

# Dropbox-vitbok för säkerhet

Ett Dropbox Security Paper

©2026 Dropbox. Med ensamrätt. V2026.03



# Innehållsförteckning

<b>Dropbox-förtroendeprogrammet</b>	<b>5</b>
<b>Enterprise-säkerhet</b>	<b>5</b>
Våra policyer	5
Engagerat och erfaret säkerhetsteam	7
Medarbetarpolicy, personalsäkerhet och åtkomst	7
Säkerhetsutbildning och ökad medvetenhet	8
Företagskontor	8
Sårbarhetsshantering	9
Fysisk säkerhet	9
Incidenthantering	9
<b>Infrastruktursäkerhet</b>	<b>10</b>
Nätverkssäkerhet	10
Närvaropunkter (PoP)	11
Peering	11
Säkerhetsövervakning	11
Tillförlitlighet	12
Datacenter och funktionstjänstleverantörer	12
Verksamhetens kontinuitet	12
Katastrofåterställning	13
<b>Applikationssäkerhet</b>	<b>14</b>
Skanning och testning av säkerhetspenetrering (intern och extern)	14
Hålla skadligt material borta från Dropbox	15
Buggpremier	15
Dataskydd och kryptering	15
Certificate pinning	17
Skydd av autentiseringsdata	17
Skanning efter sabotageprogram	17
<b>Produktsäkerhet</b>	<b>17</b>
Designgranskningar	17
Säker driftsättning	18
Förändringshantering	18
<b>Dataskydd</b>	<b>18</b>
<b>Dropbox Business</b>	<b>19</b>
<b>Under skalet</b>	<b>19</b>
Filinfrastruktur	20
Fildatalagring	21
Paper-infrastruktur	21
Paper-dokumentlagring	23
<b>Tillförlitlighet</b>	<b>24</b>
<b>Dropbox användargränssnitt</b>	<b>27</b>
<b>Paper-användargränssnitt</b>	<b>28</b>
<b>Dropbox Replay</b>	<b>28</b>

# Innehållsförteckning

Appar för Dropbox.....	28
Förbyggda komponenter .....	29
API-integreringar för Dropbox för team .....	29
API-partnerskap.....	31
Dropbox-integreringar .....	32
Produktsäkerhet.....	33
Innehållskontroller.....	33
Översikt över material.....	36
Teamkontroller .....	38
Hanterade enheter och inloggningar.....	41
Integritetscertifieringar, intyg och regelefterlevnad .....	51
Efterlevnad .....	52
Sammanfattning .....	57
<b>Dropbox Dash</b> .....	<b>58</b>
<b>Dropbox Sign</b> .....	<b>59</b>
Kryptering .....	59
Granskningslogg.....	59
Dropbox Sign-produkt.....	59
Äkthet.....	60
Autentisering .....	60
Behörigheter .....	61
Efterlevnadscertifieringar, intyg och regelefterlevnad .....	62
<b>Dropbox DocSend</b> .....	<b>66</b>
Produktinformation.....	66
Säker fildelning .....	66
Dynamiska vattenstämplar.....	66
Virtuella datarum.....	67
E-signatur .....	67
Sekretessavtal .....	67
Användarroller .....	67
Användarhantering.....	67
Överför användardata.....	67
Samlad inloggning .....	68
Underteam.....	68
Kryptering .....	68
Granskningslogg.....	68
Autentisering .....	68
Behörigheter .....	69
Efterlevnadscertifieringar, intyg och regelefterlevnad .....	69
Leverantörer av undertjänster.....	71

# Innehållsförteckning

<a href="#">Reclaim.ai</a>	72
<a href="#">Kryptering från slutpunkt till slutpunkt</a>	73
<a href="#">Avancerad nyckelhantering</a>	87

Denna information är aktuell per den engelska versionen. Denna översättning tillhandahålls endast för bekvämlighet och om det finns några avvikelser är det den engelska versionen som gäller.

# Dropbox-förtroendeprogrammet

Förtroende utgör grunden för vårt förhållande med miljontals människor och företag världen över. Vi värdesätter det förtroende du gett oss och tar vårt ansvar att skydda din information på yttersta allvar. För att förtjäna ditt förtroende, skapade vi Dropbox med tyngdpunkt på säkerhet, sekretess, transparens och efterlevnad.

Policyn för Dropbox förtroendeprogram etablerar en riskutvärderingsprocess som är utformad för att ta upp gällande lagar och förordningar för miljö, fysiska faktorer, användare och tredje part, kontraktsmässiga krav och olika andra risker som kan påverka systemsäkerhet, konfidentialitet, integritet, tillgänglighet eller sekretess. Prestandagranskningar genomförs minst en gång om året. Mer information om Dropbox förtroendeprogram finns på [dropbox.com/business/trust](https://dropbox.com/business/trust).

Dropbox har etablerat ett Trust Center som ger tillgång till information med självbetjäning om våra produkters säkerhet, sekretess, efterlevnad och tillförlitlighet. Besök Trust Center på [trust.dropbox.com](https://trust.dropbox.com) om du vill veta mer.

## Enterprise-säkerhet

Vi följer en flerskiktstrategi för att säkra företag, infrastruktur, applikationer och produkter som påverkar din organisation.

Dropbox har fastställt ett ramverk för hanteringen av informationssäkerhet. Detta ramverk beskriver syftet, inriktningen, principerna och de grundläggande reglerna för hur vi bibehåller våra kunders förtroende. Detta uppnås genom att bedöma risker och att ständigt förbättra säkerheten, sekretessen, integriteten och tillgängligheten för Dropbox för team-systemen. Vi granskar och uppdaterar regelbundet våra säkerhetspolicyer, erbjuder säkerhetsutbildning, utför tester av applikations- och nätverkssäkerhet (inklusive intrångstester), övervakar hur alla säkerhetspolicyer efterlevs samt utför interna och externa riskbedömningar.

### Våra policyer

Vi har upprättat en omfattande uppsättning säkerhetspolicyer som upprätthålls av Dropbox team för säkerhet och missbruk. Alla säkerhetspolicyer granskas och godkänns minst en gång per år. Medarbetare, praktikanter och underleverantörer deltar i en obligatorisk säkerhetsutbildning när de ansluter sig till företaget och de får kontinuerlig utbildning i säkerhetsmedvetenhet.

- **Informationssäkerhet**

Hålla användar- och Dropbox-information säker.

- **Autentisering**  
Beskriver hur Dropbox medarbetare autentiserar sig för att komma åt informationssystem och data.
- **Enhetssäkerhet**  
Minsta säkerhetskrav för mobilenheter som används för att få åtkomst till företagsinformation.
- **Logisk åtkomstkontroll**  
Hålla åtkomst till Dropbox system, användare och information säker. Detta omfattar åtkomstkontroll till både företags- och produktionsmiljöer.
- **Datasäkerhet**  
Beskriver hur Dropbox skyddar data genom specifika krav för lagring, åtkomst och användning.
- **Resesäkerhet**  
Beskriver vad Dropbox medarbetare bör göra innan de reser utomlands.
- **Säkerhetsriktlinjer för sälj- och kundupplevelse (CX)**  
Hålla användarinformationen säker, skydda våra medarbetare och ge support till våra användare.
- **Fysisk säkerhet**  
Bibehålla en trygg och säker miljö för personer och egendom på Dropbox.
- **Riktlinjer för fysisk säkerhet i produktion**  
Hantera fysisk åtkomst till produktionsanläggningar.
- **Incidenthantering**  
Beskriver hur Dropbox hanterar rapporterad säkerhet, integritet och platshändelser och dokumenterar incidenthanteringsplaner för var och en.
- **Obehörigt upphovsrättsskyddat material**  
Förbjuda personal från att använda Dropbox eller Dropbox-system för att lagra eller dela otillåtet innehåll.
- **Förändringshantering**  
Hantera ändringar i produktionssystem. Avsedd för alla Dropbox medarbetare, entreprenörer och praktikanter med åtkomst till system.
- **Sekretess för användardata**  
Skydda och hantera användarinformation och användaruppgifter på Dropbox i enlighet med vår integritetspolicy.
- **Policy för verksamhetskontinuitet och nödfallshantering**  
Beskriver bevarande, skydd och säkerhet för människor (medarbetare hos Dropbox), egendom och (affärsbaserade) processer.
- **Dropbox sekretessprogram**  
Syftet, principerna och ansvarsförhållandena för Dropbox-sekretessprogrammet.

- **Dropbox-förtroendeprogrammet**

Beskriver hur Dropbox arbetar och är trovärdigt.

- **Säkerhet för betalningsmiljön**

Säkra och underhålla den dedikerade betalningsmiljön som används på Dropbox för att acceptera kreditkortsbetalningar.

## Engagerat och erfaret säkerhetsteam

Vårt säkerhetsprogram är utformat för att utvärdera risker och bygga upp en säkerhetskultur på Dropbox. Varje enskild medarbetare på Dropbox eftersträvar säkerhet och att alltid skydda våra kunddata. Alla produkter och tjänster följer det informationssäkerhetsprogram som implementerats enligt säkerhetschefen på Dropbox. Som en del av vårt formella riskhanteringsprogram granskas säkerhetsrisker regelbundet, vilket resulterar i säkerhetsrelaterade initiativ på produkt-, infrastruktur- och företagsnivå.

Integritetsteamet ansvarar för att hantera vårt integritetsprogram. De implementerar våra viktiga integritetsinitiativ och förespråkar inbyggd integritet i vår datalivscykel.

För att garantera att alla Dropbox medarbetare kan främja skyddet av våra kunddata, arbetar vi för att säkerställa att säkerhet och integritet ingår i företagskulturen redan från ruta ett. Medarbetarna genomgår omfattande bakgrundskontroller, undertecknar och följer en uppförandekod och policyer om datoranvändning. De genomgår dessutom årliga utbildningar i säkerhetsmedvetande och integritet. En kontinuerlig medvetenhet om informationssäkerhet upprätthålls via månatliga nyhetsbrev om informationssäkerhet och säkerhetsrelevanta aviseringar.

## Medarbetarpolicy, personalsäkerhet och åtkomst

Efter anställningen måste samtliga Dropbox-medarbetare genomgå en bakgrundskontroll och underteckna en bekräftelse av säkerhetspolicyn och ett sekretessavtal, samt genomgå säkerhetsutbildning. Endast personer som har slutfört dessa procedurer får fysisk och logisk åtkomst till företagets och produktionens miljöer, enligt vad deras ansvarsområden kräver. Dessutom måste samtliga medarbetare slutföra en obligatorisk årlig säkerhets- och integritetsutbildning och de får regelbunden utbildning om säkerhetskännedom via informationsmejl, samtal och presentationer och resurser som finns på intranätet.

Medarbetaråtkomst till Dropbox-miljön upprätthålls av en central mapp och autentiseras med en kombination av starka lösenord, lösenfrasskyddade SSH-nycklar och tvåfaktoraautentisering. Fjärråtkomst kräver VPN som skyddas av tvåfaktoraautentisering och all specialåtkomst granskas och behandlas av vårt säkerhetsteam. Åtkomsten till företags- och produktionsnätverk är strikt begränsad baserat på fastställda policyer. Åtkomsten till produktionsnätverk är exempelvis baserad på SSH-nycklar och är begränsad till teknikteam som måste ha åtkomst för att kunna utföra sina arbetsuppgifter. Brandväggsconfiguration sker under rigorös kontroll och är begränsad till ett fåtal administratörer.

Våra interna policyer kräver dessutom att medarbetare som använder produktions- och företagsmiljöer följer bästa praxis för skapande och lagring av privata SSH-nycklar. Åtkomst till andra resurser, inklusive datacenter, funktioner för serverkonfiguration, produktionsserverar och funktioner för utveckling av källkod tilldelas genom uttryckligt godkännande från lämplig chef. En kopia av av åtkomstförfrågan, motivering och godkännande registreras av ledningen och åtkomsten beviljas av lämpliga personer.

Dropbox använder tekniska åtkomstkontroller och interna policyer för att hindra medarbetare från att godtyckligt komma åt användares filer och för att begränsa åtkomsten till metadata och andra uppgifter om användarnas konton. För att skydda slutanvändarnas sekretess och säkerhet har endast ett mindre antal tekniker, som är ansvariga för att utveckla Dropbox kärntjänster, åtkomst till miljön där användarnas filer lagras. Medarbetaråtkomst återkallas omedelbart när en medarbetare lämnar företaget.

I takt med att Dropbox produkter och tjänster blir en förlängning av våra kunders infrastruktur kan de lita på att vi förvaltar deras data på ett ansvarsfullt sätt. Se [sekretessavsnittet](#) för mer information.

## Säkerhetsutbildning och ökad medvetenhet

Vi ger våra programvaruutvecklingsteam bästa praxis och teknik för att bygga säkra applikationer. I ett ständigt föränderligt digitalt landskap är det av yttersta vikt att säkerställa vår programvaras säkerhet, och vi har förbundit oss att utrusta våra team med de kunskaper och färdigheter som behövs för att skydda våra produkter och skydda våra användare.

## Företagskontor

- **Fysisk säkerhet**

Dropbox team för fysisk säkerhet bär ansvaret för att genomdriva den fysiska säkerhetspolicyn och att övervaka säkerheten på kontoret.

- **Besökar- och åtkomstpolicy**

Fysisk åtkomst till företagsanläggningar, utöver allmänna ingångar och receptioner, begränsas till behörig Dropbox-personal och registrerade besökare som åtföljs av Dropbox-personal. Ett system för åtkomst med ID-bricka säkerställer att endast behöriga individer har åtkomst till begränsade områden inom företagsanläggningarna.

- **Serveråtkomst**

Åtkomst till områden med företagsserverar (som serverrum) begränsas till behörig personal med rätt behörighetsnivå som ges via systemet med ID-brickor. Listan över behöriga personer som är godkända för fysisk åtkomst till företags- och produktionsmiljöer granskas minst en gång i kvartalet.

## Sårbarhetshantering

Vårt säkerhetsteam utför regelbundna automatiska och manuella säkerhetstester och hantering av korrigeringar, och samarbetar med tredjepartsexperter för att identifiera och åtgärda eventuella sårbarheter och buggar.

Som en nödvändig komponent i vårt system för hantering av informationssäkerhet rapporteras resultat och rekommendationer från alla dessa utvärderingar till Dropbox ledning, som utvärderar informationen och vidtar lämpliga åtgärder efter behov. Allvarliga ärenden dokumenteras, spåras och åtgärdas av tilldelade säkerhetstekniker.

## Fysisk säkerhet

### Infrastruktur

Fysisk åtkomst till underleverantörernas anläggningar för produktionssystem är begränsad till personal som auktoriserats av Dropbox för att kunna utföra sina arbetsuppgifter. Alla personer som behöver ytterligare åtkomst till produktionsanläggningar tilldelas detta endast efter uttryckligt godkännande från ansvarig ledning.

En kopia av åtkomstförfrågan, motivering och godkännande registreras av ledningen och åtkomsten beviljas av lämpliga personer. När godkännandet mottagits kontaktar infrastrukturteamets behöriga medlem den aktuella underleverantören för att begära åtkomst för den godkända individen. Underleverantören anger användarens uppgifter i sitt eget system och beviljar den godkända Dropbox-personalen åtkomst genom en ID-bricka och, om möjligt, biometrisk skanning. När de godkända individerna beviljats åtkomst är det datacentrets ansvar att se till att åtkomsten begränsas till endast dessa behöriga individer.

### Anmärkningar:

Dropbox för team, Dropbox Sign och Dropbox DocSend-tjänsterna använder Amazon Web Services för SaaS och IaaS, som driver toppmoderna funktioner som utvärderas av oberoende tredjepartsbedömningar (till exempel SOC 1, SOC 2, ISO 27001). Amazon utvärderar kontinuerligt potentiella risker och genomför regelbundna utvärderingar för att säkerställa efterlevnaden av branschstandarderna. Dessutom utvärderas PaaS genom Heroku, som erbjuder Dropbox DocSend, också oberoende bedömningar av tredjepartskontroller (till exempel SOC 1, SOC 2, ISO 27001).

Mer information om AWS efterlevnadsprogram finns [här](#).

## Incidenthantering

Vi har policyer och rutiner för incidenthantering som fastställer hur vi ska hantera problem med tillgänglighet, integritet, säkerhet, sekretess och konfidentialitet för tjänsten. Som del av våra incidenthanteringsprocedurer har vi särskilda team som är utbildade för att kunna:

- Reagera snabbt på varningar om potentiella incidenter.
- Fastställ incidentens allvarlighetsgrad.
- Vidta åtgärder för minimering och begränsning vid behov.
- Kommunicera med relevanta interna och externa intressenter, inklusive meddela drabbade kunder för att uppfylla kontraktsevenliga förpliktelser om brott eller incidenter och följa relevanta lagar och förordningar.
- Samla in och lagra bevis för utredningsarbete.
- Dokumentera en efterhandsutredning och ta fram en permanent prioriteringsplan.

Regler och processer för incidentrespons revideras inom ramarna för SOC 2, ISO/IEC 27001 och andra säkerhetsutvärderingar.

## Infrastruktursäkerhet

Dropbox använder specialtjänster och anpassade tjänster som drivs på Dropbox- och AWS-infrastruktur. AWS drivs med delat ansvar mellan Dropbox och AWS. Logisk säkerhet och nätverkssäkerhet i AWS-infrastruktur tillhandahålls av AWS.

**Obs:** För närvarande finns all AWS-infrastruktur som används för Dash i USA och är utspridd över flera tillgänglighetszoner. I takt med att produktutvecklingen för Dash går framåt och kundefterfrågan växer kan ytterligare världsomspännande regioner läggas till för att uppfylla kraven på datalagring.

### Nätverkssäkerhet

Dropbox upprätthåller omsorgsfullt säkerheten i våra backend-nätverk. Vår teknik för nätverkssäkerhet och övervakning är utformad för att ge ett skydd som består av flera lager. Vi använder skyddstekniker som utgör branschstandarder, inklusive brandväggar, genomsökning av nätverkets sårbarhet, övervakning av nätverkets säkerhet, system för intrångsavkänning för att se till att bara kvalificerad och icke-skadlig trafik kan nå vår infrastruktur.

Vårt interna privata nätverk delas upp efter användning och risknivå. De primära nätverken är följande:

- DMZ mot internet
- Prioritetsinfrastruktur-DMZ
- Produktionsnätverk
- Företagsnätverk
- Dropbox tjänster och applikationer isoleras via behållare när så är möjligt

Åtkomst till produktionsmiljöer är begränsad till enbart auktoriserade IP-adresser och kräver flerfaktorsautentisering på alla slutpunkter. IP-adresser med åtkomst associeras med företagsnätverket eller godkänd Dropbox-personal. Auktoriserade IP-adresser granskas kvartalsvis för att säkerställa en säker produktionsmiljö. Åtkomst till modifiering av listan med IP-adresser är begränsad till behöriga personer.

Trafik från internet som är riktad mot vårt produktionsnätverk skyddas av flera brandväggs- och proxyskikt.

Strikt begränsning upprätthålls mellan det interna Dropbox-nätverket och det offentliga internet. Internetbunden trafik till och från produktionsnätverket kontrolleras noggrant genom en dedikerad proxytjänst. Dessa skyddas i sin tur av restriktiva brandvägsregler.

Dropbox skapar sofistikerade verktygsuppsättningar för att övervaka bärbara och stationära datorer med Mac- och Windows-operativsystem och produktionssystem för skadliga händelser. Alla säkerhetsloggar samlas på en central plats för juridisk respons och incidenthantering enligt den lagringspolicy som är branschstandard.

Dropbox identifierar och minskar risker via regelbunden testning och granskning av nätverkssäkerhet av både dedikerade interna säkerhetsteam och säkerhetsspecialister från tredje part.

## Närvaropunkter (PoP)

I syfte att optimera webbplatsprestanda för användare utnyttjar Dropbox tredjepartsnätverk för innehållsleverans (CDN:er) och närvaropunkter (PoP:er) som Dropbox är värd för på 31 platser runtom i världen. Inga användardata cachas på dessa platser och alla användardata som överförs krypteras med SSL/TLS. Fysisk och logisk åtkomst till PoP:er som Dropbox är värd för är begränsad till behörig Dropbox-personal. Dropbox utför optimeringar av både transportlagret (TCP) och applikationslagret (HTTP).

## Peering

Dropbox har en öppen peeringpolicy och samtliga kunder är välkomna att skapa peerförbindelser med oss. Mer information finns här: [dropbox.com/peering](https://dropbox.com/peering).

## Säkerhetsövervakning

Dropbox använder molnbaserade säkerhetsplattformar för att övervaka säkerheten i produktionsmiljön och övervakar aktivt om misstänkt användaraktivitet förekommer. Detta inkluderar direkteskalering av varningar för Dropbox Security.

## Tillförlitlighet

När du gör affärer behöver vi finnas där för dig. Därför strävar vi efter att uppnå högsta möjliga drifttid. Vi utvecklar Dropbox produkter och tjänster med flera lager av redundans för att skydda mot dataförluster och säkerställa tillgänglighet.

## Datacenter och funktionstjänstleverantörer

Dropbox företags- och produktionssystem förvaras i tredjepartsleverantörers datacenter och hos leverantörer av hanterade tjänster i olika regioner i USA. Alla SOC-rapporter gällande underleverantörernas datacenter och/eller avtalsvillkor och säkerhetsfrågeformulär till underleverantörer granskas minst en gång om året för att säkerställa tillräckliga säkerhetskontroller. Tjänstleverantörerna från tredje part är ansvariga för de fysiska, miljömässiga och operativa säkerhetskontrollerna inom ramen för Dropbox infrastruktur. Dropbox bär ansvaret för säkerheten rörande logik, nätverk och applikationer i den del av vår infrastruktur som förvaras hos tredjepartsdatacenter.

Vår leverantör som tillhandahåller tjänster för bearbetning och lagring, Amazon Web Services (AWS), ansvarar för den logiska säkerheten och nätverkssäkerheten som tillhandahålls genom deras infrastruktur. Anslutningarna skyddas genom deras brandvägg, som är konfigurerad att blockera allt. Dropbox begränsar åtkomst till miljön till ett begränsat antal IP-adresser och medarbetare.

Dash funktioner för intelligent dataanalys och beslutsfattande drivs av den AWS Managed OpenSearch-plattformen som tillhandahåller en komplett hanterad SaaS-lösning med säkerhet som demonstrerats genom deras ISO-certifierings- och SOC-bekräftelserapporter.

### Infrastruktur i EU, Australien, Japan och Storbritannien

Dropbox erbjuder lagring av filblock i regioner utanför USA för kvalificerade kunder.

Vår lagringsinfrastruktur i EU drivs av Dropbox och omfattas av samma kontroller och bestämmelser som beskrivits ovan för vår USA-baserade infrastruktur. Vår infrastruktur drivs av Amazon Web Services (AWS) i Australien, Japan och Storbritannien, och den replikeras inom respektive region för att säkerställa redundans och skydda mot dataförlust.

Metadata om filer lagras på servrar som ägs av Dropbox. Paper-dokument och förhandsvisningar lagras för närvarande i USA för alla kunder.

**Obs:** För närvarande finns all AWS-infrastruktur som används för Dash i USA och är utspridd över flera tillgänglighetszoner.

## Verksamhetens kontinuitet

Dropbox har infört ett system för att hantera verksamhetens kontinuitet (BCMS) som anger hur vi återupptar eller upprätthåller tjänsterna till användare – samt hur vi bedriver vår verksamhet som ett företag – om det sker ett avbrott i affärskritiska processer och aktiviteter. Vi bedriver en cyklisk process som utgörs av följande faser:

- **Affärskonsekvens- och riskbedömningar**

Vi gör en bedömning av konsekvenser för verksamheten (BIA) minst en gång om året för att identifiera processer som är avgörande för Dropbox, bedöma den potentiella effekten av avbrott, fastställa prioriterade tidsramar för återställning samt identifiera våra kritiska beroenden och leverantörer. Vi utför också en riskbedömning som rör hela företaget minst en gång om året. Riskbedömningen hjälper oss att systematiskt identifiera, analysera och utvärdera risken för incidenter som leder till avbrott för Dropbox. Riskbedömningen och BIA tillsammans ger oss uppslag för kontinuitetsprioriteringar samt strategier för riskminimering och återställning av planer för verksamhetens kontinuitet (BCP:er).

