Se ISO 27701-certifikatet for Dropbox til teams.](#)

## **SOC**

Service Organization Controls (SOC)-rapporter, der kaldes SOC 1, SOC 2 eller SOC 3, er ordninger, der er etableret af American Institute of Certified Public Accountants (AICPA) til rapportering af interne kontrolfunktioner, der er implementeret i en virksomhed. Dropbox har valideret sine systemer, programmer, medarbejdere og processer via en række revisioner udført af en uafhængigt tredjepartsvirksomhed, Ernst & Young LLP.

### **SOC 3 for sikkerhed, fortrolighed, integritet, tilgængelighed og beskyttelse af personlige oplysninger**

SOC 3-kontrolrapporten dækker de fem TSC'er (Trust Service Criteria): sikkerhed, fortrolighed, integritet, tilgængelighed og beskyttelse af personlige oplysninger (TSP sektion 100). Dropbox' rapport om almindelig brug er en sammenfatning af SOC 2-rapporten og omfatter tredjepartsrevisorens udtalelse om den effektive udformning og drift af vores kontroller.

[Se SOC 3-undersøgelsen for Dropbox til teams.](#)

### **SOC 2 for sikkerhed, fortrolighed, integritet, tilgængelighed og beskyttelse af personlige oplysninger**

SOC 2-rapporten giver kunder et detaljeret niveau af sikkerhed baseret på kontrolforanstaltninger, der dækker alle fem kriterier for troværdige tjenester: Sikkerhed, tilgængelighed, behandlingsintegritet, fortrolighed og beskyttelse af personlige oplysninger (beskrevet i afsnit 100). SOC 2-rapporten omfatter en detaljeret gennemgang af Dropbox' processer og mere end 100 kontrolforanstaltninger, som vi bruger til at beskytte dit indhold. Ud over vores uafhængige tredjepartsauditørs udtalelse om effektiviteten af vores kontrolforanstaltningers design og drift indeholder rapporten auditørens testprocedurer og resultater for samtlige kontrolforanstaltninger. Vores SOC 2-rapport (undertiden benævnt som SOC 2+-rapport) indeholder også en auditeret kortlægning af vores kontrolforanstaltninger for ovennævnte ISO-standarder, så vores kunder oplever yderligere gennemsigtighed.

[Se SOC 2-undersøgelsen for Dropbox til teams.](#)

## **SOC 1 / SSAE 18 / ISAE 3402 (tidligere SSAE 16 eller SAS 70)**

SOC 1-rapporten giver specifikke forsikringer til kunder, der anser Dropbox til teams for at være et hovedelement i deres interne kontrol over økonomisk rapportering (ICFR – Internal Controls over Financial Reporting). Disse specifikke forsikrings primære formål er at sørge for, at vores kunder overholder Sarbanes-Oxley Act (SOX). Den uafhængige tredjepartsaudit udføres i overensstemmelse med Statement on Standards for Attestation Engagements No. 18 (SSAE 18) og International Standard on Assurance Engagements No. 3402 (ISAE 3402). Disse standarder har erstattet de forældede Statement on Standards for Attestation Engagement No. 16 (SSAE16) og Statement on Auditing Standards No. 70 (SAS 70).

[Se SOC 1-undersøgelsen for Dropbox til teams.](#)

## **CSA**

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

CSA STAR (Security, Trust & Assurance Registry) er et gratis offentligt tilgængeligt register, der tilbyder et sikkerhedsprogram til cloudtjenester og dermed hjælper brugere med at vurdere sikkerhedskvaliteten hos cloudleverandører, de bruger i øjeblikket eller overvejer at indgå kontrakt med.

Dropbox til teams har fået både en CSA STAR Level 2-certificering og Level 2-attestering. CSA STAR Level 2 kræver en uafhængig tredjeparts vurdering af vores sikkerhedskontroller ved EY CertifyPoint (for certificering) og Ernst & Young LLP (for attestering), baseret på kravene i ISO/IEC 27001, SOC 2 Trust Service Criteria og CSA Cloud Controls Matrix (CCM) v4.0.2.

[Se vores CSA STAR Level 2-certificering og -attestering på CSA's websted.](#)

## **HIPAA/HITECH**

Dropbox underskriver BAA-aftaler (Business Associate Agreements) med Dropbox til teams-kunder, som skal bruge dem for at overholde HIPAA-loven (Health Insurance Portability and Accountability Act) og HITECH-loven (Health Information Technology for Economic and Clinical Health Act). Se mere information under [Dropbox og HIPAA/HITECH](#).

Dropbox har fået udarbejdet en uafhængig forsikringsrapport, der evaluerer vores kontrolfunktioner med hensyn til HIPAA-/HITECH-reglerne vedrørende sikkerhed, persondata og meddelelse om sikkerhedsbrud. Rapporten kortlægger desuden vores interne fremgangsmåder og anbefalinger til de kunder, som vil overholde HIPAA-/HITECH-kravene til sikkerhed og persondata med Dropbox til teams.

Kunder, som er interesseret i at anmode om disse dokumenter eller få flere oplysninger om køb af Dropbox til teams, kan kontakte vores [salgsteam](#). Hvis du aktuelt er Dropbox til teams-teamadministrator, kan du underskrive en BAA elektronisk fra [kontosiden i administratorpanelet](#).

Bemærk, at muligheden for at signere en elektronisk BAA fra Administratorkonsollen kun er tilgængelige for kunder i USA.

## NIST 800-171

Det amerikanske [National Institute of Standards and Technology](https://www.nist.gov/(NIST)) [https://www.nist.gov/\(NIST\)](https://www.nist.gov/(NIST)) fremmer og vedligeholder standarder og retningslinjer for at hjælpe med at beskytte informationssystemer. [NIST Special Publication \(SP\) 800171 Revision 2 \(R2\)](#) indeholder retningslinjer for beskyttelse af kontrolleret, ikke-klassificeret information (CUI) i ikke-føderale informationssystemer og organisationer. Enhver enhed, der behandler eller opbevarer CUI for de amerikanske myndigheder, såsom forskningsinstitutioner og uddannelsessektoren, skal overholde NIST SP 800-171 R2. Dropbox' systemer, processer og kontroller for CUI er valideret af en uafhængig tredjepartsauditør, Ernst & Young LLP.

NIST SP 800-171 R2-rapporten for Dropbox til teams er integreret i vores SOC 2-rapport, som er tilgængelig i Dropbox' [Trust Center](#).

Bemærk, at Dropbox Paper ikke er omfattet af NIST SP 800-171 R2-rapporten.

## FERPA og COPPA (studerende og børn)

Dropbox til teams gør det muligt for kunder at benytte tjenesterne i overensstemmelse med de leverandørforpligtelser, der er pålagt af den amerikanske FERPA-lov (Family Education Rights and Privacy Act). Uddannelsesinstitutioner må kun bruge Dropbox til teams i overensstemmelse med COPPA-loven (Children's Online Privacy Protection Act).

## FDA 21 CFR Del 11

Afsnit 21 i Code of Federal Regulations (CFR) regulerer mad og medicin i USA for Food and Drug Administration (FDA), Drug Enforcement Administration og Office of National Drug Control Policy. Afsnit 21, del 11, angiver de kriterier, hvorunder FDA anser elektroniske poster og underskrifter for at være troværdige, pålidelige og generelt tilsvarende skriftlige registreringer og håndskrevne underskrifter, der udføres skriftligt.

Se vores [Dropbox og FDA 21 CFR del 11 hvidbog](#) og [artikel i hjælpecenter](#) for at få flere oplysninger om, hvordan Dropbox kan hjælpe med at hjælpe dig med at overholde 21 CFR del 11.

## PCI DSS

Dropbox er en forhandler, som overholder Payment Card Industry Data Security Standard (PCI DSS). Dropbox til teams og Dropbox Paper er dog ikke beregnet til at behandle eller gemme kreditkorttransaktioner. PCI Attestation of Compliance (AoC) for vores forhandlerstatus er tilgængelig i Dropbox' [Trust Center](#).

Se mere information om compliance for Dropbox til teams i Dropbox' [Trust Center](#).

## ISMAP

ISMAP (Information System Security Management and Assessment Program) er en japansk certificering vedrørende brug af cloudbaserede softwareløsninger. Dette program er designet til at evaluere og registrere cloudtjenester, der opfylder de sikkerhedskrav, der er fastsat af den japanske regering. Dets primære mål er at sikre et højt sikkerhedsniveau for offentlige indkøb af cloudtjenester og facilitere en gnidningsfri implementering af cloudtjenester, der anvendes af den japanske regering.

Se Dropbox' vareoversigt i det officielle register over ISMAP-produkter [her](#).

## Resumé

Dropbox til teams tilbyder brugervenlige værktøjer, der hjælper teams med at samarbejde effektivt, samtidig med at der tilbydes de sikkerhedsforanstaltninger og overholdelsescertificeringer, som organisationer kræver. Ved hjælp af en fremgangsmåde i flere lag, der kombinerer en solid, grundlæggende infrastruktur med en række politikker, der kan tilpasses, giver vi virksomheder en avanceret løsning, der kan skræddersys til deres unikke behov. Få flere oplysninger om Dropbox til teams ved at kontakte os på [sales@dropbox.com](mailto:sales@dropbox.com).

