Sicurezza in Dropbox Business

Libro bianco di Dropbox

Dropbox

Indice

Panoramica

La continua evoluzione della trasformazione digitale in tutti i settori richiede come non mai che i dati, i team e i dispositivi siano protetti ovunque si trovino. Le organizzazioni che si affidano a soluzioni cloud come Dropbox Business per agevolare i flussi di lavoro distribuiti e da remoto hanno la necessità di ottimizzare la collaborazione, gestire in modo proattivo i rischi correlati al cloud e implementare controlli efficaci che garantiscano la riservatezza della loro proprietà intellettuale, l'integrità dei dati memorizzati e condivisi e la disponibilità dei dati tramite servizi cloud gestiti e resilienti.

Oltre 600.000 aziende e organizzazioni si affidano a Dropbox Business in quanto soluzione di collaborazione sicura e da remoto per team distribuiti. La soluzione principale di Dropbox Business include un'area di lavoro intelligente per la collaborazione e funzionalità di sincronizzazione e condivisione dei file. Le nostre soluzioni sono supportate da infrastrutture leader di settore, come anche da funzionalità per una sicurezza aziendale avanzata, la sicurezza di team e contenuti, la firma elettronica, trasferimenti sicuri e la governance dei dati. A meno che non sia specificato diversamente, le informazioni contenute all'interno di questo libro bianco si applicano a tutti i prodotti Dropbox Business (Standard, Advanced ed Enterprise) e Dropbox Education. Paper è una funzione di Dropbox Business e Dropbox Education.

Al centro di Dropbox Business c'è il nostro programma completo per la sicurezza, il Programma Dropbox sulla fiducia, che adotta un approccio multilivello alla sicurezza, fondamentale in un momento di totale apertura al lavoro da remoto come questo.

Questo whitepaper illustra le funzionalità relative alla sicurezza dei prodotti Dropbox Business, le misure di sicurezza operativa di Dropbox, il nostro impegno verso la privacy e la trasparenza, come anche nei confronti delle policy back-end, delle certificazioni indipendenti e delle misure di conformità alle normative, che rendono Dropbox una soluzione sicura per la tua organizzazione.

A meno che non sia specificato diversamente, le informazioni contenute all'interno di questo libro bianco si applicano a tutti i prodotti Dropbox Business (Standard, Advanced ed Enterprise) e Dropbox Education. Paper è una funzione di Dropbox Business e Dropbox Education.

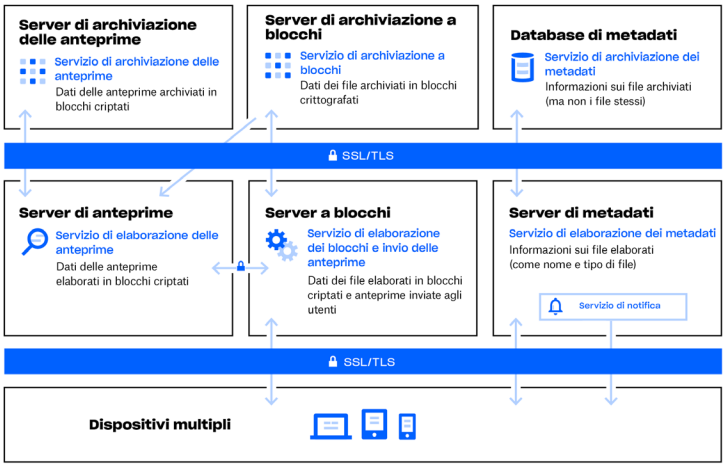
Dietro le quinte

Le nostre interfacce facili da utilizzare sono accompagnate da un'infrastruttura che lavora dietro le quinte, per garantire sincronizzazione, condivisione e collaborazione rapide e affidabili. A tale scopo, continuiamo a evolvere il nostro prodotto e la nostra architettura per accelerare il trasferimento di dati, migliorare l'affidabilità e adattarsi ai cambiamenti dell'ambiente di utilizzo. In questa sezione, descriveremo come i dati vengono trasferiti, archiviati ed elaborati in modo sicuro.

Infrastruttura di file

Gli utenti di Dropbox possono accedere a file e cartelle in qualsiasi momento da client desktop, web e mobili o tramite le applicazioni di terze parti collegate a Dropbox. Tutti questi client si collegano a server sicuri per fornire l'accesso ai file, consentirne la condivisione con altri utenti e aggiornare i dispositivi collegati quando i file vengono aggiunti, modificati o eliminati.

L'infrastruttura file di Dropbox è costituita dai componenti seguenti:



- ***Server di metadati***

  Alcune informazioni di base sui dati dell'utente, chiamate metadati, vengono conservate in un servizio di archiviazione separato che funge da indice per i dati degli account degli utenti. I metadati includono informazioni di base su account e utenti, come indirizzo email, nome e nomi dei dispositivi. I metadati includono anche informazioni di base sui file, ad esempio i nomi e i tipi di file, che consentono di supportare funzioni quali la cronologia delle versioni, il ripristino e la sincronizzazione.

- ***Database di metadati***

  Tutti i metadati dei file vengono archiviati in un archivio chiave-valore con controllo concorrenza multi-versione, che viene frammentato e replicato secondo necessità per rispondere ai requisiti relativi a prestazioni ed elevata disponibilità.

- ***Server a blocchi***

  Per proteggere i dati degli utenti, Dropbox fornisce uno speciale meccanismo di sicurezza che va ben oltre la tradizionale crittografia. I server a blocchi elaborano i file dalle applicazioni Dropbox suddividendoli in blocchi. Ogni blocco viene crittografato utilizzando un codice robusto e vengono sincronizzati solo i blocchi che sono stati modificati tra una revisione e l'altra. Quando un'applicazione Dropbox rileva un nuovo file o una modifica a un file esistente, l'applicazione notifica i server di archiviazione a blocchi. I blocchi di file nuovi o modificati saranno quindi elaborati e trasferiti ai server di archiviazione. Inoltre, i server a blocchi vengono utilizzati per inviare e consentire di visualizzare in anteprima i file agli utenti. Per informazioni dettagliate sulla crittografia utilizzata da questi servizi, sia in transito che a riposo, consulta la sezione Crittografia qui di seguito.

- ***Server di archiviazione a blocchi***

  I contenuti effettivi dei file degli utenti vengono archiviati in blocchi crittografati all'interno dei server di archiviazione a blocchi.

  Prima della trasmissione, il client Dropbox suddivide i file in blocchi per prepararli per l'archiviazione. I server di archiviazione a blocchi funzionano come un sistema Content-Addressable Storage (CAS), in cui ogni singolo blocco del file crittografato viene recuperato sulla base del suo valore hash.

- ***Server di anteprima***

  I server di anteprima producono le anteprime dei file. Le anteprime consistono in un rendering dei file di un utente in un formato file diverso, più adatto a una visualizzazione rapida sul dispositivo dell'utente finale. I server di anteprima recuperano i blocchi di file dai server di archiviazione a blocchi per generare le anteprime. Quando viene richiesta l'anteprima di un file, i server di anteprima recuperano l'anteprima memorizzata nella cache dai server di archiviazione di anteprime e la trasferiscono al server a blocchi. Le anteprime vengono infine mostrate agli utenti tramite i server a blocchi.

- ***Server di archiviazione delle anteprime***

  Le anteprime memorizzate nella cache vengono archiviate in un formato crittografato nei server di archiviazione delle anteprime.

- ***Servizio di notifica***

  Questo servizio separato monitora le eventuali modifiche apportate agli account Dropbox. Non vengono archiviati o trasferiti né file né metadati. Ogni client stabilisce una connessione long poll con il servizio di notifica e attende. Quando viene apportata una modifica a un file di Dropbox, il servizio di notifica informa i client pertinenti dell'avvenuta modifica chiudendo la connessione long poll. La chiusura della connessione segnala al client che deve collegarsi in modo sicuro al servizio metadati per sincronizzare le modifiche.

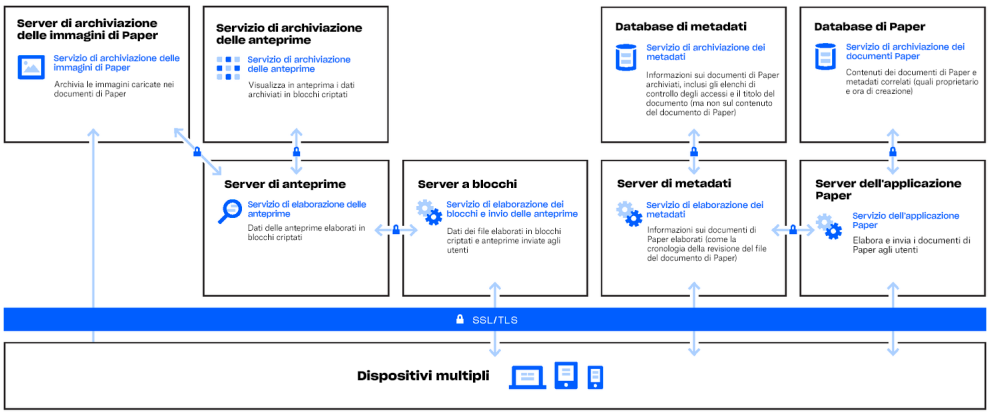
Archiviazione dei dati di file

Dropbox archivia principalmente due generi di dati: metadati sui file (come la data e l'ora dell'ultima modifica di un file) e gli effettivi contenuti dei file (blocchi di file). I metadati dei file sono archiviati nei server Dropbox, mentre i blocchi di file sono conservati in Amazon Web Services (AWS) oppure in Magic Pocket, il sistema di archiviazione di Dropbox. Magic Pocket è composto da software e hardware proprietari ed è stato progettato da zero per essere affidabile e sicuro. Sia in Magic Pocket che in AWS vengono criptati i blocchi di file inattivi ed entrambi i sistemi soddisfano standard elevati di affidabilità. Per ulteriori dettagli, consulta la sezione Affidabilità qui di seguito.

Infrastruttura di Paper

Gli utenti di Dropbox possono accedere ai documenti di Paper in qualsiasi momento da client web e mobile o tramite applicazioni di terze parti collegate all'applicazione Dropbox Paper. Tutti questi client si collegano a server sicuri per consentire l'accesso ai documenti di Paper, permettere la condivisione di documenti con altri utenti e aggiornare i dispositivi collegati quando i documenti vengono aggiunti, modificati o eliminati.

L'infrastruttura di Dropbox Paper è costituita dai componenti seguenti:



- ***Application server di Paper***

  I server dell'applicazione Paper elaborano le richieste degli utenti, restituiscono all'utente l'output dei documenti Paper modificati ed eseguono i servizi di notifica. I server dell'applicazione Paper scrivono le modifiche in entrata dell'utente nei database di Paper, in cui vengono posizionate in archiviazione permanente. Le sessioni di comunicazione tra i server dell'applicazione Paper e i database di Paper vengono protette tramite protocollo HTTPS (Secure Hypertext Transfer Protocol).

- ***Database di Paper***

  Il contenuto effettivo dei documenti Paper degli utenti, così come determinati metadati relativi a tali documenti, sono crittografati nella memoria permanente sui database di Paper. Ciò include informazioni su un documento Paper (come ad esempio il titolo, il proprietario, l'ora di creazione e altre informazioni), nonché i contenuti del documento stesso, inclusi commenti e attività. I database di Paper vengono frammentati e replicati secondo necessità per rispondere ai requisiti relativi a prestazioni ed elevata disponibilità.

- ***Server di metadati***

  Paper utilizza gli stessi server di metadati descritti nel diagramma dell'infrastruttura Dropbox per elaborare le informazioni sui documenti Paper, come la cronologia delle revisioni dei documenti Paper e la partecipazione alle cartelle condivise. Dropbox gestisce direttamente i server di metadati, che sono ubicati in data center di terze parti condivisi.

- ***Database di metadati***

  Paper usa gli stessi database dei metadati descritti nel diagramma dell'infrastruttura Dropbox per memorizzare le informazioni relative ai documenti Paper, quali condivisioni, autorizzazioni e associazioni di cartelle. Tutti i metadati dei file vengono archiviati in un servizio di database basato su MySQL, che viene frammentato e replicato secondo necessità per rispondere ai requisiti relativi a prestazioni ed elevata disponibilità.

- ***Server di archiviazione delle immagini di Paper***

  Le immagini caricate nei documenti di Paper sono archiviate e crittografate sui server di immagini di Paper. La trasmissione di dati delle immagini tra l'applicazione di Paper e i server di immagini di Paper avviene in una sessione crittografata.

- ***Server di anteprima***

  I server di anteprime forniscono un'anteprima sia delle immagini caricate su documenti di Paper, sia dei collegamenti ipertestuali incorporati nei documenti di Paper. Per le immagini caricate in documenti di Paper, il servizio Paper Image Proxy recupera i dati di immagine memorizzati nei server per le immagini di paper tramite un canale crittografato. Per i collegamenti ipertestuali incorporati nei documenti di Paper, il servizio Paper Image Proxy recupera i dati dell'immagine dal collegamento di origine ed esegue il rendering di un'anteprima dell'immagine tramite HTTP o HTTPS, come specificato dal collegamento di origine. Le anteprime vengono infine mostrate agli utenti tramite i server a blocchi.

- ***Server di archiviazione delle anteprime***

  Paper utilizza gli stessi server di archiviazione di anteprime descritti nel diagramma dell'infrastruttura di Dropbox per archiviare le anteprime delle immagini salvate nella cache. Le anteprime memorizzate nella cache vengono archiviate in un formato crittografato nei server di archiviazione delle anteprime.