- **Planer för affärskontinuitet**

Team som har identifierats som kritiska för Dropbox kontinuitet av BIA använder denna information för att utveckla BCP:er för sina kritiska processer. Dessa planer bidrar till teamets kännedom om vem som ansvarar för att återuppta processerna i en nödsituation, vem från ett annat Dropbox-kontor eller en annan plats som kan ta över deras processer under ett avbrott och vilka kommunikationsmetoder som ska användas vid en kontinuitetshändelse. Dessa planer hjälper oss även att förbereda oss för ett avbrott genom att centralisera våra återställningsplaner och annan viktig information, som när och hur planen ska användas, kontakt- och mötesuppgifter, viktiga appar och återställningsstrategier. Dropbox kontinuitetsplaner utgör en del av vår företagsomfattande krishanteringsplan (CMP), som fastställer Dropbox team för kris- och incidenthantering.

- **Plantester/övning**

Dropbox testar utvalda delar av sina planer för verksamhetens kontinuitet minst en gång om året. Testen överensstämmer med omfattningen och målen för BCMS, grundas på lämpliga scenarier och utformas med tydliga syften. Testerna kan omfatta både bordsdiskussioner och fullskaliga simulationer av verkliga incidenter. Teamen uppdaterar och förbättrar sina planer för att hantera problem och stärka insatskapaciteten baserat på resultaten från testerna samt erfarenhet från verkliga incidenter.

- **Granskning och godkännande av BCMS**

Minst en gång om året granskar vår ledning BCMS som en del av granskningen av Dropbox förtroendeprogram.

## **Katastrofåterställning**

Företaget är medvetet om att katastrofer kan inträffa när som helst, i vilken region eller på vilken plats som helst. Infrastrukturen är utformad för motståndskraft och beredskapsplaner finns implementerade för händelser som påverkar tjänsten. Vi använder Amazon Web Services (AWS), som är utspridda över flera olika datacenter för redundans för data och bearbetning. Viktiga data relaterade till systemet säkerhetskopieras dagligen. Våra tekniker meddelas vid säkerhetskopieringsfel och problem löses vid behov.

Vi har en katastrofåterställningsplan för att hantera kraven på informationssäkerhet under större kriser eller katastrofer som påverkar driften av Dropbox för team. Dropbox teknikerteam granskar planen varje år och testar utvalda delar minst en gång om året. Relevanta upptäckter dokumenteras och spåras tills problemet har lösts.

Vår katastrofplan (DRP) behandlar både katastrofer inom hållbarhet och tillgänglighet, vilka definieras enligt följande:

- En hållbarhetskatastrof består av en eller flera av följande faktorer:
  - En fullständig eller permanent förlust av ett huvudsakligt datacenter som lagrar metadata, eller av flera datacenter som lagrar filblock.
  - Förlorad förmåga att kommunicera eller serva data från ett datacenter som lagrar metadata, eller från flera datacenter som lagrar filinnehåll.
- En tillgänglighetskatastrof består av en eller flera av följande händelser:
  - Ett driftstopp på mer än 10 dagar.
  - Förlorad förmåga att kommunicera eller serva data från en lagringstjänst/ett datacenter som lagrar metadata, eller från flera lagringstjänster/datacenter som lagrar filblock.

Vi definierar ett mål för återställningstid (RTO), som den tidslängd och servicenivå som affärsprocessen eller tjänsten måste återställas på efter en katastrof, och ett mål för återställningspunkt (RPO) som är den längsta tolererbara period som data kan förloras efter ett serviceavbrott. Vi mäter också verklig återställningstid (RTA) under testning av katastrofåterställning, vilket utförs minst årligen.

Dropbox planer för incidenthantering, verksamhetens kontinuitet och katastrofåterställning kan testas vid planerade intervaller och vid betydande organisationsmässiga eller miljömässiga förändringar.

## Applikationssäkerhet

### Skanning och testning av säkerhetspenetrering (intern och extern)

Vårt säkerhetsteam utför regelbundna automatiserade och manuella säkerhetstester av applikationer för att identifiera och åtgärda potentiella sårbarheter och buggar i våra applikationer för dator, webben och mobiler.

Alla Dropbox-applikationer är helt integrerade med Dropbox säkerhetsprogram. Vi utför design- och arkitekturgranskningar av nya funktioner genom vår intagsprocess. All Dropbox-kod skannas med avseende på säkerhetsrelaterade problem med verktyg för statisk kodanalys som Semgrep och CodeScan.

Dessutom har Dropbox kontrakt med tredjepartssäljare för att utföra periodvisa intrångs- och sårbarhetstester i produktionsmiljön. Vi samarbetar även med externa säkerhetsspecialister, andra säkerhetsteam i branschen samt säkerhetsforskare för att se till att våra applikationer förblir säkra. Vi använder också automatiska analysystem för att identifiera sårbarheter. Detta inkluderar system som vi utvecklar internt, system med öppen källkod som vi modifierar efter våra behov och externa leverantörer som vi anlitar för kontinuerliga, automatiserade analyser.

## Hålla skadligt material borta från Dropbox

Vi har skanningsfunktioner som syftar till att förhindra att skadligt material lagras och distribueras i Dropbox. Våra skannrar utnyttjar vår egenutvecklade teknik samt avancerade funktioner från partnerföretag som Microsoft och Google för att göra Dropbox till en säker plats för våra kunder.

## Buggpremier

Även om vi arbetar med professionella företag för testningsarbete gällande intrång och utför testning internt, ger buggpremier (eller belöningsprogram för sårbarheter) tillgång till expertisen hos den bredare säkerhetsgruppen. Vårt buggpremieprogram ger ett incitament för utredare att på ett ansvarsfullt sätt identifiera och avslöja programvarubuggar. Denna användning av den externa gruppen ger vårt säkerhetsteam fristående granskning av våra applikationer som hjälper oss att hålla användarna säkra. Vi strävar efter att vara en branschledare i buggpremiearbetet, även vad gäller svars- och åtgärdstider.

Vi har etablerat en omfattning för kvalificerande överföringar och Dropbox-applikationer, samt en policy för ansvarsfullt avslöjande som gynnar upptäckten och rapporteringen av säkerhetssårbarheter och ökar användares säkerhet. Den här policyn fastställer följande riktlinjer:

- Berätta för oss i detalj om säkerhetsproblemet.
- Respektera våra befintliga applikationer. Att masskicka formulär genom automatiska sårbarhetsskannrar leder inte till någon bonus eftersom de uttryckligen är uteslutna.
- Ge oss rimlig tid att svara innan du offentliggör någon information om säkerhetsproblemet.
- Försök inte komma åt eller modifiera användardata utan kontoägarens tillstånd.
- Du bör inte visa, ändra, spara, lagra, överföra eller på annat sätt komma åt informationen, och omedelbart rensa all lokal information när du rapporterar sårbarheten till Dropbox
- Handla i god tro så att du undviker sekretessöverträdelser, förstörelse av data eller avbrott eller försämringar av våra tjänster (inklusive funktionsförlust, även kallat "denial of service")

Problem rapporteras genom att skicka en rapport till Intigriti på:

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

## Dataskydd och kryptering

### Dataöverföring/dataöverföringar

Dropbox använder Transport Layer Security (TLS) vid överföring av data för att skydda data som skickas mellan Dropbox-appar och våra servrar. Detta skapar en säker tunnel som skyddas av Advanced Encryption Standard-kryptering (AES) om 128 bitar eller högre. Fildata som skickas mellan en Dropbox för team-klient (för närvarande dator, mobil, API eller webb) och värdtjänsten är krypterade via SSL/TLS. För Dash-klienten och moderna webbläsare använder vi starka chiffer och på webben flaggar vi alla autentiseringskakor som säkra och aktiverar HTTP Strict Transport

Security (HSTS) med inklusive underdomäner aktiverade. På liknande vis krypteras Paper-dokumentdata som skickas mellan en Paper-klient (för närvarande API eller webb) och värdtjänsten alltid via SSL/TLS.

I Dropbox Sign och DocSend lagras dokument bakom en brandvägg och autentiseras mot avsändarens session varje gång en begäran om det aktuella dokumentet görs. Dessutom krypteras varje dokument med en unik nyckel. Som ytterligare säkerhetsåtgärd krypteras varje nyckel med en regelbundet utbytt masternyckel. Detta innebär att även om någon skulle ta sig förbi det fysiska skyddet och ta bort en hårddisk skulle personen inte kunna komma åt dina data.

För slutpunkter som vi kontrollerar (klient och mobil) samt moderna webbläsare använder vi starka chiffer och stödjer perfect forward secrecy och certificate pinning. Vi flaggar dessutom alla autentiseringscookies på webben som säkra och aktiverar HTTP Strict Transport Security (HSTS) med includeSubDomains aktiverat.

**Obs!** Dropbox använder endast TLS och har upphört med användningen av SSLv3 på grund av kända sårbarheter. TLS kallas dock ofta "SSL/TLS", så vi använder den beteckningen här.

För att förhindra mellanhandsattacker verifieras Dropbox front-end-servrar via publika certifikat hos klienten. Innan några filer eller Paper-dokument förs över förhandlas en krypterad anslutning, vilket säkerställer en säker leverans till Dropbox front-end-servrar.

### **Vilande data**

Dropbox-filer som laddas upp av användare krypterade i vila med 256-bitars Advanced Encryption Standard (AES) Filer lagras i flera datacenter i diskreta filblock. Varje block är fragmenterat och krypterat med ett starkt chiffer. Endast block som modifierats mellan revideringar synkas. Paper-dokument i vila krypteras också med 256-bitars Advanced Encryption Standard (AES). Paper-dokument lagras över flera tillgänglighetszoner med tredjepartssystem.

### **Nyckelhantering**

Dropbox infrastruktur för nyckelhantering är utformad med säkerhetskontroller för drift, teknik och rutiner, med mycket begränsad åtkomst till nycklar. Generering, utbyte och lagring av krypteringsnycklar distribueras för decentraliserad bearbetning. Nyckelhanteringstjänster är utformade med säkerhetskontroller för drift, teknik och rutiner.

- **Filkrypteringsnycklar**

Dropbox är utformat för att hantera användarnas filkrypteringsnycklar så att tjänsten blir mer lättanvänd, samt för att aktivera avancerade produktfunktioner och stark kryptografisk kontroll. Filkrypteringsnycklar skapas, lagras och skyddas av produktionssystemets säkerhetskontroller för infrastrukturen och säkerhetspolicyer.

- **Interna SSH-nycklar**

Åtkomst till produktionssystemen begränsas med hjälp av unika SSH-nyckelpar. Säkerhetspolicyer och -rutiner behöver skyddas av SSH-nycklar. Ett internt system hanterar det säkra utbytet av offentliga nycklar och privata nycklar lagras på ett säkert sätt. Interna SSH-nycklar kan inte användas för åtkomst till produktionssystem utan en separat tvåfaktorautentisering.

- **Nyckeldistribution**

Dropbox automatiserar hanteringen och distributionen av känsliga nycklar till enbart de system som krävs för drift.

## Certificate pinning

Dropbox använder certificate pinning på våra dator klienter och mobila klienter. Certificate pinning innebär en extra kontroll för att säkerställa att våra klienter endast ansluter till servrar med digitala certifikat från en auktoriserad lista över certifikatutfärdare. Vi använder det för att skydda oss mot nationalstatliga angripare som kontrollerar en oseriös certifikatutfärdare, samt för att skydda dig mot lokala sabotageprogram som kan kapa dina anslutningar.

## Skydd av autentiseringsdata

Dropbox använder mer än bara vanlig hashning för att skydda användares inloggningsuppgifter. I enlighet med bästa praxis för branschen används en slumpmässigt genererad och användarunik saltsträng för varje lösenord och vi använder iterativ hashning för att bromsa beräkningen. Dessa förfaranden bidrar till att skydda mot nyckelsöknings-, ordliste- och regnbågsattacker. Som en extra försiktighetsåtgärd krypterar vi hashvärdena med en nyckel som lagras avskilt från databasen, vilket bidrar till att hålla lösenord säkra vid en kompromettering som endast rör databasen.

## Skanning efter sabotageprogram

Vi har utvecklat ett automatiserat system som söker efter skadlig programvara vid den punkt då innehåll delas utanför den ursprungliga användarens konto. Systemet använder både intern teknik och detektionsmotorer av branschstandard, och är utformat för att förhindra att skadlig programvara sprids.

# Produktsäkerhet

## Designgranskningar

Säkerhetsteamet på Dropbox integrerar säkerhetsgranskning i produktens färdplan, så varje större version har genomgått hotmodeller och designgranskningar för att kunna leverera en säker upplevelse för våra användare.

## Säker driftsättning

Som en del av vår livscykel för programvaruutveckling, analyseras och skannas koden först när nya Dropbox-applikationsfunktioner läggs till i vår kodbas med avseende på kodkvalitet och säkerhetsbrist. Funktioner måste godkännas i denna granskningsprocess, inklusive expertutvärdering, innan de anses klara att släppas.

## Förändringshantering

Alla processer för utveckling, åtgärdande av problem och rättelser följer vår formella policy för förändringshantering som har utarbetats av Dropbox teknikteam i syfte att säkerställa att systemändringar har testats och auktoriserats innan de implementeras i produktionsmiljöerna. Källkodsändringar initieras av utvecklare som vill förbättra Dropbox-appen eller Dropbox-tjänsten. Alla ändringar lagras i ett versionskontrollsystem och måste genomgå en automatiserad kvalitetskontroll (Quality Assurance, QA) för att verifiera att säkerhetskraven uppfylls. När QA-testen har godkänts implementeras ändringen. QA-godkända ändringar implementeras automatiskt i produktionsmiljön. Vår livscykel för programvaruutveckling (SDLC) kräver att riktlinjerna för säker kodning efterlevs. Man måste även söka efter kodändringar för att hitta potentiella säkerhetsproblem via våra processer för QA och manuell granskning. Ändringar som släpps till produktion loggas och arkiveras, och varningar skickas automatiskt till Dropbox teknikteam.

Ändringar i Dropbox infrastruktur kan endast utföras av behörig personal. Dropbox säkerhetsteam ansvarar för att upprätthålla infrastrukturens säkerhet och säkerställa att servrar, brandväggar och andra säkerhetsrelaterade konfigurationer alltid lever upp till aktuell branschstandard. Vi utför regelbundna granskningar av brandväggsregler och personer med åtkomst till produktionsserverar.

## Dataskydd

Individer och organisationer anförtror Dropbox med sitt viktigaste arbete och det är vårt ansvar att skydda det. På Dropbox anser vi att du äger dina data, och vi har förbundit oss att hålla dem privata. Vår [integritetspolicy](#) beskriver tydligt hur vi hanterar och skyddar din information. Våra tredjepartsrevisorer testar våra integritetsrelaterade kontroller på årsbasis och tillhandahåller rapporter och utlåtanden som vi kan vidarebefordra till er på begäran. Mer information om våra integritetspraxis och principer finns i [vitboken om integritet och dataskydd](#).

För att rapportera ett integritetsrelaterat problem kontaktar du: [privacy@dropbox.com](mailto:privacy@dropbox.com).

# Dropbox Business

Digitala omvandlingar fortsätter att slå igenom i flera olika branscher och det är viktigt att data, team och enheter skyddas var de än befinner sig. Organisationer som förlitar sig på molnlösningar som Dropbox Business för att möjliggöra distansbaserade och distribuerade arbetsflöden måste effektivisera samarbete, hantera molnrisker proaktivt och implementera effektiva kontroller som säkerställer konfidentialiteten för deras immateriella egendom (IP), integritet för lagrade och delade data, tillgänglighet för data genom hanterade och robusta molntjänster.

Över 575 000 företag och organisationer förlitar sig på Dropbox för team som lösning för att distansteam ska kunna samarbeta på ett säkert sätt. Den centrala Dropbox för team-lösningen innehåller en smart arbetsyta för samarbete, samt filsynknings- och delningsfunktioner. Våra lösningar understöds av branschledande infrastruktur samt funktioner för avancerad företags säkerhet, team- och innehållssäkerhet, elektroniska signaturer, säker överföring och datastyrning. Om inget annat anges gäller informationen i detta faktablad för alla Dropbox för team-produkter. Paper är en funktion i Dropbox för team.

Kärnan för Dropbox för team är vårt omfattande säkerhetsprogram, Dropbox-förtroendeprogrammet, som har en flerskiktstrategi för säkerhet som är avgörande när globala metoder för distansarbete utvecklas.

Den här vitboken beskriver produktsäkerhetsfunktioner i Dropbox för team, Dropbox operativa säkerhetsåtgärder, vårt integritets- och transparensåtagande samt backend-policyer, oberoende certifieringar och åtgärder för regelefterlevnad som gör Dropbox till den säkra lösningen för din organisation.

**Obs:** Om inget anges gäller informationen i detta faktablad för alla Dropbox för team. Paper är en funktion i Dropbox för team.

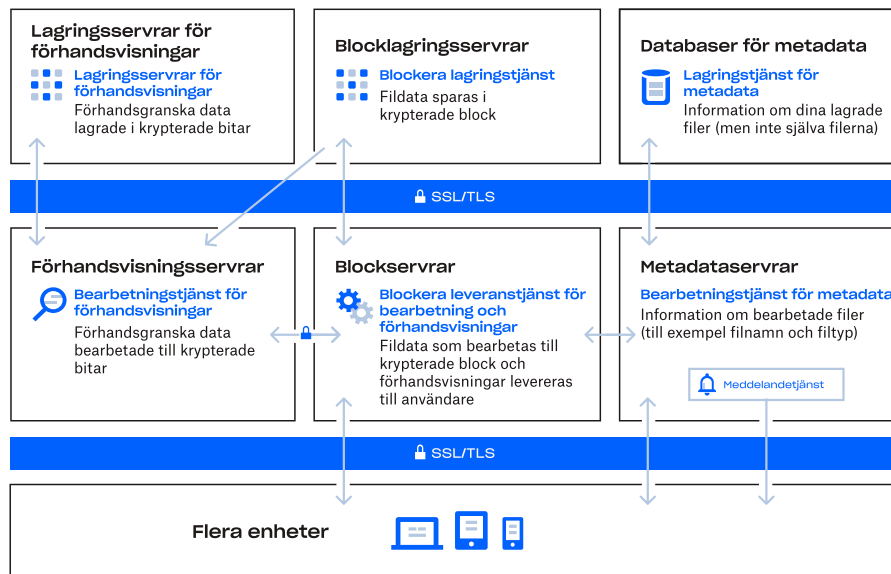
## Under skalet

Våra lättanvända gränssnitt stöds av en infrastruktur i bakgrunden som garanterar snabb, pålitlig synkning och delning och ett smidigt samarbete. Vi förbättrar ständigt vår produkt och arkitektur för att skapa snabbare dataöverföring, öka tillförlitligheten och anpassa oss efter förändringar i miljön. I detta avsnitt förklarar vi hur data överförs, lagras och bearbetas på ett säkert sätt.

## Filinfrastuktur

Dropbox-användare kan komma åt filer och mappar när som helst från datorn, webben och mobila klienter, eller genom tredjepartsappar som är kopplade till Dropbox. Alla dessa klienter ansluter till säkra servrar för att ge åtkomst till filer, möjliggöra fildelning med andra och uppdatera kopplade enheter när filer läggs till, ändras eller raderas.

Dropbox-filinfrastrukturen består av följande komponenter:



- **Metadataserver**

Vissa grunduppgifter om användardata, så kallade metadata, lagras i dess egna diskreta lagringstjänst och fungerar som ett index för uppgifterna i användarnas konton. Metadata inkluderar grundläggande konto- och användarinformation som mejladress, namn och enhetsnamn. Metadata innefattar också basinformation om filer, inklusive filnamn och typ, vilket underlättar supportfunktioner som versionshistorik, återställning och synkronisering.

- **Databaser för metadata**

Filmetadata lagras i en värdelagring för transaktionsnycklar med samtidighetskontroll i flera versioner och delas och replikeras efter behov för att uppfylla krav på prestanda och hög tillgänglighet.

- **Blockserver**

Dropbox erbjuder en unik säkerhetsmekanism som överträffar traditionell kryptering för att skydda användardata. Blockserver bearbetar filer från Dropbox-applikationerna genom att dela upp dem i block som krypteras med ett starkt chiffer. Endast block som har modifierats sedan den senaste versionen synkas. En Dropbox-applikation meddelar blockserverna att en ändring genomförts när den upptäcker en ny fil eller ändringar i en befintlig fil. De nya eller modifierade filblocken bearbetas och överförs till blocklagringsserverna. Blockserverna används dessutom för att leverera filer och förhandsvisningar till användaren. Mer information om den kryptering som dessa tjänster använder, både vid överföring och lagring, finns i avsnittet [Kryptering](#).

- **Blocklagringsserver**

Det faktiska innehållet i användarnas filer lagras i krypterade block på blocklagringsserverna. Dropbox-klienten delar upp filerna i filblock innan överföringen för att förbereda dem inför lagringen. Lagringsserverna fungerar som ett Content-Addressable Storage-system (CAS), där varje enskilt filblock tas emot baserat på dess hashvärde.

- **Förhandsvisningsserver**

Förhandsvisningsserverna ger förhandsvisningar av filer. Förhandsvisningar är en framställning av en användares fil i ett annat filformat som är mer lämpat för att snabbt visas på en slutanvändares skärm. Förhandsvisningsserver hämtar filblock från blocklagringsserverna för att generera förhandsvisningar. När en förhandsvisning av en fil begärs hämtar förhandsvisningsserverna den cachelagrade förhandsvisningen från förhandsvisningsserverna och överför den till blockserverna. I slutändan levereras förhandsvisningarna till användare via blockserverna.

- **Lagringsserver för förhandsvisningar**

Cachelagrade förhandsvisningar lagras i ett krypterat format på lagringsserverna för förhandsvisningar.

- **Meddelandetjänst**

Denna separata tjänst övervakar om några ändringar har utförts i Dropbox-konton. Inga filer eller metadata lagras eller överförs. Varje klient skapar en long poll-anslutning till meddelandetjänsten och avvaktar. När en fil i Dropbox modifieras, signalerar meddelandetjänsten detta till de relevanta klienterna genom att stänga long poll-anslutningen. När anslutningen stängs, signalerar detta att klienten måste ansluta till metadatatjänsten på ett säkert sätt för att synkronisera eventuella ändringar.

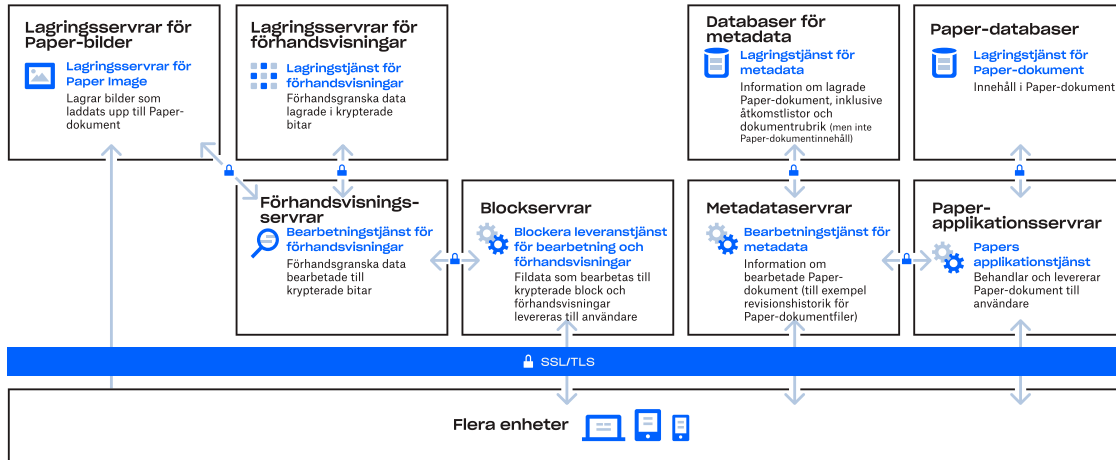
## Fildatalagring

Dropbox lagrar huvudsakligen två slags metadata: metadata om filer (till exempel datum och tid för den senaste filändringen) och det faktiska filinnehållet (filblock). Metadata om filerna lagras på Dropbox serverar. Filblock lagras i ett av två system: Amazon Web Services (AWS) eller Magic Pocket, Dropbox interna lagringssystem. Magic Pocket består av tillverkarspecifik program- och maskinvara och har designats från grunden för att vara tillförlitligt och säkert. I både Magic Pocket och AWS krypteras filblock när de är inaktiva, och båda systemen uppfyller höga krav på tillförlitlighet. Mer information finns i avsnittet [Tillförlitlighet](#).

## Paper-infrastruktur

Dropbox-användare kan komma åt Paper-dokument och mappar när som helst från webben eller genom tredjepartsappar som är kopplade till Dropbox Paper-appen. Alla dessa klienter ansluter till säkra serverar för att ge åtkomst till Paper-dokument, möjliggör dokumentdelning med andra och uppdaterar anslutna enheter när filer läggs till, ändras eller tas bort.