# Dropbox Dash

Dash er en produktivitetplatform, der kombinerer smart universel søgning og vidensadministration med dybdegående kontrol af adgang til indhold. Dash er designet til at hjælpe dig med at [finde](#), [oprette](#), [organisere](#), [dele](#) og [sikre](#) vigtigt arbejdsindhold fra SaaS og cloudapplikationer for at strømline produktiviteten og fremskynde oprettelsen af indhold. Administratorer kan overvåge og administrere adgangskontrollister (ACL'er) på tværs af forbundne arbejdsapps ét sted. Dash er bygget på en kombination af Dropbox' pålidelige infrastruktur og førende cloudbaserede infrastrukturtjenester.

Du kan se mere information om sikkerhed for Dropbox Dash i [hvidbogen om sikkerhed for Dropbox Dash](#).

# Dropbox Sign

De dokumenter, kontrakter og aftaler, du underskriver som virksomhed, er nogle af de vigtigste dokumenter, du har. Mange af denne type transaktioner omfatter en juridisk bindende underskrift og har afgørende betydning for virksomhedens drift. Eksempler på det er dokumenter til ansættelse af nye medarbejdere, salgskontrakter, forpagtningsaftaler, partnerrelationer, leverandøraftaler og mange, mange flere. Disse dokumenter indeholder ofte følsomme oplysninger, og derfor er sikkerhed af afgørende betydning. Med Dropbox Sign-tjenester, som omfatter Dropbox Sign og Dropbox Fax, har beskyttelsen af dine dokumenter og relaterede transaktioner højeste prioritet. Vi bestræber os på at sikre fortrolighed, sikkerhed og beskyttelse af ethvert dokument, der underskrives ved hjælp af Dropbox Sign-tjenester.

Sikkerhed dækker en meget bred vifte af emner, og denne hvidbog giver et ret grundigt overblik over dem alle. Dropbox kan samarbejde med kunder, der køber en bestemt minimumskontraktværdi, om skræddersyede sikkerhedsgennemgange, spørgeskemaer og vurderinger.

## Kryptering

Dokumenter gemmes bag en firewall og godkendes mod afsenderens session, hver gang der anmodes om det pågældende dokument. Dropbox Sign håndhæver brugen af branchens bedste praksis til transmission af data til vores platform (Transport Layer Security, TLS), og data gemmes i datacentre, der er certificeret iht. SOC 1 Type II, SOC 2 Type I og ISO 27001. Kundedokumenter gemmes og krypteres under opbevaring ved hjælp af 256 bits AES-kryptering.

Du kan se mere information på vores [sikkerhedsside](#).

## Revisionsspor

### Dropbox Sign-produkt

Hver underskrift på en kontrakt tilføjes og fastgøres til dokumentet. Når du anmoder om en underskrift, føjer Dropbox Sign en revisionssporside til selve dokumentet. Revisionssporet indeholder en global unik identifikator (GUID), som kan bruges til at finde en optegnelse i vores database, der viser, hvem der har underskrevet et dokument og hvornår. Læs vores [legalitetserklæring](#) for at få mere at vide.

Det manipulationssikre revisionsspor sørger for, at enhver handling på dine dokumenter spores grundigt og tidsstemples for at give et forsvarligt bevis for adgang, gennemgang og underskrift.

Der er en række forskellige revisionssporede begivenheder i Dropbox Sign, herunder:

- Dokument sendt
- Dokumentet blev vist
- Dokument underskrevet
- Afvis at underskrive
- Underskrivers navn/e-mailadresse blev opdateret
- Vedhæftet fil blev uploadet
- Personlig underskrivning blev aktiveret
- Adgangskoder for underskriver blev bekræftet
- Elektronisk registrering og videregivelse af underskrift blev accepteret
- Anmodningen om underskrift blev uddelegeret
- Anmodningen om underskrift blev fuldført
- Fuldført anmodning fortsat

En aktuel liste over alle revisionssporede hændelser kan ses på vores [sikkerhedsside](#).

## Autenticitet

Dropbox Sign er designet til at beskytte dine dokumenter og forhindre manipulation under og efter underskriftsprocessen. Ved hjælp af hashingteknologi opretter Dropbox Sign en unik registrering af det underliggende dokument, før nogen af parterne underskriver det, og opretter derefter en separat unik registrering af det underliggende dokument, der indeholder alle underskrifterne. Hvis du nogensinde får brug for at bevise, at der ikke er blevet manipuleret med dokumenterne før og efter underskrift, kan Dropbox Sign give dig de to unikke dokumentregistreringer. Dropbox Sign bruger den samme teknologi til at beskytte dine e-signaturer.

## Godkendelse

Vi tilbyder flere funktioner, der sikrer robust godkendelse af enkeltpersoner, så du kan bekræfte, at brugere er, hvem de siger, de er, før de får lov til enten at udstede et dokument til underskrift eller udføre en underskrift.

## Tofaktorgodkendelse.

Brugere kan konfigurere tofaktorgodkendelse, som kræver indtastning af en unik kode, der genereres via Google Authenticator eller sendes til den enkelte via sms. Denne kode skal bruges i tillæg til vedkommendes brugernavn og adgangskode. Teamadministratorer kan bestemme, hvilken metode der bruges til tofaktorgodkendelse.

- Enkeltlogon er tilgængeligt med en Dropbox- eller Google-konto.
- API-nøglebaseret godkendelse til API'en.
- Alle adgangskoder hashes og saltes på sikker vis.

### Sessioner udløber efter et bestemt tidsrum.

1 time som standard, hvilket kan forlænges til 30 dage, hvis brugeren vælger **Husk mig** under login.

### Godkendelsesfunktioner specifikke for Dropbox Sign:

- **Anmodninger om underskrift beskyttet med adgangskode.** Til Dropbox Sign-produktet kan brugere aktivere en adgangskode for underskriver (en alfanumerisk streng på 4 til 12 tegn), som underskrivere skal indtaste for at se et dokument.
- **OAuth.** Dropbox Sign API understøtter OAuth som en metode til at godkende API-kald på vegne af en bruger.
- **SAML.** Dropbox Sign understøtter SAML 2.0 for enkeltlogon til virksomheder.

## Tilladelser

Det er vigtigt, du kan kontrollere, hvem der kan gøre hvad i systemet.

### Dropbox Sign-produkt

Forskellige roller har forskellige adgangsrettigheder, både i Dropbox Sign API og i slutbrugerproduktet. Administratorer kan eksempelvis kontrollere indstillinger for hele teams, faktureringsoplysninger og roller.

- **Rollebaseret sikkerhed.** Muliggør forskellige tilladelsesniveauer for forskellige medlemmer af et team, lige fra administrative rettigheder til medlemmer, der kun har tilladelser til at se skabeloner og udstede anmodninger om underskrift.
- **Underskriverspecifikke adgangskoder.** Som et ekstra sikkerhedslag kan hver underskriver tildeles en adgangskode for yderligere sikkerhed for, hvem der underskriver.

# Compliance-certifikater, attestationer og lovgivningsmæssig overholdelse

Dropbox Sign, herunder planerne Dropbox Sign Standard, Premium, API Essentials, API Standard og API Premium, overholder følgende rammer, standarder og lovgivninger:

## SOC

Service Organization Controls-rapporter (SOC), der kaldes SOC 1, SOC 2 eller SOC 3, er ordninger, der er etableret af American Institute of Certified Public Accountants (AICPA) til rapportering af interne kontrolfunktioner, der er implementeret i en organisation. Dropbox Sign har valideret sine systemer, applikationer, medarbejdere og processer via en række revisioner udført af en uafhængig tredjepartsauditør, Ernst & Young LLP.

### **SOC 2 for sikkerhed, tilgængelighed og fortrolighed.**

SOC 2-rapporten giver kunderne et detaljeret niveau af sikkerhed baseret på kontrolforanstaltninger, der dækker alle fem kriterier for troværdige tjenester: Sikkerhed, tilgængelighed, behandlingsintegritet og fortrolighed (afsnit 100 i TSP). SOC 2-rapporten indeholder en detaljeret beskrivelse af Dropbox Signs processer og de mere end 100 kontrolforanstaltninger, der er indført for at beskytte dine kundedata. Ud over vores uafhængige tredjepartsauditørs udtalelse om effektiviteten af vores kontrolforanstaltningers design og drift indeholder rapporten auditørens testprocedurer og resultater for samtlige kontrolforanstaltninger.

[Se SOC 2-undersøgelsen for Dropbox Sign.](#)

### **SOC 3 for sikkerhed, tilgængelighed og fortrolighed**

SOC 3-kontrolrapporten dækker Trust Service Criteria for sikkerhed, tilgængelighed og fortrolighed (afsnit 100 i TSP). Dropbox Signs rapport om almindelig brug er en sammenfatning af SOC 2-rapporten og omfatter den uafhængige tredjepartsauditørs udtalelse om den effektive udformning og drift af vores kontroller.

[Se SOC 3-undersøgelsen for Dropbox Sign.](#)

## ISO

### **ISO/IEC 27001 (Informationssikkerhed)**

ISO/IEC 27001 er anerkendt som verdens førende ISMS-standard (Information Security Management System). Standarden anvender også den bedste praksis for sikkerhed, der er beskrevet i ISO/IEC 27002. For at gøre os fortjent til din tillid har vi fokus på løbende og omfattende administration af vores fysiske, tekniske og juridiske kontrol hos Dropbox Sign.

[Se ISO/IEC 27001-certifikatet for Dropbox Sign.](#)

## **ISO/IEC 27018 (cloudbaseret beskyttelse af personlige oplysninger og data)**

ISO/IEC 27018 er en international standard for beskyttelse af data og personlige oplysninger. Standarden finder anvendelse for udbydere af cloudtjenester, såsom Dropbox Sign, der behandler personlige oplysninger på vegne af deres kunder, og udgør grundlaget for kundernes almindelige krav eller spørgsmål i forbindelse med lovgivningsmæssige og kontraktmæssige forhold.