Archiviazione dei documenti di Paper

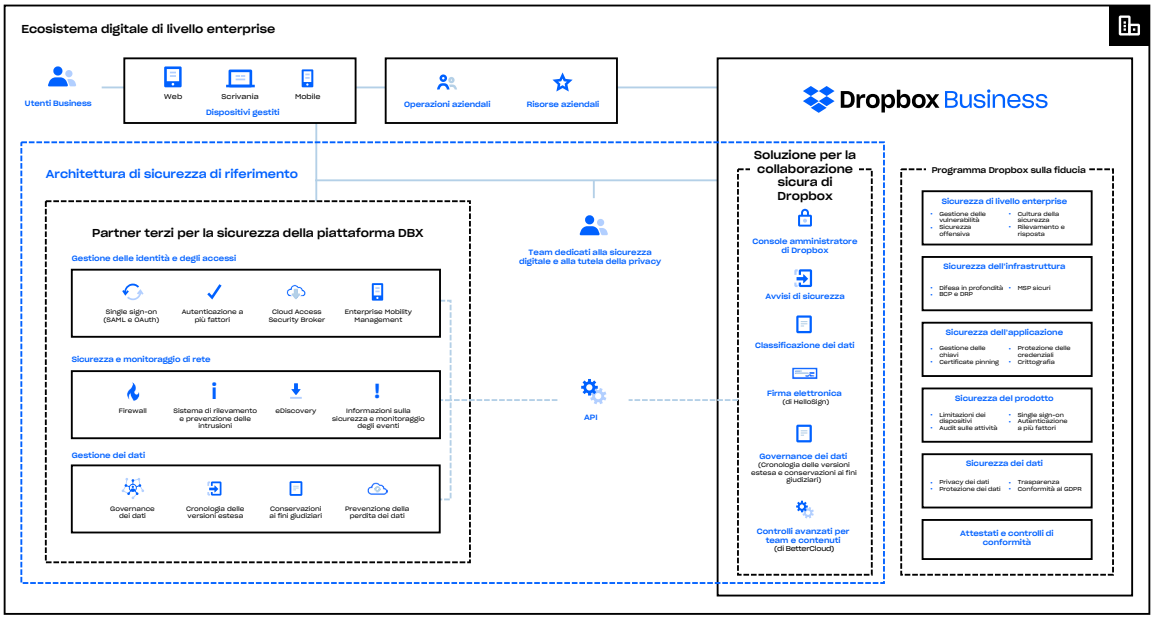
Dropbox archivia principalmente i seguenti tipi di dati nei documenti di Paper: metadati relativi a documenti di Paper (come ad esempio le autorizzazioni condivise di un documento) e contenuti effettivi dei documenti di paper caricati dall'utente. Questi sono collettivamente indicati come dati dei documenti di Paper, mentre le immagini caricate nei documenti di Paper sono note come dati di immagine di Paper. Ciascuno di questi tipi di dati viene memorizzato in Amazon Web Services (AWS). I documenti di paper sono crittografati a riposo in AWS, che soddisfa elevati standard di affidabilità. Per ulteriori dettagli, consulta la sezione Affidabilità qui sotto.

Programma Dropbox sulla fiducia

La fiducia è alla base del nostro rapporto con milioni di persone e aziende in tutto il mondo. La fiducia che hai riposto in noi è molto importante e ci assumiamo la responsabilità di proteggere le tue informazioni con la massima serietà. Per guadagnarci la tua fiducia, abbiamo creato Dropbox e continueremo a migliorarlo prestando particolare attenzione a sicurezza, privacy, trasparenza e conformità.

Le norme del Programma Dropbox sulla fiducia stabiliscono una procedura di valutazione dei rischi concepita per affrontare i rischi ambientali e fisici, nonché quelli relativi a utenti, terze parti, leggi e normative applicabili, requisiti contrattuali e diversi altri tipi di rischi che possono riguardare la sicurezza, la riservatezza, l'integrità, la disponibilità o la privacy del sistema. Le performance vengono esaminate almeno una volta all'anno. Per maggiori informazioni sul Programma Dropbox sulla fiducia, consulta la pagina dropbox.com/business/trust.

Seguiamo un approccio multilivello per proteggere l'azienda, l'infrastruttura, le applicazioni e i prodotti che influiscono sulla tua organizzazione.



Sicurezza di livello aziendale

Dropbox ha stabilito un quadro di gestione della sicurezza delle informazioni che descrive lo scopo, la direzione, i principi e le regole di base per le modalità di mantenimento della fiducia. Tutto ciò viene portato a termine tramite una valutazione dei rischi e un miglioramento continuo in termini di sicurezza, riservatezza, integrità e disponibilità dei sistemi di Dropbox Business. Effettuiamo revisioni e aggiornamenti periodici delle norme di sicurezza, offriamo corsi di formazione in materia di sicurezza, eseguiamo test sulla sicurezza di rete e delle applicazioni (inclusi test di penetrazione), monitoriamo la compliance alle norme di sicurezza e conduciamo una valutazione interna ed esterna dei rischi.

Le nostre norme

Abbiamo stabilito un set completo di norme per la sicurezza che vengono fatte rispettare dal Team dedicato alla sicurezza e agli abusi di Dropbox. Tutte le norme sulla sicurezza vengono riviste e approvate almeno su base annuale. Dipendenti, stagisti e lavoratori a contratto partecipano alla formazione sulla sicurezza al momento del loro ingresso in azienda, nonché ad attività continue di sensibilizzazione sullo stesso tema.

- ***Sicurezza delle informazioni***

  Mantenere gli utenti e le informazioni di Dropbox al sicuro.

- ***Autenticazione***

  Descrive in che modo i dipendenti Dropbox eseguono l'autenticazione per accedere ai sistemi informativi e ai dati.

- ***Sicurezza dei dispositivi***

  I requisiti minimi di sicurezza per i dispositivi mobili usati per accedere alle informazioni aziendali.

- ***Controllo degli accessi logici***

  Mantenere sicuri l'accesso ai sistemi Dropbox, gli utenti e le informazioni. Riguarda l'accesso agli ambienti aziendali e produttivi.

- ***Sicurezza dei dati***

  Descrive il modo in cui Dropbox protegge i dati tramite requisiti specifici di archiviazione, accesso e utilizzo.

- ***Sicurezza in viaggio***

  Descrive cosa dovrebbero fare i dipendenti Dropbox prima di viaggiare all'estero.

- ***Linee guida per la sicurezza dell'esperienza di vendita e del cliente***

  Mantenere al sicuro le informazioni sugli utenti, proteggere i nostri dipendenti e fornire supporto agli utenti.

- ***Sicurezza fisica***

  Mantenere un ambiente sicuro e protetto per le persone e le proprietà presso Dropbox.

- ***Linee guida per la sicurezza fisica in produzione***

  Gestire l'accesso fisico agli impianti di produzione.

- ***Risposta agli eventi imprevisti***

  Delinea il modo in cui Dropbox gestisce gli eventi riportati relativi a sicurezza, privacy e sito e documenta i piani di risposta agli incidenti per ognuno di essi.

- ***Materiali protetti da copyright non autorizzati***

  Proibire ai dipendenti di usare Dropbox o i sistemi Dropbox per archiviare o condividere contenuti non autorizzati.

- ***Gestione delle modifiche***

  Gestire le modifiche ai sistemi di produzione. Rivolto a tutti i dipendenti Dropbox, gli appaltatori e gli stagisti che abbiano accesso ai sistemi.

- ***Privacy dei dati degli utenti***

  Proteggere e gestire le informazioni utente e i dati degli utenti presso Dropbox in conformità alle nostre norme sulla privacy.

- ***Norme sulla continuità operativa e sulla gestione delle emergenze***

  Descrive i concetti di conservazione, protezione e sicurezza delle persone (dipendenti Dropbox), proprietà e processi (processi aziendali).

- ***Programma Dropbox sulla fiducia***

  Lo scopo, i principi e la responsabilità del Programma Dropbox sulla fiducia.

- ***Programma Dropbox sulla fiducia***

  Descrive come opera Dropbox e perché sia degna di fiducia.

- ***Sicurezza dell'ambiente dei pagamenti***

  Proteggere e mantenere gli ambienti dedicati ai pagamenti usati da Dropbox per poter accettare pagamenti tramite carta di credito.

Norme sull'accesso dei dipendenti

Dopo essere stato assunto, ciascun dipendente viene sottoposto ad accertamenti personali, è tenuto a firmare una dichiarazione sulla conoscenza delle norme di sicurezza e degli accordi di non divulgazione e riceve una formazione sulla sicurezza. Solo a chi ha completato tali procedure viene accordato l'accesso fisico e logico agli ambienti aziendali e di produzione, ai fini dello svolgimento delle sue responsabilità lavorative. Inoltre, tutti i dipendenti partecipano a corsi di formazione obbligatori sulla sicurezza per i nuovi assunti, alla certificazione annuale sulla sicurezza e a una sensibilizzazione continua su tali temi mediante email informative, conferenze e presentazioni e risorse disponibili sulla nostra intranet.

L'accesso dei dipendenti all'ambiente di Dropbox è gestito da una directory centrale e autenticato per mezzo dell'utilizzo di una combinazione di password sicure, chiavi SSH protette da passphrase e autenticazione a due fattori. L'accesso remoto richiede l'uso di VPN protetta da autenticazione a due fattori ed eventuali accessi speciali sono esaminati e autorizzati dal team di sicurezza. L'accesso alle reti aziendali e di produzione è severamente limitato da norme definite. Ad esempio, l'accesso alla rete di produzione è basato sulla chiave SSH e limitato ai team di tecnici che necessitano di accedervi nell'ambito delle loro mansioni. La configurazione dei firewall viene sottoposta a severi controlli ed è limitata a un numero ridotto di amministratori.

Inoltre, le nostre norme interne richiedono ai dipendenti che accedono agli ambienti di produzione e aziendali di rispettare le best practice per la creazione e l'archiviazione di chiavi SSH private. L'accesso ad altre risorse, compresi data center, utilità per la configurazione di server, server di produzione e utilità per lo sviluppo di codice sorgente viene accordato dietro esplicita approvazione da parte degli opportuni responsabili. I responsabili registrano le richieste, le motivazioni e le approvazioni relative agli accessi, i quali vengono concessi da individui competenti.

Dropbox utilizza controlli tecnici sugli accessi e norme interne per impedire ai dipendenti di accedere di loro iniziativa a file di utenti e per limitare l'accesso ai metadati e altre informazioni relative agli account degli utenti. Al fine di tutelare la privacy e la sicurezza degli utenti finali, solo un numero ristretto di tecnici responsabile della progettazione dei servizi principali di Dropbox può accedere all'ambiente in cui vengono archiviati i file. L'accesso viene immediatamente sospeso nel momento in cui il dipendente lascia l'azienda.

Nel momento in cui Dropbox diventa un'estensione dell'infrastruttura dei nostri clienti, questi ultimi hanno la garanzia che custodiremo con responsabilità i loro dati. Per maggiori informazioni, vedi la sezione sulla Privacy riportata di seguito.

Gestione delle vulnerabilità

Il nostro team dedicato alla sicurezza effettua test automatizzati e manuali su sicurezza e gestione delle patch e collabora con specialisti di terze parti per identificare e risolvere potenziali vulnerabilità e bug di sicurezza.

Secondo quanto previsto dal nostro sistema di gestione della sicurezza delle informazioni (information security management system: ISMS), le conclusioni e i suggerimenti che risultano da tali attività di valutazione vengono comunicati al team addetto alla gestione di Dropbox ed esaminati. Successivamente si intraprendono le azioni necessarie. Gli elementi di particolare gravità vengono documentati, monitorati e risolti dagli ingegneri incaricati della sicurezza.

Gestione delle modifiche

Tutti i processi di sviluppo, risoluzione dei problemi e di applicazione delle patch seguono le nostre Norme formali sulla gestione delle modifiche, che vengono definite dal team tecnico di Dropbox per garantire che le modifiche al sistema siano state testate e autorizzate prima dell'implementazione negli ambienti di produzione. Le modifiche del codice sorgente vengono avviate dagli sviluppatori che desiderano apportare migliorie all'applicazione o al servizio Dropbox. Le modifiche vengono archiviate in un sistema di controllo delle versioni e devono superare procedure di test di controllo qualità (QA) automatiche per verificare che siano rispettati i requisiti di sicurezza. Il completamento delle procedure di controllo qualità porta all'implementazione della modifica. Tutte le modifiche approvate dal controllo qualità vengono implementate automaticamente nell'ambiente di produzione. Il nostro ciclo di vita di sviluppo del software (Software Development Lifecycle, SDLC) richiede l'adesione a linee guida per la codifica sicura, così come lo screening delle modifiche al codice per individuare potenziali problemi per la sicurezza attraverso il nostro controllo qualità e processi di revisione manuali. Le modifiche che entrano nel ciclo produttivo vengono registrate e archiviate, mentre ai responsabili del team tecnico di Dropbox viene inviato automaticamente un avviso.

Le modifiche all'infrastruttura di Dropbox sono limitate unicamente al personale autorizzato. Il team responsabile della sicurezza di Dropbox si occupa di mantenere la sicurezza dell'infrastruttura e di garantire che le configurazioni di server, firewall e altre configurazioni correlate siano aggiornate e in linea con gli standard di settore. L'insieme di regole firewall e i soggetti con accesso ai server di produzione vengono esaminati a intervalli regolari.

Scansioni e test di penetrazione della sicurezza (interni ed esterni)

Il nostro team che si occupa della sicurezza esegue con regolarità test automatici e manuali della sicurezza delle applicazioni per identificare e risolvere eventuali vulnerabilità e bug di sicurezza nelle nostre applicazioni desktop, web (Dropbox e Paper) e per dispositivi mobili (Dropbox e Paper).

Inoltre, Dropbox si avvale di fornitori terzi per eseguire con regolarità test della penetrazione e delle vulnerabilità sugli ambienti aziendali e di produzione. Collaboriamo con specialisti esterni, con altri team di sicurezza del settore e con chi si occupa di ricerca nel campo della sicurezza al fine di mantenere protette le nostre applicazioni. Sfruttiamo inoltre sistemi automatici di analisi dei dati per identificare le vulnerabilità. Questo processo include sistemi da noi sviluppati internamente, sistemi open source modificati in base alle nostre esigenze o fornitori esterni da noi assunti per analisi automatizzate continue.

Tenere i contenuti dannosi lontano da Dropbox

Disponiamo di funzionalità di scansione che mirano a prevenire l'archiviazione e la distribuzione di contenuti dannosi all'interno di Dropbox. I nostri scanner si basano su una tecnologia di nostra produzione e su funzionalità all'avanguardia dei nostri partner come Microsoft e Google per rendere Dropbox un posto sicuro per i nostri clienti.

Premi per il rilevamento di bug

Sebbene collaboriamo con aziende specializzate per i test di penetrazione ed eseguiamo anche test interni all'azienda, i premi per il rilevamento di bug (o programmi di ricompense per l'individuazione di vulnerabilità) consentono di usufruire delle competenze di una più vasta community esperta in sicurezza. Il nostro programma di premi per il rilevamento di bug rappresenta un incentivo per i ricercatori a identificare e divulgare in modo responsabile i bug dei software. Tale coinvolgimento della community esterna fornisce al team addetto alla sicurezza una verifica indipendente delle nostre applicazioni, contribuendo così alla sicurezza degli utenti. Ci impegniamo a essere tra i leader del settore in termini di premi di rendimento, tempi di risposta e di correzione.