Dropbox Paper-infrastrukturen består av följande komponenter:



- **Papers programservrar**

Paper-applikationsservrar behandlar användarbegäranden, renderar redigerade Paper-dokument tillbaka till användaren och hanterar aviseringstjänster. Paper-applikationsservrar skriver inkommande användarredigeringar till Paper-databaser där de lagras permanent. Kommunikationssessioner mellan Paper-applikationsservrar och Paper-databaser säkras med Transport Layer Security (TLS).

- **Paper-databaser**

Det faktiska innehållet i användarnas Paper-dokument, samt vissa metadata om dessa Paper-dokument, lagras permanent i Paper-databaser. Detta omfattar informationen om Paper-dokumentet (som titel, ägare, skapelsetid och annan information) samt innehållet i själva Paper-dokumentet, inklusive kommentarer och uppgifter. Paper-databaser shardas och replikeras efter behov för att uppfylla höga krav på prestanda och tillgänglighet.

- **Metadataservrar**

Paper använder samma metadata-servrar som beskrivs i Dropbox-infrastrukturdiagrammet för att hantera information om Paper-dokument, till exempel filrevisionshistorik för Paper-dokument och delat mappmedlemskap. Dropbox hanterar metadata-servrarna direkt. Servrarna är placerade i datacenter som drivs av tredje part.

- **Databaser för metadata**

Paper använder samma metadata-servrar som beskrivs i Dropbox-infrastrukturdiagrammet för att lagra information om Paper-dokument, t.ex. delning, behörigheter och mappassociationer. Alla metadata för Paper-dokument lagras i en databastjänst med MySQL-stöd, samt delas och replikeras efter behov för att leva upp till våra krav på prestanda och hög tillgänglighet.

- **Lagringsservrar för Paper-bilder**

Bilder som laddas upp till Paper-dokument lagras och krypteras i vila på lagringsservrar för Paper-bilder. Överföringen av bilddata mellan Paper-applikationen och Paper-bildservrar sker över en krypterad session.

- **Förhandsvisningsservrar**

Förhandsvisningsservrar levererar förhandsvisningar av både bilder som laddats upp till Paper-dokument och hyperlänkar som bäddats in i Paper-dokument. För bilder som laddats upp i Paper-dokumentet hämtar förhandsvisningsservrarna bilddata som lagrats i lagringsservrarna för Paper-bilder via en krypterad kanal. För hyperlänkar som bäddats in i Paper-dokument hämtar förhandsvisningsservrarna bilddata och renderar en förhandsvisning av bilden med användning av kryptering i enlighet med källänkens specifikationer. I slutändan levereras förhandsvisningarna till användare via blockservrarna.

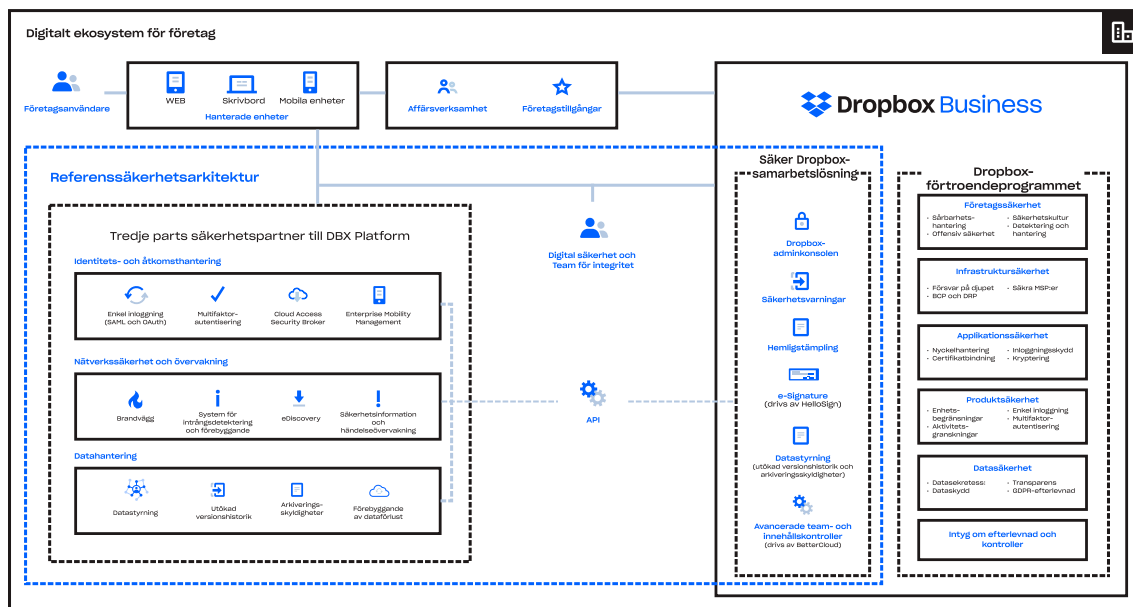
- **Lagringsservrar för förhandsvisningar**

Paper använder sig av samma förhandsvisningsservrar som beskrivs i infrastrukturdiagrammet för Dropbox för att lagra cachelagrade förhandsvisningar av bilder. Cachelagrade förhandsvisningar lagras i ett krypterat format på lagringsservrarna för förhandsvisningar.

## Paper-dokumentlagring

Dropbox lagrar huvudsakligen följande datatyper i Paper-dokument: metadata om Paper-dokument (som ett dokumentets delade tillstånd) och det faktiska innehållet i Paper-dokumentet som laddats upp av användaren. Dessa data benämns gemensamt som Paper-dokumentdata, och bilder som laddats upp till Paper-dokument benämns Paper-bilddata. Var och en av dessa datatyper lagras i Amazon Web Services (AWS). Paper-dokument är krypterade i vila AWS, och AWS uppfyller kraven i stränga standarder med avseende på tillförlitlighet. Mer information finns i avsnittet [Tillförlitlighet](#).

Vi följer en flerskiktsstrategi för att säkra företag, infrastruktur, applikationer och produkter som påverkar din organisation.



# Tillförlitlighet

Ett lagringssystem är aldrig bättre än dess tillförlitlighet. Därför har vi gett Dropbox flera redundanta lager som skyddar mot dataförluster och säkerställer tillgänglighet.

## Filmetadata

Överblivna metadatakopior fördelas över oberoende enheter inom ett datacenter i en N+2-tillgänglighetsmodell (som minimum). Inkrementella säkerhetskopieringar utförs minst varje timme, och fullständiga säkerhetskopieringar utförs var 36:e timme. Metadata lagras på servrar som Dropbox driver och hanterar i USA.

## Filblock

Redundanta kopior av filblock lagras separat i minst två olika geografiska regioner och replikeras på ett säkert sätt i varje region. (Observera: För kunder som har sina filer lagrade i vår tyska, australiensiska, japanska eller brittiska infrastruktur, replikeras filblocken enbart inom sina respektive regioner. Mer information finns i avsnittet [Datacenter och funktionstjänstleverantörer](#) nedan.) Både Magic Pocket och AWS är utformade för att ge en årlig datahållbarhet på minst 99,999999999 %.

Dropbox arkitektur, applikationer och synkningsmekanismer bildar tillsammans ett skydd för användardata och gör dem lättillgängliga. I de sällsynta fall då en tjänst inte är tillgänglig kan Dropbox-användare fortfarande komma åt de senaste synkade kopiorna av filerna i den lokala Dropbox-mappen på anslutna datorer. Kopior av filer som synkroniserats i Dropbox-skrivbordsklienten/lokala mappen kan nås från din hårddisk under driftstörningar, strömavbrott eller när datorn är offline. Ändringar som görs i filer och mappar synkroniseras till Dropbox när tjänsten eller anslutningen har återställts.

## Paper-dokument

Redundanta kopior av Paper-dokumentdata fördelas över oberoende enheter i ett datacenter i en N+1-tillgänglighetsmodell. Fullständiga säkerhetskopieringar av Paper-dokumentdata genomförs också dagligen. För Paper-dokumentlagring använder Dropbox AWS-infrastruktur i USA som har utformats för att ge en årlig datahållbarhet på minst 99,999999999 %.

## Filsynkning

Dropbox erbjuder branschens bästa filsynkning. Våra synkmekanismer garanterar snabba, responsiva filöverföringar och möjliggör åtkomst till data oavsett plats och enhet. Dropbox-synkningen är dessutom mycket robust. Om anslutningen till Dropbox-tjänsten misslyckas återupptar en klient smidigt åtgärden när anslutningen återupprättas. Filer uppdateras endast på den lokala klienten om

de har synkats och validerats helt med Dropbox-tjänsten. Genom att sprida ut belastningen över flera servrar säkerställer vi redundans och konsekvent synkning för slutanvändaren.

### Delta-synkning

Med den här synkningsmetoden laddas bara ändrade delar av filer ner eller upp. Dropbox lagrar varje fil i diskreta, krypterade block och uppdaterar bara de block som har ändrats.

### Strömmande synkning

I stället för att vänta på att en filuppladdning ska slutföras börjar strömmande synkronisering att ladda ner synkade block till en annan enhet innan alla block har laddats upp helt från den första enheten. Detta tillämpas automatiskt när separata datorer är kopplade till samma Dropbox-konto eller när olika Dropbox-konton delar en mapp.

### Spara hårddiskutrymme

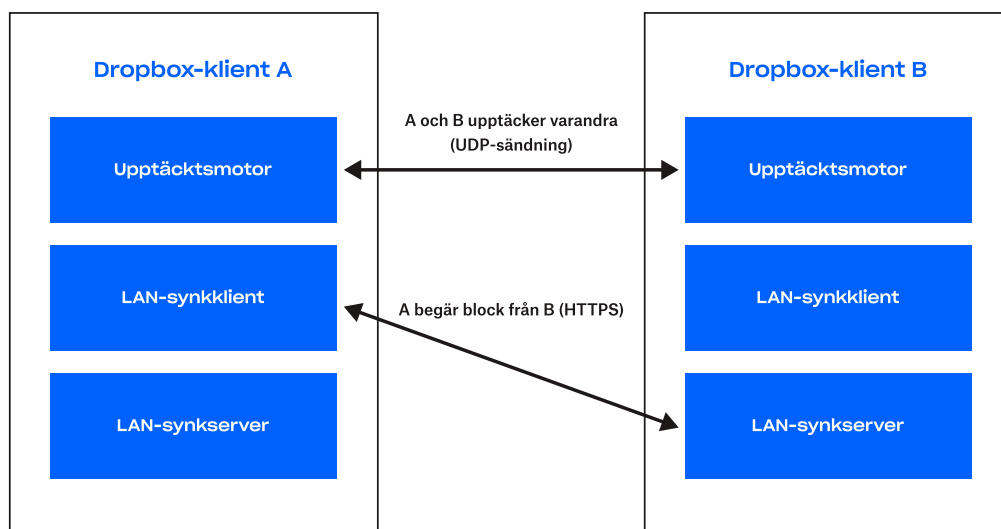
Användare kan frigöra lagringsutrymme på sina datorer genom att göra enbart de filer de vill ha på hårddisken tillgängliga offline. Det frigör datorutrymme genom att hålla allt annat enbart online på [dropbox.com](https://dropbox.com).

### LAN-synk

När denna funktion är aktiverad laddas nya och uppdaterade filer från andra datorer på samma LAN-nätverk ner, vilket sparar tid och bandbredd jämfört med att ladda ner filerna från Dropbox-servrarna.

### Arkitektur

Det LAN-synkssystem som körs i klienten består av tre huvudkomponenter: daemon, servern och klienten. Daemon hittar maskiner i nätverket att synkronisera med. Detta är begränsat till maskiner som har auktoriserad åtkomst till samma personliga eller delade Dropbox-mappar. Servern hanterar begäranden från andra maskiner i nätverket och serverar de begärda filblocken. Klienten begär filblock från nätverket.



## Upptäcktsmotor

Samtliga maskiner i LAN-systemet skickar och lyssnar periodvis efter UDP-sändningspaket över port 17500 (som reserverats för LAN-synk av IANA). Paketet innehåller protokollversionen som används av den datorn, de personliga och delade Dropbox-mapparna som stöds, den TCP-port som används för att köra servern (som kan vara en annan än 17500 om den porten inte är tillgänglig) och en slumpmässig identifierare för maskinen. När ett paket upptäcks läggs maskinen till i en lista för varje personlig och delad mapp, vilket indikerar ett potentiellt mål.

## Protokoll

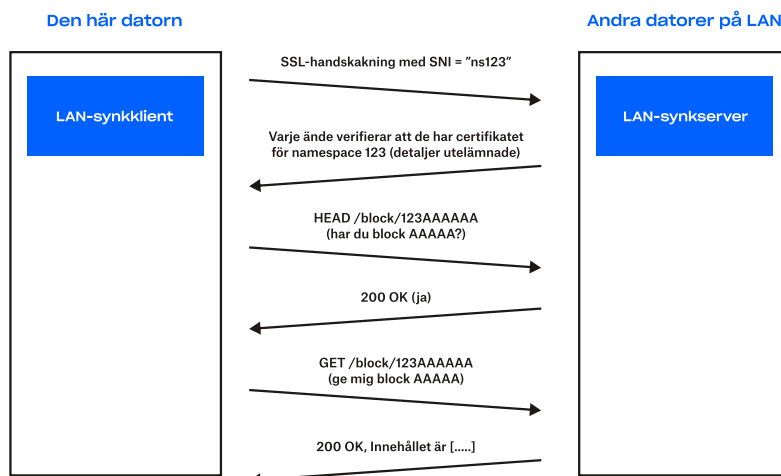
Den faktiska överföringen av filblock görs över HTTPS. Varje dator kör en HTTPS-server med slutpunkter. En klient avser flera peers för att se om de har blocken, men laddar endast ner blocken från en server.

I syfte att hålla dina data säkra ser vi till att endast klienter som är autentiserade för en viss mapp kan begära filblock. Vi ser också till att datorer inte kan utge sig för att vara servrar för mappar som de inte kontrollerar. För att lösa detta genererar vi SSL-nyckel-/certifikatpar för varje personlig Dropbox eller delad mapp. Dessa distribueras från Dropbox-serverar för de användardatorer som är auktoriserade för mappen. Nyckel-/certifikatparen roteras så fort medlemskapet ändras (till exempel när någon tas bort från en delad mapp). Vi kräver att båda ändarna av HTTPS-anslutningen autentiserar med samma certifikat (certifikatet för Dropbox-kontot eller den delade mappen). Detta bevisar att båda ändarna i anslutningen är auktoriserade.

När vi upprättar en anslutning meddelar vi servern vilken personlig Dropbox eller mapp som vi försöker ansluta till genom att använda SNI (Server Name Indication), så att servern vet vilket certifikat som ska användas.



Dropbox distribuerar cert/  
nyckelpar för namespace 123



## Server/klient

Med det protokoll som beskrivs ovan behöver servern bara veta vilka block som är relevanta och var de finns.

Klienten för en lista över peers för varje personlig Dropbox-mapp och delad mapp baserat på resultaten från daemon. När LAN-synksystemet får en begäran om att ladda ner ett filblock skickar det en begäran till ett slumpmässigt utvalt antal peers som den har upptäckt för den personliga Dropbox-mappen eller delade mappen och begär sedan blocket från den första som svarar att den har blocket.

Vi använder anslutningspooler som gör att vi kan återanvända redan upprättade anslutningar i syfte att undvika latens. Vi öppnar inte en anslutning innan den behövs. När den har öppnats håller vi den aktiv ifall vi behöver den på nytt. Vi begränsar också antalet anslutningar till en enskild peer.

Om ett filblock inte hittas eller kan laddas ner, eller om anslutningen visar sig vara långsam, förlitar sig systemet på Dropbox-servrarna för att hämta blocket.

# Dropbox användargränssnitt

Dropbox-tjänsten kan användas och nås via ett antal olika gränssnitt. Alla har säkerhetsinställningar och säkerhetsfunktioner som bearbetar och skyddar användardata och gör dem lätta att komma åt.

- **WEB**

Det här gränssnittet kan nås via alla moderna webbläsare. Användare kan ladda upp, ladda ner, visa och dela sina filer. Med webbgränssnittet kan användare också öppna befintliga lokala versioner av filer från sina datorers standardprogram.

- **Skrivbord**

Dropbox-klienten är en kraftfull synkroniseringsklient som sparar filer lokalt för åtkomst offline. Den ger användarna full åtkomst till sina Dropbox-konton och fungerar med operativsystemen Windows och Mac. Filer visas och kan delas direkt i operativsystemets filfästare.

- **Mobila enheter**

Dropbox-appen är tillgänglig för iOS- och Android-enheter så att användare har åtkomst till alla sina filer, var de än är. Med mobilappen kan användare också göra filer tillgängliga offline.

- **API**

Dropbox-API:erna är ett flexibelt sätt att läsa och skriva till Dropbox-användarkonton, och ger åtkomst till avancerade funktioner, som sökning, revidering och återställning av filer. API:erna kan användas för att hantera användarlivscykeln för ett Dropbox för team-konto, utföra åtgärder för alla medlemmar i ett team och aktivera åtkomst till adminfunktioner för Dropbox för team.

# Paper-användargränssnitt

Paper-tjänsten kan användas och nås via ett antal olika gränssnitt. Alla har säkerhetsinställningar och säkerhetsfunktioner som bearbetar och skyddar användardata och gör dem lätta att komma åt.

- **WEB**

Det här gränssnittet kan nås via alla moderna webbläsare. Det låter användarna skapa, visa redigera, ladda ner och dela sina Paper-dokument.

- **API**

Dropbox-API:n som beskrivs ovan innehåller slutpunkter och datatyper för hantering av dokument och mappar i Dropbox Paper, inklusive stöd för funktionalitet som åtkomsthantering, arkiv och permanent borttagning.

## Dropbox Replay

Dropbox Replay är ett verktyg för mediegranskning och godkännande som gör det möjligt för användare att markera, kommentera och slutföra video-, bild- och ljudfiler tillsammans. Den har stöd för feedback i realtid, enkel delning utan Dropbox-konton för andra användare och funktioner som livegranskning, jämförelse med versioner och avancerade kommentarer.

Replay har flera säkerhetsåtgärder för att skydda medieinnehåll och användardata. Lösningen kan integreras med Dropbox-adminkonsolen för åtkomstkontroll, delningsbegränsningar och användarhantering, inklusive granskningsloggar och funktioner för användarrensning. Replay utför också auktoriseringskontroller av sökresultat för att se till att användarna bara ser innehåll de har åtkomst till, och tillämpar indatavalidering och sanering för att förhindra säkerhetsrisker som Cross-Site Scripting (XSS). Dessutom har Replay stöd för säker hantering av filer, inklusive PDF-filer och PSD-filer, med försiktighetsåtgärder som minimerar JavaScript-baserade attacker.

## Appar för Dropbox

Dropbox-plattformen består av ett stabilt ekosystem med utvecklare som bygger på vårt flexibla applikationsprogrammeringsgränssnitt (API). Fler än 750 000 utvecklare har byggt applikationer och tjänster för produktivitet, samarbete, säkerhet, administration med mera.

## Förbyggda komponenter

Chooser, Saver och Embedder är färdiga webb- och mobilkomponenter som gör det lätt att komma åt Dropbox i tredjepartsappar och -webbplatser med bara några få rader kod.

- Med Chooser är det möjligt att välja filer från Dropbox.
- Saver låter användarna spara filer direkt i Dropbox.
- Embedder låter användarna visa filer och mappar från Dropbox.

Auktoriseringen för dessa komponenter görs helt via Dropbox. Appar beviljas åtkomst till filer valda genom delade länkar från Dropbox eller kortlivade nerladdningslänkar. Dessa färdiga komponenter kan användas oberoende eller i samband med API:t, som beskrivs nedan.

## API-integreringar för Dropbox för team

Det offentliga Dropbox API:t ger tredjepartsutvecklare möjlighet att komma åt och interagera med Dropbox från deras appar. Det omfattar interaktioner med filer och metadata, delning och teamfunktioner.

### Auktorisering

Dropbox använder OAuth, ett protokoll som är branschstandard för auktorisering, så att användarna kan ge appar olika typer av kontoåtkomst utan att avslöja sina kontouppgifter. Vi stöder OAuth 2.0 för auktorisering av API-förfrågningar. Förfrågningar verifieras genom Dropbox-webbplatsen eller mobilappen. Dropbox stöder OAuth bästa praxis, inklusive kortlivade åtkomsttokens och PKCE för distribuerade appar.

### Användarbehörigheter

Appar som använder Dropbox-API:t kan byggas med följande nivå av åtkomst till innehållet i slutanvändarens Dropbox:

- **Appmapp**  
En dedikerad mapp som döps efter appen skapas i appmappen för en användares Dropbox. Appen får endast läs- och skrivåtkomst till mappen i fråga och användare kan tillhandahålla innehåll för appen genom att flytta filer till mappen. Dessutom kan appen begära åtkomst till filer/mappar via Väljaren eller Spararen.
- **Hela Dropbox**  
Appen får full åtkomst till alla filer och mappar i en användares Dropbox och kan även begära åtkomst till filer/mappar via Chooser eller Saver.

Program kan också begära specifika omfattningar som begränsar deras beteenden genom åtkomst till undergrupper av API-slutpunkter. Till exempel kan programmen begränsas till skrivskyddad åtkomst till filer – eller möjligheten att ladda upp innehåll, men inte att skapa delningar.

## Teambehörigheter

Administratörer för Dropbox för team kan ge applikationer behörighet till administrationsfunktioner som finns i teamets adminkonsol. Vilka åtgärder teamets länkade appar kan utföra begränsas genom omfattningar som specificerar vilka teaminställningar appen kan läsa eller hantera. Vilka åtgärder teamets länkade appar kan utföra begränsas genom omfattningar, som anger vilka teaminställningar appen kan läsa eller hantera.

*Vanliga kombinationer av omfattningar inkluderar:*

- **Teaminformation**  
Skrivskyddad information om teamet och användning på hög nivå.
- **Teamgranskning**  
Skrivskyddad åtkomst till teaminfo och den detaljerade händelseloggen.
- **Filåtkomst för teammedlemmar**  
Möjligheten att utföra åtgärder för teamanvändares räkning, till exempel hantera deras filer och mappar.
- **Teammedlemshantering**  
Lägga till eller ta bort medlemmar till och från teamet.

## Webhooks

Webhooks är ett sätt för webbappar att skaffa sig realtidsmeddelanden om förändringar i en användares Dropbox. När en URI registrerats för att ta emot webhooks skickas en HTTP-begäran till denna URI varje gång en förändring för någon av appanvändarna registrerats. Med API för Dropbox för team kan webhooks också användas för att generera meddelanden om ändringar i teammedlemskapet. Många säkerhetsappar använder webhooks för att hjälpa administratörer spåra och hantera teamaktiviteter.

## Tillägg

Appar kan registrera tilläggs-URI:er, så att åtgärder kan visas i menyerna "Dela" och "Öppna" i Dropbox-gränssnittet. Tilläggen gör att användare kan starta anpassade arbetsflöden från tredje part direkt från en fil i en Dropbox-yta. När en åtgärd utlöses omdirigerar Dropbox användare till den angivna URI:n och skickar en filidentifierare som kan användas med API:t för att utföra alla filåtgärder. En app måste auktoriseras innan ett registrerat tillägg syns för användaren. Vi kan komma att marknadsföra en utvald uppsättning tilläggsintegreringar på menyerna Dela och Öppna, men dessa appar får inte åtkomst till innehåll förrän användaren godkänner det.

## Dropbox-utvecklarriktlinjer

Vi tillhandahåller ett antal riktlinjer och förfaranden för att hjälpa utvecklare att skapa API-appar som respekterar och skyddar användarnas sekretess samtidigt som de förbättrar deras Dropbox-upplevelse.

- **Appnycklar**

För varje enskild app som en utvecklare kodar måste en unik appnyckel för Dropbox användas. Och om en app tillhandahåller tjänster eller programvaror som bäddar in Dropbox-plattformen så att andra utvecklare kan använda den, måste varje utvecklare även registrera en egen appnyckel för Dropbox.

- **Appbehörigheter**

Utvecklare informeras om att en app ska använda en så låg privilegierad åtkomst som möjligt. När en utvecklare skickar in en app för godkännande av produktionsstatus, granskar vi för att säkerställa att appen inte begär onödigt bred åtkomst baserad på den funktion den erbjuder.

- **Granskningsprocess för appar**

- **Utvecklingsstatus**

När en app för Dropbox-API skapas får den utvecklingsstatus. Appen fungerar på samma sätt som andra appar med produktionsstatus, förutom att den endast kan anslutas till upp till 500 Dropbox-användare. När en app ansluter till 50 Dropbox-användare har utvecklaren två veckor på sig att ansöka om och få ett godkännande om produktionsstatus innan appens möjlighet att ansluta till fler Dropbox-användare fryses.