[Se ISO/IEC 27018-certifikatet for Dropbox Sign.](#)

## **HIPAA/HITECH**

Dropbox Sign understøtter overholdelse af HIPAA-loven (Health Insurance Portability and Accountability Act) og HITECH-loven (Health Information Technology for Economic and Clinical Health Act).

Disse love skal sikre udbredelsen af teknologi inden for sundhedsindustrien, når der udvikles sikkerhed og beskyttelse af persondata i helbredsoplysninger. Organisationer såsom hospitaler, lægeklinikker og tandlægepraksisser samt enkeltpersoner, der interagerer med beskyttet sundhedsinformation (PHI), kan være underlagt HIPAA/HITECH. Dette kan også omfatte virksomheder, som samarbejder med disse virksomheder og kommer i berøring med PHI på deres vegne.

Dropbox Sign udarbejder en rapport med relation til HIPAA-sikkerhedsregler og krav til oplysning om overtrædelse af HITECH.

[Se HIPAA-rapporten for Dropbox Sign.](#)

## **PCI DSS**

Dropbox Sign overholder Payment Card Industry Data Security Standard (PCI DSS). Beviset for vores overholdelse af PCI som forhandler kan ses i Dropbox Signs [Trust Center](#).

## **Den amerikanske E-SIGN-akt fra 2000**

E-SIGN-loven (Electronic Signatures in Global and National Commerce Act) er en føderal lov, der foreskriver en generel regel for validitet af elektroniske registre og underskrifter til transaktioner. [Den amerikanske E-SIGN-lov](#) kræver blandt andet tilkendegivelse af en hensigt om at underskrive, visse forbrugeroplysninger og registeropbevaring.

## Uniform Electronic Transactions Act (UETA) fra 1999

Loven [Uniform Electronic Transaction Act](#) blev vedtaget i 1999 af National Conference of Commissions on Uniform State Laws og tillader brugen af elektroniske kommunikationstransaktioner ved at give elektroniske underskrifter samme juridiske vægt som håndskrevne underskrifter på papir. UETA er blevet indført i alle delstater med undtagelse af New York.

## eIDAS-forordningen (eIDAS-forordningen for EU fra 2016 (EU-forordning 910/2014), som erstattede det tidligere direktiv EF/1999/93)

eIDAS-forordningen definerer tre typer elektronisk underskrift (SES, AES og QES) og er en forordning om elektroniske identifikations- og tillidstjenester til elektroniske transaktioner på det europæiske indre marked. Det udgør en juridisk ramme for personer, virksomheder (især små og mellemstore virksomheder) og offentlige administrationer til sikkert at tilgå tjenester og udføre transaktioner digitalt i alle EU's medlemsstater. Dropbox Sign understøtter elektroniske underskrifter af typen SES og QES. Du kan se mere information om eIDAS på vores [compliance-side](#).

## Databeskyttelsesramme

Dropbox Sign overholder programmet til værn om privatlivets fred mellem EU og USA og Schweiz og USA samt den britiske udvidelse af programmet til værn om privatlivets fred mellem EU og USA som fastsat af det amerikanske handelsministerium vedrørende behandling af persondata, der overføres fra EU, det Europæiske Økonomiske Samarbejdsområde, Storbritannien og Schweiz til USA. Du kan få mere at vide om databeskyttelsesrammen og se vores certificering på <https://www.dataprivacyframework.gov>.

## EU's generelle forordning om databeskyttelse (GDPR)

Den generelle forordning om databeskyttelse (GDPR) er en EU-forordning fra 2018, der markant ændrede den tidligere ramme for behandling af persondata om fysiske personer i EU. GDPR introducerede en række nye eller udvidede krav, der gælder for virksomheder som Dropbox, der behandler persondata. Dropbox Sign overholder GDPR, så kunder kan benytte Dropbox Sign til at facilitere deres egen overholdelse af GDPR. Du kan se alle oplysninger om overholdelse af GDPR på vores [compliance-side](#).

## Underleverandører

Mindst en gang årligt gennemfører Dropbox Sign en evaluering af vores underleverandører. Hvis disse evalueringer afslører væsentlige forhold, som vi mener udgør risici for Dropbox Sign eller vores kunder, samarbejder vi med tjenesteudbyderen for at forstå potentielle indvirkninger på kundedata og følge afhjælpningen heraf, indtil problemet er løst.

I vores [persondatapolitik](#) er forklaret de begrænsede omstændigheder, under hvilke dine data kan blive delt med tredjeparter.

Dropbox Sign anvender Amazon Web Services som IaaS-leverandør, som løbende administrerer risici og foretager løbende vurderinger for at sikre overholdelse af branchestandarder (f.eks. SOC 1, SOC 2 og ISO 27001).

Du kan se flere oplysninger om AWS' complianceprogram [her](#).

Revisioner og rapporter for Dropbox Sign er tilgængelige i Dropbox Signs [Trust Center](#).

### Links til vigtige ressourcer

[Dropbox Signs persondatapolitik](#)

[Dropbox Signs Trust Center](#)

[Dropbox Sign-sikkerhed](#)

[Dropbox Sign-compliance](#)

# Dropbox DocSend

Dropbox DocSend er en sikker platform til dokumentdeling, som alle kan bruge. Vi gør det lige så nemt at administrere, dele og spore dine vigtige filer som bare at dele et link. DocSends avancerede funktioner til dokumentsikkerhed passer på dig og dine følsomme oplysninger – lige fra e-mailgodkendelse til en integreret fortrolighedsaftale. Ud over DocSends analyser på dokumentniveau, som giver dig indsigt i, hvem der har set dit dokument, og hvor de specifikt har brugt tid, omfatter DocSends avancerede sikkerhedsfunktioner også tilladelseslister (begrænsning af adgang til dit indhold ud fra domæne eller e-mailadresse), vandmærkning, e-mailbekræftelse for dokumentvisning og fortrolighedsaftaler med ét klik, der gør det obligatorisk at underskrive en fortrolighedsaftale, før man kan se et fortroligt dokument. Med DocSend kontrollerer du samtlige aspekter af dine delte filer – også efter du har trykket på send.

DocSend-tjenester er udviklet med en sikker, distribueret infrastruktur med beskyttelse i flere lag. Vi arbejder på at sikre, at dine data er beskyttet, og give vores kunder adgang til værktøjer, der giver kontrol og synlighed.

Du kan få mere at vide om DocSends produktfunktioner på <https://www.docsend.com/>.

## Produktinformation

Dropbox DocSend indeholder en lang række funktioner, der varierer alt efter planen. Du kan finde flere oplysninger i [DocSend-priserne](#). Afhængigt af plantypen har vores brugere adgang til følgende funktioner:

### Sikker fildeling

Kontrollér alle aspekter af delte filer, få sikker fildeling med DocSend-links og adgangskoder, og angiv udløbsdatoer for downloads.

### Dynamiske vandmærker

Hjælper med at forhindre uønsket deling, viser oplysninger om seere med mere.

## Virtuelle datarum

Virtuelle datarum (VDR) gør det muligt at dele flere dokumenter med et enkelt link og leverer indhold til seerne og giver dem mulighed for at uploade filer med eller uden en DocSend-konto. De kan understøtte specifikke e-mailadresser og domæner samt adgangskoder og underskrifter på fortrolighedsaftaler.

## E-signatur

Konverter filer til dokumenter, der kan underskrives, eller opret dem direkte fra DocSend. Overholder ESIGN- og UETA-reglerne og understøtter flere brugere og de analyser, der er forbundet med deres dokumentinteraktioner. Når aftalen er underskrevet, kan du modtage et revisionsspor for underskrivningsprocessen eller eksportere en liste over underskrifter for et dokument.

## Fortrolighedserklæringer

Konfigurer fortrolighedsaftaler eller andre aftaler til følsomt indhold, så seerne skal underskrive, før de får adgang til et dokument, også selvom det er videresendt til en ny person.

## Brugerroller

Brug flere niveauer af brugeradgang, herunder [rollebaserede sikkerhedstilladelser](#). Brugerne spænder fra medlemmer, der uploader og opdaterer indhold, til de administratorer, der administrerer dem og deres konti. Alle planer indeholder også en kontoejer, som kan få adgang til fakturerings siden og overføre kontoejerskab.

## Brugeradministration

Beskyt dokumenter, og hold fakturering opdateret. DocSend-ejere og administratorer kan tilføje, deaktivere, suspendere og reaktivere brugere.

## Overfør brugerdata

DocSend-ejere og administratorer kan bruge Overfør brugerdata til at flytte alle data fra en suspenderet eller deaktiveret bruger til en anden aktiv bruger for at sikre, at den inaktive brugers links og dokumenter stadig er tilgængelige.

## Enkeltlogon

Teams kan logge på sikkert ved hjælp af Okta eller OneLogin via SAML 2.0, hvor DocSend også understøtter SCIM til klargøring af brugere.

## Underteams

Brug underordnede teams til at organisere og give adgang til specifikt indhold, der er relevant for hvert team i en organisation. Det er med til at beskytte indholdet og sikre, at kun autoriserede brugere kan tilgå det. Adgang til mapper kan også administreres med underordnede teams.

# Kryptering

DocSend beskytter data både under overførsel mellem vores apps og servere og under opbevaring. Dokumenter gemmes bag en firewall og godkendes mod afsenderens session, hver gang der anmodes om det pågældende dokument. Vi håndhæver brugen af branchens bedste praksis til transmission af data til vores platform, Transport Layer Security (TLS), og data gemmes i datacentre, der er certificeret iht. SOC 1 Type II, SOC 2 Type II eller ISO 27001. Dine dokumenter gemmes og krypteres under opbevaring ved hjælp af 256-bits AES-kryptering.