Abbiamo stabilito l'ambito per proposte e applicazioni Dropbox idonee, oltre che un insieme di norme per la divulgazione responsabile che promuove l'individuazione e la segnalazione di vulnerabilità della sicurezza e migliora la protezione degli utenti. Tali norme comprendono le seguenti linee guida:

- Descriverci in dettaglio il problema di sicurezza.
- Rispetta le nostre applicazioni esistenti. I moduli di spamming tramite gli scanner automatizzati delle vulnerabilità non comporteranno alcuna ricompensa o premio fino alla loro completa esclusione.
- Concedici un tempo ragionevole per rispondere prima di rendere pubbliche le informazioni relative al problema di sicurezza.
- Non accedere o modificare i dati di un utente senza il permesso del proprietario dell'account.
- Non visualizzare, alterare, salvare, archiviare, trasferire i dati o altrimenti accedervi e rimuovere immediatamente qualsiasi informazione locale dopo aver segnalato la vulnerabilità a Dropbox.
- Agisci in buona fede per evitare violazioni della privacy, distruzione di dati e l'interruzione o il peggioramento dei nostri servizi (inclusi gli attacchi denial of service).

I problemi possono essere segnalati inviando un rapporto a Bugcrowd alla pagina bugcrowd.com/dropbox.

Sicurezza fisica

Infrastruttura

L'accesso fisico alle strutture delle aziende fornitrici di servizi secondari in cui risiedono i sistemi di produzione è limitato a personale autorizzato da Dropbox ai fini dello svolgimento delle proprie funzioni lavorative. A chiunque lo richieda, verranno concesse ulteriori autorizzazioni per accedere alle strutture dell'ambiente di produzione dietro esplicita approvazione da parte degli opportuni responsabili.

I responsabili registrano le richieste, le motivazioni e le approvazioni relative agli accessi, i quali vengono concessi da opportuni soggetti. Una volta ricevuta l'approvazione, un membro responsabile del team dell'infrastruttura contatterà l'opportuna azienda fornitrice di servizi secondari per richiedere l'accesso per l'individuo in questione. L'azienda fornitrice di servizi secondari inserisce le informazioni dell'utente nel proprio sistema e garantisce al personale Dropbox approvato un accesso con badge e, se possibile, con scansione biometrica. Una volta che gli individui approvati hanno ottenuto l'accesso, è responsabilità del data center garantire che tale accesso sia limitato esclusivamente agli individui summenzionati.

Sedi dell'azienda

- ***Sicurezza fisica***

  Il Team Dropbox per la sicurezza fisica è responsabile dell'applicazione delle norme sulla sicurezza fisica e della supervisione della sicurezza all'interno dei nostri uffici.

- ***Norme relative a visitatori e accesso***

  L'accesso fisico alle strutture aziendali, ad esclusione degli ingressi e delle entrate pubblici, è limitato al personale autorizzato da Dropbox e ai visitatori registrati e accompagnati dal personale di Dropbox. Un sistema di accesso con badge garantisce che soltanto gli individui autorizzati abbiano accesso alle aree soggette a restrizioni all'interno delle strutture aziendali.

- ***Accesso ai server***

  L'accesso ad aree che ospitano server aziendali e strutture di rete è limitato a personale autorizzato per mezzo di badge che ne dimostrino il ruolo. L'elenco di individui autorizzati, per i quali è stato approvato l'accesso fisico agli ambienti aziendali e produttivi, viene riesaminato con cadenza almeno trimestrale.

Risposta agli eventi imprevisti

Abbiamo previsto norme e procedure di risposta agli eventi imprevisti per risolvere problemi legati a disponibilità del servizio, integrità, sicurezza, privacy e riservatezza. Nel quadro delle nostre procedure di risposta agli incidenti, disponiamo di team dedicati, appositamente formati per:

- Rispondere rapidamente agli avvisi di potenziali eventi imprevisti.
- Determinare la gravità dell'evento imprevisto.
- Se necessario, adottare misure di attenuazione e contenimento.

- Comunica con le parti interessate interne ed esterne, e notifica i clienti coinvolti, per ottemperare agli obblighi contrattuali di notifica in caso di violazione o evento imprevisto e al fine di rispettare le leggi e le normative pertinenti.
- Raccogliere e conservare prove a scopo investigativo.
- Effettuare un'analisi retrospettiva e sviluppare un piano di assegnazione delle priorità definitivo.

Le norme e le procedure in materia di risposta agli eventi imprevisti sono controllate nell'ambito degli audit SOC 2+, ISO/IEC 27001 e di altre valutazioni di sicurezza.

Sicurezza dell'infrastruttura

Sicurezza della rete

Dropbox mantiene diligentemente la sicurezza della nostra rete di back-end. Le nostre tecniche di protezione e monitoraggio della rete sono studiate per fornire più livelli di protezione e difesa. Al fine di garantire che solo il traffico idoneo e non dannoso sia in grado di raggiungere la nostra infrastruttura, utilizziamo tecniche di protezione rispondenti agli standard del settore, compresi firewall, analisi delle vulnerabilità della rete, monitoraggio della sicurezza della rete e sistemi di rilevamento delle intrusioni.

La nostra rete privata interna è segmentata in base all'utilizzo e al livello di rischio. Le reti primarie sono:

- DMZ con connessione Internet
- DMZ con infrastruttura prioritaria
- Rete di produzione
- Rete aziendale

L'accesso all'ambiente di produzione è riservato agli indirizzi IP autorizzati e richiede l'autenticazione a più fattori in tutti gli endpoint. Gli indirizzi IP che dispongono dell'accesso sono associati alla rete aziendale oppure approvati dal personale di Dropbox. Gli indirizzi IP autorizzati vengono riesaminati a cadenza trimestrale per garantire un ambiente di produzione sicuro. L'accesso che consente la modifica dell'elenco degli indirizzi IP è riservato a soggetti autorizzati.

Il traffico da Internet destinato alla nostra rete di produzione viene protetto utilizzando diversi livelli di firewall e proxy.

La rete interna di Dropbox è separata con sistemi rigorosi dalla rete Internet pubblica. Il traffico Internet da e verso la rete di produzione è controllato attentamente tramite servizi proxy dedicati, i quali, a loro volta, sono protetti da rigide regole di firewall.

Grazie ai sofisticati strumenti di Dropbox, per individuare la presenza di eventi dannosi è possibile monitorare laptop e computer desktop con sistemi operativi Mac e Windows e i sistemi di produzione. Tutti i registri di sicurezza vengono raccolti in un luogo centrale per una risposta forense e agli eventi indesiderati in base alle norme sulla conservazione dei dati standard del settore.

Dropbox identifica e attenua i rischi attraverso test periodici della sicurezza della rete, nonché tramite verifiche da parte di team interni per la sicurezza e terze parti specializzate nel settore della sicurezza.

Points of presence (PoP)

Per ottimizzare le prestazioni del sito Web per gli utenti, Dropbox sfrutta le reti per la consegna di contenuti di terze parti (third-party content delivery networks: CDN) e i point of presence ospitati su Dropbox (POP) in 31 sedi nel mondo. In queste posizioni nessun dato utente viene memorizzato nella cache e tutti i dati in transito vengono crittografati con SSL/TLS. L'accesso fisico e logico ai POP ospitati su Dropbox è limitato esclusivamente al personale autorizzato di Dropbox. Dropbox esegue ottimizzazioni sia a livello di trasporto (TCP) che a livello di applicazione (HTTP).

Peering

Dropbox dispone di normative di peering aperto e tutti i clienti sono i benvenuti nel nostro peering. Per maggiori dettagli, visita il sito dropbox.com/peering.

Affidabilità

Un sistema di archiviazione è utile solo se è affidabile. Per questo motivo, abbiamo sviluppato diversi livelli di ridondanza per Dropbox che impediscono la perdita di dati e assicurano la loro disponibilità.

Metadati dei file

Le copie ridondanti dei metadati sono distribuite su dispositivi indipendenti all'interno di un data center con almeno un modello di disponibilità N+2. Vengono eseguiti backup incrementali con cadenza oraria e backup completi ogni 36 ore. I metadati vengono archiviati su server ospitati e gestiti da Dropbox negli USA.

Blocchi di file

Le copie ridondanti dei blocchi di file vengono archiviate indipendentemente in almeno due regioni geografiche distinte e replicate in modo affidabile all'interno di ciascuna regione (**nota:** per i clienti che scelgono di archiviare i file in un'infrastruttura in Germania, in Australia, in Giappone o nel Regno Unito, i blocchi di file sono replicati solo nelle rispettive regioni. Per maggiori informazioni, consulta Data center e provider di servizi gestiti di seguito). Sia Magic Pocket che AWS sono stati progettati per fornire una robustezza dei dati annuale almeno del 99,999999999%.

L'architettura, le applicazioni e i meccanismi di sincronizzazione di Dropbox operano insieme per proteggere i dati degli utenti e renderli altamente disponibili. Nella rara eventualità di un'interruzione del servizio, gli utenti Dropbox avranno comunque accesso alle più recenti copie sincronizzate dei propri file nella cartella locale di Dropbox presente sui computer associati. Le copie dei file sincronizzati nella cartella del client desktop/locale di Dropbox sono accessibili da un hard disk dell'utente durante i periodi di inattività, le interruzioni di servizio o in modalità offline. Le modifiche apportate ai file e alle cartelle vengono sincronizzate su Dropbox una volta ripristinati il servizio o la connettività.

Documenti di Paper

Le copie ridondanti dei dati dei documenti di Paper sono distribuite su dispositivi indipendenti all'interno di un data center con un modello di disponibilità N+1. Vengono inoltre eseguiti con cadenza giornaliera backup completi dei dati dei documenti di Paper. Per l'archiviazione dei documenti di Paper, Dropbox si avvale di un'infrastruttura ospitata negli USA, progettata per offrire una durabilità dei dati del 99,999999999%. Nella rara eventualità di un'interruzione di servizio, gli utenti avranno comunque accesso alle copie sincronizzate più recenti dei propri documenti di Paper in modalità "offline" nell'applicazione mobile.

Sincronizzazione di file

Dropbox offre una sincronizzazione dei file all'avanguardia riconosciuta in tutto il settore. I nostri meccanismi di sincronizzazione garantiscono trasferimenti di file rapidi e immediati e consentono l'accesso ai dati da più dispositivi e ovunque ci si trovi. Dropbox è inoltre resiliente. In caso di una mancata connessione al servizio Dropbox, il client riprenderà tranquillamente la sincronizzazione una volta ristabilita la connessione. I file verranno aggiornati nel client locale solo se sono stati sincronizzati completamente e convalidati correttamente dal servizio Dropbox. Il bilanciamento del carico tra più server garantisce la ridondanza e un'esperienza di sincronizzazione uniforme per l'utente finale.

Sincronizzazione delta

Utilizzando questo metodo di sincronizzazione, vengono scaricate/caricate solo le porzioni modificate dei file. Dropbox memorizza ogni file caricato in blocchi crittografati distinti e aggiorna solo quelli che sono cambiati.

Sincronizzazione streaming

Anziché attendere che termini il caricamento di un file, la sincronizzazione streaming inizia il download dei blocchi sincronizzati su un secondo dispositivo prima che sia terminato il caricamento di tutti i blocchi dal primo dispositivo. Questo metodo viene utilizzato automaticamente quando computer distinti sono collegati allo stesso account Dropbox o quando account Dropbox diversi condividono una cartella.

Spazio risparmiato sul disco rigido

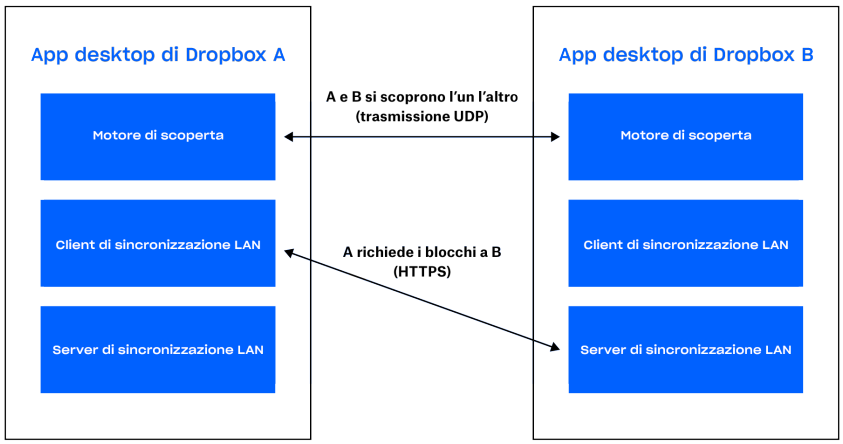
Gli utenti possono liberare spazio di archiviazione sui loro computer rendendo disponibili offline sui loro dischi rigidi solo determinati file. Questa operazione libererà spazio sui loro computer mantenendo tutto il resto solo online su dropbox.com.

Sincronizzazione LAN

Quando viene abilitata, questa funzionalità consente di scaricare file nuovi e aggiornati da altri computer sulla stessa rete Local Area Network (LAN), risparmiando tempo e larghezza di banda rispetto al download dei file dai server di Dropbox.

Architettura

Il sistema di sincronizzazione LAN è formato da tre componenti principali, che vengono eseguiti sull'app desktop: il motore di scoperta, il server e il client. Il motore di scoperta trova i computer in rete con cui sincronizzarsi. Ciò si limita ai computer che dispongono di un'autorizzazione per accedere alle stesse cartelle personali o condivise di Dropbox. Il server gestisce le richieste dagli altri computer presenti nella rete, distribuendo i blocchi di file richiesti. Il client richiede i blocchi di file dalla rete.