- **Produktionsstatus och godkännande**

För att godkännas för produktionsstatus måste alla API-appar följa våra riktlinjer för varumärkesutveckling för utvecklare, samt de allmänna villkoren som beskriver otillåtna sätt att använda DBX Platform. Dessa otillåtna sätt inkluderar följande: att främja överträdelser av immateriella rättigheter eller brott mot upphovsrätten, att skapa fildelningsnätverk, samt att ladda ner innehåll olagligt. Utvecklare uppmanas först att ange ytterligare information om appens funktionalitet och hur den använder Dropbox API innan de skickar in appen för granskning. När appen godkänts för produktionsstatus kan ett obegränsat antal användare ansluta till appen.

## Teamappsadministration

Inuti teamets administrationskonsol kan Dropbox för teams administratörer [hantera](#) länkade appar och integrationer för sina team.

## API-partnerskap

Dropbox har haft ett nära samarbete med sina teknikpartnerföretag för att de ska kunna utveckla integrationer med sina populära programvarupaket. Dessa partnerföretag bygger applikationer med Dropbox-API:er och har ett nära samarbete med Dropbox-arkitekter för att följa bästa praxis för säkerhet och användarupplevelse. Dessa inkluderar en mängd produktivtetsappar för slutanvändare, samt säkerhets- och hanteringsverktyg som:

- **Säkerhetsinformation och händelsehantering (SIEM) och analys**

Anslut Dropbox Business-kontot till SIEM och analysverktyg för att övervaka och utvärdera användarnas delning, inloggningsförsök, administrativa åtgärder med mera. Få åtkomst till och hantera medarbetarnas aktivitetsloggar och säkerhetsrelevanta data genom ert centrala logghanteringsverktyg.

- **Förebyggande av dataförlust (DLP)**  
Skanna filernas metadata och innehåll automatiskt för att utlösa meddelanden, rapportering och åtgärder när viktiga ändringar har gjorts i ditt Dropbox för team-konto. Tillämpa företagets regler vid driftsättningen av Dropbox för team och få hjälp att följa efterlevnadskraven.
- **eDiscovery och arkiveringsskyldighet**  
Hantera rättstvister, skiljedomar och regelmässiga utredningar med data från ert Dropbox för team-konto. Sök efter och samla relevant elektroniskt lagrad information och spara era data genom eDiscovery-processen, vilket sparar företaget både tid och pengar.
- **Digital rättighetshantering (DRM)**  
Lägg till innehållsskydd från tredjepart för känsliga eller upphovsrättsskyddade data som lagras på medarbetarnas konton. Få åtkomst till kraftfulla DRM-funktioner, inklusive kryptering på klientsidan, vattenstämplar, revisionsspårning, återkallande av åtkomst och blockering av användare/enheter.
- **Dataöverflyttning och säkerhetskopiering på plats**  
För över data till Dropbox från befintliga servrar eller andra molnbaserade lösningar och spara tid, pengar och arbete. Automatisera säkerhetskopieringar från ert Dropbox för team-konto till lokala servrar.
- **Autentisering och samlad inloggning (SSO)**  
Automatisera etableringen och borttagningen av användare och påskynda processen för att registrera nya användare. Effektivisera hanteringen och öka säkerheten genom att integrera Dropbox för team med ett befintligt identitetssystem.
- **Anpassade arbetsflöden**  
Skapa interna appar som integrerar Dropbox med befintliga företagsprocesser för att förbättra interna arbetsflöden.  
  
På sidan [Dropbox-appintegreringar](#) finns en lista över dessa teknikpartnerföretag. Slut användare kan ta del av utvalda första- och tredjepartsappar och -integreringar i [App Center](#).

## Dropbox-integreringar

Vi har också samarbetat med några av våra främsta teknikpartner för att skapa integreringar som marknadsförs på Dropbox-tytor. Dessa djupare integreringar utvecklas av Dropbox och partnern i samarbete. Dessa inkluderar:

### Dropbox-tillägg

Med de här integreringarna kan du använda olika typer av apptillägg för att utföra åtgärder sömlöst, som att publicera en video, lägga till filer i e-post och chatt, skicka en fil för e-signatur och mycket mer, direkt från Dropbox. Dessa applikationer byggs av partnern, medan Dropbox gör det lättare att upptäcka utvalda tilläggsparter via menyn "Öppna med" och "Dela med".

## Slack

Denna integrering är byggd av första part av Dropbox, vilket gör det möjligt för användare att starta Slack-konversationer från Dropbox. Slut användare autentiserar till Slack via OAuth.

## Microsoft Office för mobila enheter och webben

Med våra integrationer med Microsoft Office kan användare öppna Word-, Excel- och PowerPoint-filer som har sparats i deras Dropbox, utföra ändringar i Offices mobilappar eller webbappar och spara dessa ändringar direkt i Dropbox. Användare blir ombudda att ge åtkomst vid första försöket att öppna en Dropbox-fil i respektive Office-mobilapp eller -webbapp. Därefter kommer dessa länknings att bibehållas.

## Adobe Acrobat och Acrobat Reader

Våra integrationer med skrivbords- och mobilversionerna (Android och iOS) av dessa appar ger användare möjlighet att visa, redigera och dela PDF-filer som lagras i deras Dropbox-konton. Användare ombeds bevilja åtkomst vid första försöket att öppna en Dropbox-fil i varje app. Ändringar i PDF-filer sparas automatiskt i Dropbox.

# Produktsäkerhet

Med Dropbox får både IT-avdelningar och slut användare de funktioner för kontroll och översikt de behöver för att hantera sina verksamheter och data. Med Dropbox får du allt du behöver för att arbeta – dina verktyg, material och andra användare – allt på ett ställe. Dropbox är mer än säkert lagringsutrymme – det är ett smart, användarvänligt sätt att optimera ditt befintliga arbetsflöde.

Nedan finns exempel på funktioner för administratörer och slut användare, samt tredjepartsintegrationer för att hantera viktiga IT-processer.

**Obs!** Vilka funktioner som är tillgängliga varierar beroende på prenumerationsplan. Mer information finns under [dropbox.com/business/plans](https://dropbox.com/business/plans).

## Innehållskontroller

Förmågan att skydda känsliga affärstillgångar – som immateriell egendom (IP) och personlig identifierbar information (PII) – är avgörande för IT- och datasäkerhetsteam. Dropbox tillhandahåller branschledande lösningar för att hantera, övervaka och skydda ditt material, från detaljerade innehållsbehörigheter till policyer för arkiveringsskyldighet. Nedan visas de viktiga produkter och funktioner i Dropbox som har stöd för innehållskontroll.

## Detaljerade behörigheter, samt behörigheter för delade filer och mappar

- **Behörigheter för delade filer**

En teammedlem som äger en delad fil kan inaktivera åtkomst för specifika användare och inaktivera kommentering för filen.

- **Behörigheter för delade mappar**

En teammedlem som äger en delad mapp kan inaktivera mappåtkomst för specifika användare, ändra/visa/redigera åtkomst för specifika användare och överföra ägarskap för mappar. Beroende på teamets globala delningsåtkomst kan samtliga ägare av delade mappar också kontrollera om mapparna kan delas med personer utanför teamet, om andra med redigeringsåtkomst kan hantera medlemskap och om länkar kan delas med personer utanför teamet.

- **Lösenord för delade länkar**

Alla delade länkar kan skyddas med ett lösenord som anges av ägaren. Innan fil- eller mappdata skickas används ett åtkomstkontrollager för att verifiera att rätt lösenord har angetts och att alla andra krav (som team-, grupp- eller mapp-ACL) uppfylls. I så fall lagras en säkerhetscookie i användarens webbläsare och gör att den tidigare verifieringen av lösenordet blir ihågkommen. Med delningskontroller kan administratörer också konfigurera standardlösenord, istället för att de ska vara självvalda, för att bättre kunna skydda teamens material.

- **Utgångsdatum för delade länkar**

Användare kan ställa in ett utgångsdatum för alla delade länkar för att tillhandahålla tillfällig åtkomst till filer eller mappar. Med delningskontroller kan administratörer också konfigurera standardgiltigheter, istället för att de ska vara självvalda, för att bättre kunna skydda teamens material.

## Åtkomst till Paper-dokument och delade Paper-mappar

- **Åtkomst till Paper-dokument och delade Paper-mappar**

En teammedlem som äger ett Paper-dokument eller en delad Paper-mapp kan ta bort åtkomsten för specifika användare och inaktivera redigering för dokumentet.

- **Behörigheter för Paper-dokument**

En teammedlem som äger ett Paper-dokument kan ta bort åtkomsten för specifika användare som är uttryckligen listade i delningspanelen. Både Paper-dokumentets ägare och redigerare kan ändra visnings- och redigeringsstillstånd för specifika användare samt ändra dokumentets länkningspolicy. Länkningspolicyn styr vilka användare som kan öppna dokumentet och vilka behörigheter de har. Teamadministratören kan ställa in teamöverskridande policyer för länkar och dokumentdelning.

- **Behörigheter för Paper-mappar**

En teammedlem som är medlem i mappen kan ändra dess delningspolicy och ta bort åtkomst för specifika användare som uttryckligen lagts till i mappen.

## Fil- och mappåtgärder

- **Teammappar för filer**

Administratörer kan skapa teammappar som automatiskt ger grupper och andra användare rätt åtkomstnivå (visa eller redigera) för det innehåll de behöver.

- **Detaljerade åtkomst- och delningskontroller**

Med delningskontroller kan administratörer hantera medlemskap och åtkomst för mappar på högsta nivå eller undermappnivå, så att användare och grupper i och utanför företaget endast har åtkomst till de mappar som de behöver.

- **Hanterare för teammapp**

Administratörer kan visa alla sina teammappar och skraddarsy inställningar för delning från en central plats för att förhindra att konfidentiellt material delas av misstag.

- **Delade mappar för Paper-dokument**

Administratörer kan skapa delade Paper-mappar som automatiskt ger andra användare rätt åtkomstnivå – kommentera eller redigera – för det innehåll de behöver.

- **Fjärrradering**

När medarbetare lämnar teamet eller tappar bort en enhet kan administratörer fjärradera Dropbox-data och lokala filkopior. Filer tas bort från både datorer och mobila enheter när de kopplas upp mot internet och Dropbox körs.

- **Kontoöverföring**

När en användare tagits bort från ett team (manuellt eller via katalogtjänster) kan administratören föra över filer och ägarskap till Paper-dokument som skapats av den före detta teammedlemmen från denna användares konto till en annan teammedlem. Kontoöverföringsfunktionen kan användas när en användare tas bort, eller när som helst efter att en användares konto har raderats.

Följande funktioner finns tillgängliga som tilläggsfunktioner (kontakta [försäljningsavdelningen](#) för mer information).

- **Skanna material**

Med tillägget för avancerade team- och innehållskontroller kan Advanced- och Enterprise-kunder till Dropbox för team skanna efter nytt och befintligt innehåll i Dropbox för att hitta och undvika datasårbarheter.

- **Konfigurera och lös ut anpassade arbetsflöden**

Med tillägget för avancerade team- och innehållskontroller kan administratörer vidta anpassbara åtgärder mot filer som bryter mot företagets policyer.

- **Konfigurera varningar**

Administratörer kan övervaka säkerhetsproblem i realtid och undvika datasårbarheter. Få varningar om filer som delas externt och skanningar av känsliga data.

## Översikt över material

### Säkerhetsvarningar och aviseringar

Administratörer på Dropbox Enterprise kan få aviseringar i realtid när kränkande aktiviteter, riskfylld aktivitet eller potentiella dataläckor identifieras på deras konton. Följande händelser kan övervakas:

- Massraderingar
- Massdataflyttningar
- Känsligt innehåll som delas externt
- Skadlig kod som delas utifrån med ditt team
- Sabotageprogram som delas inifrån ditt team
- För många misslyckade inloggningsförsök
- Inloggning från ett högriskland
- Upptäckt av ransomware

Dropbox tillhandahåller också möjligheten att konfigurera trösklar för varningar, justera mottagare för aviseringar och utlösa varningar när mappar med känsligt innehåll delas externt. Administratörer kan också markera varningar efterhand som de granskas, blir lösta eller avvisas. En kontrollpanelwidget visar dessutom övergripande statistik och trender för teamvarningarna för den senaste veckan.

### Sida och rapporter över extern delning

Dropbox erbjuder mer synlighet med rapport över extern delning och sida. Administratörer kan skapa en rapport från antingen panelen Insikter eller sidan över extern delning. Rapporten listar teamets alla filer och mappar som delas utanför teamet, och alla delade länkar. Sidan för extern delning är en extra sida i adminkonsolen, som ger administratörer möjlighet att se och filtrera (filtyp, vem som delat, länkställningar och mycket annat) genom filerna och mapparna som delas direkt utanför teamet och delade länkar.

### Delningskontroller

Delningsinställningar ger team-administratörer mer kontroll över delningen och åtkomsten till deras teams innehåll. Administratörer kan konfigurera standardgiltigheter, lösenordsbegränsningar eller båda på team-nivå. Dessa begränsningar minskar risken för dataförlust genom att man tar bort ansvaret från användarna att konfigurera begränsningar.

### Hemligstämpling

Team på Dropbox Enterprise kan automatiskt få etiketter på personliga och känsliga data för att skydda dem bättre från att exponeras. Administratörer får varningar om förebyggande av dataförlust (DLP) via e-post och i adminkonsolen när filer och mappar sparades i teamets mappar med känsligt innehåll delas utanför deras team. Administratörer har möjligheten att automatiskt identifiera och klassificera data som finns sparade i delade mappar och teammedlemmars personliga mappar. Dropbox Enterprise-administratörer kan aktivera automatisk dataklassificering från adminkonsolen.

## Tillägg för datastyrning

Datastyrning är en övergripande uppsättning processer, tekniker och team, som förenas för att hantera och skydda en organisations datatillgångar. Detta inkluderar möjligheten att lagra, identifiera, upptäcka och hämta företagsdata efter behov.

Dropbox-tillägget fr datastyrning innehåller en uppsättning funktioner som ger organisationer möjlighet att kontrollera och skydda sina data bättre, samtidigt som risker och kostnader förknippade med att följa lagar och efterlevnadskrav minskas. För närvarande inkluderar detta tillägg fyra viktiga funktioner för team- och efterlevnadsadministratörer.

### **Utökad versionshistorik**

Vilken filversionshistorik du har som standard beror på vilket typ av Dropbox-konto du har. Men med Dropbox för team kan du köpa en separat utökad versionshistorik (EVH) som tillägg eller som en del av datastyrningstillägget, som ger möjlighet att återställa filer som raderats eller ändrats under de senaste 10 åren.

- **Arkiveringsskyldigheter**

Genom att lägga arkiveringsskyldighet för en teammedlem kan team- och efterlevnadsadministratörer se och exportera material som har skapats eller modifierats av denna medlem. Medlemmar som påverkas av arkiveringsskyldighet meddelas inte om skyldigheten och behåller sina behörigheter att skapa, redigera och radera filer.

- **Datalagring**

Datalagring ger teamet och efterlevnadsadministratörerna möjlighet att hindra oavsiktlig radering av material, som enligt lag måste sparas under en bestämd tid. Denna funktion ger kunder möjlighet att spara data mer än 10 år efter senaste datum för "revision".

- **Datadisposition**

Datadisposition ger team och efterlevnadsadministratörer möjlighet att radera data permanent vid ett speciellt datum, för att tillgodose kraven för datalagring och disposition. Administratörer kan övervaka aktivitet genom att få rapporter som varnar dem för kommande radering av filer.

## **Återställning och versionskontroll**

Dropbox för team-kunder har möjlighet att återskapa raderade filer och Paper-dokument, och återställa tidigare versioner av filer och Paper-dokument. Detta garanterar att ändringar av viktiga data kan spåras och hämtas.

## **Datasäkerhet på mobila enheter**

- **Radera data**

För ytterligare säkerhet kan en användare aktivera möjligheten att radera alla Dropbox-data från enheten efter tio misslyckade försök att ange åtkomstkoden.

- **Intern lagring och offlinefiler**

Som standard lagras inte filer internt på mobila enheter. Dropbox-mobilklienter kan spara individuella filer och mappar på enheten för offlinevisning. När en enhet avlänkas från Dropbox-kontot, antingen via mobil- eller webbgränssnittet, raderas dessa filer och mappar automatiskt från enhetens interna lagring.

- **Paper-offlinedokument**

När en enhet avlänkas från Paper via Dropbox-kontots säkerhetssida loggas användaren ut och Paper-dokument i offlineläge raderas automatiskt från enhetens interna lagring.

## Teamkontroller

Eftersom alla organisationer är olika har vi tagit fram ett antal verktyg som ger administratörer möjlighet att anpassa Dropbox för team efter teamets särskilda behov. Dropbox för team har verktyg som hjälper slutanvändare att skydda sina konton och data ytterligare. Autentisering, återställning, loggning och andra säkerhetsfunktioner nedan är tillgängliga genom Dropbox olika användargränssnitt.

Nedan visas flera kontroll- och översiktsfunktioner som är tillgängliga via adminkonsolen för Dropbox för team.

### Detaljerade innehållsbehörigheter

- **Nivåindelade administratörsroller**

Dropbox erbjuder nivåindelade adminroller som ger en mer effektiv teamstyrning. Kontoadministratörer kan tilldelas en av tre åtkomstnivåer. Det finns inga begränsningar för hur många administratörer ett team kan ha och alla teammedlemmar kan ges en adminroll.

- **Teamadministratör**

Kan ställa in säkerhets- och delningsåtkomst för hela teamet, skapa administratörer och hantera medlemmar. Teamadministratören har heltäckande administratörsåtkomst. Endast teamadministratörer kan tilldela eller ändra administratörsroller, och det måste alltid finnas minst en teamadministratör för ett Dropbox för team-konto.

- **Administratör för användarhantering**

Kan utföra de flesta teamhanteringsuppgifterna, inklusive att lägga till och ta bort teammedlemmar, hantera grupper och visa ett teams aktivitetsflöde.

- **SUPPORTADMINISTRATÖR**

Kan hantera vanliga tjänstebegäranden från teammedlemmar, som att återställa raderade filer eller hjälpa teammedlemmar som har blivit utelåsta från tvåstegsautentiseringen. Supportadministratörer kan även återställa lösenord åt personer som inte är administratörer, samt exportera aktivitetsloggar för specifika teammedlemmar.

- **Faktureringsadministration**

Kan komma åt faktureringsidor i adminkonsolen.

- **Innehållsadministration**

Kan skapa och hantera teamets mappar i Innehållshanteraren.

- **Rapporteringsadministration**

Kan skapa rapporter i adminkonsolen och har åtkomst till aktivitetssidan.

- **Säkerhetsadministration**

Kan hantera säkerhetsvarningar, extern delning och säkerhetsrisker.

- **Efterlevnadsadministratör (finns bara för team med datastyrningstillägget)**  
Kan hantera datastyrningssidor (bevarande av juridiska skäl, datalagring och datadisposition) och åtkomst till Innehållshanteraren.
- **Grupper**  
Team kan skapa och hantera medlemslistor inom Dropbox och enkelt ge medlemmarna åtkomst till specifika mappar. Dropbox kan även synka Active Directory-grupper med hjälp av Active Directory Connector.
- **Företagshanterade grupper**  
Enbart administratörer kan skapa, radera och hantera medlemskap för den här typen av grupp. Användarna kan inte göra förfrågningar om att gå med i eller lämna en företagshanterad grupp.
- **Användarhanterade grupper**  
Administratörer kan välja om användarna ska kunna skapa och hantera sina egna grupper. Administratörer kan även när som helst ändra en användarhanterad grupp till en företagshanterad grupp för att få kontroll över den.
- **Begränsa flera konton på datorer**  
Administratörer kan blockera teammedlemmar från att länka ett andra Dropbox-konto till datorer som är länkade till deras Dropbox-konton för arbetet.
- **Läge för inaktiverade användare**  
Administratörer kan inaktivera en användares åtkomst till sitt konto samtidigt som användarens data och delningsrelation bevaras i syfte att hålla företagsinformation säker. Administratörer kan senare återaktivera eller radera kontot.
- **Gå in som användare**  
Teamadministratörer kan logga in som medlemmar i sina team. Detta ger administratörerna direktåtkomst till filer, mapparna och Paper-dokument i teammedlemmarnas konton, så att de kan genomföra ändringar, dela för teammedlemmars räkning eller granska händelser på filnivå. "Logga in som användare"-händelser registreras i teamets aktivitetslogg och administratörerna kan avgöra om medlemmarna ska meddelas om dessa händelser.
- **Delningstillstånd**  
Teamadministratörer har övergripande kontroll över teamets delningsåtkomst vid användning av Dropbox, däribland följande:
  - Om teammedlemmar kan dela filer och mappar med personer utanför teamet.
  - Om teammedlemmar kan redigera mappar som ägs av personer utanför teamet.
  - Om delade länkar som skapats av teammedlemmar fungerar för personer utanför teamet.
  - Om teammedlemmar kan skapa filinlämningar och samla in filer från teammedlemmar och/eller personer utanför teamet.
  - Om personer kan visa och infoga kommentarer i filer som ägs av teamet.
  - Om teammedlemmar kan dela Paper-dokument och Paper-mappar med personer utanför teamet.
  - Behörighet att radera permanent beviljas.

Teamadministratören för ett Dropbox för team-konto kan begränsa möjligheten att radera filer och Paper-dokument permanent till att endast gälla teamadministratörer.

## Onboarding och användaretablering

### Metoder för användaretablering och identitetshantering

- **E-postinbjudningar**

Det finns ett verktyg i adminkonsolen för Dropbox för team som låter administratörerna generera mejlinbjudningar manuellt.

- **Active Directory**

Administratörer för Dropbox för team kan automatisera konfiguration och borttagning av konton i ett befintligt Active Directory-system via vår Active Directory-koppling eller en tredje parts identitetsleverantör. När Active Directory har integrerats kan det användas för hantering av medlemskap.

- **Samlad inloggning (SSO)**

Dropbox för team kan konfigureras för att ge teammedlemmarna åtkomst genom inloggning via en central identitetsleverantör. Vår SSO-implementering använder Security Assertion Markup Language 2.0 (SAML 2.0), vilket gör etableringen enklare och säkrare genom att en betrodd identitetsleverantör autentiserar och ger teammedlemmar åtkomst till Dropbox utan ytterligare lösenord att hantera. Dropbox har dessutom inlett ett partnerskap med ledande identitetshanteringsleverantörer så att användare kan etableras och avetableras automatiskt. Läs mer i avsnittet [API-integreringar för Dropbox för team](#).

- **Lösenordsnycklar**

Åtkomstnycklar använder offentlig nyckelkryptering för att möjliggöra säker autentisering utan att förlita sig på lösenord eller sms-koder. De finns för närvarande tillgängliga som inloggningsmetod på Dropbox webb och använder en autentisering, en PIN-kod eller biometri. Den privata nyckeln lämnar aldrig din enhet – Dropbox lagrar bara den offentliga nyckeln.

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

Dropbox har stöd för SCIM-integrering, vilket gör det enklare att hantera användaridentiteter i molnbaserade applikationer, inklusive att lägga till användare, uppdatera användare, ta bort användare, skapa grupper och lägga till eller ta bort användare från grupper. I stället för att kräva att tredje part implementerar anpassad logik via APIv2-slutpunkter, definierar SCIM ett gemensamt gränssnitt som leverantörer kan använda för att etablera användare och grupper för alla tjänster som har stöd för det, inklusive Dropbox.

- **API**

Dropbox för team-API:t kan användas av kunder för att skapa anpassade lösningar för användaretablering och identitetshantering. Läs mer i avsnittet [API-integreringar för Dropbox för team](#).

## Tvåstegsverifiering

Denna starkt rekommenderade säkerhetsfunktion skapar ett extra skyddslager för en användares Dropbox-konto. När tvåstegsverifiering har aktiverats måste man alltid ange lösenord och en sexsiffrig säkerhetskod när man loggar in eller ansluter till en ny dator, telefon eller surfplatta.

- Administratörer kan välja att kräva tvåstegsverifiering för alla teammedlemmar, eller bara vissa.
- Kontoadministratörer kan spåra vilka teammedlemmar som har aktiverat tvåstegsverifieringen.
- Dropbox koder för tvåstegsautentisering kan fås via sms eller appar med algoritmstandarden Time-based One-Time Password (TOTP).
- Om en användare inte kan få säkerhetskoder med hjälp av dessa metoder kan hon eller han använda en 16-siffrig säkerhetskod för nödfall som endast används en gång. Användaren kan också använda ett sekundärt telefonnummer för att få en reservkod via sms.
- Dropbox har också stöd för den öppna standarden FIDO Universal 2nd Factor (U2F), som ger användare möjlighet till autentisering med en USB-säkerhetsnyckel de konfigurerat i stället för en sexsiffrig kod.