# Revisionsspor

Sammen med DocSends e-signaturtjenester sikrer et revisionsspor, at enhver handling spores grundigt og tidsstemples for at give et forsvarligt bevis for adgang, gennemgang og underskrift. Disse optegnelser indeholder et hash af PDF-dokumentet, som vi kan sammenligne med et tvivlsomt PDF-dokuments hash for at afgøre, om det er blevet ændret eller manipuleret.

# Godkendelse

Vi tilbyder flere funktioner, der sikrer robust godkendelse af enkeltpersoner, så du kan bekræfte, at brugere er, hvem de siger, de er, før de får adgang til dit indhold, får lov at udstede et dokument til underskrift eller udføre en underskrift.

**Alle adgangskoder hashes og saltes på sikker vis**

## Enkeltlogon

DocSend kan konfigureres til at give teammedlemmer adgang ved at logge ind på en central identitetsudbyder. Vores SSO-implementering, der benytter branchestandarden Security Assertion Markup Language 2.0 (SAML 2.0), gør klargøring af brugere mere enkelt og sikkert ved at gøre en pålidelig identitetsudbyder ansvarlig for godkendelse og give teammedlemmer adgang til Dropbox uden behov for at administrere endnu en adgangskode.

## Godkendelsesfunktioner specifikke for DocSend

- **Adgangskodebeskyttet fildeling:** Brugere kan angive en adgangskode, bekræfte via e-mail og begrænse adgangen for at sikre, at kun de rette personer kan se deres filer. Brugere kan også angive udløbsdatoer og slå muligheden for at downloade filerne til eller fra.
- **Beskyt adgang med aftaler:** Brugere kan beskytte adgang til indhold med en aftale, for eksempel en fortrolighedsaftale.

# Tilladelser

Det er vigtigt, du kan kontrollere, hvem der kan gøre hvad i systemet.

## DocSend-produkt

Forskellige roller har forskellige adgangsrettigheder. Administratorer kan eksempelvis kontrollere indstillinger for hele teams, faktureringsoplysninger og roller.

- **Rollebaseret sikkerhed:** Muliggør forskellige tilladelsesniveauer for forskellige medlemmer af et team, lige fra administrative rettigheder til medlemmer.
- **Underordnede teams:** Med underordnede teams i DocSend kan brugere give adgang til specifikt indhold, der er relevant for de enkelte teams i en organisation. Underordnede teams beskytter følsomt indhold og sikrer, at kun autoriserede brugere kan tilgå det.

# Compliance-certifikater, attestationer og lovgivningsmæssig overholdelse

Dropbox DocSend, herunder planerne Dropbox DocSend Personal, Standard, Advanced og Advanced Data Rooms, overholder følgende rammer, standarder og lovgivninger:

## SOC

Service Organization Controls-rapporter (SOC), der kaldes SOC 1, SOC 2 eller SOC 3, er ordninger, der er etableret af American Institute of Certified Public Accountants (AICPA) til rapportering af interne kontrolfunktioner, der er implementeret i en organisation. Dropbox DocSend har valideret sine systemer, applikationer, medarbejdere og processer via en række revisioner udført af en uafhængig tredjepartsauditør, Ernst & Young LLP.

### **SOC 2 for sikkerhed**

SOC 2-rapporten giver kunderne et detaljeret niveau af sikkerhed baseret på kontrolforanstaltninger, der dækker Trust Service Criteria for sikkerhed (afsnit 100 i TSP). SOC 2-rapporten indeholder en detaljeret beskrivelse af Dropbox DocSends processer og de mere end 100 kontrolforanstaltninger, der er indført for at beskytte dine kundedata. Ud over vores uafhængige tredjepartsauditørs udtalelse om effektiviteten af vores kontrolforanstaltningers design og drift indeholder rapporten auditørens testprocedurer og resultater for samtlige kontrolforanstaltninger.

[Se SOC 2-undersøgelsen for Dropbox DocSend.](#)

### **SOC 3 for sikkerhed**

SOC 3-kontrolrapporten dækker Trust Service Criteria for sikkerhed (afsnit 100 i TSP). Dropbox DocSends rapport om almindelig brug er en sammenfatning af SOC 2-rapporten og omfatter den uafhængige tredjepartsauditørs udtalelse om den effektive udformning og drift af vores kontroller.

[Se SOC 3-undersøgelsen for Dropbox DocSend](#)

## PCI DSS

Dropbox DocSend overholder Payment Card Industry Data Security Standard (PCI DSS). Beviset for vores overholdelse af PCI som forhandler kan ses i Dropbox DocSends [Trust Center](#).

### **Databeskyttelsesramme**

Dropbox DocSend overholder programmet til værn om privatlivets fred mellem EU og USA og Schweiz og USA samt den britiske udvidelse af programmet til værn om privatlivets fred mellem EU og USA som fastsat af det amerikanske handelsministerium vedrørende behandling af persondata, der overføres fra EU, det Europæiske Økonomiske Samarbejdsområde, Storbritannien og Schweiz til USA. Du kan få mere at vide om databeskyttelsesrammen og se vores certificering på <https://www.dataprivacyframework.gov>.

### **EU's generelle forordning om databeskyttelse (GDPR)**

Den generelle forordning om databeskyttelse (GDPR) er en EU-forordning fra 2018, der markant ændrede den tidligere ramme for behandling af persondata om fysiske personer i EU. GDPR introducerede en række nye eller udvidede krav, der gælder for virksomheder som Dropbox, som behandler persondata. Dropbox DocSend overholder GDPR, så kunder kan benytte Dropbox DocSend til at facilitere deres egen overholdelse af GDPR.

# Underleverandører

Mindst en gang årligt gennemfører Dropbox DocSend en evaluering af vores underleverandører. Hvis disse evalueringer afslører væsentlige forhold, som vi mener udgør risici for Dropbox DocSend eller vores kunder, samarbejder vi med tjenesteudbyderen for at forstå potentielle indvirkninger på kundedata og følge afhjælpningen heraf, indtil problemet er løst.

I vores [persondatapolitik](#) er forklaret de begrænsede omstændigheder, under hvilke dine data kan blive delt med tredjeparter.

Dropbox DocSend-tjenester anvender Amazon Web Services til SaaS og IaaS, som løbende administrerer risici og foretager løbende vurderinger for at sikre overholdelse af branchestandarder (f.eks. SOC 1, SOC 2 og ISO 27001). Derudover bliver PaaS gennem Heroku også uafhængigt evalueret ved eksterne sikkerhedsvurderinger (f.eks. SOC 1, SOC 2 og ISO 27001).

Du kan se flere oplysninger om AWS' complianceprogram [her](#).

Revisioner og rapporter for Dropbox DocSend er tilgængelige i Dropbox DocSends [Trust Center](#).

DocSend har desuden gennemført den strenge sikkerhedskontrolproces, som Salesforce har iværksat som led i at blive optaget på Salesforce AppExchange.

## Links til vigtige ressourcer

[Dropbox DocSends servicebetingelser](#)

[Dropbox DocSends persondatapolitik](#)

[Dropbox DocSends politik for copyright og intellektuel ejendom](#)

[Dropbox DocSends cookiepolitik](#)

# Reclaim.ai

Reclaim.ai er et produktivitetsværktøj, der hjælper enkeltpersoner, teams og virksomheder med at afstemme deres kalendere med deres prioriteter for at få tid til de ting, der betyder mest. Reclaim leverer en fleksibel og effektiv planlægningsløsning med kunstig intelligens (AI) til Google Kalender og Microsoft Outlook-kalender, der hjælper virksomheder og enkeltpersoner med at passe på tiden til dybdegående arbejde, optimere møder, reducere omkostningstunge afbrydelser og forbedre work-life-balancen.

Reclaim.ai er 100 % cloudbaseret med primær infrastruktur hostet i Amazon AWS og alle data opbevaret i amerikanske datacentre/regioner. Reclaim er primært serverløst og benytter AWS-tjenester, herunder AWS RDS Aurora til databasehosting, AWS API Gateway, AWS MSK til Streaming Kafka, AWS ElastiCache til Redis-caching og AWS ECS Fargate til alle belastninger. Reclaim bruger Java med Micronaut til backend-stack og TypeScript med React til frontend.

Sikkerheds- og databeskyttelsesforpligtelser over for brugere og tredjeparter er fundamentalt for Reclaim.ai's mission. Data beskyttes gennem flere sikkerhedsforanstaltninger, hvor alle data er krypteret både under overførsel og opbevaring, forskellige godkendelsesforanstaltninger som SSO og Google-/Microsoft-godkendelse, SCIM (System for Cross-domain Identity Management), JWT-sessionstokens, multifaktorgodkendelse (MFA) til administratoradgang samt compliance, rapportering, onboarding og support af SOC 2 Type II. Administratorportalen kræver MFA og API-nøgler, og API-nøgler udløber efter en uge. Yderligere oplysninger om Reclaims politikker for sikkerhed og databeskyttelse, procedurer og tekniske implementeringer kan ses i Reclaims SOC 2 Type II-rapport, der er tilgængelig i [Reclaims Trust Center](#).