Motore di scoperta

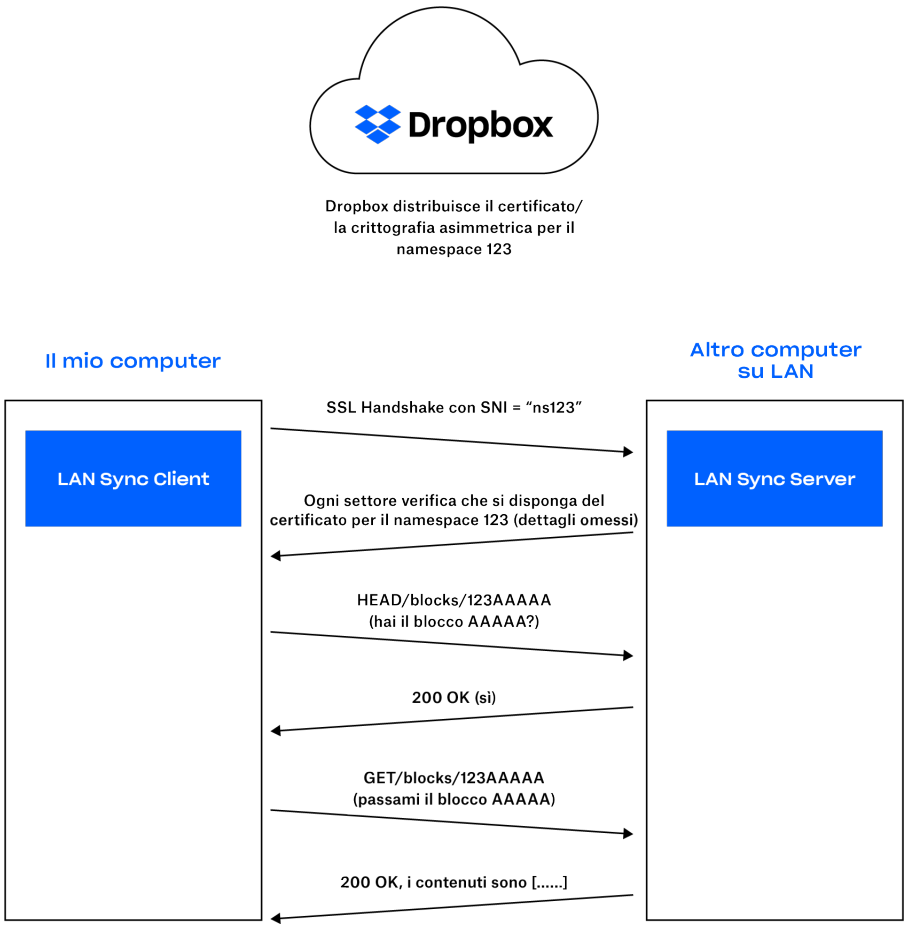
Ciascuna macchina nella LAN invia e ascolta a intervalli regolari pacchetti con protocollo di trasmissione UDP tramite la porta 17500 (che viene riservata dallo IANA per la sincronizzazione LAN). Questi pacchetti contengono la versione del protocollo utilizzato da tale computer, le cartelle personali e condivise di Dropbox supportate, la porta TCP utilizzata per eseguire il server (che potrebbe essere diversa da 17500 se quest'ultima non è disponibile) e un identificatore casuale per la macchina. Quando un pacchetto viene letto, l'indirizzo IP della macchina viene aggiunto a un elenco per ciascuna cartella personale o condivisa, indicando un potenziale target.

Protocollo

L'effettivo trasferimento dei blocchi di file viene effettuato tramite il protocollo HTTPS. Ciascun computer esegue un server HTTPS con endpoint. Un client eseguirà il polling su più peer per verificare se dispongono dei blocchi, ma scaricherà i blocchi soltanto da un server.

Per mantenere al sicuro tutti i tuoi dati, ci assicuriamo che soltanto i client autenticati per una determinata cartella possano richiedere blocchi di file. Ci assicuriamo inoltre che i computer non si sostituiscano ai server per cartelle di cui non hanno il controllo. Per risolvere questo problema, generiamo coppie di certificati/chiavi SSL per ciascuna cartella personale o condivisa di Dropbox. Queste vengono distribuite dai server di Dropbox ai computer degli utenti autenticati per la cartella. Le coppie di chiavi/certificati vengono alternate a ogni modifica dell'adesione (ad esempio, quando un utente viene rimosso da una cartella condivisa). Richiediamo che entrambe le estremità della connessione HTTPS siano autenticate con lo stesso certificato (il certificato per la cartella personale o condivisa di Dropbox). Ciò dimostra che entrambe le estremità della connessione sono autenticate.

Quando si stabilisce una connessione, viene indicata al server la cartella personale o condivisa di Dropbox che si sta tentando di collegare tramite l'utilizzo di un'indicazione del nome del server (SNI). In questo modo, il server usa il certificato corretto.



Server/client

Con il protocollo descritto sopra, il server deve conoscere soltanto i blocchi presenti e la relativa posizione.

Sulla base dei risultati del motore di scoperta, il client mantiene un elenco dei peer per ciascuna cartella personale e condivisa di Dropbox. Quando il sistema di sincronizzazione LAN riceve la richiesta di scaricare un blocco di file, invia una richiesta a un campione casuale dei peer che ha scoperto per la cartella personale o condivisa di Dropbox, quindi richiede il blocco dal primo che invia la conferma della presenza dello stesso.

Per evitare le latenze, utilizziamo pool di connessioni che ci consentono di riutilizzare le connessioni già avviate. Apriamo una connessione soltanto quando questa è necessaria, e una volta aperta, la manteniamo attiva nel caso in cui serva nuovamente. Limitiamo inoltre il numero di connessioni per ogni singolo peer.

Se un blocco di file non viene trovato o scaricato correttamente, o se la connessione si rivela troppo lenta, il sistema richiede nuovamente il blocco ai server di Dropbox.

Data center e provider di servizi gestiti

I sistemi aziendali e di produzione di Dropbox sono ospitati in data center di organizzazioni di servizi secondari e provider di servizi gestiti di terze parti, ubicati in diverse regioni degli Stati Uniti. Tutti i rapporti SOC dei data center delle organizzazioni di servizi secondari vengono esaminati almeno una volta all'anno per verificare la presenza di controlli di sicurezza sufficienti. Questi provider di servizi di terze parti sono responsabili dei controlli di sicurezza fisici, ambientali e operativi dei confini dell'infrastruttura di Dropbox. Dropbox è responsabile della sicurezza logica, di rete e applicativa della nostra infrastruttura ospitata in data center di terze parti.

Amazon Web Services (AWS), il nostro attuale provider di servizi gestiti per l'elaborazione e l'archiviazione, è responsabile della sicurezza logica e di rete dei servizi Dropbox offerti attraverso la sua infrastruttura. Le connessioni sono protette dal firewall del provider, configurato in modalità deny-all. Dropbox limita l'accesso all'ambiente a un numero ristretto di indirizzi IP e dipendenti.

Infrastruttura in Germania, Australia, Giappone e Regno Unito

Ai clienti idonei, Dropbox offre la possibilità di archiviare blocchi di file in regioni al di fuori degli Stati Uniti. La nostra infrastruttura è ospitata da Amazon Web Services (AWS) in Germania, Australia, Giappone e Regno Unito ed è replicata nelle rispettive regioni per garantire la ridondanza e la tutela dalla perdita di dati. I metadati dei file sono archiviati negli Stati Uniti sui server di proprietà di Dropbox. I documenti e le anteprime di Paper sono al momento archiviati negli Stati Uniti per tutti i clienti.

Continuità aziendale

Dropbox ha stabilito un sistema di gestione della continuità aziendale (business continuity management system: BCMS) per risolvere i problemi relativi all'interruzione o alla continuazione dell'erogazione del servizio agli utenti, e a come svolgere le funzioni aziendali, se le procedure e le attività business-critical vengono interrotte. Conduciamo un processo ciclico che consiste nelle seguenti fasi:

- ***Impatto aziendale e valutazione dei rischi***

  Conduciamo una valutazione dell'impatto aziendale (business impact assessment: BIA) almeno una volta all'anno per individuare i processi critici per Dropbox, valutare il potenziale impatto delle interruzioni, stabilire le priorità per i periodi di ripristino e individuare le nostre dipendenze critiche e i nostri fornitori. Conduciamo inoltre una valutazione dei rischi estesa a tutta l'azienda almeno una volta all'anno. La valutazione dei rischi ci consente di individuare, analizzare e valutare il rischio di eventi imprevisti per Dropbox. La valutazione dei rischi e la BIA ispirano le priorità di continuità e le strategie di attenuazione e ripristino relative ai piani di continuità aziendale (business continuity plans: BCP).

- ***Piani di continuità aziendale***

  I team riconosciuti come cruciali dalla BIA per la continuità di Dropbox utilizzano queste informazioni per sviluppare piani di continuità aziendale per i propri processi critici. Questi piani consentono ai team di conoscere il responsabile incaricato di riprendere i processi in caso di emergenza, il quale, direttamente da un altro ufficio di Dropbox o da un'altra posizione, sarà in grado di subentrare nei processi dei team durante un'interruzione e di identificare i metodi da utilizzare per le comunicazioni durante un evento di continuità. Questi piani consentono inoltre di prepararci a un evento di disturbo tramite la centralizzazione dei nostri piani di ripristino e delle altre informazioni importanti, come l'eventualità e la modalità di utilizzo del piano, le informazioni su contatti e riunioni, le applicazioni importanti e le strategie di ripristino. I piani di continuità di Dropbox sono legati al piano di gestione delle crisi a livello aziendale (company-wide crisis management plan: CMP), che stabilisce i team di gestione delle crisi e di risposta agli eventi.

- ***Valutazione/attuazione dei piani***

  Dropbox valuta determinati elementi dei propri piani di continuità aziendale almeno una volta all'anno. Questi test sono coerenti con l'ambito e gli obiettivi del sistema di gestione della continuità aziendale (business continuity management system: BCMS), si basano su situazioni appropriate e sono appositamente progettati con scopi chiaramente definiti. Le valutazioni possono spaziare dagli esercizi pratici a simulazioni su vasta scala di eventi imprevisti di vita reale. Sulla base dei risultati della valutazione e sull'esperienza derivante da eventi imprevisti avvenuti realmente, i team aggiornano e migliorano i propri piani per far fronte ai problemi e rafforzare le proprie capacità di risposta.

- ***Revisione e approvazione del sistema di gestione della continuità aziendale (business continuity management system: BCMS)***

  Almeno una volta all'anno, il nostro personale esecutivo esamina il sistema di gestione della continuità aziendale in quanto parte della revisione del programma Dropbox sulla fiducia.

Ripristino di emergenza

Manteniamo un piano di ripristino di emergenza al fine di soddisfare i requisiti di sicurezza delle informazioni durante una grave crisi o emergenza con impatto sull'attività aziendale di Dropbox. Il team di progettazione di Dropbox esamina annualmente questo piano e ne valuta gli elementi almeno una volta all'anno. I risultati pertinenti vengono documentati e monitorati fino alla risoluzione.

Il nostro piano di ripristino di emergenza è pensato per risolvere emergenze in termini di durabilità e disponibilità, che vengono definite come segue:

- Un'emergenza in termini di durabilità consiste in una o più delle seguenti situazioni:
  - Una perdita completa o permanente di un data center principale in cui sono archiviati metadati o di più data center in cui sono archiviati i blocchi di file.
  - Una perdita della capacità di comunicare o distribuire dati da un data center in cui sono archiviati metadati o da più data center in cui è archiviato il contenuto dei file.
- Un'emergenza in termini di disponibilità consiste in una o più delle seguenti situazioni:
  - Un'interruzione di servizio superiore a 10 giorni.
  - Una perdita della capacità di comunicare o distribuire i dati da un servizio di archiviazione/data center in cui sono archiviati i metadati, o da più servizi di archiviazione/data center in cui è archiviato il contenuto dei blocchi di file.

Definiamo un obiettivo di tempo di ripristino (Recovery Time Objective: RTO), ossia il periodo di tempo e un livello di servizio in cui il processo aziendale o il servizio deve essere ripristinato dopo un'emergenza e un obiettivo di punto di ripristino (Recovery Point Objective: RPO), ossia il periodo massimo tollerabile in cui i dati possono andare perduti in seguito a un'interruzione del servizio. Inoltre, misuriamo il tempo di ripristino effettivo (Recovery Time Actual: RTA) durante il test del piano di recupero di emergenza, eseguito almeno una volta all'anno.

I piani di risposta agli eventi imprevisti, di continuità aziendale e di ripristino di emergenza di Dropbox sono soggetti a verifiche a intervalli pianificati e in caso di modifiche organizzative o ambientali significative.

Sicurezza delle applicazioni

Interfacce utente di Dropbox

È possibile utilizzare e accedere al servizio di Dropbox tramite diverse interfacce. Ciascuna dispone di impostazioni e funzionalità di sicurezza che elaborano e proteggono i dati degli utenti garantendo un facile accesso.

- ***WEB***

  È possibile accedere a questa interfaccia utilizzando qualsiasi browser web recente. Consente agli utenti di caricare, scaricare, visualizzare e condividere i propri file. L'interfaccia web consente inoltre agli utenti di aprire le versioni locali esistenti dei file tramite l'applicazione predefinita del computer.

- ***Desktop***

  L'applicazione desktop Dropbox è un potente client di sincronizzazione che archivia i file localmente per l'acceso offline. Offre agli utenti un accesso completo agli account Dropbox e funziona su sistemi operativi Windows e Mac. È possibile visualizzare i file e condividerli direttamente dall'utilità di selezione file remota del sistema operativo.

- ***Dispositivi mobili***

  L'app Dropbox è disponibile per i dispositivi iOS e Android, consentendo agli utenti di accedere ai file mentre sono in viaggio. L'app per dispositivi mobili permette inoltre agli utenti l'archiviazione locale dei file per accedervi offline.

- ***API***

  Le API di Dropbox forniscono agli account utente di Dropbox una modalità di lettura e scrittura flessibile, oltre all'accesso a funzionalità avanzate come la ricerca, le revisioni e il ripristino dei file. Le API possono essere utilizzate per gestire il ciclo di vita dell'utente per un account Dropbox Business, eseguire azioni su tutti i membri di un team e consentire l'accesso alla funzione di amministratore di Dropbox Business.

Interfacce utente di Paper

Il servizio Paper può essere utilizzato attraverso varie interfacce. Ciascuna di esse ha impostazioni e funzionalità di sicurezza che elaborano e proteggono i dati degli utenti assicurando al contempo la facilità di accesso.

- ***Web***

  È possibile accedere a questa interfaccia utilizzando qualsiasi browser web recente. Consente agli utenti di caricare, visualizzare, modificare, scaricare e condividere i propri documenti di Paper.

- ***Dispositivi mobili***

  L'applicazione di Paper è disponibile per tablet e dispositivi mobili iOS e Android e consente agli utenti di accedere ai loro documenti di Paper ovunque si trovino. L'applicazione mobile è progettata come un'applicazione ibrida composta da un codice nativo (iOS o Android) contenuto in un browser Webview interno.