## Företagsinstallatör

Administratörer som kräver storskalig etablering kan använda vår företagsinstallatör för Windows för att fjärrinstallera Dropbox-klienten via mekanismer för hanterad programvara och distribution.

## Hanterade enheter och inloggningar

- **Enterprise Mobility Management (EMM)**

Dropbox integrerar med EMM-leverantörer från tredje part för att ge administratörer för Dropbox för team med en Enterprise-plan större kontroll över hur teammedlemmar använder Dropbox på mobila enheter. Administratörer kan begränsa användningen av mobilappen för Dropbox Enterprise-konton till endast hanterade enheter (oavsett om de tillhandahålls av företaget eller är personliga), se information om appanvändning (inklusive tillgängligt lagringsutrymme och åtkomstplatser) och fjärradera en borttappad eller stulen enhet.

- **Enhetsgodkännande**

Med Dropbox kan Dropbox för team med Advanced- och Enterprise-planer ställa in begränsningar för hur många enheter som en användare kan synka med Dropbox. De kan även välja om godkännanden ska hanteras av användarna eller av administratörerna. Administratörer kan också skapa en undantagslista över användare som inte är begränsade till ett visst antal enheter.

- **Krav på tvåstegsverifiering**

Administratörer kan välja att kräva tvåstegsverifiering för alla eller bara vissa teammedlemmar. Andra krav på multifaktorverifiering kan integreras genom teamets SSO-implementering.

- **Lösenordskontroll**

Administratörer för Education-, Advanced- och Enterprise-team kan kräva att medlemmarna skapar och upprätthåller starka och komplexa lösenord till sina konton. När denna funktion är aktiverad kommer teammedlemmarna att loggas ut från sina webbsessioner och tvingas skapa nya lösenord när de loggar in igen. Ett inbyggt verktyg analyserar lösenordets styrka genom att jämföra det med en databas med vanliga ord, namn, mönster och siffror. En användare som anger ett vanligt lösenord ombes komma på ett nytt som är unikt och svårare att gissa för en utomstående. Administratörer kan också återställa lösenord för hela teamet eller för enskilda användare.

- **Domänhantering**

Dropbox erbjuder en uppsättning verktyg som ger företag möjlighet att förenkla och påskynda processen för etablering av nya användare och kontroll av Dropbox-användningen.

- **Domänverifiering**

Företag kan göra anspråk på äganderätten till sina egna domäner och låsa upp resten av verktygen för domänhantering.

- **Tvingande inbjudan**

Administratörer kan kräva att enskilda Dropbox-användare, som har bjudits in till företagets Dropbox-team, överförs till teamet eller ändrar e-postadress i sina personliga konton.

- **Domäninsikter**

Administratörer kan se viktig information, till exempel hur många enskilda Dropbox-konton som använder företagets e-postadresser.

- **Kontotillägg**

Administratörer kan tvinga alla Dropbox-användare som använder en av företagets e-postadresser att gå med i företagets team eller ändra e-postadress i sitt personliga konto.

- **Webbsessionskontroll**

Administratörer kan styra hur länge teammedlemmar kan vara inloggade på dropbox.com. Administratörer kan begränsa varaktigheten för alla webbsessioner och/eller sessioner som är i vänteläge. Sessioner som når dessa gränser kommer automatiskt att loggas ut. Administratörer kan också spåra och avsluta webbsessioner för individuella användare.

- **Appåtkomst**

Administratörerna kan visa och återkalla tredjepartsappars åtkomst till användarkonton.

- **Koppla från enheter**

Datorer och mobila enheter som är anslutna till användarkonton kan kopplas från av administratören i adminkonsolen eller av användaren själv i det enskilda kontots säkerhetsinställningar. När du kopplar från en dator raderas autentiseringsdata och du har möjlighet att radera lokala kopior av filer nästa gång datorn ansluter till internet (se [Fjärradring](#)). När du kopplar från en mobil enhet raderas favoritmarkerade filer, cachelagrade data och inloggningsinformation. Om tvåstegsverifiering är aktiverad måste användaren återautentisera varje enhet vid återkoppling. Användarnas kontoinställningar ger dessutom möjligheten att skicka en automatisk avisering via e-post när enheter kopplas samman.

- **Nätverksstyrning**

Administratörer för Dropbox för team med Enterprise-plan kan begränsa Dropbox-användningen på företagsnätverket till bara Enterprise-teamkontot. Med denna funktion integreras företagets nätverkssäkerhetsleverantör för att blockera eventuell trafik som görs utanför det sanktionerade kontot på datorer. Observera att Paper för närvarande inte hanteras genom nätverkskontroll.

## Mobilsäkerhet

- **Fingeravtrycksskanning**

Användare kan aktivera Touch ID eller Face ID på iOS-enheter och fingeravtryckslås (när detta stöds) på Android-enheter som ett sätt att låsa upp Dropbox-mobilappen.

## Åtkomstöversikt

- **Identitetsverifiering för teknisk support**

Innan Dropbox Support utför en felsökning eller lämnar ut kontouppgifter måste kontoadministratören verifiera sin identitet genom att tillhandahålla en slumpgenererad engångskod. Denna PIN-kod är endast tillgänglig via adminkonsolen.

## Användarkontoaktiviteter

Alla användare kan se följande sidor i kontoinställningarna för att kunna hämta aktuell information angående den egna kontoaktiviteten.

- **Delningssida**

På denna sida visas de delade mapparna som för närvarande finns i användarens Dropbox, samt delade mappar som användaren kan lägga till. En användare kan sluta dela mappar och filer och ange delningsbehörigheter.

- **Filsida**

Denna sida visar de filer som delats med användare och respektive datum då varje fil delades. Användaren har möjlighet att ta bort åtkomst till dessa filer. För att visa Paper-dokument som har delats med användaren av andra personer kan användaren gå till "Delat med mig"-sidan i navigeringsgränssnittet för Paper-dokument.

- **Länksida**

Denna sida visar alla aktiva delade länkar som användaren har skapat och skapandedatumet för dem. Den visar även alla länkar som andra delar med användaren. Användaren kan inaktivera länkar eller ändra behörigheter.

- **E-postaviseringar**

En användare kan välja att få e-postaviseringar omedelbart när en ny enhet eller app kopplas till deras Dropbox-konto.

## Behörigheter för användarkonto

- **Länkade enheter**

Enhetsdelen i en användares kontosäkerhetsinställningar visar alla datorer och mobila enheter som är kopplade till användarens konto. För varje dator visas IP-adress, land och ungefärlig tid för senaste aktivitet. En användare kan koppla från valfri enhet, med möjlighet att få filer på kopplade enheter raderade nästa gång de ansluts till internet.

- **Aktiva webbsessioner**

Sessionsdelen visar alla webbläsare som är inloggade på en användares konto. Varje webbläsare visas IP-adress, land och inloggningstid för den senaste sessionen, samt ungefärlig tid för den senaste aktiviteten. En användare kan fjärravsluta alla sessioner via användarkontots säkerhetsinställningar.

- **Länkade appar**

I delen för kopplade appar visas en lista över alla tredjepartsappar med åtkomst till en användares konto, samt vilken typ av åtkomst varje app har. En användare kan återkalla alla appars behörighet till användarens Dropbox.

## **Aktivitetsflöde**

Dropbox för team registrerar filåtgärder i teamets aktivitetsflöde, som nås från adminkonsolen. Aktivitetsflödet erbjuder flexibla filtreringsalternativ som gör att administratörer kan utföra målinriktade utredningar av konto-, fil- eller Paper-dokumentaktivitet. De kan till exempel visa hela historiken för en fil eller ett Paper-dokument och hur användarnas interaktion ser ut, eller visa all aktivitet för teamet under en specifik tidsperiod. Aktivitetsflödet kan exporteras som en nerladdningsbar rapport i CSV-format och integreras direkt i en SIEM-produkt (Security Information and Event Management) eller något annat analysverktyg genom lösningar från tredje part. Följande materialhändelser registreras i aktivitetsflödet:

- **Delning för filer, mappar och länkar**

I förekommande fall anger rapporter huruvida händelser omfattar personer utanför teamet.

### **Delade filer**

- Lade till eller tog bort en teammedlem eller icke-teammedlem.
- Ändrade åtkomstbehörigheter för en teammedlem eller icke-teammedlem.
- Lade till eller tog bort en grupp.
- Lade till en delad fil i användarens Dropbox.
- Visade innehållet i en fil som delades via en fil- eller mappinbjudan.
- Kopierade delat innehåll till användarens Dropbox.
- Laddade ner delat innehåll.
- Kommenterade en fil.
- Markerade en kommentar som löst eller olöst.
- Raderade en kommentar.
- Påbörjade eller avslutade prenumeration på meddelanden om kommentarer.
- Gjorde anspråk på en inbjudan till en fil som ägs av teamet.
- Begärde åtkomst till en fil som ägs av teamet.
- Slutade dela en fil.

### **Delade mappar**

- Skapade en ny delad mapp.
- Lade till eller tog bort en teammedlem, icke-teammedlem eller grupp.

- Lade till en delad mapp i användarens Dropbox, eller så tog användaren bort sin egen åtkomst till en delad mapp.
- Lade till en delad mapp från en länk.
- Ändrade åtkomstbehörigheter för en teammedlem eller icke-teammedlem.
- Överförde ägarskapet av en mapp till en annan användare.
- Slutade dela en mapp.
- Gjorde anspråk på medlemskapet för en delad mapp.
- Begärde åtkomst till en delad mapp.
- Lade till en begärande användare till en delad mapp.
- Blockerade eller avblockerade icke-teammedlemmar från att läggas till i en mapp.
- Tillät samtliga teammedlemmar att lägga till personer i en mapp eller bara ägaren.
- Ändrade gruppåtkomst till en delad mapp.

#### **Delade länkar**

- Skapade eller tog bort en länk.
- Gjorde innehållet i en länk synligt för alla med länken eller endast teammedlemmar.
- Gjorde innehållet i en länk lösenordsskyddat.
- Angav eller tog bort ett utgångsdatum för en länk.
- Visade en länk.
- Laddade ner innehållet i en länk.
- Kopierade innehållet i en länk till användarens Dropbox.
- Skapade en länk till en fil via en API-app.
- Delade en länk med en teammedlem, icke-teammedlem eller grupp.
- Blockerade eller avblockerade icke-teammedlemmar från att visa länkar till filer i en delad mapp.
- Delade ett album.

#### **Filinlämningar**

- Skapade, ändrade, stängde eller raderade en filinlämning.
- Lade till användare till en filinlämning.
- Lade till eller tog bort en deadline för filinlämning.
- Ändrade en filinlämningsmapp.
- Tog emot filer via en filinlämning.
- Tog emot filer via mejl till Dropbox.

### **Enskilda fil- och mapphändelser**

- Lade till en fil i Dropbox.
- Skapade en mapp.
- Visade en fil.
- Redigerade en fil.
- Laddade ner en fil.
- Kopierade en fil eller mapp.
- Flyttade en fil eller mapp.
- Gav en fil eller mapp ett nytt namn.
- Ändrade tillbaka en fil till en tidigare version.
- Återställde ändringar i filer.
- Återställde en raderad fil.
- Raderade en fil eller mapp.
- Raderade en fil eller mapp permanent.

### **Lyckade och misslyckade inloggningar**

- Lyckat eller misslyckat inloggningsförsök.
- Misslyckat inloggningsförsök eller fel via samlad inloggning (SSO).
- Misslyckat inloggningsförsök eller fel via EMM.
- Utloggad.
- Ändring av IP-adress för webbsession.

### **Lösenord**

Byt lösenord eller ändra inställningar för tvåstegsverifiering. Administratörer har inte tillgång till användares lösenord.

- Ändrade eller återställde lösenord.
- Aktiverad, återställd eller inaktiverad tvåstegsverifiering.
- Konfigurerade eller ändrade tvåstegsverifiering för användning av sms eller mobilapp.
- Lade till, redigerade eller tog bort säkerhetstelefon för tvåstegsverifiering.
- Lade till eller tog bort säkerhetsnyckel för tvåstegsverifiering.

## **Medlemskap**

Tillägg och borttagning av personer i teamet.

- Bjud in en teammedlem.
- Gick med i teamet.
- Tog bort en teammedlem.
- Stängde av eller upphävde avstängning av en teammedlem.
- Återställde en borttagen teammedlem.
- Begärde att få gå med i teamet baserat på kontodomän.
- Godkände eller avböjde en begäran om att gå med i teamet baserat på kontodomän.
- Skickade domäinbjudningar till befintliga domänkonton.
- Användare gick med i teamet som svar på kontotillägg.
- Användare lämnade domän som svar på kontotillägg.
- Blockerade eller avblockerade teammedlemmar från att föreslå nya medlemmar.
- Föreslog en ny teammedlem.

## **Appar**

Koppling av tredjepartsappar till Dropbox-konton.

- Godkände eller tog bort en applikation.
- Godkände eller tog bort en teamapplikation.

## **Enheter**

Länka datorer eller mobila enheter till Dropbox-konton.

- Länkade eller kopplade från en enhet.
- Använde fjärradering och raderade alla filer eller misslyckades med att radera vissa filer.
- Ändring av IP-adress för skrivbordsdatorer eller mobil enhet.

## **Administratörsåtgärder**

Ändring av inställningar i administratörskonsolen, till exempel behörighet till delade mappar.

- **Autentisering och enkel inloggning (SSO)**
  - Återställde teammedlemmens lösenord.
  - Återställde alla teammedlemmars lösenord.
  - Blockerade eller avblockerade teammedlemmar från att inaktivera tvåstegsverifiering.
  - Aktiverade eller inaktiverade SSO.
  - Gjorde inloggning via SSO obligatorisk.
  - Ändrade eller tog bort SSO-URL.
  - Uppdaterade SSO-certifikat.
  - Ändrade SSO-identitetsläge.
- **Medlemskap**
  - Blockerade eller avblockerade användare från att begära anslutning till teamet baserat på kontodomän.
  - Ställde in begäranden för teammedlemskap på att automatiskt godkännas eller kräva manuellt administratörsgodkännande.
- **Hantering av medlemskonto**
  - Ändrade en teammedlems namn.
  - Ändrade en teammedlems mejladress.
  - Tilldelade eller tog bort administratörsstatus, eller ändrade administratörsrollen.
  - Loggade in eller ut som teammedlem.
  - Överförde eller raderade innehållet i en borttagen medlems konto.
  - Raderade innehållet i en borttagen medlems konto permanent.
- **Globala delningsinställningar**
  - Blockerade eller avblockerade teammedlemmar från att lägga till delade mappar ägda av icke-teammedlemmar.
  - Blockerade eller avblockerade teammedlemmar från att dela mappar med icke-teammedlemmar.
  - Aktiverade varningar som visas för användare innan de delar mappar med icke-teammedlemmar.
  - Blockerade eller avblockerade icke-teammedlemmar från att se delade länkar.
  - Ställde in delade länkar på att endast visas för teamet som standard.
  - Blockerade eller avblockerade personer från att lämna kommentarer i filer.
  - Blockerade eller avblockerade teammedlemmar från att skapa filinlämningar.
  - Lade till, ändrade eller tog bort en logo för delade länksidor.
  - Blockerade eller avblockerade teammedlemmar från att dela Paper-dokument och Paper-mappar med personer som inte är medlemmar i teamet.

- **Teammappshantering för filer**
  - Skapade en teammapp.
  - Bytte namn på en teammapp.
  - Arkiverade en teammapp eller återställde den från arkivering.
  - Raderade en teammapp permanent.
  - Nedgraderade en teammapp till en delad mapp.
- **Domänhantering**
  - Försökte verifiera eller verifierade en domän eller tog bort en domän.
  - Dropbox Support verifierade eller tog bort en domän.
  - Aktiverade eller inaktiverade sändningen av domäninbjudningar.
  - Slog på eller av "Bjud in nya användare automatiskt".
  - Ändrade läge för kontotillägg.
  - Dropbox Support beviljade eller drog in kontotillägg.
- **Enterprise Mobility Management (EMM)**
  - Aktiverade EMM för testläge (valfritt) eller distributionsläge (krav).
  - Uppdaterade EMM-token.
  - Lade till eller tog bort teammedlemmar från listan över EMM-undantagna användare.
  - Inaktiverade EMM.
  - Skapade en rapport med EMM-undantagslista.
  - Skapade en användningsrapport för EMM-mobilapp.
- **Ändringar i andra teaminställningar**
  - Slog samman team.
  - Uppgraderade teamet till Dropbox för team eller nedgraderade det till ett kostnadsfritt team.
  - Ändrade teamnamnet.
  - Skapade en teamaktivitetsrapport.
  - Blockerade eller avblockerade teammedlemmar från att ha fler än ett konto kopplat till en dator.
  - Tillät alla medlemmar eller endast administratörer att skapa grupper.
  - Blockerade eller avblockerade teammedlemmar från att radera filer permanent.
  - Inledde eller avslutade en Dropbox Support-session för en återförsäljare.

## Grupper

Information om skapande, radering och medlemskap för grupper.

- Skapade, döpte om, flyttade eller raderade en grupp.
- Lade till eller tog bort en medlem.
- Ändrade en gruppmedlems åtkomsttyp.
- Ändrade grupp till teamhanterad eller administratörshanterad.
- Förändrat externt ID för en grupp.

## Paper-aktivitetslogg

Administratörer kan välja en typ av Paper-aktivitet i aktivitetsflödet eller hämta en fullständig aktivitetsrapport. Paper-händelser registreras för:

- Paper aktiverat eller inaktiverat.
- När Paper-dokument skapas, redigeras, exporteras, arkiveras, raderas permanent och återställs.
- När Paper-dokument kommenteras, och när kommentarer blir lösta.
- När Paper-dokument delas med teammedlemmar och andra personer, och när delningen tas bort.
- När åtkomst till Paper-dokument begärs av teammedlemmar och andra personer.
- När teammedlemmar och andra personer taggas i Paper-dokument.
- När Paper-dokument visas av teammedlemmar och andra personer.
- Paper-dokument följt.
- När Paper-dokuments medlemsåtkomster förändras (redigera, kommentera eller skrivskyddat).
- När extern delningspolicy för Paper-dokument ändras.
- När Paper-mappar skapas, arkiveras och raderas permanent.
- När Paper-dokument läggs till i eller tas bort från en mapp.
- Paper-mapp har fått nytt namn.
- När Paper-dokument och Paper-mappar flyttas.

# Integritetscertifieringar, intyg och regelefterlevnad

Följande standarder innehåller våra krav angående hur Dropbox ska och inte ska använda din organisations information:

- **Din organisation kontrollerar era data**

Vi använder bara den personliga information ni ger oss för att erbjuda de tjänster ni registrerat er för. Ni kan lägga till, ändra eller ta bort data från Paper-dokument och Dropbox närhelst ni behöver.

- **Vi är transparenta med avseende på era data**

Vi är transparenta angående var era data förvaras på våra servrar. Vi låter er också veta vilka våra betrodda partner är. Vi berättar vad som händer när ni avslutar ett konto eller tar bort en fil eller ett Paper-dokument. Slutligen berättar vi om några av dessa saker förändras.

- **Era data är säkra och skyddade**

ISO/IEC 27018 och ISO/IEC 27701 utformades som förbättringar och tillägg till ISO/IEC 27001, en av världens mest accepterade informationssäkerhetsstandarder. Vi fick förnyad ISO/IEC 27001-certifiering i oktober 2021.

- **Våra rutiner ses över regelbundet**

Som en del av vår efterlevnad av ISO/IEC 27018, ISO/IEC 27701 och ISO/IEC 27001 genomgår vi årliga granskningar av en oberoende tredje part för att upprätthålla dessa certifieringar. Du kan se alla våra ISO-certifikat i vårt [Trust Center](#).

## Dataöverföringar

Vid överföring av data från Europeiska unionen, Europeiska ekonomiska samarbetsområdet, Storbritannien och Schweiz använder sig Dropbox av flera olika rättsliga mekanismer, som till exempel avtal med våra kunder och dotterbolag, [standardklausuler](#), ramverket för dataskydd mellan EU och USA, det brittiska tillägget till ramverket för dataskydd mellan EU och USA, ramverket för dataskydd mellan Schweiz och USA samt Europeiska kommissionens [lämplighetsbeslut](#) gällande vissa länder, beroende på vad som är tillämpligt.

Dropbox följer ramverken för dataskydd mellan EU och USA och mellan Schweiz och USA, samt det brittiska tillägget till ramverket för dataskydd mellan EU och USA, enligt vad som fastställts av amerikanska Department of Commerce gällande behandlingen av personuppgifter som överförs till USA från Europeiska unionen, Europeiska ekonomiska samarbetsområdet, Storbritannien och Schweiz. Dropbox har försäkrat för amerikanska Department of Commerce att företaget följer principerna i dessa ramverk för dataskydd med avseende på sådana uppgifter, men detta omfattar inte Formswift-delen av tjänsterna. Skulle det förekomma en konflikt mellan denna integritetspolicy och principerna i ramverken för dataskydd ska principerna gälla. I enlighet med principerna ska Dropbox vara fortsatt ansvarig för vidare överföring om ett personuppgiftsbiträde behandlar personuppgifter på ett sätt som inte följer principerna. Du kan läsa mer om ramverken för dataskydd och se vår certifiering på <https://www.dataprivacyframework.gov>.

Klagomål och dispyter relaterade till vår efterlevnad av ramverken för dataskydd undersöks och löses genom JAMS, en oberoende tredje part. Mer information finns i vår sekretesspolicy ([dropbox.com/privacy](https://dropbox.com/privacy)).

## EU:s allmänna dataskyddsförordningen (GDPR)

Dropbox värnar om säkerheten och skyddet av våra användares data i enlighet med lagliga krav och bästa praxis som ständigt beaktas. I linje med vårt engagemang för våra användare har vi arbetat hårt för att se till att Dropbox efterlever kraven i GDPR, inklusive att utse ett dataskyddsombud, att förändra vårt integritetsprogram för att säkerställa att användare kan utöva sina rättigheter i egenskap av registrerade personer, att dokumentera våra databearbetsaktiviteter och att stärka våra interna processer i händelse av en säkerhetsöverträdelse. Vi gör hela tiden justeringar för att se till att vår process och praxis uppfyller eller överskrider specifika krav i de nya reglerna, i takt med att vi kontinuerligt får ytterligare vägledning från dataskyddsmyndigheter.

Mer information om vår policy och vårt arbete med sekretess finns i Dropbox-vitboken om [sekretess och dataskydd](#).

## EU:s uppförandekod för molntjänster

EU:s uppförandekod för molntjänster är ett frivilligt instrument som gör det möjligt för en molntjänsteleverantör, som Dropbox, att visa vårt åtagande för GDPR-efterlevnad. Dropbox för team, som består av planerna Standard, Advanced, Enterprise, Education, Business och Business Plus för team, har förklarats följa EU:s uppförandekod för molntjänster och tilldelats efterlevnadsmärket på "nivå 2", vilket innebär att dessa tjänster har vidtagit tekniska, organisatoriska och avtalsrelaterade åtgärder i enlighet med kraven i koden. Mer information om EU:s uppförandekod för molntjänster och Dropbox efterlevnad av koden finns på [kodens officiella webbplats](#).

Mer information om våra integritetsrutiner och våra integritetspolicyer finns i Dropbox [vitbok om sekretess och dataskydd](#).

# Efterlevnad

Det finns många olika regelverksrelaterade och branschspecifika krav för säkerhet och sekretess som organisationer kan behöva efterleva. Vårt sätt är att kombinera de mest erkända standarderna med efterlevnadsåtgärder anpassade till de specifika behoven hos våra kunders företag eller branscher. Dropbox för team, inklusive planerna Dropbox Standard, Advanced, Enterprise, Education, Dropbox Business och Dropbox Business Plus, följer följande ramverk, standarder och förordningar:

## ISO

Internationella standardiseringsorganisationen (ISO) har utvecklat en serie standarder i världsklass för säkerhet i fråga om information och samhälle. De finns till för att hjälpa organisationer att ta fram tillförlitliga och innovativa produkter och tjänster. Dropbox har certifierat datacenter, system, applikationer, personal och processer genom en serie revisioner utförda av det oberoende och fristående företaget EY CertifyPoint i Nederländerna. Det upprätthåller sina ISO-ackrediteringar från [Raad voor Accreditatie](#) (det nederländska ackrediteringsrådet).