# Kryptering fra start til slut

Kryptering fra start til slut (E2EE) er tilgængeligt i Dropbox til teams. Med E2EE til udvalgte teammapper kan kunderne overholde reglerne, beskytte intellektuel ejendom og skabe tillid til enhedernes sikkerhed. Kryptering fra start til slut giver et sikkert miljø til deling og samarbejde om følsomme data, der forhindrer uautoriseret opsnapping og sikkerhedsbrud fra eksterne parter og endda fra Dropbox selv. Med E2EE genereres krypterings- og dekrypteringsnøglerne på brugerens enhed. Det betyder, at dataene krypteres på selve brugerens enhed, inden de sendes til Dropbox' servere. Ved at integrere kryptering fra start til slut kan virksomheder trygt benytte Dropbox og samtidig mindske risici for uautoriseret adgang og kompromittering af data.

## Protokolroller

### Dropbox-servere (PKI, dataopbevaring, protokolkoordinering)

Vi antager, at hver server er en enkelt enhed. Dens formål er at opbevare og distribuere offentlige nøgler og krypterede private eller symmetriske nøgler. Det er en kernekomponent i vores PKI (systemet til administration af krypterede nøgler, EKMS). Den gemmer mapperne, filerne og deres metadata og er ansvarlig for regelmæssig, ikke-kryptografisk autorisation og godkendelse.

### Teams (filejer)

Et team er en samling af brugere, der repræsenteres kryptografisk af en delt, kryptografisk teamnøgle. Teamet ejer sine filer, og protokollen sikrer, at medlemmerne kun har adgang til de filer, som deres team ejer.

### Brugere

Brugere bidrager til deres teams filsamling. De godkendes til Dropbox-serveren og deltager i protokollen via deres enheder. Protokollen sikrer, at de kun har adgang til de filer, som deres team ejer.

### Administratorer

Administratorer er en undergruppe af brugere. De er godkendt gennem almindelig godkendelse (f.eks. ACL'er) til at administrere parametre og brugere for deres team. Fra et kryptografisk synspunkt har de adgang til en gendannelsesnøgle, som giver dem mulighed for at udføre kryptografiske handlinger, såsom tilmelding af nye brugere eller enheder, selvom de ikke selv har nogen tilmeldte enheder.

### Enheder

Enheder tilbyder en grænseflade, hvor brugeren kan deltage i protokollen. Enheder er "pålidelige", fordi de anses for acceptable til at gemme og beskytte hemmelige oplysninger, for eksempel kryptografiske nøgler.

## Dropbox-medarbejdere

Dropbox-medarbejdere deltager ikke direkte i protokollen, men har øget adgang til Dropbox-serveren. Vi skelner mellem medarbejdere med skrivebeskyttet adgang, medarbejdere med skriveadgang til en brugers data og medarbejdere med mulighed for at ændre serverens/protokollens adfærd.

## Tredjeparter

Tredjeparter deltager ikke direkte i protokollen. Med andre ord er det entiteter, der ikke er autoriseret til at få adgang til en brugers filer. Protokollen sikrer, at de ikke kan dekryptere brugerens filer. På den måde beskytter det brugerne mod trusler af enhver art.

## Personalepolitik og -adgang

Ved ansættelsen skal alle Dropbox-medarbejders baggrund kontrolleres, de skal underskrive en accept af sikkerhedspolitikken og en fortrolighedsaftale, og de skal gennemføre sikkerhedstræning. Baseret på de enkeltes jobroller og ansvarsområder kan de blive tildelt fysisk og/eller logisk adgang til virksomheds- og produktionsmiljøer. En medarbejders adgang fjernes med det samme, når medarbejderen forlader virksomheden. Desuden skal alle medarbejdere fuldføre årlig sikkerhedstræning, og de får regelmæssigt sikkerhedsorienteret uddannelsesmateriale i form af e-mails med oplysninger, seminarer og præsentationer samt ressourcer på vores intranet og træningsportal.

Medarbejders adgang til Dropbox-miljøet opbevares og godkendes ved hjælp af en kombination af robuste adgangskoder, SSH-nøgler beskyttet med adgangssætninger samt totrinsbekræftelse. Fjernadgang kræver brug af VPN, der er beskyttet med totrinsbekræftelse, og alle særlige adgangshændelser gennemgås og vurderes af sikkerhedsteamet. Adgang til virksomheds- og produktionsnetværk er stærkt begrænset i henhold til definerede politikker. Adgang til produktionsnetværket er SSH-nøglebaseret og begrænset til ingeniørteams, der har brug for adgang for at udføre deres arbejdsopgaver. Konfiguration af firewalls kontrolleres omhyggeligt og er begrænset til et lille antal administratorer.

Desuden kræver vores interne politikker, at de medarbejdere, der får adgang til produktions- og virksomhedsmiljøer, skal overholde bedste praksis for oprettelse og opbevaring af private SSH-nøgler. Adgang til andre ressourcer, herunder datacentre, programmer til serverkonfigurering, produktionsservere og programmer til udvikling af kildekode, tildeles udelukkende efter specifik godkendelse af den relevante ledelse. Registrering af anmodningen om adgang, begrundelsen herfor og godkendelsen heraf udføres af ledelsen, og de relevante personer giver adgang.

Dropbox benytter teknisk adgangskontrol og interne politikker til at forhindre ansatte i at opnå vilkårlig adgang til brugerfiler og til at begrænse adgang til metadata og andre oplysninger om kryptering fra start til slut. For at beskytte slutbrugernes persondata og sikkerhed er det kun et lille antal ingeniører, som er ansvarlige for at udvikle Dropbox' kernetjenester til kryptering fra start til slut, der har adgang til produktionsmiljøet.

Efterhånden som Dropbox bliver en udvidelse af vores kunders infrastruktur, kan kunderne være forvisset om, at vi beskytter deres data på en ansvarlig måde.

## Mål og trusselsmodel

### Mål

Med kryptering fra start til slut beskyttes brugerne mod et defineret sæt scenarier, hvilket øger brugertilliden til Dropbox. Scenarierne er skitseret i vores trusselsmodel nedenfor.

**Vigtig bemærkning:** Dette dokument dækker kun kryptografisk beskyttelse. Almindelige adgangskontrolmekanismer supplerer protokollen, for eksempel ved at tillade en mere finmasket adgangskontrol blandt individuelle teammedlemmer. Alle protokolroller anvender en sikker kommunikationskanal (f.eks. TLS 1.2) til at kommunikere med serveren.

### Trusselsmodel

Protokollen for kryptering fra start til slut skal sikre:

- Fortrolighed med hensyn til Dropbox-serveren.
- Fortrolighed med hensyn til Dropbox-medarbejdere.
- Fortrolighed med hensyn til andre teams, deres brugere og tredjeparter.
- Integritet for krypterede filer til ændringer.
- Krypterede filers tilgængelighed uden for servermiljøet
- Fortrolighed for nye filer eller ændringer efter en nøgleudskiftning (et tidligere teammedlem, der mistes tilliden til, er et almindeligt scenarie, hvor eksisterende filer kan betragtes som kompromitterede, og fortroligheden bør sikres kryptografisk gennem nøgleudskiftning fra det tidspunkt).
  - Enheder behøver ikke at være online, for at der kan foretages en nøgleudskiftning, hvilket gør udskiftningsprocessen ret hurtig.

### Reduceret trusselsmodel gennem deaktivering af nøglebekræftelse

Nøglebekræftelse kræver bekræftelse uden for det primære bånd, hvilket kan være upraktisk i visse brugsscenarier. Nøglebekræftelse er valgfrit for at tage højde for disse scenarier. Hvis nøglebekræftelse deaktiveres, reduceres trusselsmodellen som følger:

- **Integritet og fortrolighed** er ikke længere garanteret mod en aktivt skadelig Dropbox-server eller mod Dropbox-medarbejdere med skriveadgang til brugerdata (dvs. mod aktive angreb).

### Rationaler

Kryptering fra start til slut er designet til at balancere de informationssikkerhedsmæssige behov for datafortrolighed, integritet og tilgængelighed, hvilket udvides til brugervenlighed, så teamets produktivitet ikke hæmmes.

## Den teamcentrerede tilgang

Hvis den kryptografiske sikkerhedsgrænse trækkes omkring den enkelte bruger, placerer det ansvaret for nøglen hos den bruger. Tab af data på grund af mistet nøgle er en risiko i systemer krypteret fra start til slut, og at enkelte brugere kan miste deres nøgler, medfører en risiko for tilgængeligheden af virksomhedens data. Der findes løsninger på den risiko, men de øger produktets kompleksitet og reducerer dets anvendelighed – især i betragtning af, at funktionen opererer i et asynkront miljø kun for teams.

Med sikkerhedsgrænsen trukket omkring teamet har vi et beskyttelseslag: Så længe én bruger stadig har adgang til teamnøglen, kan alle data gendannes, også hvis en eller flere brugere mister adgang til nøglen. Derudover forbedrer den teamcentrerede tilgang brugeroplevelsen og forenkler protokollens kompleksitet, hvilket reducerer risikoen for sikkerhedsproblemer.

## Automatisk enhedstilmelding

Manuel konfiguration af kryptering fra start til slut på en ny enhed kan være en stor udfordring for ikke-tekniske brugere, hvilket resulterer i lave implementeringsrater. Ved at benytte tilmeldinger fra enhed til enhed godkendt af Dropbox' standardmekanismer for godkendelse og adgangskontrol slipper brugerne for denne byrde gennem definerede trussels- og tillidsmodeller.

## Begrænsninger

- Klienter anses for at være troværdige, hvilket er en almindelig antagelse i forbindelse med kryptering fra start til slut. Det skyldes, at klienten er mindre dynamisk og betragtes som manuelt godkendt under installationsprocessen. Sikkerhedsgarantierne fra webklienten er svagere end dem, der tilbydes af indbyggede applikationer, fordi de leveres mere dynamisk.
- De enkelte filers friskhed kan ikke garanteres, fordi det ikke er kryptografisk muligt at bevise, at en fil er den seneste version.