- ***API***

  L'API di Dropbox descritta sopra contiene endpoint e tipi di dati per la gestione di documenti e cartelle in Dropbox Paper, incluso il supporto per funzionalità come la gestione delle autorizzazioni, l'archiviazione e l'eliminazione permanente.

Crittografia

Dati in transito

Per proteggere i dati in transito tra le app Dropbox e i suoi server, Dropbox utilizza la tecnologia Secure Sockets Layer (SSL)/Transport Layer Security (TLS) per il trasferimento dei dati, creando un tunnel sicuro protetto da crittografia Advanced Encryption Standard (AES) a 128 bit o superiore. I file in transito tra un client Dropbox (al momento desktop, mobile, API o web) e il servizio in hosting è crittografato mediante SSL/TLS. Allo stesso modo, i dati dei documenti di Paper in transito tra un client Paper (al momento mobile, API o web) e il servizio in hosting sono crittografati mediante SSL/TLS. Per i punti finali che controlliamo (desktop e dispositivi mobili) e i browser più recenti, utilizziamo un solido algoritmo di cifratura e supportiamo la forward secrecy perfetta e il pinning dei certificati. Inoltre, sul Web contrassegniamo tutti i cookie di autenticazione come sicuri e abilitiamo la HTTP Strict Transport Security (HSTS) con includeSubDomains attivato.

Nota: Dropbox utilizza esclusivamente TLS e giudica obsoleto l'utilizzo di SSLv3 a causa delle note vulnerabilità. Tuttavia, TLS spesso viene definito come "SSL/TLS", motivo per cui utilizziamo questo nome.

Per impedire attacchi man-in-the-middle, l'autenticazione dei server di front-end di Dropbox avviene attraverso certificati pubblici mantenuti dal client. Prima del trasferimento di qualsiasi file si negozia una connessione criptata, che favorisce l'arrivo dei file ai server di front-end di Dropbox.

Dati archiviati

Il file di Dropbox caricati dagli utenti vengono crittografati a riposo con lo standard AES (Advanced Encryption Standard) a 256 bit. I file sono archiviati in più data center in blocchi di file distinti. Ogni blocco è frammentato e criptato utilizzando un codice robusto. Solo i blocchi modificati tra una revisione e l'altra vengono sincronizzati. Anche i documenti di Paper a riposo vengono crittografati con lo standard AES (Advanced Encryption Standard) a 256 bit. i documenti di Paper a riposo sono archiviati in più aree di disponibilità tramite sistemi di terze parti.

Gestione delle chiavi

L'infrastruttura di gestione delle chiavi di Dropbox è progettata con controlli di sicurezza operativi, tecnici e procedurali che prevedono un accesso diretto molto limitato alle chiavi. La generazione, lo scambio e l'archiviazione di chiavi di crittografia sono distribuiti per decentralizzare l'elaborazione.

- ***Chiavi di crittografia dei file***

  Per come è stato progettato, Dropbox gestisce le chiavi di crittografia dei file per conto degli utenti in modo da rimuovere la complessità e permettere l'uso di funzionalità avanzate del prodotto e controlli crittografici avanzati. Le chiavi di crittografia dei file vengono create, archiviate e protette mediante controlli di sicurezza dell'infrastruttura del sistema di produzione e norme di sicurezza.

- ***Chiavi SSH interne***

  L'accesso ai sistemi di produzione è limitato mediante coppie di chiavi SSH uniche. Le norme e le procedure di sicurezza richiedono la protezione delle chiavi SSH. Un sistema interno gestisce il processo di scambio sicuro delle chiavi pubbliche, mentre le chiavi private vengono archiviate in modo sicuro. Le chiavi SSH

interne non possono essere utilizzate per accedere ai sistemi di produzione senza un secondo fattore di autenticazione separato.

- ***Distribuzione di chiavi***
  Dropbox automatizza la gestione e la distribuzione di chiavi sensibili solo ai sistemi obbligatori per le operazioni.

Pinning dei certificati

Dropbox fornisce il pinning dei certificati nei browser moderni che supportano la specifica sul pinning delle chiavi pubbliche HTTP e sui client desktop e per dispositivi mobili. Il pinning dei certificati è una verifica supplementare che assicura che il servizio a cui ci si connette è realmente quello previsto e non un impostore. Lo utilizziamo come protezione nei confronti di alcuni metodi che gli hacker più abili potrebbero utilizzare per spiare le tue attività.

Protezione dei dati di autenticazione

Dropbox non si limita al normale hashing per proteggere le credenziali di accesso degli utenti. In linea con le best practice del settore, ciascuna password è salata con un sale univoco generato in maniera casuale per ogni utente, e utilizziamo un hashing ripetitivo per rallentare il calcolo. Queste pratiche facilitano la protezione contro attacchi a forza bruta, a dizionario e con tabelle arcobaleno. Come precauzione aggiuntiva, crittografiamo gli hash con una chiave memorizzata separatamente dai database, che consente di mantenere le password al sicuro in caso di compromissione del solo database.

Scansione anti-malware

Abbiamo sviluppato un sistema automatizzato che scansiona i contenuti per verificare la presenza di malware nel momento in cui vengono condivisi dall'account di origine dell'utente. Il sistema sfrutta una tecnologia proprietaria e motori di rilevamento standard di settore ed è progettato per fermare la diffusione di eventuali malware.

Sicurezza del prodotto

Dropbox fornisce le funzionalità di controllo amministrativo e visibilità che consentono al team IT e agli utenti finali di gestire i loro dati in modo efficace e sicuro. Con Dropbox hai tutto ciò che ti occorre per lavorare, dagli strumenti ai contenuti, ai collaboratori, in un unico posto. Dropbox non è solo uno spazio di archiviazione sicuro, ma è un modo pratico e intelligente per ottimizzare i flussi di lavoro esistenti.

Di seguito sono indicate le funzionalità disponibili per amministratori e utenti, nonché le integrazioni di terze parti per la gestione dei principali processi IT.

Nota: la disponibilità delle funzioni varia in base al tipo di abbonamento. Vedi dropbox.com/business/plans per i dettagli.

Controlli dei contenuti

Proteggere le risorse aziendali sensibili, come la proprietà intellettuale e le informazioni di identificazione personale, è fondamentale per i team IT e per quelli dedicati alla sicurezza dei dati. Dalle autorizzazioni granulari dei contenuti ai criteri di conservazione dei dati, alla conservazione ai fini giudiziari, Dropbox fornisce soluzioni leader di settore per gestire, monitorare e proteggere i tuoi contenuti. Seguono alcuni prodotti e funzionalità chiave di Dropbox che supportano il controllo dei contenuti.

Autorizzazioni granulari per i contenuti e autorizzazioni per file e cartelle condivisi

- ***Autorizzazioni per i file condivisi***

  Un membro del team che possiede un file condiviso può revocare l'accesso a specifici utenti e disattivare l'aggiunta di commenti al file.

- ***Autorizzazioni per i file condivisi***

  Un membro del team che possiede una cartella condivisa può revocare l'accesso alla cartella a utenti specifici, modificare le autorizzazioni di visualizzazione/modifica per utenti specifici e trasferire la proprietà della cartella. A seconda delle autorizzazioni di condivisione globali del team, il proprietario di ogni cartella condivisa può anche controllare se la cartella può essere condivisa con persone esterne al team, se le altre persone con autorizzazioni di modifica possono gestirne l'appartenenza e se i link all'interno della cartella possono essere condivisi con persone esterne alla cartella.

- ***Password per link condivisi***

  Qualsiasi link condiviso può essere protetto con una password definita dal proprietario. Prima che venga trasmesso qualsiasi dato relativo a file o cartelle, un livello di controllo dell'accesso verifica che sia stata inviata la password corretta e che siano stati soddisfatti tutti gli altri requisiti (come l'ACL del team, del gruppo o della cartella). In tal caso, un cookie di sicurezza viene memorizzato nel browser dell'utente per ricordare che la password è stata verificata in precedenza. Con i controlli di condivisione, gli amministratori possono anche impostare password predefinite, anziché mantenerle come opzioni facoltative, per salvaguardare meglio i contenuti del loro team.

- ***Scadenza dei link condivisi***

  Per consentire l'accesso temporaneo a file o cartelle, gli utenti possono impostare una scadenza per i link condivisi. Con i controlli di condivisione, gli amministratori possono anche impostare date di scadenza predefinite, anziché mantenerle come opzioni facoltative, per salvaguardare meglio i contenuti del proprio team.

Autorizzazioni per i documenti e le cartelle condivise di Paper

- ***Autorizzazioni per documenti e cartelle condivise di Paper***

  Un membro del team che possiede un documento o una cartella condivisa di paper può revocare l'accesso a specifici utenti e disattivare l'aggiunta di commenti al documento di Paper.

- ***Autorizzazioni per i documenti di Paper***

  Un membro del team che possiede un documento Paper può rimuovere l'accesso da parte di utenti specifici, esplicitamente elencati nel pannello di condivisione. Sia il proprietario che gli editor di un documento Paper possono modificare le autorizzazioni di visualizzazione/modifica per utenti specifici e cambiare la policy sui collegamenti relativa al documento. La policy sui collegamenti definisce quali utenti possono aprire il documento e le autorizzazioni di cui godono. L'amministratore del team può impostare una vasta gamma di policy su collegamenti e condivisione di documenti a livello di team.

- ***Autorizzazioni per le cartelle di Paper***

  Un membro del team che sia membro della cartella può modificare la policy di condivisione della cartella e rimuovere l'accesso a utenti specifici che siano stati precedentemente aggiunti alla cartella in modo esplicito.

Azioni su file e cartelle

- ***Cartella del team per i file***

  Gli amministratori possono creare cartelle del team che forniscono automaticamente ai gruppi e ad altri collaboratori il livello di accesso corretto (visualizzazione o modifica) ai contenuti di cui hanno bisogno.

- ***Accesso granulare e controlli di condivisione***

  I controlli di condivisione consentono agli amministratori di gestire l'appartenenza e le autorizzazioni a livello superiore o di sottocartella in modo che gli individui e i gruppi all'interno e all'esterno dell'azienda abbiano accesso unicamente a cartelle specifiche.

- ***Gestione delle cartelle del team***

  Gli amministratori possono visualizzare tutte le cartelle del loro team e personalizzare le politiche di condivisione da una posizione centrale, in modo da evitare l'errata condivisione di materiali riservati.

- ***Cartelle condivise per i documenti di Paper***

  Gli amministratori possono creare cartelle Paper che forniscono automaticamente ad altri collaboratori il livello di accesso corretto (visualizzazione o modifica) ai contenuti di cui hanno bisogno.

- ***Pulizia remota***

  Quando i dipendenti abbandonano il team o in caso di perdita del dispositivo, gli amministratori possono eliminare in remoto i dati di Dropbox e le copie locali dei file. I file saranno rimossi dai computer e dai dispositivi mobili quando sono online e l'applicazione Dropbox è in esecuzione.

- ***Trasferimento di account***

  Dopo aver eseguito il deprovisioning di un utente (manualmente o con i servizi di directory), gli amministratori possono trasferire i file e la proprietà dei documenti di Paper creati dall'utente in questione a un altro utente del team. La funzione di trasferimento dell'account può essere usata quando si rimuove un utente o in qualunque momento dopo l'eliminazione dell'account di un utente.

Le seguenti caratteristiche sono disponibili come funzionalità aggiuntive (contatta l'ufficio vendite per ulteriori informazioni).

- ***Scansione dei contenuti***

  Con il componente aggiuntivo Controlli avanzati per team e contenuti, i clienti Dropbox Business Advanced ed Enterprise potranno scansionare contenuti nuovi ed esistenti in Dropbox per individuare ed evitare vulnerabilità dei dati.

- ***Configurare e attivare flussi di lavoro personalizzati***

  Con il componente aggiuntivo Controlli avanzati per team e contenuti, gli amministratori possono intraprendere azioni personalizzabili sui file che violano le policy aziendali.

- ***Configurare gli avvisi***

  Gli amministratori possono monitorare i problemi correlati alla sicurezza in tempo reale ed evitare vulnerabilità dei dati. Ricevi avvisi sui file condivisi all'esterno e sui dati sensibili scansionati.

Visibilità sui contenuti

Avvisi e notifiche di sicurezza

Gli amministratori di Dropbox Enterprise possono ricevere notifiche in tempo reale quando vengono rilevate attività abusive, attività rischiose o potenziali perdite di dati sui loro account. È possibile monitorare i seguenti eventi:

- Eliminazioni di massa
- Spostamenti di massa dei dati
- Contenuti sensibili condividi esternamente
- Malware condivisi dall'esterno del team
- Malware condivisi nel team
- Troppi tentativi di accesso falliti
- Accesso da un Paese ad alto rischio
- Rilevamento ransomware

Dropbox fornisce anche la possibilità di configurare le soglie di avviso, modificare i destinatari delle notifiche e attivare avvisi quando le cartelle con file sensibili vengono condivise esternamente. Gli amministratori possono anche contrassegnare gli avvisi come in corso, risolti o respinti. Inoltre, un widget della dashboard mostra le informazioni e le tendenze generali del team nell'ultima settimana.

Report e pagina sulla condivisione esterna

Dropbox fornisce ulteriore visibilità con il report e la pagina di condivisione esterna. Gli amministratori possono creare un report dalla pagina delle statistiche o dalla pagina di condivisione esterna. Nel report sono presenti tutti i file e le cartelle del team condivisi all'esterno del team e tutti i link condivisi. La pagina di condivisione esterna è una pagina aggiuntiva della Console amministratore che consente agli amministratori di visualizzare e filtrare (per tipo di file, persona che ha effettuato la condivisione, impostazioni dei link e molto altro) i file e le cartelle condivisi direttamente dal team e dai link condivisi.

Controlli di condivisione

Le impostazioni di condivisione offrono agli amministratori del team un maggiore controllo sulla condivisione e sull'accesso ai contenuti del team. Gli amministratori possono impostare date di scadenza, limitazioni con password o entrambe a livello di team. Queste misure riducono il rischio di perdita di dati togliendo agli utenti la responsabilità di impostare restrizioni.

Classificazione dei dati

I team di Dropbox Enterprise possono etichettare automaticamente i propri dati sensibili per proteggerli evitando che vengano esposti. Quando i file o le cartelle salvati nelle cartelle del team contenenti informazioni sensibili vengono condivisi all'esterno del team, gli amministratori ricevono avvisi di prevenzione della perdita di dati (DLP) via e-mail e nella Console amministratore. Gli amministratori possono identificare e classificare automaticamente i dati sensibili archiviati nelle cartelle condivise e nelle cartelle personali dei membri del team. Gli amministratori di Dropbox Enterprise possono attivare la classificazione automatica dei dati dalla Console amministratore.