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

ISO/IEC 27001 är erkänt som världens främsta standard för informationssäkerhet (ISMS). Standarden utnyttjar också bästa praxis som beskrivs i ISO/IEC 27002. Eftersom vi vill behålla ditt förtroende bedriver vi hela tiden en ingående hantering av våra fysiska, tekniska och juridiska kontroller på Dropbox.

[Visa Dropbox för teams ISO/IEC 27001-certifikat.](#)

### **ISO/IEC 27017 (molnsäkerhet)**

ISO/IEC 27017 är en internationell standard för molnsäkerhet. Den ger riktlinjer för säkerhetskontroller i fråga om tillhandahållande och användning av molntjänster. I vår [guide om delat ansvar](#) förklaras flera av kraven för säkerhet, sekretess och efterlevnad som Dropbox och våra kunder kan lösa tillsammans.

[Visa Dropbox för teams ISO/IEC 27017-certifikat.](#)

### **ISO/IEC 27018 (molnsekretess och dataskydd)**

ISO/IEC 27018 är en internationell standard för sekretess och dataskydd som gäller för molntjänstleverantörer som Dropbox som hanterar personuppgifter å sina kunders vägnar. Den blir en utgångspunkt för våra kunder vad gäller vanliga krav eller frågor beträffande föreskrifter och kontrakt.

[Visa Dropbox för teams ISO/IEC 27018-certifikat.](#)

### **ISO/IEC 22301 (affärskontinuitet)**

ISO/IEC 22301 är en internationell standard för kontinuitetsplanering som hjälper organisationer att minska risken för störande händelser och hantera dem på ett lämpligt sätt med minsta möjliga skada om de skulle inträffa. Dropbox system för verksamhetskontinuitet (BCMS) är en del av vår övergripande strategi för riskhantering för att skydda människor och verksamheter under kriser.

[Visa Dropbox för teams ISO/IEC 22301-certifikat.](#)

## **ISO/IEC 27701 (hantering av personuppgifter)**

ISO 27701 är en internationell standard för hantering av sekretessinformation. Standarden ger ett ramverk för att förbättra och utöka systemet för informations säkerhets hantering under ISO 27001 till ett system för hantering av sekretessinformation (PIMS). Dropbox för team har certifierats som personuppgiftsbiträde.

[Visa Dropbox för teams ISO 27001-certifikat.](#)

## **SOC**

SOC-rapporterna (Service Organization Controls), kända som SOC 1, SOC 2 och SOC 3 är ramverk som är framtagna av AICPA (American Institute of Certified Public Accountants) för att rapportera om interna kontroller som implementeras i en organisation. Dropbox har certifierat sina system, applikationer, medarbetare och processer i en serie revisioner med hjälp av den oberoende och utomstående revisionsfirman Ernst & Young LLP.

### **SOC 3 för säkerhet, konfidentialitet, integritet, tillgänglighet och sekretess**

SOC 3-rapporten täcker alla fem principerna för betrodda tjänster: säkerhet, konfidentialitet, integritet, tillgänglighet och sekretess (TSP, avsnitt 100). Dropbox rapport om allmän användning är en administrativ sammanfattning av SOC 2-rapporten och innehåller den oberoende, utomstående granskarens omdöme om hur våra kontroller är utformade och fungerar.

[Visa Dropbox för teams SOC 3-undersökning.](#)

### **SOC 2 för säkerhet, konfidentialitet, integritet, tillgänglighet och sekretess**

SOC 2-rapporten förser kunder med ett detaljerat kontrollbaserat bestyrkande, som omfattar alla fem säkerhetskategorierna för förtroendetjänster: säkerhet, tillgänglighet, behandlingsintegritet, sekretess och integritet (TSP Section 100). SOC 2-rapporten innehåller en detaljerad beskrivning av Dropbox processer och mer än 100 kontroller som vi använder för att skydda din egendom. Utöver omdömet från vår oberoende, utomstående revisor om hur våra kontroller är utformade och fungerar, innehåller rapporten granskarens testmetoder och resultaten för varje kontroll. Vår SOC 2-rapport (ibland kallad SOC 2+-rapport) innehåller även en granskad mappning av våra kontroller enligt ISO-standarderna ovan, vilken ger ytterligare transparens till våra kunder.

[Visa Dropbox för teams SOC 2-undersökning.](#)

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

SOC 1-rapporten tillhandahåller specifika garantier för kunder som ser Dropbox för team som en viktig del av sitt program för interna kontroller vid ekonomisk rapportering. Dessa specifika garantier används huvudsakligen för våra kunders efterlevnad av Sarbanes-Oxley-lagen (SOX). Den oberoende tredjepartsgranskningen genomförs i enlighet med SSAE 18 (Statement on Standards for Attestation Engagements No. 18) och ISAE 3402 (International Standard on Assurance Engagements No. 3402). Dessa standarder har ersatt inaktuella SSAE 16 (Statement on Standards for Attestation Engagement No. 16) och SAS 70 (Statement on Auditing Standards No. 70).

[Visa Dropbox för teams SOC 1-undersökning.](#)

## **CSA**

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

CSA STAR är ett kostnadsfritt, offentligt register som erbjuder ett program för säkerhetsförsäkring i fråga om molntjänster. Det hjälper användare att bedöma säkerhetstillståndet hos molnleverantörer som de använder eller överväger att börja använda.

Dropbox för team har fått både CSA STAR 2-certifiering och attestering på nivå 2. CSA STAR nivå 2 kräver en oberoende tredjepartsutvärdering av våra säkerhetskontroller som genomförts av EY CertifyPoint (för certifiering) och Ernst & Young LLP (för attestering) utifrån kraven i ISO/IEC 27001, SOC 2 Trust Service Criteria samt CSA Cloud Controls Matrix (CCM) v.4.0.2.

[Se vår certifiering och attestering för CSA STAR nivå 2 på CSA-webbplatsen.](#)

## **HIPAA/HITECH**

Dropbox kommer att teckna affärspartneravtal (BAA) med Dropbox för teams kunder som begär sådana för att kunna följa HIPAA (Health Insurance Portability and Accountability Act) och HITECH (Health Information Technology for Economic and Clinical Health Act). Mer information finns under [Dropbox och HIPAA/HITECH](#).

Dropbox tillhandahåller en bestyrkanderapport från tredje part, där våra kontroller utvärderas för regelverket för säkerhet, sekretess och anmälan om överträdelser enligt HIPAA/HITECH. Även våra interna rutiner och rekommendationer kartläggs för kunder som önskar följa regelkraven för säkerhet och sekretess enligt HIPAA/HITECH med Dropbox för team.

Kunder som är intresserade av att begära dessa dokument eller att ta reda på mer om köp av Dropbox för team kan kontakta vårt [försäljningsteam](#). Om du är teamadministratör för Dropbox för team, kan du skriva under ett BAA elektroniskt från [kontosidan i adminkonsolen](#).

Observera att möjligheten att underteckna ett elektroniskt BAA via adminkonsolen endast finns för USAbaserade kunder.

## NIST 800-171

Amerikanska [National Institute of Standards and Technology](https://www.nist.gov/(NIST)) [https://www.nist.gov/\(NIST\)](https://www.nist.gov/(NIST)) främjar och underhåller standarder och riktlinjer för att skydda informationssystem. [NIST Special Publication \(SP\) 800171 Revision 2 \(R2\)](#) ger riktlinjer för att skydda Controlled Unclassified Information (CUI) i icke-federala informationssystem och hos organisationer. Varje enhet som hanterar eller lagrar amerikansk statlig CUI, såsom forskningsinstitutioner och utbildningssektorn, bör följa NIST SP 800-171 R2. Dropboxes CUI-system, processer och kontroller validerades av en oberoende tredjepartsrevisor, Ernst & Young LLP.

NIST SP 800-171 R2-rapporten för Dropbox för team är integrerad i vår SOC 2-rapport som finns i Dropbox [Trust Center](#).

Observera att Dropbox Paper inte ingår i NIST SP 800-171 R2-rapportens omfattning.

## FERPA och COPPA (studenter och barn)

Med Dropbox för team kan kunder använda tjänster i överensstämmelse med de skyldigheter leverantören har enligt Family Education Rights and Privacy Act (FERPA). Lärosäten får endast använda Dropbox för team i enlighet med Children's Online Privacy Protection Act (COPPA).

## FDA 21 CFR Part 11

Title 21 i Code of Federal Regulations (CFR) reglerar livsmedel och läkemedel i USA för Food and Drug Administration (FDA), Drug Enforcement Administration och Office of National Drug Control Policy. Del 11 i Title 21 anger kriterierna enligt vilka FDA anser att elektroniska register och signaturer är tillförlitliga, pålitliga och i allmänhet likvärdiga med pappersregister och handskrivna signaturer som utförs på papper.

Se vår [vitbok om Dropbox och FDA 21 CFR Part 11](#) och [hjälpcenterartikel](#) för mer information om hur Dropbox kan underlätta ert efterlevnadsarbete med 21 CFR Part 11.

## PCI DSS

Dropbox efterlever kraven som handlare för Payment Card Industry Data Security Standard (PCI DSS). Dropbox för team och Dropbox Paper är emellertid inte avsedda att behandla eller lagra kreditkortstransaktioner. PCI Attestation of Compliance (AoC) för vår handlarstatus finns tillgänglig i Dropbox [Trust Center](#).

Mer information om Dropbox för teams efterlevnad finns i Dropbox [Trust Center](#).

## ISMAP

Information System Security Management and Assessment Program (ISMAP) är en japansk certifiering för användning av molnlösningar. Detta program är utformat för att utvärdera och registrera molntjänster som uppfyller de säkerhetskrav som upprättats av den japanska staten. Dess huvudmål är att säkerställa en hög säkerhetsnivå för statliga upphandlingar av molntjänster och underlätta ett smidigt införande av de molntjänster som används av den japanska staten.

Se Dropbox annons i det officiella registret över ISMAP-produkter [här](#).

## Sammanfattning

Dropbox för team erbjuder användarvänliga verktyg så att team kan samarbeta effektivt, samtidigt som tjänsten tillhandahåller de säkerhetsåtgärder och efterlevnadscertifikat som verksamheter kräver. Vårt tillvägagångssätt består av flera skikt och kombinerar en robust backend-infrastruktur tillsammans med anpassningsbara policyer. Detta ger företag en kraftfull lösning som kan skräddarsys efter deras specifika behov. Om du vill ha mer information om Dropbox för team kan du kontakta oss på [sales@dropbox.com](mailto:sales@dropbox.com).

# Dropbox Dash

Dash är en produktivitetssplattform som kombinerar smart universell sökning och kunskapshantering med djupgående åtkomstkontroll av innehåll. Dash är utformat för att hjälpa dig att [hitta](#), [skapa](#), [organisera](#), [dela](#), och [skydda](#) viktigt jobbinnehåll från SaaS- och molnapplikationer för att effektivisera produktiviteten och påskynda innehållsskapande. Administratörer kan övervaka och hantera åtkomstlistor (ACL) över anslutna jobbappar från en och samma plats. Dash bygger på en kombination av Dropbox tillförlitliga infrastruktur och ledande molntjänster.

Mer information om säkerhet i Dropbox Dash finns i [Dropbox Dash säkerhetsfaktablad](#).

# Dropbox Sign

De dokument, kontrakt och avtal ni skriver under som företag hör till de viktigaste dokumenten ni har. Många av dessa typer av transaktioner kräver en juridiskt bindande underskrift och är avgörande för ett företags verksamhet. Exempel på detta är rekryteringsdokument för nyanställda, säljaval, hyresavtal, partnerrelationer, leverantörsavtal och mycket annat. Dessa dokument innehåller ofta känslig information, så säkerheten är viktigast. Med Dropbox Sign-tjänsterna, som omfattar Dropbox Sign och Dropbox Fax, är skydd av dina dokument och relaterade transaktioner av högsta prioritet. Vi har förbundet oss att säkerställa sekretessen, säkerheten och skyddet för varje dokument som signeras med Dropbox Sign-tjänsterna.

Säkerhet omfattar ett mycket brett spektrum av ämnen, och detta faktablad ger en ganska grundlig översikt över dem alla. För kunder som köper ett visst lägsta avtalsvärde kan Dropbox arbeta med anpassade säkerhetsgranskningar, frågeformulär och bedömningar med dig.

## Kryptering

Dokument lagras bakom en brandvägg och autentiseras mot avsändarens session varje gång en begäran om det aktuella dokumentet görs. Dropbox Sign tillämpar branschens bästa praxis för överföring av data till vår plattform (Transport Layer Security TLS) och data lagras på datacenter som är certifierade med SOC 1 Type II, SOC 2 Type I och ISO 27001. Kunddokument lagras och krypteras i vila med 256 bitars AES-kryptering.

Mer information finns på vår [säkerhetssida](#).

## Granskningslogg

### Dropbox Sign-produkt

Varje underskrift på ett avtal verkställs och infogas i dokumentet. När du begär en signatur fäster Dropbox Sign en sida med en granskningslogg i själva dokumentet. Granskningsloggen innehåller en globalt unik identifierare (GUID) som kan användas för att slå upp en post i vår databas som visar vem som har undertecknat ett dokument och när. Läs vår [redogörelse rättsgiltighet](#) om du vill ha mer information.

Den manipulerings säkra granskningsloggen säkerställer att alla åtgärder i era dokument spåras och tidsstämplas noggrant så att klara bevis på åtkomst, granskning och underskrift finns.

Det finns ett antal olika granskningsloggade händelser i Dropbox Sign, bland annat:

- Dokument skickas
- Dokument visas
- Dokument signerat
- Avböj signering
- Undertecknarens namn/mejladress uppdaterad
- Bilaga laddas upp
- Personlig underskrift aktiverad
- Undertecknarens åtkomstkod autentiseras
- Avtal angående elektroniska handlingar och underskrifter har godkänts
- Begäran om underskrift delegerad
- Begäran om underskrift slutförd
- Slutförd begäran är fortgående

En aktuell lista över alla granskningsspårade händelser finns på vår [säkerhetssida](#).

## Äkthet

Dropbox Sign har tagits fram för att hålla dina dokument säkra och förhindra manipulering under och efter signaturprocessen. Med hashteknik skapar Dropbox Sign en unik post för det underliggande dokumentet innan någon part skriver under det och skapar därefter en unik post för det underliggande dokumentet med alla signaturer. Behöver du kunna bevisa att ingen manipulering har skett i dokumentet före och efter signering kan Dropbox Sign tillhandahålla två unika dokumentposter. Dropbox Sign använder samma teknik för att skydda dina e-signaturer.

## Autentisering

Vi erbjuder flera funktioner som säkerställer stark autentisering av enskilda personer så att du kan verifiera att en användare är den de säger sig vara innan du får tillåtelse att antingen utfärda ett dokument för underskrift eller verkställa en signatur.

## 2-faktorsautentisering

Användare kan konfigurera 2-faktorsautentisering vilket kräver en unik kod som genereras via Google Authenticator eller skickas till personen via sms. Denna kod måste användas utöver deras användarnamn och lösenord. Teamadministratörer kan bestämma vilken metod som används för 2-faktorsautentisering.

- Samlad inloggning är tillgängligt med ett Dropbox- eller Google-konto.
- API-nyckelbaserad autentisering för API.
- Alla lösenord hashas och saltas på ett säkert sätt.

### Sessioner löper ut efter en viss tid.

1 timme som standard, vilket kan förlängas till 30 dagar om användaren väljer **Kom ihåg mig** under inloggningen.

### Dropbox Signs produktspecifika autentiseringsfunktioner:

- **Begäran om underskrifter skyddad med åtkomstkod.** För Dropbox Sign-produkten kan användare aktivera en åtkomstkod för undertecknare (en alfanumerisk sträng med 4 till 12 tecken) som undertecknare måste ange för att kunna visa ett dokument.
- **OAuth.** Dropbox Sign API har stöd för OAuth som ett sätt att autentisera API-anrop för en användares räkning.
- **SAML.** Dropbox Sign har stöd för SAML 2.0 för samlad inloggning på företag.

# Behörigheter

Det är helt avgörande att ni kan kontrollera vem som kan göra vad i systemet.

## Dropbox Sign-produkt

Olika roller har olika åtkomsträttigheter, både i Dropbox Sign API och i slutanvändarprodukten. Administratörer kontrollerar till exempel inställningar i hela teamet, faktureringsinformation och roller.

- **Rollbaserad säkerhet.** Aktiverar olika nivåer av behörigheter för olika medlemmar i ett team, allt från administrativa rättigheter till medlemmar som bara har behörighet att se mallar och utfärda begäranden om underskrift.
- **Undertecknarspecifika åtkomstkoder.** Som ett extra säkerhetslager kan varje undertecknare tilldelas en åtkomstkod för undertecknare för ytterligare försäkran om vem som skriver under.

# Efterlevnads-certifieringar, intyg och regelefterlevnad

Dropbox Sign, inklusive planerna Dropbox Sign Standard, Premium, API Essentials, API Standard och API Premium, följer följande ramverk, standarder och förordningar:

## SOC

SOC-rapporterna (Service Organization Controls), kända som SOC 1, SOC 2 och SOC 3 är ramverk som är framtagna av AICPA (American Institute of Certified Public Accountants) för att rapportera om interna kontroller som implementeras i en organisation. Dropbox Sign har certifierat sina system, applikationer, medarbetare och processer i en serie revisioner med hjälp av den oberoende och utomstående revisionsfirman Ernst & Young LLP.

### **SOC 2 för säkerhet, tillgänglighet och sekretess.**

SOC 2-rapporten förser kunder med ett detaljerat kontrollbaserat bestyrkande, som omfattar säkerhetskriterierna för förtroendetjänster vad gäller säkerhet, tillgänglighet och sekretess (TSP Section 100). SOC 2-rapporten inkluderar en detaljerad beskrivning av Dropbox Signs processer och de fler än 100 kontroller vi har implementerat för att skydda dina kunddata. Utöver omdömet från vår oberoende, utomstående revisor om hur våra kontroller är utformade och fungerar, innehåller rapporten granskarens testmetoder och resultaten för varje kontroll.

[Visa SOC 2-undersökningen för Dropbox Sign.](#)

### **SOC 3 för säkerhet, tillgänglighet och sekretess**

SOC 3-rapporten täcker kriterierna för betrodda tjänster för säkerhet, tillgänglighet och konfidentialitet (TSP, avsnitt 100). Dropbox Signs rapport om allmän användning är en administrativ sammanfattning av SOC 2-rapporten och innehåller den oberoende, utomstående granskarens omdöme om hur våra kontroller är utformade och fungerar.

[Visa SOC 3-undersökningen för Dropbox Sign.](#)

## ISO

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

ISO/IEC 27001 är erkänt som världens främsta standard för informationssäkerhet (ISMS). Standarden utnyttjar också bästa praxis som beskrivs i ISO/IEC 27002. Eftersom vi vill behålla ditt förtroende bedriver vi hela tiden en ingående hantering av våra fysiska, tekniska och juridiska kontroller på Dropbox Sign.

[Visa DropboxSignISO/IEC 27001-certifikatet.](#)

## **ISO/IEC 27018 (molnsekretess och dataskydd)**

ISO/IEC 27018 är en internationell standard för sekretess och dataskydd som gäller för molntjänstleverantörer som Dropbox Sign som hanterar personuppgifter å sina kunders vägnar. Den blir en utgångspunkt för våra kunder vad gäller vanliga krav eller frågor beträffande föreskrifter och kontrakt.

[Visa DropboxSignISO/IEC 27018-certifikatet.](#)

## **HIPAA/HITECH**

Dropbox Sign stöder efterlevnad av Health Insurance Portability and Accountability Act (HIPAA) och HITECH (Health Information Technology for Economic and Clinical Health Act).

Dessa lagar syftar till att uppmuntra spridningen av teknik inom hälso- och sjukvårdsindustrin samtidigt som skydd skapas för säkerheten och sekretessen för hälsoinformation. Organisationer såsom sjukhus, läkar- och tandläkarmottagningar och enskilda personer som använder skyddad hälsoinformation (PHI) kan omfattas av HIPAA/HITECH. Det kan även omfatta företag som arbetar med dessa verksamheter och kommer i kontakt med skyddad hälsoinformation för deras räkning.

Dropbox Sign tillgängliggör en rapport relaterad till HIPAA-säkerhetsregeln och HITECH-kraven för överträdelsemeddelanden.

[Visa Dropbox Signs HIPAA-rapport.](#)

## **PCI DSS**

Dropbox Sign följer betalkortbranschens datasäkerhetsstandard (Payment Card Industry Data Security Standard, PCI DSS). Efterlevnadsintyget (PCI Attestation of Compliance) angående vår status som försäljare finns tillgängligt i Dropbox Signs [Trust Center](#).

## **Amerikanska E-SIGN Act från 2000**

The Electronic Signatures in Global and National Commerce Act är en federal lag som ger en allmän regel om giltighet för elektroniska register och signaturer av transaktioner. [USESIGN Act](#) kräver bland annat att det går att påvisa en avsikt om underskrift, vissa konsumentupplysningar samt registerhållning.

## Uniform Electronic Transactions Act (UETA) från 1999

Denna lag antogs 1999 av National Conference of Commissioners on Uniform State Laws. [Uniform Electronic Transaction Act](#) tillåter användningen av transaktioner via elektronisk kommunikation genom att ge elektroniska signaturer samma juridiska vikt som handskrivna papperssignaturer. UETA har antagits av alla stater utom New York.

## eIDAS-förordningen (eIDAS-förordningen för EU från 2016 (EU-förordningen 910/2014), som ersatte det tidigare EG-direktivet EG/1999/93)

eIDAS-förordningen definierar tre typer av elektroniska signaturer (SES, AES, QES) och är en ny förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den europeiska inre marknaden. Den fastställer ett regelverk som ger personer, bolag (i synnerhet små och medelstora företag) och offentlig förvaltning trygg åtkomst till tjänster och möjlighet att kunna utföra transaktioner digitalt i alla EU:s medlemsländer. Dropbox Sign har stöd för elektroniska signaturer av SES- och QES-klass. Mer information om eIDAS finns på vår [efterlevnadssida](#).

## Ramverk för dataskydd

Dropbox Sign följer dataskyddsramverken mellan EU, USA och Schweiz och USA, samt det brittiska tillägget till dataskyddsramverket mellan EU och USA, som fastställts av det amerikanska handelsdepartementet beträffande behandling av personuppgifter som överförs från den europeiska unionen, Europeiska ekonomiska samarbetsområdet, Storbritannien och Schweiz till USA. Läs mer om ramverken för dataskydd och vår certifiering på <https://www.dataprivacyframework.gov>.

## EU:s allmänna dataskyddsförordningen (GDPR)

Dataskyddsförordningen (GDPR) är en EU-förordning från 2018 som innebär en betydande förändring i förhållande till det tidigare ramverket för behandling av personuppgifter tillhörande EU:s personer. GDPR införde en rad nya eller utökade krav som gäller för företag som Dropbox som behandlar personuppgifter. Dropbox Sign följer GDPR så att kunder kan använda Dropbox Sign för att underlätta sin GDPR-efterlevnad. Få all information om GDPR-efterlevnad på vår [efterlevnadssida](#).

## Leverantörer av undertjänster

Dropbox Sign utför en granskning av våra undertjänstleverantörer minst en gång om året. Om dessa granskningar skulle få väsentliga resultat som vi bedömer utgör risker för Dropbox Sign eller våra kunder kommer vi att samarbeta med tjänstleverantören för att förstå eventuella effekter på kunddata och följa upp deras saneringsinsatser tills problemet är löst.

Vår [integritetspolicy](#) förklarar de begränsade omständigheter under vilka dina uppgifter kan delas med tredje part.

Dropbox Sign använder Amazon Web Services som IaaS-leverantör, som löpande hanterar risker och genomgår återkommande utvärderingar för att säkerställa efterlevnaden av branschstandarder (t.ex. SOC 1, SOC 2, ISO 27001).

Mer information om AWS efterlevnadsprogram finns [här](#).

Granskningar och rapporter för Dropbox Sign finns på Dropbox Signs [Trust Center](#).