## Tillidsmodel

- Brugere på et team er betroede, og indbyrdes adgangsrestriktioner håndhæves ikke kryptografisk, men af ACL'er.
- Brugeren er ansvarlig for at passe på sin enhed.
- Funktionen med kryptering fra start til slut beskytter kryptografisk mod alle andre, også Dropbox.

**Vigtigt:** Når nøglebekræftelse er deaktiveret, udvides tilliden til Dropbox-serveren og medarbejdere med skriveadgang. Ved at overholde protokollen leverer serveren de rigtige nøgler til hver filhandling, og enhver potentiel angribende part med adgang til en Dropbox-database kan ikke opnå nogen viden om indholdet af teamets filer. Dropbox er heller ikke i stand til at dekryptere data under opbevaring.

## Relation med almindelig adgangskontrol

Funktionen med kryptering fra start til slut er en sikkerhedsoptimering, der supplerer allerede eksisterende adgangskontrolmekanismer. I dette afsnit beskrives, hvordan Dropbox' standardmæssige sikkerhedsfunktioner fungerer sammen med tilføjelsen af kryptering fra start til slut.

### Adgangskontrol internt i teamet

Funktionen med kryptering fra start til slut beskytter mod trusler uden for et team. Derfor kræves eller implementeres ingen kryptografisk beskyttelse mellem medlemmer af det samme team. Adgangskontrol blandt medlemmer af det samme team implementeres uden for protokollen gennem almindelige ACL'er.

### Beskyttelsesstatus på filer, når et medlem forlader teamet

Indtil et medlem forlader et team, har teammedlemmet protokolmæssigt haft adgang til alle teamfiler. Nyt indhold krypteres med en ny nøgle. Almindelig adgangskontrol blokerer uden forsinkelse adgang til filer, som det tidligere teammedlem havde adgang til.

## Kryptografiske primitiver, typer og definitioner

### Nøgler og nøglemateriale

Alle nøgler og nøglematerialer oprettes på enheden.

### Entitetsnøglepar

Et entitetsnøglepar repræsenterer et asymmetrisk kryptografisk nøglepar, der består af en offentlig entitetsnøgle og en privat entitetsnøgle. Nøgleparrene oprettes altid på enheden, og den private entitetsnøgle skal krypteres, før den forlader enheden. Entitetsnøglepar gemmes enten på Dropbox' servere (krypteret), forbliver på enheden eller kan eksporteres med henblik på sikkerhedskopiering.

### Datanøgle

En entitet krypterer alle former for data med symmetriske datanøgler. Hver enkelt dataenhed (for eksempel en fil) krypteres med en ny, unik datanøgle. Symmetriske nøgler opbevares aldrig på Dropbox' servere uden kryptering. De krypteres altid med en anden nøgle.

Den anvendte algoritme er Blockwise AES-GCM.

## Algoritmer til nøgler

### Symmetriske nøgler

Til al symmetrisk kryptering bruges AES-256-GCM med et 128-bit godkendelsesteg og en 96-bit nonce. Denne nonce genereres vilkårligt på enhedssiden.

## Asymmetriske nøgler

- Til al asymmetrisk kryptering anvendes HPKE, single shot, base mode med kem (Kem. DhkemP256HkdfSha256, kdf: Kdf.HkdfSha256, aead: Aead.Aes256Gcm).
- Når nøglebekræftelse er aktiveret, tilføjes aad: utf8(algorithmID), og HPKE-**godkendelsestilstand** bruges til at kryptere navneområde og filnøgler.
  - Nøglebekræftelse for teamnøglen udføres implicit uden for det primære bånd.
  - Afsenderen af krypteringen af navneområdets nøgle er teamets private nøgle.
  - Afsenderen af filnøglekrypteringen er navneområdets private nøgle.

## System til administration af krypterede nøgler (EKMS)

Systemet til administration af krypterede nøgler (EKMS) er en løsning til at administrere kryptografiske nøgler designet til både sikkerhed og effektivitet. Med EKMS beskyttes datafortrolighed gennem kryptering på klientsiden, mens Zero Knowledge-princippet nøje overholdes. Det sikrer, at alle kryptografiske nøgler er krypteres sikkert på enheden, hvilket gør dem ubrugelige på serversiden. Af den grund skaber EKMS robust kryptering fra start til slut.

EKMS anvender en "teamcentreret tilgang til administration af nøgler", hvor hver bruger på et team tildeles kryptografisk adgang til andre nøgler i det specifikke team. Den tilgang sikrer effektiv administration af nøgler og opretholder samtidig sikkerheden.

EKMS sikrer, at alle teammedlemmer med kryptografisk adgang til teamnøgler også har adgang til alle filnøgler. Men adgangen til krypterede binære data (krypterede filer) er fortsat underlagt streng adgangskontrol. Hvis et teammedlem ikke har adgangsrettigheder, kan vedkommende ikke downloade de krypterede binære data.

## Nøgletyper i EKMS

### Filnøgle

Filnøgler er symmetriske nøgler. Enheder har fleksibiliteten til at angive den kryptografiske algoritme til deres brug. Nøglerne genereres på enheden og krypteres før afsendelse til serveren. Det sikrer, at nøglerne og de data, de beskytter, forbliver fortrolige.

### Krypterede teammappenøgler

Krypterede teammappenøgler er asymmetriske nøgler, der tildeles mapper beskyttet med kryptering fra start til slut. Enheder kan definere de kryptografiske algoritmer, der bruges til disse nøgler. Disse nøgler genereres på enheden, og den private nøgle krypteres med den aktive teamnøgle, før den overføres til serveren på sikker vis.

## Teamnøgle

Teamnøgler er også asymmetriske og tildeles specifikt til teams. Nøglerne genereres på enheden og beskyttes yderligere ved at kryptere den private nøgle med gendannelses- og enhedsnøgler, før de sendes til serveren.

## Enhedsnøgle

Enhedsnøgler er asymmetriske nøgler, der unikt tildeles til individuelle enheder og ejes af en bruger. Kun den offentlige nøgle er registreret på serveren, mens den private nøgle udelukkende forbliver på enheden. Disse nøgler bruges til at kryptere teamnøgler på en brugers team.

## Gendannelsesnøgle

Gendannelsesnøgler er asymmetriske nøgler, der allokeres til et bestemt team og genereres af en administrator. Administratorer har mulighed for at slette gendannelsesnøgler, men der skal altid bevares mindst én gendannelsesnøgle. Ligesom med enhedsnøgler er kun den offentlige nøgle registreret på serveren, og den private nøgle opbevares sikkert af administratoren.

## Dekryptering af private nøgler

Når en privat nøgle dekrypteres, og dens offentlige nøgle leveres separat, bliver den private nøgle verificeret ud fra den offentlige nøgle, og brugen af den dekrypterede nøgle vil blive afvist i tilfælde af uoverensstemmelse.

## Teamtilmelding

Vi har implementeret et design, der sikrer beskyttelse af kritiske kryptografiske nøgler, for at øge sikkerheden og effektiviteten af vores proces for teamtilmelding.

Processen begynder med generering af et gendannelsesnøglepar på enheden. Den private nøgle præsenteres derefter på sikker vis for administratoren til opbevaring.

Den offentlige gendannelsesnøgle registreres på serveren, mens et nyt teamnøglepar genereres på enheden, og den private teamnøgle krypteres ved hjælp af gendannelsesnøglen.

**Når nøglebekræftelse er aktiveret**, vises et fingeraftryk fra den offentlige teamnøgle til administratoren og skal transmitteres uden for det primære bånd til alle medlemmer af teamet, der endnu ikke er tilmeldt.

Den offentlige teamnøgle i klartekst og den krypterede private teamnøgle registreres på serveren for at fuldføre teamtilmeldingen. Disse trin resulterer i et fuldt ud tilmeldt team.

## Enhedstilmelding

Processen for enhedstilmelding udgøres af to dele.

1. En enhed, der anmoder om adgang til en krypteret teammappe. Dette trin består af lokal generering og registrering af unikke enhedsnøgler.
2. En allerede tilmeldt enhed eller en administrator, der giver enheden adgang ved at kryptere den private teamnøgle til de tidligere registrerede enhedsnøgler igen.

### **Enheden anmoder om adgang som følger (dette svarer til trin 1):**

1. En enhed tilmeldes ved at generere et unikt nøglepar, der består af en offentlig nøgle og en privat nøgle, på den lokale enhed.
2. Enheden beskytter den private nøgle på sikker vis på enheden, da den er nøglen til at dekryptere følsomme oplysninger.
3. Enhedens offentlige nøgle registreres på serveren.

**Bemærk:** Når nøglebekræftelse er aktiveret, påkræves brugeren af administratoren at sende enhedens offentlige nøgles fingeraftryk uden for det primære bånd. Enheden genkender det faktum, at nøglebekræftelse er aktiveret, og viser teamnøglen og enhedens fingeraftryk til brugeren. Behovet for at bekræfte teamnøglen fingeraftryk og videresende enhedens fingeraftryk skal kommunikeres til brugeren af administratoren. Enheden husker teamnøglen fingeraftryk, når det er godkendt af brugeren.

### **En allerede tilmeldt enhed giver adgang som følger (dette svarer til trin 2):**

**Bemærk:** En autoriseret enhed kan tilmelde nye enheder. En sådan autoriseret enhed kan være en allerede tilmeldt enhed eller administratoren, der bruger gendannelsesnøgler i administratorpanelet. Hvis funktionen til nøglebekræftelse er aktiveret, understøttes kun sidstnævnte tilgang.