Componente aggiuntivo per la governance dei dati

La governance dei dati è l'insieme di tutti i processi, le tecnologie e i team che vengono impiegati per gestire e proteggere i dati di un'organizzazione. Nella governance dei dati rientra anche la possibilità di archiviare, identificare, scoprire e recuperare i dati aziendali.

Il componente aggiuntivo Governance dei dati di Dropbox riunisce un set di funzionalità che consentiranno alle organizzazioni di controllare e proteggere al meglio i propri dati, riducendo al contempo i rischi e i costi associati alla soddisfazione dei requisiti normativi e di conformità. Attualmente questo componente aggiuntivo include quattro funzioni chiave per gli amministratori del team e gli amministratori della conformità.

- ***Cronologia delle versioni estesa***

  La cronologia delle versioni dei file predefinita dipende dal tipo di account Dropbox di cui disponi. Tuttavia, con Dropbox Business puoi acquistare il componente aggiuntivo Cronologia delle versioni estesa (CVE) separatamente o all'interno del pacchetto del componente aggiuntivo Governance dei dati per poter ripristinare i file eliminati o modificati negli ultimi 10 anni.

- ***Conservazione ai fini giudiziari***

  Applicando la conservazione ai fini giudiziari su un membro del team, gli amministratori del team e gli amministratori della conformità possono visualizzare ed esportare tutti i contenuti creati o modificati da quel membro. I membri su cui è stata applicata la conservazione ai fini giudiziari non riceveranno una notifica in merito e continueranno a mantenere le loro autorizzazioni per creare, modificare ed eliminare i file.

- ***Conservazione dei dati***

  Con la conservazione dei dati, gli amministratori del team e della conformità possono impedire l'eliminazione accidentale dei contenuti richiesti dalle normative per un certo periodo di tempo. Questa funzione consentirà ai clienti di conservare i dati per oltre 10 anni dalla data di modifica più recente.

- ***Eliminazione dei dati***

  Attraverso l'eliminazione dei dati, gli amministratori del team e della conformità possono eliminare i dati in maniera permanente per soddisfare i requisiti di conservazione ed eliminazione dei dati. Gli amministratori possono monitorare l'attività attraverso la ricezione di report che li avvisano dell'imminente eliminazione dei file.

Ripristino e controllo versioni

Tutti i clienti di Dropbox Business hanno la possibilità di ripristinare file e documenti Paper eliminati e recuperare le versioni precedenti degli stessi, assicurandosi che le modifiche ai dati importanti possano essere monitorate e recuperate.

Sicurezza dei dati sui dispositivi mobili

- ***Cancellazione dei dati***

  Per un ulteriore livello di sicurezza, l'utente può attivare l'opzione di eliminazione dal dispositivo di tutti i dati salvati in Dropbox dopo dieci tentativi di inserimento di un passcode errato.

- ***Archiviazione interna e file salvati***

  Per impostazione predefinita, i file non sono archiviati nello spazio di archiviazione interno dei dispositivi mobili. I client di Dropbox per dispositivi mobili permettono di salvare singoli file e cartelle sul dispositivo per visualizzarli offline. Quando un dispositivo viene disconnesso da un account Dropbox, tramite l'interfaccia mobile o web, i file e le cartelle salvati vengono cancellati automaticamente dallo spazio di archiviazione interno del dispositivo.

- ***Documenti di Paper offline***

  Quando un dispositivo è scollegato da Paper tramite la pagina di sicurezza dell'account Dropbox, l'utente viene disconnesso e i documenti Paper offline vengono automaticamente eliminati dalla memoria interna del dispositivo.

Controlli del team

Poiché non esistono due organizzazioni esattamente uguali, abbiamo sviluppato vari strumenti che consentono agli amministratori di personalizzare Dropbox Business in base alle specifiche esigenze dei loro team. Dropbox Business include strumenti che consentono agli utenti finali di proteggere ulteriormente i propri account e dati. L'autenticazione, il recupero, la registrazione e le altre funzionalità di sicurezza riportate qui di seguito sono disponibili nelle diverse interfacce utente di Dropbox.

Di seguito sono riportate varie funzioni di controllo e visibilità disponibili tramite la Console amministratore di Dropbox Business.

Autorizzazioni granulari sui contenuti

- ***Livelli per ruoli amministrativi***

  Dropbox offre più livelli per i ruoli amministrativi, in modo da consentire una gestione più efficace dei team. Agli amministratori account può essere assegnato uno dei tre livelli di accesso previsti. Non vi è alcun limite al numero di amministratori attribuibili a un team; i ruoli amministrativi, inoltre, possono essere assegnati a qualsiasi membro del team.

- ***Amministratore team***

  Possono impostare autorizzazioni di sicurezza e di condivisione per tutto il team, creare amministratori e gestire i membri. L'amministratore team possiede tutte le autorizzazioni di amministrazione disponibili. Solo gli amministratori team possono assegnare o modificare i ruoli di amministratore. In un account Dropbox Business deve sempre essere presente almeno un amministratore team.

- ***Amministratore gestione utenti***

  Possono occuparsi della maggior parte delle attività di gestione del team, tra cui l'aggiunta e la rimozione dei membri del team, la gestione dei gruppi e la visualizzazione del feed delle attività di un team.

- ***Amministratore supporto***

  Possono occuparsi delle richieste di servizio comuni da parte dei membri del team, come il ripristino di file eliminati o l'assistenza a membri del team che non riescono a effettuare la verifica in due passaggi. Gli amministratori del supporto sono inoltre in grado di ripristinare le password di utenti non amministratori ed esportare un registro delle attività per un membro del team specifico.

- ***Amministratore della fatturazione***

  Può accedere alle pagine di fatturazione nella Console amministratore.

- ***Amministratore dei contenuti***

  Può creare e gestire le cartelle del team all'interno di Content Manager.

- ***Amministratore dei report***

  Può creare report all'interno della Console amministratore e ha accesso alla pagina Attività.

- ***Amministratore della sicurezza***

  Può gestire gli avvisi di sicurezza, la condivisione esterna e i rischi per la sicurezza.

- ***Amministratore della conformità (disponibile solo per i team con il componente aggiuntivo Governance dei dati)***

  Può gestire le pagine di Governance dei dati (conservazione ai fini giudiziari, conservazione dei dati ed eliminazione dei dati) e accedere a Content Manager.

- ***Gruppi***

  I team possono creare e gestire elenchi di membri all'interno di Dropbox e fornire loro accesso a cartelle specifiche in modo semplice. Inoltre, Dropbox può sincronizzare i gruppi di Active Directory tramite il connettore Active Directory.

- ***Gruppi gestiti dall'azienda***

  Solo gli amministratori possono creare, eliminare e gestire l'appartenenza a questo tipo di gruppi. Gli utenti non possono richiedere di partecipare a un gruppo gestito dall'azienda o di abbandonarlo.

- ***Gruppi gestiti dagli utenti***

  Gli amministratori possono scegliere se gli utenti possono creare e gestire i loro gruppi. Gli amministratori possono modificare un gruppo gestito dagli utenti in un gruppo gestito dall'azienda e assumerne il controllo.

- ***Limitazione di più account sui computer***

  Gli amministratori possono impedire che i membri del team associno un secondo account Dropbox ai computer associati al proprio account Dropbox.

- ***Sospensione dello stato di utente***

  Gli amministratori hanno la possibilità di disattivare l'accesso di un utente al proprio account salvando i relativi dati e le relazioni di condivisione al fine di mantenere al sicuro le informazioni aziendali. Gli amministratori possono riattivare o eliminare l'account in un secondo momento.

- ***Accesso come utente***

  Gli amministratori team possono effettuare l'accesso come membri dei propri team. Ciò fornisce loro un accesso diretto ai file, alle cartelle e ai documenti di Paper contenuti negli account dei membri del team in modo da apportare modifiche, eseguire condivisioni per conto dei membri del team o condurre audit di eventi a livello di file. Gli eventi "Accesso come utente" vengono registrati nel registro delle attività del team e gli amministratori possono stabilire se notificarli o meno ai membri.

- ***Autorizzazioni di condivisione***

  Gli amministratori del team esercitano un controllo completo sulle possibilità di condivisione del proprio team tramite Dropbox, tra cui:

  - La possibilità per i membri del team di condividere file e cartelle con persone esterne al team.
  - La possibilità per i membri del team di modificare cartelle di proprietà di persone esterne al team.
  - La possibilità alle persone esterne al team di accedere ai link condivisi creati dai membri del team.
  - La possibilità per i membri del team di creare richieste di file e accedere ai file di altri membri del team e/o di persone esterne al team.
  - La possibilità per gli utenti di visualizzare i file di proprietà del team e aggiungere commenti.
  - La possibilità per i membri del team di condividere documenti e cartelle di Paper con persone esterne al team.
  - La possibilità di concedere le autorizzazioni per l'eliminazione definitiva.

L'amministratore del team di un account Dropbox Business può limitare la possibilità di eliminare in via definitiva file e documenti Paper ai soli amministratori del team.

Onboarding e provisioning degli utenti

Metodi di provisioning degli utenti e gestione delle identità

- ***Invito tramite email***

  Uno strumento della console amministratore di Dropbox Business consente agli amministratori di generare manualmente un invito tramite email.

- ***Active Directory***

  Gli amministratori di Dropbox Business possono automatizzare la creazione e la rimozione di account da un sistema Active Directory esistente tramite il nostro connettore Active Directory o un provider di identità di terze parti. Una volta integrato, Active Directory può essere utilizzato per gestire l'adesione.

- ***Accesso singolo (Single sign-on, SSO)***

È possibile configurare Dropbox Business in modo da consentire l'accesso ai membri del team attraverso un provider di identità centralizzato. La nostra implementazione SSO, che utilizza lo standard di settore Security Assertion Markup Language 2.0 (SAML 2.0), semplifica e rende più sicuro il provisioning incaricando un

provider di identità attendibile dell'autenticazione e fornendo ai membri del team l'accesso a Dropbox senza un'ulteriore password da gestire. Dropbox ha inoltre avviato una partnership con i principali provider di gestione delle identità in modo che sia possibile eseguire automaticamente il provisioning e il deprovisioning degli utenti. Consulta la sezione Integrazioni API Dropbox Business qui di seguito.

- ***API***

  L'API Dropbox Business può essere utilizzata dai clienti per creare un provisioning personalizzato degli utenti e soluzioni di gestione delle identità. Consulta la sezione Integrazioni API Dropbox Business qui di seguito.

Verifica in due fasi

Questa funzionalità di sicurezza vivamente consigliata aggiunge un livello supplementare di protezione all'account Dropbox di un utente. Una volta attivata la verifica in due passaggi, Dropbox chiederà un codice di sicurezza a sei cifre, oltre alla password, ogni volta che si accede a Dropbox o si collega un nuovo computer, telefono o tablet.

- Gli amministratori possono scegliere di richiedere la verifica in due passaggi per tutti i membri del team o solo per alcuni membri specifici.
- Gli amministratori dell'account possono tenere traccia dei membri del team che hanno attivato la verifica in due passaggi.
- I codici dell'autenticazione in due passaggi di Dropbox possono essere ricevuti tramite messaggio di testo o applicazione conformi allo standard dell'algoritmo Time-based One-Time Password (TOTP).
- Nel caso in cui un utente non riceva i codici di sicurezza tramite questi metodi, può optare per l'utilizzo di un codice backup di emergenza monouso a 16 cifre. In alternativa, può utilizzare un numero di telefono secondario per ricevere un codice di backup tramite messaggio di testo.
- Dropbox supporta inoltre lo standard aperto FIDO Universal 2nd Factor (U2F), che consente agli utenti di eseguire l'autenticazione con una chiave di sicurezza USB configurata da loro anziché un codice a sei cifre.

Programma di installazione aziendale

Gli amministratori che richiedono un provisioning su vasta scala possono utilizzare il nostro programma di installazione aziendale per Windows per installare il client desktop di Dropbox in modalità silenziosa e in remoto tramite soluzioni di software gestiti e meccanismi di implementazione.

Dispositivi gestiti e login

- ***Enterprise mobility management - Gestione mobilità aziendale (EMM)***

  Dropbox si integra con provider di gestione di EMM di terze parti per fornire agli amministratori di Dropbox Business con un piano Enterprise un maggiore controllo sulle modalità di utilizzo di Dropbox su dispositivi mobili da parte dei membri del team. Gli amministratori possono limitare l'uso delle applicazioni mobile per gli account Dropbox Enterprise ai soli dispositivi mobili gestiti (forniti dall'azienda o personali), ottenere visibilità sull'uso delle applicazioni (tra cui lo spazio di archiviazione disponibile e le posizioni di accesso) ed eseguire una pulizia remota di un dispositivo smarrito o rubato. Si noti che l'applicazione Paper per dispositivi mobili non è gestibile tramite EMM.

- ***Approvazioni dispositivo***

  Dropbox permette agli amministratori di Dropbox Education e Dropbox Business con piani Advanced ed Enterprise di impostare il numero limite di dispositivi che un utente può sincronizzare con Dropbox e

scegliere se le approvazioni siano gestite dall'utente o dall'amministratore. Gli amministratori possono inoltre creare un elenco delle eccezioni di utenti non soggetti a uno specifico numero di dispositivi. Si noti che l'applicazione Paper per dispositivi mobili non è soggetta alle approvazioni dispositivo.

- ***Requisiti della verifica in due passaggi***

  Gli amministratori possono scegliere di richiedere la verifica in due passaggi per tutti i membri del team o solo per alcuni. Altri requisiti di autenticazione multifattore possono essere applicati tramite la propria implementazione SSO.

- ***Controllo password***

  Gli amministratori di team Education, Advanced ed Enterprise possono richiedere ai membri l'impostazione e la preservazione di password robuste e complesse per gli account. Quando questa funzione è abilitata, i membri del team verranno disconnessi da tutte le sessioni Web, per poi creare nuove password all'accesso. Uno strumento integrato analizza la robustezza delle password confrontandole con un database di termini, nomi, modelli e numeri comunemente usati. All'utente che inserisca una password comune verrà richiesto di crearne una più particolare e difficile da indovinare. Gli amministratori possono ripristinare le password per tutto il team o utente per utente.

- ***Gestione dei domini***

  Dropbox fornisce un set di strumenti per le aziende al fine di semplificare e velocizzare il processo di onboarding degli utenti e controllare l'utilizzo di Dropbox.