### Länkar till viktiga resurser

[Dropbox Sign-sekretesspolicy](#)

[Dropbox Sign Trust Center](#)

[Dropbox Sign Security](#)

[Dropbox Sign Compliance](#)

# Dropbox DocSend

Dropbox DocSend är den säkra dokumentdelningsplattformen alla kan använda. Med bara en länk gör vi det lättare att hantera, dela och spåra dina viktiga filer. DocSends avancerade dokumentssäkerhetsfunktioner täcker dig och din känsliga information, med allt från mejlaутентisering till ett inbäddat NDA. Utöver DocSends analyser på dokumentnivå, som ger dig insikter i vem som har tittat på ditt dokument och var specifikt de har spenderat tid, inkluderar DocSends avancerade säkerhetsfunktioner godkännandelistor (begränsar åtkomsten till ditt innehåll efter domän eller e-postadress), vattenstämplar och e-postverifiering i dokumentvisning och NDA med ett klick, vilket gör det obligatoriskt att underteckna ett sekretessavtal innan ett konfidentiellt dokument visas. Kontrollera alla aspekter av dina delade filer – även efter att du har tryckt på skicka – med DocSend.

DocSend-tjänsterna har utformats med en säker, distribuerad infrastruktur som har byggts upp med flera lagers säkerhet. Vi arbetar för att säkerställa att dina data skyddas och ger våra kunder verktyg som ger kontroll och översikt.

Mer information om DocSends produktfunktioner hittar du på <https://www.docsend.com/>.

## Produktinformation

Dropbox DocSend innehåller ett brett utbud av funktioner som varierar beroende på plan. Mer information finns i [Dropbox DocSends prissättning](#). Beroende på typ av plan omfattar de funktioner som våra användare har tillgång till följande:

### Säker fildelning

Kontrollera alla aspekter av delade filer, aktivera säker fildelning med DocSend-länkar och lösenord, samt ställ in utgångsdatum för nedladdningar.

### Dynamiska vattenstämplar

Förhindrar oönskad delning, visar läsarinfo med mera.

## Virtuella datarum

Virtuella datarum (VDR) gör det möjligt att dela flera dokument med en enda länk och ge läsarna innehåll och möjlighet att ladda upp filer med eller utan DocSend-konto. De har stöd för specificerade mejladresser och domäner, såväl som åtkomstkoder och NDA-signaturer.

## E-signatur

Konvertera filer till signerbara dokument eller skapa dem direkt från DocSend. Följer e-signatur- och UETA-regler och ger stöd för flera användare och den analys som är kopplad till deras dokumentinteraktioner. När dokumentet signerats får du en granskningslogg över signeringsprocessen eller kan exportera en lista med signaturer av ett dokument.

## Sekretessavtal

Skapa sekretessavtal eller andra avtal för känsligt innehåll som kräver att läsarna lämnar sin signatur innan de får tillgång till ett dokument, även om det vidarebefordrats till någon annan.

## Användarroller

Använd användaråtkomst i flera nivåer, inklusive [rollbaserade säkerhetsbehörigheter](#). Användarna är allt från medlemmar som laddar upp och uppdaterar innehåll till administratörer som hanterar dem och deras konton. Alla planer inkluderar även en kontoägare som har åtkomst till faktureringsidan och överför kontots ägarskap.

## Användarhantering

Håll dina dokument säkra och fakturera regelbundet. DocSend-ägare och DocSend-administratörer kan lägga till, inaktivera, stänga av och återaktivera användare.

## Överför användardata

DocSend-ägare och DocSend-administratörer kan använda överföring av användardata för att flytta alla uppgifter om en avstängd eller inaktiverad användare till en annan aktiv användare och säkerställa att den inaktiva användarens länkar och dokument förblir tillgängliga.

## Samlad inloggning

Team kan logga in säkert via Okta eller OneLogin via SAML 2.0, med vilket DocSend också stöder SCIM för användaretablering.

## Underteam

Använd underteam för att organisera och ge åtkomst till specifikt innehåll som är relevant för varje team i en organisation. Detta skyddar innehållet och säkerställer att endast behöriga användare kan komma åt det. Åtkomst till mappar kan även hanteras av underteam.

# Kryptering

DocSend skyddar data under överföringen mellan våra appar och våra servrar, och i viloläge. Dokument lagras bakom en brandvägg och autentiseras mot avsändarens session varje gång en begäran om det aktuella dokumentet görs. Vi tillämpar branschens bästa praxis för överföring av data till vår plattform Transport Layer Security, (TLS) och data lagras i datacenter som är certifierade med SOC 1 typ II, SOC 2 typ I och ISO 27001. Dina dokument lagras och krypteras i vila med 256 bitars AES-kryptering.

# Granskningslogg

I anslutning till DocSends e-signaturtjänster säkerställer en granskningslogg att varje åtgärd spåras och tidsstämplas, vilket ger rimliga bevis på åtkomst, granskning och signatur. Dessa poster inkluderar en hash-kod av PDF-dokumentet som vi kan jämföra med hash-koden för ett tvivelaktigt PDF-dokument för att avgöra om det har modifierats, manipulerats eller inte.

# Autentisering

Vi erbjuder flera funktioner som säkerställer stark autentisering av enskilda personer så att du kan verifiera att en användare är den de säger sig vara innan de får tillgång till ditt innehåll, får tillåtelse att utfärda ett dokument för underskrift eller verkställa en signatur.

## Alla lösenord hashas och saltas på ett säkert sätt

## Enkel inloggning

DocSend kan konfigureras för att ge teammedlemmarna åtkomst genom inloggning via en central identitetsleverantör. Vår SSO-implementering använder Security Assertion Markup Language 2.0 (SAML 2.0), vilket gör etableringen enklare och säkrare genom att en betrodd identitetsleverantör autentiserar och ger teammedlemmar åtkomst till Dropbox utan ytterligare lösenord att hantera.

## DocSends produktspecifika autentiseringsfunktioner

- **Lösenordsskyddad fildelning:** användare kan ställa in en lösenord, verifiera dem via mejl och begränsa åtkomsten för att säkerställa att bara rätt personer kan se deras filer. Användare kan också ställa in utgångsdatum och aktivera eller inaktivera möjligheten att ladda ner filerna.
- **Styr åtkomst med avtal:** användare kan styra åtkomst till innehåll med ett avtal, till exempel ett sekretessavtal.

# Behörigheter

Det är helt avgörande att ni kan kontrollera vem som kan göra vad i systemet.

## DocSend-produkt

Olika roller har olika åtkomsträttigheter. Administratörer kontrollerar till exempel inställningar i hela teamet, faktureringsinformation och roller.

- **Rollbaserad säkerhet:** möjliggör olika nivåer av behörigheter för olika medlemmar i ett team, allt från administrativa rättigheter till medlemmar.
- **Underteam:** Med DocSend-underteam kan användare ge åtkomst till specifikt innehåll som är relevant för varje team i en organisation. Underteam håller känsligt innehåll säkert och ser till att endast behöriga användare har åtkomst till det.

# Efterlevnads-certifieringar, intyg och regelefterlevnad

Dropbox DocSend, inklusive Dropbox-planerna DocSend Personal, DocSend Standard, DocSend Advanced och DocSend Advanced Data Rooms, följer följande ramverk, standarder och förordningar:

## SOC

SOC-rapporterna (Service Organization Controls), kända som SOC 1, SOC 2 och SOC 3 är ramverk som är framtagna av AICPA (American Institute of Certified Public Accountants) för att rapportera om interna kontroller som implementeras i en organisation. Dropbox DocSend har certifierat sina system, applikationer, medarbetare och processer i en serie revisioner med hjälp av den oberoende och utomstående revisionsfirman Ernst & Young LLP.

### **SOC 2 för säkerhet**

SOC 2-rapporten förser kunder med ett detaljerat kontrollbaserat bestyrkande, som omfattar säkerhetskriterierna för förtroendetjänster (TSP, avsnitt 100). SOC 2-rapporten inkluderar en detaljerad beskrivning av Dropbox DocSend-processerna och de fler än 100 kontroller vi har implementerat för att skydda dina kunddata. Utöver omdömet från vår oberoende, utomstående revisor om hur våra kontroller är utformade och fungerar, innehåller rapporten granskarens testmetoder och resultaten för varje kontroll.

[Visa SOC 2-undersökningen för Dropbox DocSend.](#)

### **SOC 3 för säkerhet**

SOC 3-rapporten täcker säkerhetskriterierna för betrodda tjänster (TSP, avsnitt 100). Dropbox DocSends rapport om allmän användning är en administrativ sammanfattning av SOC 2-rapporten och innehåller den oberoende, utomstående granskarens omdöme om hur våra kontroller är utformade och fungerar.

[Visa SOC 3-undersökningen för Dropbox DocSend](#)

## PCI DSS

Dropbox DocSend följer betalkortbranschens datasäkerhetsstandard (Payment Card Industry Data Security Standard, PCI DSS). Efterlevnadsintyget (PCI Attestation of Compliance) angående vår status som försäljare finns tillgängligt i Dropbox DocSends [Trust Center](#).

### **Ramverk för dataskydd**

Dropbox DocSend följer dataskyddsramverken mellan EU och USA och Schweiz-USA, samt det brittiska tillägget till dataskyddsramverket EU-USA, som fastställts av det amerikanska handelsdepartementet avseende behandling av personuppgifter som överförs från den europeiska unionen, Europeiska ekonomiska samarbetsområdet, Storbritannien och Schweiz till USA. Läs mer om ramverken för dataskydd och vår certifiering på <https://www.dataprivacyframework.gov>.

### **EU:s allmänna dataskyddsförordningen (GDPR)**

Dataskyddsförordningen (GDPR) är en EU-förordning från 2018 som innebär en betydande förändring i förhållande till det tidigare ramverket för behandling av personuppgifter tillhörande EU:s personer. GDPR introducerade en rad nya eller utökade krav som gäller för företag som Dropbox som behandlar personuppgifter. Dropbox DocSend uppfyller GDPR-kraven så att våra kunder kan använda Dropbox DocSend för att underlätta sin egen GDPR-efterlevnad.

# Leverantörer av undertjänster

Dropbox DocSend utför en granskning av våra undertjänstleverantörer minst en gång om året. Om dessa granskningar skulle få väsentliga resultat som vi bedömer utgör risker för Dropbox DocSend eller våra kunder, kommer vi att samarbeta med tjänstleverantören för att förstå eventuella effekter på kunddata och följa upp deras saneringsinsatser tills problemet är löst.

Vår [integritetspolicy](#) förklarar de begränsade omständigheter under vilka dina uppgifter kan delas med tredje part.

Dropbox DocSend använder Amazon Web Services för SaaS och IaaS, som löpande hanterar risker och genomgår återkommande utvärderingar för att säkerställa efterlevnaden av branschstandarder (t.ex. SOC 1, SOC 2, ISO 27001). Dessutom utvärderas PaaS genom Heroku också av oberoende personer genom utvärderingar av tredje part (till exempel SOC 1, SOC 2, ISO 27001).

Mer information om AWS efterlevnadsprogram finns [här](#).

Granskningar och rapporter för Dropbox DocSend finns i Dropbox DocSends [Trust Center](#).

Dessutom har DocSend genomgått den rigorösa säkerhetsgranskning som tagits fram av Salesforce för att kunna listas i Salesforce AppExchange.

## Länkar till viktiga resurser

[Villkor för Dropbox DocSend](#)

[Dropbox DocSends integritetspolicy](#)

[Dropbox DocSends upphovsrätts- och IP-policy](#)

[Dropbox DocSends kakpolicy](#)

# Reclaim.ai

Reclaim.ai är ett produktivitetstverktyg som hjälper individer, team och företag att anpassa sina kalendrar efter deras prioriteringar, så att de kan ägna sig åt de saker som betyder mest. Reclaim tillhandahåller en flexibel och kraftfull schemaläggningslösning med artificiell intelligens (AI) för Google Kalender och Microsoft Outlook-kalendern som hjälper företag och individer att spara tid som i stället kan läggas på viktigt arbete, optimering av möten, minskning av kostsamma avbrott och förbättring av balansen mellan arbete och fritid.

Reclaim.ai är helt molnbaserat med en primär infrastruktur som drivs i Amazon AWS med alla data på datacenter/regioner i USA. Reclaim utnyttjar främst serverlösa AWS-tjänster som AWS RDS Aurora för databaslagring, AWS API Gateway, AWS MSK för Streaming Kafka, AWS ElastiCache för Redis-cachelagring och AWS ECS Fargate för alla arbetsbelastningar. Reclaim använder Java med Micronaut som backend-stack och TypeScript med React för frontend.

Säkerhets- och integritetsåtaganden gentemot användare och tredje part är grundläggande för Reclaim.ai-uppdrag. Data skyddas genom flera säkerhetsåtgärder, med alla data krypterade under överföring och krypterade i vila, olika autentiseringsåtgärder inklusive SSO och Google/Microsoft-autentisering, SCIM (System for Cross-domain Identity Management), JWT-sessionstoken, multifaktorautentisering (MFA) för administratörsåtkomst och SOC 2 typ II-efterlevnad, rapportering, introduktion och support. Adminportalen kräver MFA- och API-nycklar, och API-nycklar går ut efter en vecka. Ytterligare information om Reclaims säkerhets- och integritetspolicyer, rutiner och tekniska implementeringar finns i Reclaim SOC2 Type II-rapporten som finns i [Reclaim Trust Center](#).

# Kryptering från slutpunkt till slutpunkt

Kryptering från slutpunkt till slutpunkt (E2EE) är nu tillgängligt i Dropbox för team. Med E2EE för utvalda teammapor kan kunderna följa förordningar, skydda immateriella rättigheter och öka tilliten till säkerhet på enheter. Kryptering från slutpunkt till slutpunkt ger en säker miljö för delning och samarbete med känsliga data, vilket förhindrar obehörig avlyssning och intrång från externa parter, och till och med Dropbox själv. Med E2EE genereras krypterings- och dekrypteringsnycklar på användarens enhet. Detta innebär att informationen krypteras på själva användarens enhet innan den skickas till Dropbox serverar. Genom att integrera kryptering från slutpunkt till slutpunkt kan företag på ett tryggt sätt utnyttja Dropbox och samtidigt minimera riskerna för obehörig åtkomst och äventyrande av data.

## Protokollroller

### Dropbox-serverar (PKI, datalagring, protokollsamordning)

Vi antar att varje server är en unik enhet. Dess syfte är att lagra och distribuera offentliga nycklar och krypterade privata eller symmetriska nycklar. Den är en kärnkomponent i vårt PKI (EKMS eller Encrypted Key Management System). Den lagrar mapor, filer och deras metadata och ansvarar för regelbunden, icke-kryptografisk auktorisering och autentisering.

### Team (filägare)

Ett team är en samling användare som kryptografiskt representeras av en delad kryptografisk teamnyckel. Teamet äger sina filer och protokollet säkerställer att medlemmarna endast kan komma åt de filer som teamet äger.

### Användare

Användare bidrar till teamets filsamling. De autentiseras till Dropbox server och deltar i protokollet via sina enheter. Protokollet säkerställer att de endast kan komma åt filer som deras team äger.

### Administratörer

Administratörer är en del av alla användare. De auktoriseras genom regelbunden auktorisering (t.ex. ACL) för att hantera parametrar och användare för sitt team. Ur ett kryptografiskt perspektiv har de tillgång till en återställningsnyckel vilket gör att de kan utföra kryptografiska åtgärder, som att registrera nya användare eller enheter, även om de själva inte har några registrerade enheter.

### Enheter

Enheter erbjuder ett gränssnitt så att användaren kan delta i protokollet. Enheter är "betrodna" på så vis att de bedöms kunna lagra och skydda hemlig information, som kryptografiska nycklar.

## Dropbox medarbetare

Dropbox medarbetare deltar inte direkt i protokollet, men har utökad åtkomst till Dropbox-servern. Vi skiljer på medarbetare med läsbehörighet, medarbetare med skrivåtkomst till en användares data och medarbetare med möjlighet att ändra serverns/protokollets beteende.

## Tredje parter

Tredje parter deltar inte direkt i protokollet. Detta är med andra ord enheter som inte är behöriga att komma åt en användares filer. Protokollet säkerställer att de inte kan dekryptera användarens filer. På detta sätt skyddar den användare från alla slags hotaktörer.

## Medarbetarpolicy och åtkomst

Efter anställningen måste samtliga Dropbox-medarbetare genomgå en bakgrundskontroll och underteckna en bekräftelse av säkerhetspolicyn och ett sekretessavtal, samt genomgå säkerhetsutbildning. Beroende på varje enskild persons arbetsroll och ansvarsområden kan de få fysisk och/eller logisk åtkomst till företags- och produktionsmiljöer. Medarbetaråtkomst återkallas omedelbart när en medarbetare lämnar företaget. Dessutom måste samtliga medarbetare slutföra en obligatorisk årlig säkerhetsutbildning och de får regelbunden utbildning om säkerhetskännedom via informationsmejl, samtal och presentationer och resurser som finns på intranätet och vår utbildningsportal.

Medarbetaråtkomst till Dropbox-miljön upprätthålls och autentiseras med en kombination av starka lösenord, lösenfrasskyddade SSH-nycklar och tvåfaktorsautentisering. Fjärråtkomst kräver VPN som skyddas av tvåfaktorsautentisering och all specialåtkomst granskas och behandlas av vårt säkerhetsteam. Åtkomsten till företags- och produktionsnätverk är strikt begränsad baserat på fastställda policyer. Åtkomsten till produktionsnätverk är exempelvis baserad på SSH-nycklar och är begränsad till teknikteam som måste ha åtkomst för att kunna utföra sina arbetsuppgifter. Brandväggskonfiguration sker under rigorös kontroll och är begränsad till ett fåtal administratörer.

Våra interna policyer kräver dessutom att medarbetare som använder produktions- och företagsmiljöer följer bästa praxis för skapande och lagring av privata SSH-nycklar. Åtkomst till andra resurser, inklusive datacenter, funktioner för serverkonfiguration, produktionsservrar och funktioner för utveckling av källkod tilldelas genom uttryckligt godkännande från lämplig chef. En kopia av åtkomstförfrågan, motivering och godkännande registreras av ledningen och åtkomsten beviljas av lämpliga personer.

Dropbox använder tekniska åtkomstkontroller och interna policyer för att hindra medarbetare från att godtyckligt komma åt användares filer och för att begränsa åtkomsten till metadata och andra uppgifter om kryptering från slutpunkt till slutpunkt. För att skydda slutanvändarnas integritet och säkerhet har endast ett litet antal tekniker som ansvarar för utvecklingen av Dropbox grundläggande kryptering från slutpunkt till slutpunkt åtkomst till produktionsmiljön.

När Dropbox blir en förlängning av våra kunders infrastruktur kan de lita på att vi förvaltar deras data på ett ansvarsfullt sätt.

## Mål- och hotmodell

### Mål

Kryptering från slutpunkt till slutpunkt skyddar användare från en definierad uppsättning scenarier och ökar förtroendet för Dropbox. Dessa scenarier beskrivs i vår hotmodell nedan.

**Viktigt:** Det här dokumentet omfattar endast kryptografiskt skydd. Vanliga mekanismer för åtkomstkontroll kommer att komplettera protokollet, till exempel genom att möjliggöra en finare åtkomstkontroll för enskilda teammedlemmar. Alla protokollroller använder en säker kommunikationskanal (till exempel TLS 1.2) för att kommunicera med servern.

### Hotmodell

Protokollet för kryptering från slutpunkt till slutpunkt måste säkerställa följande:

- Sekretess vad gäller Dropbox Server.
- Sekretess vad gäller Dropbox medarbetare.
- Sekretess vad gäller andra team, deras användare och tredje part.
- Krypterade filers integritet för ändringar.
- Tillgänglighet för krypterade filer utanför servermiljön
- Sekretess för nya filer eller ändringar efter en nyckelväxling (när en tidigare teammedlem inte längre är betrodd, är ofta befintliga filer att betrakta som äventyrade, och från och med den tidpunkten bör sekretess säkerställas genom nyckelrotation).
  - Enheter måste inte vara online för att en nyckelrotation ska kunna genomföras, vilket gör rotationsprocessen ganska snabb.

### Minskad hotmodell genom att inaktivera nyckelverifiering

Nyckelverifiering kräver verifieringar utanför bandet, vilket kan vara opraktiskt i vissa användnings-scenarier. För att ta hänsyn till dessa scenarier är nyckelverifiering valfri. Om nyckelverifiering inaktiveras minskas hotmodellen enligt följande:

- **Integritet och sekretess** kan inte längre garanteras mot aktivt skadlig Dropbox-server, eller mot Dropbox-medarbetare med skrivåtkomst till användardata (dvs. mot aktiva attacker).

### Motiv

Kryptering från slutpunkt till slutpunkt har utformats för att balansera informationssäkerhetsbehoven i form av datasekretess, integritet och tillgänglighet, utökat med användbarhet så att teamets produktivitet inte skulle hämmas.

## Den teamcentrerade strategin

Om den kryptografiska säkerhetsgränsen dras runt den enskilda användaren läggs ansvaret för nyckeln på denna användare. Dataförlust på grund av nyckelförlust är en risk för krypterade system från slutpunkt till slutpunkt, och att användare kan bli av med sina nycklar medför risk för tillgängligheten till företagets data. Lösningar för denna risk finns, men de ökar komplexiteten hos produkten och minskar dess användbarhet, särskilt med tanke på att funktionen fungerar i en asynkron miljö som endast sker för team.

Med en säkerhetsgräns kring teamet har vi ett skyddslager: Så länge en användare fortfarande har åtkomst till teamnyckeln kan alla data återställas, även om en eller flera användare förlorar åtkomsten till nyckeln. Dessutom förbättrar det teamcentrerade tillvägagångssättet användarupplevelsen, förenklar protokollets komplexitet, vilket minskar risken för säkerhetsproblem.

## Automatisk enhetsregistrering

Att manuellt installera kryptering från slutpunkt till slutpunkt på en ny enhet kan vara en stor utmaning för icke-tekniska användare, vilket ger låg användningsgrad. Genom att utnyttja registreringar från enhet till enhet som autentiseras med Dropbox standardmekanismer för autentisering och åtkomstkontroll, befrias användarna från denna börda genom definierade hot- och förtroendemodeller.

## Begränsningar

- Klienter anses vara pålitliga, vilket är ett vanligt antagande för kryptering från slutpunkt till slutpunkt. Detta beror på att klienten är mindre dynamisk och anses manuellt godkänd i installationsprocessen. Säkerhetsgarantierna som webbklienten erbjuder är svagare än de som erbjuds av inbyggda applikationer eftersom de levereras mer dynamiskt.
- Enskilda filers uppdateringar kan inte garanteras, eftersom det inte går att kryptografiskt bevisa att en fil är dess senaste version.

## Förtroendemodell

- Användare i ett team är betrodda och åtkomstbegränsningar mellan dem tillämpas inte kryptografiskt utan genom ACL.
- Användaren ansvarar för att hålla sin enhet säker.
- Funktionen för kryptering från slutpunkt till slutpunkt ger kryptografiskt skydd mot alla andra, inklusive Dropbox.

**Viktigt:** När nyckelverifiering är inaktiverat utökas förtroendet för Dropbox server och medarbetare med skrivåtkomst. Genom att följa protokollet levererar servern rätt nycklar för varje filåtgärd och eventuella angripare med tillgång till en Dropbox-databas kan inte få reda på något om teamets filinnehåll. På samma sätt kan Dropbox inte dekryptera data i vila.

## Samarbete med ordinarie åtkomstkontroll

Funktionen för kryptering från slutpunkt till slutpunkt är en säkerhetsförbättring som kompletterar befintliga mekanismer för åtkomstkontroll. I detta avsnitt beskrivs hur standardsäkerhetsfunktionerna i Dropbox fungerar med kryptering från slutpunkt till slutpunkt.

### Teamintern åtkomstkontroll

Funktionen för kryptering från slutpunkt till slutpunkt skyddar mot hot utanför ett team. Som sådant krävs eller implementeras inget kryptografiskt skydd mellan medlemmar i samma team. Åtkomstkontroll bland medlemmar i samma team implementeras utanför protokollet, genom vanliga ACL:er.

### Skyddsstatus för filer när en medlem lämnar teamet

Fram till den punkt då en medlem lämnar ett team har denna teammedlem haft åtkomst till alla teamfiler, vad gäller protokollet. Nytt innehåll krypteras med en ny nyckel. Vanlig åtkomstkontroll blockerar åtkomsten till filer som den tidigare teammedlemmen hade tillgång till utan dröjsmål.

## Primitiver, typer och definitioner för kryptografi

### Nycklar och nyckelmateriel

Alla nycklar och viktigt material skapas på enheten.

### Enhetsnyckelpar

Ett enhetsnyckelpar representerar ett asymmetriskt kryptografiskt nyckelpar som består av en offentlig enhetsnyckel och en privat enhetsnyckel. Nyckelparen skapas alltid på enheten och den privata enhetsnyckeln måste krypteras innan den lämnar enheten. Nyckelpar för enheter antingen lagras på Dropbox servrar (krypteras), finns kvar på enheten eller kan exporteras för säkerhetskopiering.