1. Den autoriserede enhed henter den offentlige nøgle til den nye enhed fra serveren. Når nøglebekræftelse er aktiveret, er det kun administratoren, der kan tilmelde den nye enhed. I så fald bekræfter administratoren fingeraftrykket fra den modtagne offentlige nøgle uden for det primære bånd med det, der vises på den tilmeldte enhed.
2. Den autoriserede enhed indlæser også den krypterede private teamnøgle fra serveren eller henter den fra sin cache.
3. Ved hjælp af sin egen private nøgle eller gendannelsesnøgle dekrypterer den autoriserede enhed den private teamnøgle. Når nøglebekræftelse er aktiveret, bekræftes det, at den dekrypterede private teamnøgle passer til teamnøglen lokalt gemte fingeraftryk.
4. Den autoriserede enhed tager den dekrypterede private teamnøgle og krypterer den igen ved hjælp af den nye enheds offentlige nøgle. Dette trin sikrer, at kun den nye enhed med den tilhørende private nøgle har adgang til teamnøglen.
5. Den genkrypterede private teamnøgle registreres på serveren.

**Bemærk:** Når nøglebekræftelse er aktiveret, og hvis serveren på noget tidspunkt leverer en krypteret teamnøgle med et andet fingeraftryk, advarer enheden brugeren om det og kræver en bekræftelse af denne nye teamnøgles gyldighed. Det kan ske under en nøgleudskiftning. I så fald ville den nye teamnøgles fingeraftryk være blevet distribueret uden for det primære bånd under udskiftningsprocessen.

6. I tilfælde, hvor en tilmeldt enhed muligvis ikke er tilgængelig under tilmeldingsprocessen, kan administratorer benytte konceptet gendannelsesnøgler. Denne metode muliggør sikker tilmelding af nye enheder, selv når eksisterende enheder er offline eller utilgængelige. I øjeblikket er det kun muligt at tilmelde enheder med nøglebekræftelse aktiveret i administratorpanelet ved hjælp af gendannelsesnøglerne.

7. Når nøglebekræftelse er deaktiveret, og tilmeldte enheder er online, downloader de automatisk de offentlige nøgler til de enheder, der skal tilmeldes, og starter på strømlinet vis tilmeldingsprocessen i baggrunden. Denne strømlinede tilgang sørger for, at tilmelding af enheder kan foregå effektivt og sikkert.

## Tilføjelse af gendannelsesnøgler

En administrator kan tilføje flere gendannelsesnøgler.

### Følg denne vejledning for at oprette en ny gendannelsesnøgle:

1. Til at begynde med skal administratoren have adgang til en eksisterende gendannelsesnøgle. Denne eksisterende nøgle er en forudsætning for at tilføje en ny.
2. I browseren genereres et nyt gendannelsesnøglepar. Nøgleparret indeholder en offentlig nøgle og en privat nøgle. Den private nøgle skal bruges i senere trin.
3. Den nyligt genererede offentlige gendannelsesnøgle registreres på serveren. Dette trin sikrer, at systemet genkender og knytter den nye nøgle til teamet.
4. Administratoren skal angive den eksisterende private gendannelsesnøgle.
5. Når den eksisterende private gendannelsesnøgle er angivet, skal du hente den krypterede private teamnøgle. Denne nøgle er krypteret med den angivne gendannelsesnøgle.
6. Dekrypter den private teamnøgle ved hjælp af den eksisterende private gendannelsesnøgle. Det giver adgang til den private teamnøgle.
7. Derefter skal du kryptere den private teamnøgle med den nyligt genererede offentlige gendannelsesnøgle. Dette trin sikrer, at den private teamnøgle nu er knyttet til den nye gendannelsesnøgle.
8. Endelig skal du registrere den krypterede private teamnøgle på serveren. Denne handling fuldender processen for at oprette en ny gendannelsesnøgle og sørger for, at den nye nøgle opbevares sikkert og genkendes af serveren til fremtidig gendannelse.

## Administration og udskiftning af nøgler

**Bemærk:** I øjeblikket nøgleudskiftning og nøglebekræftelse indbyrdes uforenelige, hvilket vil sige, at du ikke kan have begge dele aktiveret.

### Tilbagekaldelse af adgang

I øjeblikket er tilbagekaldelse af adgang ikke implementeret. Teammedlemmer kan fjernes, men forhindres fra et kryptografisk synspunkt kun i fortsat adgang til filerne via almindelige ACL'er. Følgende er det koncept for tilbagekaldelse af adgang, der vil blive implementeret i fremtiden.

Tilbagekaldelse af adgang er en afgørende sikkerhedsfunktion, der sikrer kontrolleret sletning af både enhed- og gendannelsesnøgler. Det sikrer gennem kryptering, at tidligere teammedlemmer ikke kan kompromittere sikkerheden for teamets data. Denne proces spiller en grundlæggende rolle for at opretholde dataenes integritet og fortrolighed. Tilbagekaldelse af adgang omfatter følgende aspekter:

**Tilbagekaldelse af gendannelsesnøgler:** Autoriserede administratorer har mulighed for at tilbagekalde gendannelsesnøgler. Når udskiftning af teamnøgler påbegyndes, krypteres den nye teamnøgle ikke igen med den berørte offentlige gendannelsesnøgle. Det garanterer sikkerheden for nyoprettede eller ændrede filer.

**Tilbagekaldelse af enhedsnøgler:** Når en bruger forlader teamet, kan der påbegyndes udskiftning af teamnøgler, og den nye teamnøgle krypteres ikke igen med den berørte enheds offentlige nøgle.

**Nøgleudskiftning:** Nøgleudskiftning er en essentiel proces for at opretholde vores datas sikkerhed og fortrolighed. Det giver en mekanisme til at opdatere krypteringsnøgler.

**Forudsætning - tilbagekaldelse af adgang:** Nøgleudskiftning afhænger af tilbagekaldelse af adgang. Før nøgler kan udskiftes, skal alle bruger- eller gendannelsesnøgler, der skal tilbagekaldes, enten slettes eller markeres som deaktiverede.

**Administratorstyret nøgleudskiftning:** Administratorer har mulighed for at påbegynde nøgleudskiftning via administratorpanelet.

Følgende trin er nødvendige for at udskifte nøglerne:

#### 1. Udskift teamnøgle:

- a. Der oprettes en ny teamnøgle lokalt.
- b. Fingeraftrykket for den nye teamnøgle vises til administratoren til distribution uden for det primære bånd (**kun med nøglebekræftelse aktiveret**)
- c. Alle tilgængelige og aktive gendannelsesnøgler og enhedsnøgler hentes fra serveren. Hvis nøglebekræftelse er aktiveret, godkendes enhedens offentlige nøgles fingeraftryk uden for det primære bånd af administratoren
- d. Den nye private teamnøgle krypteres igen med **alle aktive gendannelses- og enhedsnøgler** for at bevare dataadgang.

**2. Udskift navneområdenøgler:** Der indføres en ny navneområdenøgle for hvert eksisterende navneområde. Den nye nøgle krypteres med det nye teams offentlige nøgle.

**3. Aktivér teamnøgle:** Når den nye teamnøgle er krypteret med alle aktive gendannelses- og enhedsnøgler og krypterer alle nye navneområdenøgler, markeres den som aktiv. Det betyder, at den vil blive brugt til krypteringshandlinger.

**4. Udløb og brug:** De eksisterende teamnøgler, navneområdenøgler og filnøgler udløber. Udløbne nøgler vil ikke længere have tilladelse til krypteringshandlinger. De kan kun bruges til dekrypteringshandlinger.

**5. Forbyd filafsendinger med eksisterende filnøgler:** I situationer, hvor filnøgler er udløbet, vil filafsendinger blive afvist. Enheder skal generere nye filnøgler og kryptere indholdet igen, før det uploades igen. Det sikrer, at ingen følsomme data kompromitteres som følge af brug af forældede krypteringsnøgler.

- 6. Når nøglebekræftelse er aktiveret**, verificerer og bekræfter brugerne, at deres enhed anvender den nye teamnøgle via det teamnøglefingeraftryk, der distribueres uden for det primære bånd, og deres enheds evne til at vise den aktuelt anvendte teamnøgle.

## Ekstern deling

Ekstern deling giver kryptografisk beskyttelse, når der samarbejdes med et andet team, hvis begge har kryptering fra start til slut aktiveret.

### Deling med eksterne teams

Eksterne teams skal være tilmeldt kryptering fra start til slut, hvilket betyder, at de har et gyldigt teamnøglepar. Deling sker derefter på teammappeniveau ved at kryptere teamets private nøgle med det eksterne teams offentlige nøgle. Det giver det eksterne team kryptografisk adgang til teammappen og dens indhold.

### Nøgleudskiftning ved ekstern deling

Nøgleudskiftning udføres som beskrevet ovenfor og begynder med teamnøglen for det team, der udfører udskiftningen. Hvis team A for eksempel har en delt mappe sammen med team B, og team B udskifter sine nøgler, vil nøglerne til den delte mappe også blive udskiftet. Den nye nøgle til den delte mappe deles automatisk med team A igen for at give begge teams adgang. Det giver kryptografisk beskyttelse, når nogen forlader et team.