  - **Verifica del dominio.**
    Le aziende possono rivendicare la proprietà dei propri domini e sbloccare gli altri strumenti di gestione dei domini.

  - **Invito con imposizione.**
    Gli amministratori possono richiedere ai singoli utenti di Dropbox che sono stati invitati dal team Dropbox aziendale di migrare nel team o modificare l'indirizzo email del proprio account personale.

  - **Statistiche del dominio.**
    Gli amministratori sono in grado di visualizzare informazioni importanti, come il numero dei singoli account Dropbox che utilizzano indirizzi email aziendali.

  - **Cattura dell'account.**
    Gli amministratori possono obbligare tutti gli utenti Dropbox che utilizzano un indirizzo email aziendale a unirsi al team aziendale o modificare l'indirizzo email sul proprio account personale.

- ***Controllo sessioni web***

  Gli amministratori possono controllare per quanto tempo i membri del team possono mantenere attivo l'accesso a dropbox.com. Gli amministratori possono limitare la durata di tutte le sessioni Web e/o delle sessioni inattive. Le sessioni che raggiungono questi limiti verranno automaticamente disconnesse. Gli amministratori possono anche monitorare e chiudere le sessioni Web dei singoli utenti.

- ***Accesso alle applicazioni***

  Gli amministratori hanno la possibilità di visualizzare e revocare l'accesso delle app di terze parti agli account utente.

- ***Disconnessione di dispositivi***

  I computer e dispositivi mobili collegati agli account utente possono essere disconnessi dall'amministratore attraverso la Console amministratore o dall'utente nelle singole impostazioni di sicurezza dell'account. Sui computer, la disconnessione rimuove i dati di autenticazione e fornisce l'opzione di eliminare le copie locali dei file la volta successiva che il computer è online (vedi **Pulizia remota** di seguito). Sui dispositivi mobili, la disconnessione rimuove i file contrassegnati come preferiti, i dati nella cache e le informazioni di accesso, oltre ai documenti di Paper offline dall'applicazione Paper. Nel caso in cui fosse attiva la verifica in due passaggi, gli utenti devono autenticare nuovamente qualsiasi dispositivo al momento della nuova connessione. Inoltre, le impostazioni dell'account degli utenti offrono la possibilità di inviare un'email di notifica automatica quando viene collegato un dispositivo.

- ***Controllo di rete***

  Gli amministratori di Dropbox Business con piani Enterprise possono limitare l'uso di Dropbox sulla rete aziendale al solo account del team Enterprise. Questa funzionalità si integra con il provider di sicurezza di rete dell'azienda per bloccare l'eventuale traffico esterno all'account autorizzato sui computer. Si noti che Paper attualmente non è gestito attraverso il controllo della rete.

Sicurezza per dispositivi mobili

- ***Scansione delle impronte digitali***

  Come metodo per sbloccare l'applicazione Dropbox per dispositivi mobili, gli utenti possono attivare Touch ID o Face ID su dispositivi iOS e lo sblocco tramite impronte digitali (dove supportato) su dispositivi Android.

Visibilità sugli accessi

- ***Verifica dell'identità dell'assistenza tecnica***

  Prima che il Supporto Dropbox fornisca qualsiasi informazione relativa all'account o alla risoluzione di problemi, l'amministratore dell'account deve fornire un codice di sicurezza monouso generato in modo casuale per convalidare la sua identità. Tale PIN è disponibile solo attraverso la console amministratore.

Attività dell'account utente

Ogni utente può visualizzare le seguenti pagine dalle impostazioni del proprio account per ottenere informazioni aggiornate sull'attività dell'account.

- ***Pagina di condivisione***

  In questa pagina vengono visualizzate le cartelle condivise presenti attualmente nell'account Dropbox dell'utente, oltre alle cartelle condivise che l'utente può aggiungere. Un utente può annullare la condivisione di cartelle e file e impostare autorizzazioni di condivisione.

- ***Pagina File***

  Questa pagina mostra i file che sono stati condivisi con l'utente e la data in cui ogni file è stato condiviso. L'utente ha la possibilità di rimuovere il proprio accesso a questi file. Per visualizzare i documenti di Paper che sono stati condivisi con l'utente da altri, l'utente può accedere alla pagina "Condivisi con me" dall'interfaccia di navigazione dei documenti di Paper.

- ***Pagina Link***

  In questa pagina vengono visualizzati tutti i link condivisi attivi che l'utente ha creato e la data di creazione per ciascuno di essi. Inoltre, vengono visualizzati tutti i link che altre persone hanno condiviso con l'utente. L'utente può disattivare i link o modificare le autorizzazioni.

- ***Notifiche email***

  Un utente può decidere di ricevere una notifica via email immediatamente quando un nuovo dispositivo o una nuova app vengono collegati all'account Dropbox.

Autorizzazioni degli account utente

- ***Dispositivi collegati***

  La sezione **Dispositivi** delle impostazioni di sicurezza dell'account dell'utente mostra tutti i computer e i dispositivi mobili collegati all'account dell'utente. Per ogni computer viene visualizzato l'indirizzo IP, il Paese e l'ora approssimativa dell'attività più recente. Un utente può scollegare qualsiasi dispositivo, con l'opzione di eliminazione dei file sui computer collegati al successivo collegamento a Internet.

- ***Sessioni web attive***

  La sezione **Sessioni** mostra tutti i browser web al momento connessi all'account di un utente. Per ciascuno di essi viene visualizzato l'indirizzo IP, il Paese e l'ora di accesso della sessione più recente, oltre all'ora approssimativa dell'attività più recente, se indicata. L'utente può chiudere in remoto qualsiasi sessione dalle impostazioni di sicurezza dell'account.

- ***App collegate***

  La sezione **App collegate** fornisce un elenco di tutte le app di terze parti con accesso all'account di un utente e il tipo di accesso concesso a ogni app. Un utente può revocare le autorizzazioni di ogni app ad accedere al proprio Dropbox.

Feed delle attività

Dropbox Business registra le azioni intraprese sui file nel feed delle attività del team, accessibile dalla Console amministratore. Il feed delle attività offre opzioni di filtraggio flessibili che permettono agli amministratori di condurre analisi mirate sulle attività di account, file e documenti Paper. Ad esempio, possono visualizzare la cronologia completa di un file o documento Paper e come gli utenti hanno interagito con esso, oppure possono visualizzare tutte le attività del team in un determinato periodo di tempo. Il feed delle attività può essere esportato come report scaricabile in formato CSM ed essere integrato direttamente in un prodotto SIEM (gestione delle informazioni e degli eventi di sicurezza) o in un altro strumento di analisi attraverso soluzioni di terze parti. Nel feed delle attività sono registrati i seguenti eventi relativi ai contenuti:

- ***Condivisione di file, cartelle e link***

  Dove applicabile, i report specificano se le azioni coinvolgono persone esterne al team.

  File condivisi

  - Aggiunta o rimozione di un membro del team o di un non membro del team.
  - Modifica delle autorizzazioni per un membro del team o per un non membro del team.
  - Aggiunta o rimozione di un gruppo.
  - Aggiunta di un file condiviso all'account Dropbox dell'utente.
  - Visualizzazione del contenuto di un file condiviso tramite un invito di file o cartella.
  - Copia di contenuti condivisi nell'account Dropbox dell'utente.
  - Download di contenuti condivisi.
  - Commento su un file.

- Contrassegno di un commento come risolto o non risolto.
- Eliminazione di un commento.
- Sottoscrizione o annullamento dell'iscrizione alle notifiche dei commenti.
- Rivendicazione di un invito a un file di proprietà del team.
- Richiesta di accesso a un file di proprietà del team.
- Annullamento della condivisione di un file.

Cartelle condivise

- Creazione di una nuova cartella condivisa.
- Aggiunta o rimozione di un membro del team, di un non membro del team o di un gruppo.
- Aggiunta di una cartella condivisa all'account Dropbox dell'utente o rimozione da parte dell'utente del proprio accesso a una cartella condivisa.
- Aggiunta di una cartella condivisa da un link.
- Modifica delle autorizzazioni di un membro del team o di un non membro del team.
- Trasferimento di proprietà di una cartella a un altro utente.
- Annullamento della condivisione di una cartella.
- Rivendicazione dell'adesione a una cartella condivisa.
- Richiesta di accesso a una cartella condivisa.
- Aggiunta di un utente richiedente a una cartella condivisa.
- Blocco o sblocco di non membri del team dall'essere aggiunti a una cartella.
- Concessione a qualsiasi membro del team o soltanto al proprietario di aggiungere persone a una cartella.
- Modifica dell'accesso del gruppo a una cartella condivisa.

Link condivisi

- Creazione o rimozione di un link.
- Visualizzazione dei contenuti di un link da chiunque disponga del link o soltanto dai membri del team.
- Protezione con password dei contenuti di un link.
- Impostazione o rimozione della data di scadenza di un link.
- Visualizzazione di un link.
- Download dei contenuti di un link.
- Copia dei contenuti di un link nell'account Dropbox dell'utente.
- Creazione di un link a un file tramite un'applicazione API.
- Condivisione di un link con un membro del team, un non membro del team o un gruppo.
- Blocco o sblocco di non membri del team dal visualizzare link relativi a un file in una cartella condivisa.
- Condivisione di un album.

Richieste di file

- Creazione, modifica, chiusura o eliminazione di una richiesta di file.
- Aggiunta di utenti a una richiesta di file.
- Aggiunta o rimozione di una scadenza a una richiesta di file.
- Modifica di una cartella di richiesta di file.
- Ricezione di file tramite una richiesta di file.
- Ricezione di file tramite Email to Dropbox.

Eventi di cartelle e file individuali.

- Aggiunta di un file in Dropbox.
- Creazione di una cartella.
- Visualizzazione di un file.
- Modifica di un file.
- Download di un file.
- Copia di un file o di una cartella.
- Spostamento di un file o di una cartella.
- Ridenominazione di un file o una cartella.
- Ripristino di un file a una versione precedente.
- Annullamento delle modifiche di un file.
- Ripristino di un file eliminato.
- Eliminazione di un file o di una cartella.
- Eliminazione definitiva di un file o di una cartella.

Accessi andati a buon fine e non riusciti.

- Tentativo di accesso riuscito o non riuscito.
- Tentativo di accesso non riuscito o errore tramite Single sign-on (SSO).
- Tentativo di accesso non riuscito o errore tramite EMM.
- Disconnessione.
- Modifica dell'indirizzo IP per la sessione web.

Password

Modifiche alla password o alle impostazioni della verifica in due passaggi. Gli amministratori non possono visualizzare le password degli utenti.

- Modifica o ripristino della password.
- Attivazione, reimpostazione o disattivazione della verifica in due passaggi.

- Configurazione o modifica della verifica in due passaggi da utilizzare via SMS o tramite un'applicazione per dispositivi mobili.
- Aggiunta, modifica o rimozione di un telefono di backup per la verifica in due passaggi.
- Aggiunta o rimozione di una chiave di sicurezza per la verifica in due passaggi.

Adesione

Aggiunte al team e rimozioni.

- Invito a un membro del team.
- Aggiunta di un membro al team.
- Rimozione di un membro del team.
- Sospensione o annullamento della sospensione di un membro del team.
- Recupero o rimozione di un membro del team.
- Richiesta di partecipazione al team sulla base del domino dell'account.
- Approvazione o rifiuto di una richiesta di partecipazione al team sulla base del dominio dell'account.
- Invio di inviti di dominio ad account di domini esistenti.
- Ingresso dell'utente nel team in risposta alla cattura dell'account.
- Abbandono del dominio da parte dell'utente in risposta alla cattura dell'utente.
- Blocco o sblocco di membri del team dal suggerire nuovi membri del team.
- Suggerimento di un nuovo membro del team.

Applicazioni

Collegamento di app di terze parti agli account Dropbox.

- Autorizzazione o rimozione di un'applicazione.
- Autorizzazione o rimozione di un'applicazione del team.

Dispositivi

Collegamento di computer o dispositivi mobili agli account Dropbox.

- Collegamento o scollegamento di un dispositivo.
- Utilizzo della pulizia remota ed eliminazione di tutti i file riuscita o eliminazione di alcuni file non riuscita.
- Modifica di indirizzo IP per computer desktop o dispositivo mobile.

Azioni amministratore

Modifica alle impostazioni nella console amministratore, ad esempio le autorizzazioni delle cartelle condivise.

- ***Autenticazione e accesso singolo (SSO)***
  - Reimpostazione della password di un membro del team.
  - Reimpostazione della password di tutti i membri del team.

- Blocco o sblocco dei membri del team dal disattivare la verifica in due passaggi.
- Attivazione o disattivazione dell'SSO.
- Accesso tramite SSO impostato come obbligatorio.
- Modifica o rimozione dell'URL SSO.
- Aggiornamento del certificato SSO.
- Modifica della modalità di identificazione tramite SSO.

- ***Iscrizione***
  - Blocco o sblocco degli utenti dal richiedere di partecipare al team sulla base del dominio dell'account.
  - Impostazione delle richieste di adesione al team in modalità di approvazione automatica o manuale da parte dell'amministratore.

- ***Gestione degli account dei membri***
  - Modifica del nome di un membro del team.
  - Modifica dell'indirizzo email di un membro del team.
  - Assegnazione o rimozione dello stato di amministratore o modifica del ruolo di amministratore.
  - Accesso o disconnessione come membro del team.
  - Trasferimento o eliminazione dei contenuti dell'account di un membro rimosso.
  - Eliminazione definitiva dei contenuti dell'account di un membro rimosso.

- ***Impostazioni di condivisione globale***
  - Blocco o sblocco di membri del team dall'aggiungere cartelle condivise di proprietà di non membri del team.
  - Blocco o sblocco di membri del team dal condividere cartelle con non membri del team.
  - Attivazione di avvisi che vengono visualizzati dagli utenti prima di condividere cartelle con non membri del team.
  - Blocco o sblocco di non membri del team dal visualizzare i link condivisi.
  - Impostazione predefinita di link condivisi limitati ai membri del team.
  - Blocco o sblocco di persone dall'aggiungere commenti ai file.
  - Blocco o sblocco di membri del team dal creare richieste di file.
  - Aggiunta, modifica o rimozione di un logo per pagine di link condivisi.
  - Blocco o sblocco di membri del team dal condividere documenti e cartelle di Paper con non membri del team.

- ***Gestione delle cartelle del team per i file***
  - Creazione di cartelle del team.
  - Ridenominazione di una cartella del team.
  - Archiviazione o annullamento dell'archiviazione di una cartella del team.
  - Eliminazione definitiva di una cartella del team.
  - Downgrade di una cartella del team in una cartella condivisa.