### Datanyckel

En enhet krypterar alla slags data med symmetriska datanycklar. Varje dataenhet (till exempel en fil) krypteras med en ny, unik datanyckel. Symmetriska nycklar lagras aldrig okrypterade på Dropbox servrar. De krypteras alltid av en annan nyckel.

Använd algoritm är Blockwise AES-GCM.

## Algoritm för nycklar

### Symmetriska nycklar

För all symmetrisk kryptering används AES-256-GCM med en 128 bitars autentiseringstagg och en 96 bitars nonce. Nonce genereras slumpmässigt på enhetssidan.

## Asymmetriska nycklar

- För all asymmetrisk kryptering används HPKE, single shot, basläge med kem (Kem.DhkemP256HkdfSha256, kdf: Kdf.HkdfSha256, aead: Aead.Aes256Gcm).
- När nyckelverifiering är aktiverad läggs aad: utf8(algorithmID) till och HPKE-**autentiseringsläget** används för att kryptera namnutrymmet och filnycklar.
  - Nyckelverifieringen för teamnyckeln utförs underförstått utanför bandet.
  - Avsändaren för namespace-nyckelns kryptering är teamets privata nyckel.
  - Avsändaren för namespace-nyckelns kryptering är teamets privata nyckel.

## Encrypted Key Management System (EKMS)

EKMS (Encrypted Key Management System) är en kryptografisk nyckelhanteringslösning utformad för både säkerhet och effektivitet. EKMS bevarar datasekretess genom kryptering på klientsidan, och följer nollkunskapsprincipen strikt. Detta säkerställer att alla kryptografiska nycklar är säkert krypterade på enheten, vilket gör dem oanvändbara på serversidan. Följaktligen skapar EKMS en robust kryptering från slutpunkt till slutpunkt.

EKMS använder en "teamcentrerad nyckelhantering", där varje användare i ett team beviljas kryptografisk åtkomst till andra nycklar i det specifika teamet. På det sättet kan du säkerställa effektiv nyckelhantering samtidigt som säkerheten bibehålls.

EKMS säkerställer att varje teammedlem med kryptografisk åtkomst till teamnycklar också har åtkomst till alla filnycklar. Åtkomst till krypterade binära data (krypterade filer) regleras dock fortfarande av strikta åtkomstkontroller. Om en teammedlem saknar åtkomsträttigheter kommer hen inte att kunna ladda ner krypterade binära data.

## Typer av nycklar i EKMS

### Filnyckel

Filnycklar är symmetriska nycklar. Enheter har flexibiliteten att specificera den kryptografiska algoritmen som de ska använda. Dessa nycklar genereras på enheten och krypteras innan de överförs till servern. Detta säkerställer att nycklarna och den information de skyddas förblir konfidentiell.

### Krypterade teamappsnycklar

Krypterade teamappsnycklar är asymmetriska nycklar som tilldelas mappar som skyddas med kryptering från slutpunkt till slutpunkt. Enheter kan definiera de kryptografiska algoritmer som används för dessa nycklar. Dessa nycklar genereras på enheten och den privata nyckeln krypteras med den aktiva teamnyckeln innan den överförs på ett säkert sätt till servern.

## Teamnyckel

Teamnycklar är också asymmetriska och tilldelas specifikt till team. Dessa nycklar genereras på enheten och skyddas ytterligare genom att den privata nyckeln krypteras med återställnings- och enhetsnycklar innan de skickas till servern.

## Enhetsnyckel

Enhetsnycklar är asymmetriska nycklar som tilldelas unikt till enskilda enheter och ägs av en användare. Endast den offentliga nyckeln registreras på servern, medan den privata nyckeln bara finns kvar på enheten. Dessa nycklar används för att kryptera teamnycklar i en användares team.

## Återställningsnyckel

Återställningsnycklar är asymmetriska nycklar som allokeras till ett visst team och genereras av en administratör. Administratörer kan ta bort återställningsnycklar, men minst en återställningsnyckel måste behållas hela tiden. Precis som med enhetsnycklar registreras endast den offentliga nyckeln på servern och den privata nyckeln lagras säkert av administratören.

## Dekryptering av privata nycklar

När en privat nyckel avkrypteras och dess offentliga nyckel tillhandahålls separat, verifieras den privata nyckeln mot den offentliga nyckeln och användning av den avkrypterade nyckeln avslås vid felaktig matchning.

## Teamregistrering

För att förbättra säkerheten och effektiviteten i vår teamregistreringsprocess har vi implementerat en design som säkerställer skydd av kritiska kryptonycklar.

Processen börjar med genereringen av ett återställningsnyckelpar på enheten. Den privata nyckeln presenteras sedan på ett säkert sätt för administratören för förvaring.

Den offentliga återställningsnyckeln registreras på servern, ett nytt teamnyckelpar genereras på enheten och den privata teamnyckeln krypteras med återställningsnyckeln.

**När nyckelverifiering har aktiverats**, visas ett fingeravtryck av den offentliga teamnyckeln för administratören som måste sändas utanför bandet till alla medlemmar i teamet som ännu inte behöver registreras.

För att slutföra registreringen av teamet registreras teamets offentliga nyckel och den krypterade privata nyckeln på servern. Dessa steg resulterar i ett färdigt team.

## Enhetsregistrering

Registreringsprocessen för enheter består av två delar:

1. En enhet som begär åtkomst till en krypterad teammapp. Detta steg består i att man lokalt genererar och registrerar unika enhetsnycklar.
2. En redan registrerad enhet eller en administratör som ger enheten åtkomst genom att kryptera den privata teamnyckeln igen för de tidigare registrerade enhetsnycklarna.

### **Enheten begär åtkomst enligt följande (detta motsvarar steg 1):**

1. En enhet registreras genom att generera ett unikt nyckelpar, bestående av en offentlig och en privat nyckel, på den lokala enheten.
2. Enheten skyddar den privata nyckeln på enheten, eftersom den är nyckeln till att dekryptera känslig information.
3. Enhetens offentliga nyckel har registrerats på servern.

**Obs:** När nyckelverifiering är aktiverad måste användaren på begäran av administratören skicka enhetens offentliga nyckelfingeravtryck utanför bandet. Enheten identifierar det faktum att nyckelverifiering är aktiverad och visar teamnyckeln och enhetens fingeravtryck för användaren. Administratören måste meddela användaren nödvändigheten att verifiera teamnyckelns fingeravtryck och vidarebefordra enhetens fingeravtryck. Enheten kommer ihåg teamnyckelns fingeravtryck när det har godkänts av dess användare.

### **En redan registrerad enhet ger åtkomst enligt följande (detta motsvarar steg 2):**

**Obs:** En auktoriserad enhet kan registrera nya enheter. En sådan auktoriserad enhet kan vara en redan registrerad enhet eller administratören som använder återställningsnycklar i adminkonsolen. Om nyckelverifieringsfunktionen är aktiverad stöds endast den senare metoden.

1. Den auktoriserade enheten hämtar den nya enhetens offentliga nyckel från servern. När nyckelverifiering är aktiverad kan endast administratören registrera den nya enheten. I så fall verifierar administratören fingeravtrycket för den mottagna publika nyckeln utanför bandet med det som visas på registreringsenheten.
2. Den auktoriserade enheten läser också in den krypterade privata teamnyckeln från servern eller hämtar den från sin cache.
3. Den auktoriserade enheten dekrypterar den privata teamnyckeln med sin egen privata nyckel eller återställningsnyckel. När nyckelverifiering är aktiverad verifierar den att den avkrypterade privata teamnyckeln passar det lokalt lagrade fingeravtrycket för teamnyckeln.
4. Den auktoriserade enheten tar den avkrypterade privata teamnyckeln och omkrypterar den med den nya enhetens offentliga nyckel. Det här steget säkerställer att endast den nya enheten med motsvarande privata nyckel kan komma åt teamnyckeln.
5. Den omkrypterade privata teamnyckeln har registrerats på servern.

**Obs:** När nyckelverifiering är aktiverad och om servern vid någon tidpunkt levererar en krypterad teamnyckel med ett annat fingeravtryck varnar enheten användaren om detta och kräver en bekräftelse på den nya teamnyckelns giltighet. Detta kan hända under ett nyckelväxling. I det här fallet skulle den nya teamnyckelns fingeravtryck ha delats ut utanför bandet under rotationsprocessen.

6. I fall där en registrerad enhet kanske inte är tillgänglig under registreringsprocessen kan administratörer utnyttja konceptet med återställningsnycklar. Denna metod gör det möjligt att registrera nya enheter på ett säkert sätt även när befintliga enheter är offline eller inte är tillgängliga. För närvarande går det endast att registrera enhet med nyckelverifiering aktiverad i adminkonsolen med återställningsnycklar.

7. När nyckelverifiering är inaktiverad och registrerade enheter är online laddar de automatiskt ner de offentliga nycklarna för enheterna som ska registreras och initierar sömlöst registreringsprocessen i bakgrunden. Detta effektiviserade tillvägagångssätt säkerställer att enhetsregistrering kan ske effektivt och säkert.

## Lägger till återställningsnycklar

En administratör kan lägga till flera återställningsnycklar.

### Följ dessa steg för att skapa en ny återställningsnyckel:

1. Till att börja med måste administratören ha åtkomst till en befintlig återställningsnyckel. Denna befintliga nyckel är en förutsättning för att lägga till en ny.
2. I webbläsaren genereras ett nytt återställningsnyckelpar. Detta nyckelpar innehåller en offentlig nyckel och en privat nyckel. Den privata nyckeln kommer att användas i senare steg.
3. Den nyligen genererade offentliga återställningsnyckeln har registrerats på servern. Detta steg säkerställer att systemet känner igen och associerar den nya nyckeln till teamet.
4. Administratören måste ange den befintliga privata återställningsnyckeln.
5. När den befintliga privata återställningsnyckeln har angetts hämtar du den krypterade privata teamnyckeln. Den här nyckeln krypteras med den angivna återställningsnyckeln.
6. Dekryptera den privata teamnyckeln med den angivna befintliga privata återställningsnyckeln. Detta ger åtkomst till den privata teamnyckeln.
7. Kryptera sedan den privata teamnyckeln med den nyligen genererade offentliga återställningsnyckeln. Det här steget säkerställer att den privata teamnyckeln nu associeras med den nya återställningsnyckeln.
8. Slutligen registrerar du den krypterade privata teamnyckeln på servern. Denna åtgärd slutför processen med att skapa en ny återställningsnyckel och säkerställer att den nya nyckeln säkert lagras och identifieras av servern för framtida återställningsändamål.

## Nyckelhantering och rotation

**Obs:** För närvarande utesluter nyckelrotation och nyckelverifiering varandra, det vill säga du kan inte ha båda aktiverade.

### Återkallande av åtkomst

För närvarande är återkallande av åtkomst inte implementerat. Teammedlemmar kan tas bort men är, ur kryptografisk synpunkt, begränsade från att fortsätta komma åt filerna genom vanliga ACL:er. Här följer konceptet för återkallande av åtkomst som kommer att implementeras i framtiden.

Återkallande av åtkomst är en viktig säkerhetsfunktion som säkerställer kontrollerad radering av både enhets- och återställningsnycklar. Det säkerställer att tidigare teammedlemmar inte kan

äventyra säkerheten för teamets data genom kryptering. Denna process spelar en grundläggande roll för att upprätthålla uppgifternas integritet och sekretess. Återkallande av åtkomst omfattar följande aspekter:

**Återkallande av återställningsnycklar:** Auktoriserade administratörer har möjlighet att återkalla återställningsnycklar. När en teamnyckelrotation initieras krypteras den nya teamnyckeln inte igen med den offentliga återställningsnyckeln som påverkas. Detta garanterar säkerheten för nyskapade eller modifierade filer.

**Återkallande av enhetsnycklar:** När en användare lämnar teamet kan en teamnyckelrotation initieras och den nya teamnyckeln omkrypteras inte med den berörda enhetens offentliga nyckel.

**Nyckelrotation:** Nyckelrotation är en nödvändig process för att upprätthålla säkerheten och sekretessen för våra uppgifter. Det tillhandahåller en mekanism för att uppdatera krypteringsnycklar.

**Förutsättning – återkallad åtkomst:** Nyckelrotation är beroende av återkallad åtkomst. Innan nycklar kan roteras måste alla användar- eller återställningsnycklar som behöver återkallas antingen raderas eller markeras som inaktiverade.

**Administratörskontrollerad nyckelrotation:** Administratörer har möjlighet att initiera nyckelrotation via administratörskonsolen.

Följande steg krävs för att rotera nycklarna:

#### 1. Roter teamnyckel:

- a. En ny teamnyckel skapas lokalt.
- b. Det nya teamets nyckelfingeravtryck visas för administratören för distribution utanför bandet **(endast nyckelverifiering aktiverad)**
- c. Alla tillgängliga och aktiva återställningsnycklar och enhetsnycklar hämtas från servern. Om nyckelverifiering är aktiverad valideras enhetens offentliga nyckelfingeravtryck utanför bandet av administratören
- d. Teamets nya privata nyckel krypteras igen med **alla aktiva återställnings- och enhetsnycklar** för att bibehålla dataåtkomsten.

**2. Roter namnrymdsnycklar:** En ny namnrymdsnyckel införs för varje befintlig namnrymd. Den nya nyckeln krypteras med det nya teamets offentliga nyckel.

**3. Aktivera teamnyckel:** När den nya teamnyckeln krypteras med alla aktiva återställnings- och enhetsnycklar och krypterar alla nya namnrymdsnycklar markeras den som aktiv. Det innebär att den kommer att användas för krypteringsåtgärder.

**4. Utgångsdatum och användning:** Befintliga teamnycklar, namnrymdsnycklar och filnycklar upphör att gälla. Utgångna nycklar kommer inte längre att vara tillåtna för krypteringsåtgärder. De kan endast användas för dekrypteringsåtgärder.

**5. Förbjuda filbeslut med befintliga filnycklar:** I situationer där filnycklar har gått ut kommer filåtkomst att avvisas. Enheterna måste generera nya filnycklar och kryptera innehållet igen innan de laddas upp igen. Detta säkerställer att inga känsliga uppgifter äventyras med användning av föråldrade krypteringsnycklar.

- 6. När nyckelverifiering är aktiverad** verifierar och bekräftar användare att deras enhet använder den nya teamnyckeln genom det teamnyckelfingeravtryck som distribuerats utanför bandet och deras enhet kan visa den teamnyckel som för närvarande används.

## Extern delning

Extern delning ger kryptografiskt skydd vid samarbete med ett annat team när båda har kryptering från slutpunkt till slutpunkt aktiverad.

### Dela med externa team

Externa team måste registreras i kryptering från slutpunkt till slutpunkt, vilket innebär att de har ett giltigt teamnyckelpar. Delning sker sedan på teammappsnivå genom att teamets privata nyckel krypteras med det externa offentliga teamets nyckel. Detta ger det externa teamet kryptografisk åtkomst till teammappen och dess innehåll.

### Nyckelrotation för externa delningar

Nyckelrotation utförs enligt beskrivningen ovan, med början i teamnyckeln för det team som roterar. Till exempel, om team A har en delad mapp med team B och team B roterar sina nycklar, kommer nycklarna i den delade mappen också att roteras. Den nya nyckeln till delade mappar delas automatiskt med team A igen för att ge åtkomst för båda team. Detta ger kryptografiskt skydd när någon lämnar ett team.

**Viktig anmärkning:** Extern delning är endast tillgänglig när nyckelvalidering är inaktiverad.

## Teamets nyckelfingeravtryck

Med nyckelrotation kan flera teamnycklar användas när som helst. Teamets nyckelfingeravtryck eliminerar en situation där nyckelrotation kan minska säkerheten. Till exempel skulle ett säkerhetsproblem uppstå om servern hade kunnat skapa en oseriös teamnyckel, kryptera den med en kunds enhetsnyckel och presentera den som en utgången teamnyckel. Enheter skulle avvisa skrivningar med den här teamnyckeln eftersom den redan har upphört, men servern kan fortfarande lägga till godtyckligt innehåll som skrivskyddat och presentera det som äldre teamdata. Detta skulle vara ett brott mot integriteten.

Teamets nyckelfingeravtryck förhindrar detta genom att inte bara autentisera den aktuella teamnyckeln utan även alla teamnycklar som har gått ut. Denna process görs genom [Sparse Merkle Trees](#).

### Inledande skapande

Teamets nyckelfingeravtryck består av en Merkle Tree-hash som består av ett löv. Det betyder att teamets första offentliga nyckel-hash redan är teamets nyckelfingeravtryck.

Teamets offentliga nyckels hash beräknas genom att koppla samman algoritmnamnet, ett separationstecken och den offentliga nyckeln, och hasha resultatet med Sha256.

## Omberäkning efter nyckelrotation

En nyckelrotation introducerar en ny teamnyckel. Den administratör som utför nyckelrotationen har fingeravtrycket från den tidigare teamnyckeln via roten till Merkle-trädet. Servern förser administratören med den information som krävs för att utöka Merkle-trädet med den nya teamnyckelns hash och för att beräkna **den nya roten i Merkle-trädet (dvs. teamnyckelns nya fingeravtryck)**. Under denna process kan servern inte införa ogiltiga värden, eftersom administratören känner till den tidigare rot-hashen från Merkle Tree och lätt kan upptäcka ett sådant försök.

Den nya teamnyckelns hash ersätter det första **nullvärdet** från vänster i det glesa trädet. Den senaste teamnyckelns hash kan bestämmas genom att titta på det första icke-null-värdet i trädets löv från höger.

## Verifiering av valfri teamnyckel

Vid leverans av en teamnyckel, oavsett om den har upphört att gälla eller är aktiv, kommer servern att tillhandahålla ett medlemsbevis för nyckeln. Enheten kan, efter att ha verifierat och lokalt lagrat teamnyckelns fingeravtryck (dvs. rot-hash för Merkle), verifiera korrektheten och sedan acceptera teamnyckeln.

## Filkryptering

Algoritmen som används för att kryptera filinnehållet är utformad för att kunna ersättas. Varje krypterad nyckel på servern inkluderar identifieraren för den algoritmen med vilken den är avsedd att användas. För närvarande används endast en algoritm: Blockwise AES-GCM.

## Algoritm för råfil

Fil innehåll krypteras med en symmetrisk krypteringsalgoritm som heter Blockwise AES-GCM.

### Kryptering

1. Ange  $|authTag| = 128$  bitar och  $|blocksize| = 4$  MB.
2. Skapa en ny  $hmac\_key := random(256 \text{ bitar})$  och  $nonce\_hmac\_key := random(96 \text{ bitar})$ .
3. Beräkna  $(encrypted\_hmac\_key, hmac\_auth\_tag) := AES\text{-}GCM\text{-}encrypt(revision\_key, nonce\_hmac\_key, hmac\_key)$ .
4. Förvänta er  $oformaterat := f_0 || f_1 || \dots || f_n$  med  $|f_i| = \text{blockstorlek}$ .  
Det sista blocket kan vara mindre än blockstorleken.
5. För varje  $f_i$ :
  - a. Välj  $nonce_i := random(96 \text{ bitar})$ .
  - b. Beräkna  $(encrypted\_f_i, auth\_tag_i) := AES\text{-}GCM\text{-}encrypt(revision\_key, nonce_i, f_i)$ .

6. Beräkna `authSetHmac := HMAC_SHA256(hmac_key, auth_tag_0 || auth_tag_1 || ... || auth_tag_n)`.
7. Returnera `encrypted_hmac_key`, `nonce_hmac_key`, `hmac_auth_tag`, `all nonce_i`, `all auth_tag_i`, `all encrypted_f_i` och `authSetHmac`.

## Dekryptering

1. Dekryptera `hmac_key`.
2. Verifiera `authSetHmac` genom att beräkna om den och jämföra den med det lagrade värdet.  
Beräkna `f_i := AES-GCM-decrypt(revision_key, nonce_i, auth_tag_i, encrypted_f_i)`.

## AES-GCM

AES-GCM används som ett underliggande primitiv på grund av dess breda tillgänglighet i kryptobibliotek.

## Kryptera en fil

Ett hash-värde för varje oformaterat textblock lagras på Dropbox Server. Detta hash-värde måste inte vara avkrypteringsbart av servern, men det måste vara avkrypteringsbart av enheten. För att ta hänsyn till detta, och ta bort revisionsbegränsningen för Blockwise-AES-256-GCM, introducerar vi en revisionsnyckel som infogas mellan filnyckeln och råfilsalgoritmen.

Stegen för att kryptera en fil med en given `filnyckel` är följande:

1. Skapa en ny, slumpmässig AES-256-nyckel (`revisionsnyckeln`).
2. Kryptera `revision_key` med `file_key`.
3. Kryptera filen med `revision_key`.
4. Hasha varje block med oformaterad text och kryptera varje block med oformaterad text med `revisionsnyckeln`.
5. Skicka den krypterade filen, dess metadata, den krypterade revisionsnyckeln och de krypterade hashblocken i oformaterad text till Dropbox-servern.

Steg för att dekryptera en fil:

1. Gör stegen för filkryptering i omvänd ordning.
2. För varje avkrypterat block i filen beräknar du det avkrypterade blockets hashvärde och ser till att den matchar förväntat hashvärde (hashvärden för de krypterade blocken med oformaterad text tillhandahålls avkrypteringsförfarandet).

Varje kryptering, och varje modifiering av en befintlig fil, görs med en nyskapad [revision\\_key](#). Detta minskar revisionsgränsen för Blockwise-AES-256-GCM från *antalet block i en fil och dess revisioner till antalet block i en fil*.

**Obs:** Det går för närvarande inte att flytta filer mellan olika krypterade teammappar, utan endast inom dem. Om du till exempel arbetar i en teammapp kan du flytta filer fritt – till och ut ur undermappar. Men om du har en andra krypterad teammapp går det inte att flytta filer mellan de båda teammapparna.

# Avancerad nyckelhantering

Avancerad nyckelhantering finns i Dropbox för team. Företag behöver sofistikerade säkerhetslösningar som uppfyller efterlevnadskraven. Säkerhetsteam behöver insyn i och kontroll över det sätt på vilket företagsdata skyddas för att skydda känsligt innehåll. Detta kan göras i Dropbox, utan tredjepartslösningar för dataskydd. Vi gör det enkelt att implementera denna nya förbättrade datakrypteringsmodell som utnyttjar en infrastruktur för nyckelhantering av branschstandard. Hantera krypteringsnycklar säkert på Dropbox och dra nytta av följande funktioner.

## Automatisering och styrning

- Automatisk schemalagd rotation av teamets krypteringsnycklar varje år för ett säkert skydd.
- Återkalla teamets krypteringsnyckel manuellt när som helst för att permanent ta bort åtkomsten till teamets data när ett hot upptäcks.

## Ökat dataskydd

- Krypteringsmodell i flera lager med en unik teamassocierad krypteringsnyckel på högsta nivå.
- Team Encryption Key (TEK) genereras och lagras med branschstandardiserade Hardware Security Modules (HSM).

## Revisionsmöjlighet

- Visa aktivitet relaterad till din krypteringsnyckel, inklusive rotationer och återkallelser, med granskningsloggar.

## Kryptering på flera nivåer

Alla data som lagras på Dropbox är krypterade, men för extra lager med kontroll och säkerhet kan du välja att låta Dropbox generera en unik teamkrypteringsnyckel för ditt team.

Som en del av Dropbox krypteringsprocess på flera nivåer kommer data i vila för team som aktiverar Dropbox-hanterade krypteringsnycklar att krypteras med Dropbox krypteringsprocess på flera nivåer, där vilande data som lagras på Dropbox krypteras i tre lager med olika nycklar – på blocknivå, namnrymdsnivå och teamnivå. Dropbox-funktionen med hanterade krypteringsnycklar (DMEK) ger kunderna en unik krypteringsnyckel på teamnivå (TEK), vilket ger större flexibilitet vad gäller datasäkerhet och regelefterlevnad. Dropbox kommer att hantera lagring, organisation och rotation för TEK med hjälp av AWS KMS (Key Management Service) av branschstandard.

Nycklar är unika för varje kund. Varje team tilldelas en unik nyckel på teamnivå. TEK genereras, lagras och granskas med funktioner som är kompatibla med FIPS 140-2 i AWS Key Management Service (KMS). När du väl aktiverat DMEK i adminkonsolen krävs ingen installation.

**Obs:** Aktivering av DMEK påverkar inte Dropbox-funktionerna. Samarbetsfunktioner som förhandsvisning, delning och sökning fortsätter att fungera som väntat.

### **Aktivering av Dropbox-hanterade krypteringsnycklar (DMEK).**

Du kan aktivera DMEK genom Advanced Key Management i Dropbox adminkonsol.