**Vigtig bemærkning:** Ekstern deling er kun tilgængeligt, når nøglevalidering er deaktiveret.

## Fingeraftryk til teamnøgler

Med nøgleudskiftning kan flere teamnøgler være i brug på et givet tidspunkt. Fingeraftryk til teamnøgler mindsker scenarier, hvor nøgleudskiftning kan reducere sikkerheden. For eksempel ville der opstå et sikkerhedsproblem, hvis serveren var i stand til at oprette en teamnøgle uden for kontrol, kryptere den med en kundes enhedsnøgle og præsentere den som en udløbet teamnøgle. Enheder ville afvise skrivning med denne teamnøgle, fordi den allerede er udløbet, men serveren ville stadig kunne indsætte vilkårligt indhold som skrivebeskyttet og præsentere det som ældre teamdata. Det ville ødelægge integriteten.

Det forhindrer fingeraftryk til teamnøgler ved at godkende ikke kun den aktuelle teamnøgle, men også alle udløbne nøgler. Processen udføres gennem [Sparse Merkle-træer](#).

### Indledende oprettelse

Fingeraftrykket til teamnøgler udgøres af et Merkle træ-hash bestående af ét blad. Det betyder, at første hash for teamets offentlige nøgle allerede er teamnøglens fingeraftryk.

Den offentlige teamnøgles hash beregnes ved at sammenkæde algoritmenavnet, et separationstegn og den offentlige nøgle og så hashe resultatet med Sha256.

## Genberegning efter nøgleudskiftning

Ved en nøgleudskiftning introduceres en ny teamnøgle. Den administrator, der udfører nøgleudskiftningen, har det tidligere teamnøglefingeraftryk via roden af Merkle-træet. Serveren giver administratoren de oplysninger, der kræves for at udvide Merkle-træet med den nye teamnøgles hash og til at beregne **Merkle-træets nye rod (dvs. det nye fingeraftryk til teamnøglen)**. Under denne proces kan serveren ikke indsætte ugyldige værdier, fordi administratoren er opmærksom på Merkle-træets tidligere rodhash og nemt ville kunne registrere et sådant forsøg.

Den nye teamnøgles hash erstatter den første **ugyldige** værdi fra venstre i Sparse-træet. Det nyeste teamnøglehash kan bestemmes ved at se på den første gyldige værdi i træets blade fra højre.

## Bekræftelse af enhver teamnøgle

Med leveringen af en teamnøgle – uanset om den er udløbet eller aktiv – sender serveren et medlemsbevis for nøglen. Enheden, der tidligere har bekræftet og lokalt gemt teamnøglen fingeraftryk (dvs. Merkle-rodens hash), kan bekræfte beviset og derefter acceptere teamnøglen.

## Filkryptering

Den algoritme, der bruges til at kryptere filindholdet, er designet til at kunne udskiftes. Hver krypteret nøgle på serveren indeholder identifikatoren for den algoritme, som den er beregnet til at blive brugt sammen med. I øjeblikket bruges kun én algoritme: Blockwise AES-GCM.

## Algoritme for råfiler

Filindhold krypteres med en symmetrisk krypteringsalgoritme kaldet Blockwise AES-GCM.

### Kryptering

1. Angiv `|authTag| = 128 bit` og `|blocksize| = 4 MB`.
2. Opret en ny `hmac_key := random(256 bit)` og `nonce_hmac_key := random(96 bit)`.
3. Beregn `(encrypted_hmac_key, hmac_auth_tag) := AES-GCM-encrypt(revision_key, nonce_hmac_key, hmac_key)`.
4. Forvent `plaintext := f_0 || f_1 || ... || f_n` with `|f_i| = blocksize`.  
Den sidste blok kan være mindre end blokstørrelsen.
5. For hver `f_i`:
  - a. Vælg `nonce_i := random(96 bit)`.
  - b. Beregn `(encrypted_f_i, auth_tag_i) := AES-GCM-encrypt(revision_key, nonce_i, f_i)`.

6. Beregn `authSetHmac := HMAC_SHA256(hmac_key, auth_tag_0 || auth_tag_1 || ... || auth_tag_n)`.
7. Returner `encrypted_hmac_key`, `nonce_hmac_key`, `hmac_auth_tag`, `all nonce_i`, `all auth_tag_i`, `all encrypted_f_i` and `authSetHmac`.

## Dekryptering

1. Dekrypter `hmac_key`.
2. Bekræft `authSetHmac` ved at genberegne den og sammenligne den med den gemte værdi.  
Beregn `f_i := AES-GCM-decrypt(revision_key, nonce_i, auth_tag_i, encrypted_f_i)`.

## AES-GCM

AES-GCM bruges som en underliggende primitiv på grund af dens brede tilgængelighed i kryptografiske biblioteker.

## Kryptering af en fil

Der gemmes en hashværdi for hver blok med klartekst på Dropbox-serveren. Denne hashværdi behøver ikke at kunne dekrypteres af serveren, men den skal kunne dekrypteres af enheden. Vi introducerer en revisionsnøgle, som indsættes mellem filnøgle- og råfilalgoritmen, for at tage højde for det og for at fjerne revisionsbegrænsningen for Blockwise-AES-256-GCM.

Trinene til at kryptere en fil med en given `file_key` er som følger:

1. Opret en ny, vilkårlig AES-256-nøgle (`revision_key`).
2. Kryptér `revision_key` med `file_key`.
3. Kryptér filen med `revision_key`.
4. Hash hver blok med klartekst, og kryptér hver blok med klartekst med `revision_key`.
5. Send den krypterede fil, dens metadata, den krypterede revisionsnøgle og de krypterede hash for blokke med klartekst til Dropbox-serveren.

Trin for dekryptering af en fil:

1. Trinene i filkrypteringen udføres baglæns.
2. For hver dekrypteret blok i filen skal du beregne den dekrypterede bloks hash og sikre, at den svarer til det forventede hash (de krypterede hash for blokke med klartekst leveres til dekrypteringsrutinen).

Hver kryptering og hver ændring af en eksisterende fil udføres ved hjælp af en nyoprettet [revision\\_key](#). Det reducerer revisionsbegrænsningen for Blockwise-AES-256-GCM fra *antal blokke for en fil og revisioner af den til antal blokke for en fil*.

**Bemærk:** Filer kan i øjeblikket ikke flyttes mellem forskellige krypterede teammapper, men kun internt i dem. Hvis du for eksempel arbejder i en teammappe, kan du frit flytte filer – både ind i og ud af undermapper. Men hvis du har endnu en krypteret teammappe, er det ikke muligt at flytte filer mellem de to teammapper.

# Avanceret nøgleadministration

Avanceret nøgleadministration er tilgængeligt i Dropbox til teams. Virksomheder har brug for sofistikerede sikkerhedsløsninger, der opfylder compliance-kravene. Sikkerhedsteams skal bruge indsigt i og kontrol over den måde, hvorpå virksomhedens data beskyttes, for at beskytte følsomt indhold. Det kan opnås med Dropbox – uden eksterne løsninger til databeskyttelse. Vi gør det nemt at indføre denne nye og forbedrede datakrypteringsmodel, der benytter en infrastruktur til nøgleadministration, der er standard i branchen. Administrer dine krypteringsnøgler sikkert i Dropbox, og drag fordel af følgende funktioner.

## Automatisering og kontrol

- Automatisk, planlagt udskiftning af teamkrypteringsnøgler hvert år for garanteret beskyttelse.
- Du kan til enhver tid tilbagekalde din teamkrypteringsnøgle manuelt for at fjerne adgangen til dit teams data permanent, når der registreres en trussel.

## Øget databeskyttelse

- Krypteringsmodel i flere lag med en unik, teamtilknyttet krypteringsnøgle på øverste niveau.
- Teamkrypteringsnøgle (TEK) genereres og gemmes ved hjælp af branchestandardmæssige hardware-sikkerhedsmoduler (HSM).

## Auditerbarhed

- Se aktiviteter relateret til din krypteringsnøgle, herunder udskiftninger og tilbagekaldelser, med overvågningslogfiler.

## Kryptering på flere niveauer

Alle data opbevaret i Dropbox er krypteret, men du kan vælge et ekstra lag kontrol og sikkerhed ved at få Dropbox til at generere en unik teamkrypteringsnøgle til dit team.

Som en del af Dropbox' krypteringsproces på flere niveauer vil data under opbevaring for teams, der aktiverer Dropbox-administrerede krypteringsnøgler, blive krypteret ved hjælp af Dropbox' krypteringsproces på flere niveauer, hvor data under opbevaring i Dropbox krypteres i tre lag med forskellige nøgler – på blokniveau, navneområdeniveau og teamniveau. Funktionen til Dropbox-administrerede krypteringsnøgler (DMEK) giver kunderne en unik krypteringsnøgle på teamniveau (TEK), hvilket giver større fleksibilitet til datasikkerhed og overholdelse af lovgivning. Dropbox

administrerer opbevaring, organisering og udskiftning af TEK'er ved hjælp af branchestandarden AWS KMS (Key Management Service).

Nøgler er unikke for hver enkelt kunde. Hvert team tildeles en unik nøgle på teamniveau. TEK'er genereres, opbevares og revideres ved hjælp af funktionerne i AWS KMS (Key Management Service), der overholder FIPS 140-2. Når du har aktiveret DMEK i administratorpanelet, kræver det ingen konfiguration.

**Bemærk:** Aktivering af DMEK påvirker ikke Dropbox-funktionalitet. Samarbejdsfunktioner såsom forhåndsvisning, deling og søgning vil fortsat fungere som forventet.

### **Aktivering af Dropbox-administrerede krypteringsnøgler (DMEK)**

Du kan aktivere DMEK via Avanceret nøgleadministration i Dropbox' administratorpanel.