- ***Gestione del dominio***
  - Tentativo di verifica o verifica riuscita di un dominio o rimozione di un dominio.
  - Verifica o rimozione di un dominio da parte del supporto Dropbox.
  - Attivazione o disattivazione dell'invio di inviti ai domini.
  - Attivazione o disattivazione dell'opzione "Invita automaticamente nuovi utenti".
  - Modifica della modalità di cattura dell'account.
  - Concessione o revoca della cattura di un account da parte del supporto Dropbox.
- ***Gestione della mobilità aziendale (EMM)***
  - Attivazione di EMM per la modalità di verifica (facoltativa) o di implementazione (obbligatoria).
  - Aggiornamento del token EMM.
  - Aggiunta o rimozione dei membri del team dall'elenco di utenti esclusi da EMM.
  - Disattivazione di EMM
  - Creazione di un rapporto della lista delle eccezioni EMM.
  - Creazione di un rapporto sull'utilizzo delle applicazioni per dispositivi mobili nell'ambito di EMM.
- ***Modifiche ad altre impostazioni del team***
  - Unione di team.
  - Upgrade del team a Dropbox Business o downgrade al team gratuito.
  - Modifica del nome del team.
  - Creazione di un report sull'attività del team.
  - Blocco o sblocco dei membri del team dall'associare uno o più account a un computer.
  - Concessione a tutti i membri del team o solo agli amministratori di creare gruppi.
  - Blocco o sblocco di membri del team dall'eliminare file definitivamente.
  - Avvio o chiusura di una sessione di supporto Dropbox per un rivenditore.

Gruppi

Informazioni su creazione, eliminazione e appartenenza relative ai gruppi.

- Creazione, ridenominazione, spostamento o eliminazione di un gruppo.
- Aggiunta o rimozione di un membro.
- Modifica del tipo di accesso per un membro del gruppo.
- Modifica del gruppo in gestito dal team o gestito dall'amministratore.
- Modifica dell'ID esterno di un gruppo.

Registro attività di Paper

Gli amministratori possono selezionare una tipologia di attività in Paper nel feed Attività o scaricare un report delle attività completo. Gli eventi di Paper sono registrati per:

- Attivazione o disattivazione di Paper.
- Creazione, modifica, esportazione, archiviazione, eliminazione permanente e ripristino di documenti di Paper.
- Aggiunta e risoluzione di commenti a documenti di Paper.
- Condivisione e annullamento della condivisione di documenti di Paper con membri e non membri del team.
- Richieste di accesso a documenti di Paper da parte di membri e non membri del team.
- Inserimento di tag in documenti di Paper relativi a membri e non membri del team.
- Visualizzazione di documenti di Paper da parte di membri e non membri del team.
- Attivazione della funzione "Segui" per un documento di Paper.
- Modifiche alle autorizzazioni dei membri di un documento di Paper (modifica, aggiunta di commenti o sola visualizzazione).
- Modifica della policy di condivisione esterna dei documenti di Paper.
- Creazione, archiviazione ed eliminazione permanente di un documento di Paper.
- Aggiunta o rimozione di un documento di Paper in una cartella.
- Ridenominazione di una cartella di Paper.
- Trasferimenti di documenti e cartelle di Paper.

Dropbox Passwords

Dropbox Passwords è una soluzione semplice e sicura per archiviare, sincronizzare e inserire automaticamente nome utente, password e dati di carte di credito o debito su diversi dispositivi, proteggendo al contempo le tue credenziali online. Dropbox Passwords protegge i nomi utente, le password e le carte di credito e di debito sensibili dei tuoi account online con una crittografia a conoscenza zero nel cloud e sui dispositivi degli utenti. I nostri prodotti sono creati per l'uso quotidiano e progettati per garantire la massima sicurezza.

Crittografia a conoscenza zero

Dropbox Passwords archivia i tuoi dati crittografati nel cloud, ma le chiavi per decrittografare tali dati vengono memorizzate solo sui tuoi dispositivi. **Dropbox non ha mai accesso a esse.** Queste chiavi sono lunghe, casuali e generate sul tuo dispositivo. Non lasciano mai il dispositivo, tranne quando decidi di associare o registrare un nuovo dispositivo. Questo trasferimento usa la crittografia a chiave pubblica per firmare a livello di crittografia e proteggere le chiavi durante il trasferimento, per garantirti che nessun altro utente possa decrittografarle e verificare al contempo la loro autenticità. Questa proprietà spesso è chiamata crittografia a conoscenza zero perché i dati crittografati sono inutili per chiunque non disponga delle chiavi, Dropbox incluso. Questo significa **che solo tu potrai vedere le tue informazioni** e che nell'improbabile caso in cui Dropbox venisse violato, le tue informazioni sarebbero comunque al sicuro. I dati crittografati sono separati dalle cartelle visibili di Dropbox e non possono essere incrociati dai client o dalle API Dropbox.

Dettagli crittografia

Dropbox crittografa i tuoi dati usando XChaCha20-Poly1305 in modalità combinata per l'autenticazione implicita. Le nostre estensioni browser e le applicazioni mobili utilizzano implementazioni di crittografia supportate da libsodium, che è un fork di NaCl verificato e ampiamente distribuito.

Ogni operazione di crittografia genera un nonce casuale a 192 bit, che viene memorizzato con il payload crittografato per la successiva decrittografia. A differenza di AES-GCM, XChaCha20-Poly1305 supporta nonce casuali. Durante la decrittografia, il nonce a 192 bit viene letto dal payload e utilizzato per decrittografare il payload crittografato. Tutte le crittografie successive generano un nonce a 192 bit casuale indipendente dal nonce precedente. Dropbox Passwords genera numeri casuali utilizzando libsodium, che utilizza per impostazione predefinita un generatore di numeri casuali a livello di crittografia, sicuro su tutte le piattaforme supportate.

Chiavi e parole di ripristino

Generiamo una chiave simmetrica a 256 bit (la chiave di crittografia) da 128 bit di entropia (la chiave utente) tramite hashing Blake2. Questa chiave di crittografia rimane solo sui dispositivi del proprietario e, quando possibile, nell'archivio più sicuro a cui abbiamo accesso su tali dispositivi. Ad esempio, in un iPhone la chiave di crittografia viene memorizzata nel portachiavi iOS.

Utilizziamo 128 bit di entropia come fonte perché offre una sicurezza sufficiente e richiede solo 12 parole di ripristino utilizzando lo standard BIP-39 per il backup. BIP-39 fornisce un modo intuitivo per rappresentare chiavi casuali di grandi dimensioni trasformandole in un elenco di 12 parole. Qualsiasi chiave a 128 bit ha un elenco corrispondente di parole e ogni elenco di 12 parole identifica in modo univoco i 128 bit. Una sola precisazione: le 12 parole corrispondono ai 132 bit, quindi i 4 bit extra vengono usati come checksum per identificare gli errori. Le parole di ripristino forniscono un modo per ripristinare la chiave di crittografia in caso il dispositivo venga smarrito o rubato. Consigliamo di stamparle e memorizzarle in un posto sicuro. Potresti persino pensare di darle a un amico fidato o a un membro della famiglia, oppure di conservarle su chiavetta.

Registrazione dei dispositivi

Quando un utente accede a Dropbox Passwords su un nuovo dispositivo, tale dispositivo dovrà completare una procedura di registrazione di sicurezza per accedere ai dati Passwords dell'utente. Questa procedura garantisce che la chiave segreta di un utente e i dati Passwords siano accessibili solo sui dispositivi registrati dell'utente. Fa anche in modo che un utente possa registrare unicamente dispositivi aggiuntivi che abbiano accesso a un dispositivo registrato esistente o alle parole di ripristino. La procedura di registrazione del dispositivo avviene come segue.

Un dispositivo in fase di registrazione genera casualmente una coppia di chiavi del dispositivo pubblica/privata a 256 bit e carica la chiave pubblica sul server Dropbox. Quindi, possono verificarsi 3 tipi di scenario: **A**, **B** o **C** .

A: se l'utente non ha registrato un dispositivo in precedenza, il dispositivo in fase di registrazione genera in modo casuale una chiave segreta a 128 bit. Sia la chiave utente sia la chiave dispositivo vengono memorizzate in una posizione specifica sicura del sistema operativo, come descritto nella sezione Memorizzazione delle chiavi di seguito. Il dispositivo inizializza i dati Passwords dell'utente, li crittografa e carica il payload crittografato nel server Dropbox.

B: se l'utente ha già registrato dispositivi in precedenza, viene inviata una richiesta di approvazione della registrazione a tutti i dispositivi registrati. La chiave pubblica del dispositivo in fase di registrazione viene allegata a ogni richiesta. L'utente dovrà quindi approvare la richiesta su uno dei dispositivi registrati. Se approvata, il dispositivo registrato crittograferà la chiave utente usando la sua chiave privata e la chiave pubblica del dispositivo in fase di registrazione tramite X25519 ECDH con XSalsa20-Poly1305. Il dispositivo registrato caricherà la chiave utente crittografata nel server Dropbox per inviarla al dispositivo in fase di registrazione, che scaricherà ed eseguirà la decrittografia della chiave utente usando la sua chiave privata e la chiave pubblica del dispositivo registrato. Il dispositivo in fase di registrazione scaricherà quindi i dati del payload Passwords crittografati ed eseguirà la loro decrittografia con la chiave utente.

C: se l'utente ha registrato un dispositivo in precedenza, ma non può più accedervi, potrà immettere le 12 parole di ripristino per ricostruire localmente la chiave utente. Quindi, il dispositivo in fase di registrazione scaricherà i dati del payload Passwords crittografati e procederà alla loro decrittografia con la chiave utente.

Memorizzazione delle chiavi

Estensioni browser

Nei browser web, la chiave utente viene memorizzata nell'area di archiviazione locale dell'estensione. I valori dello spazio di archiviazione locale dell'estensione del browser sono accessibili solo dall'estensione. Qualsiasi codice in esecuzione nei siti web visitati dall'utente non può leggere l'area di archiviazione locale dell'estensione del browser. Inoltre, le estensioni del browser impediscono l'esecuzione di qualsiasi codice non incluso nel pacchetto dell'estensione firmata, eliminando il rischio di una vulnerabilità XSS che potrebbe accedere a valori di archiviazione locale.

Un utente malintenzionato con accesso illimitato al dispositivo dell'utente può accedere alla chiave utente leggendo il file di archiviazione locale sul disco. Esempi di tali minacce includono: un utente malintenzionato con accesso fisico al dispositivo o un utente malintenzionato che esegue malware dannoso sul dispositivo. Per proteggersi da questi scenari, l'utente può configurare una passphrase sul dispositivo locale.

Quando viene configurata una passphrase, viene crittografata la chiave utente inattiva nello spazio di archiviazione locale dell'estensione del browser. La chiave di crittografia deriva dalla passphrase tramite l'hashing della password Argon2 e il metodo di crittografia usato è XChaCha20-Poly1305. Ogni volta in cui viene riavviata l'estensione del browser, l'utente deve fornire la passphrase per decrittografare la chiave utente e sbloccare i suoi dati. Di conseguenza, un utente malintenzionato senza la passphrase non potrà decrittografare la chiave utente memorizzata nel file di archiviazione locale su disco.

iOS

Su iOS, la chiave utente viene memorizzata nel portachiavi iOS, un file di database crittografato su disco. Il file viene crittografato con una chiave segreta memorizzata nel modulo hardware Secure Enclave, usando AES256-GCM come metodo di crittografia. Solo l'app iOS Dropbox Passwords firmata può accedere agli elementi memorizzati nel portachiavi. Questo eviterà che altro codice in esecuzione sul dispositivo dell'utente possa accedere alla chiave utente.

Android

Su Android, la chiave utente viene memorizzata in un oggetto EncryptedSharedPreferences, un file delle preferenze crittografato su disco. Il file viene crittografato con una chiave master memorizzata nell'hardware protetto Android Keystore, usando AES256-GCM come metodo di crittografia. Solo l'app Android Dropbox Passwords firmata può accedere alla chiave master usata per decrittografare il file delle preferenze.

Autenticazione locale

Dropbox Passwords fornisce misure di autenticazione locale facoltative per restringere ulteriormente l'accesso ai dati Passwords degli utenti sui loro dispositivi fisici. Per le applicazioni mobile, la tipologia di autenticazione del sistema operativo locale può essere riutilizzata (ad esempio, passcode con autenticazione biometrica aggiuntiva). Per le estensioni del browser, può essere configurata una passphrase facoltativa. Questi meccanismi forniscono un livello aggiuntivo di sicurezza delle applicazioni quando il sistema operativo del dispositivo dell'utente è sbloccato. Questo consente all'utente di proteggere i dati di Passwords nel caso in cui un altro utente accedesse al suo dispositivo, come un collega o un membro della famiglia.

Suggerimenti sulla sicurezza della password

Dropbox ha creato lo strumento open-source zxcvbn, che viene usato da diversi gestori di password per valutare la sicurezza delle password. Lo strumento confronta le password con un database di 30.000 password comuni, nomi e cognomi comuni in base ai dati del censimento USA, parole inglesi di uso popolare tratte da Wikipedia, film e programmi TV americani e altri modelli ordinari come date, ripetizioni (aaa), sequenze (abcd), modelli da tastiera (qwertyuiop) e Leet Speak. Se la password che l'utente prova a immettere è comune, lo strumento chiederà all'utente di provare a immettere una password più univoca e difficile da indovinare. Usando l'impostazione **Molto complessa** avrai la certezza di disporre del massimo livello di sicurezza dell'account per gli utenti.

Sicurezza dei dati, privacy e trasparenza

Le persone e le organizzazioni affidano ogni giorno a Dropbox i propri file di lavoro più importanti e, pertanto, è nostra responsabilità proteggere questi dati e garantirne la riservatezza.

Norme sulla privacy

Le nostre Norme sulla privacy sono disponibili alla pagina www.dropbox.com/privacy. Le Norme sulla privacy, il Contratto di servizio, i Termini di servizio e le Norme sull'uso accettabile di Dropbox richiamano l'attenzione sui seguenti argomenti:

- Che tipo di dati raccogliamo e perché.
- Con chi possiamo condividere informazioni.

- In che modo proteggiamo i dati e per quanto tempo li conserviamo.
- Dove conserviamo e come trasmettiamo i dati.
- Che cosa succede in caso di modifiche alle norme o in caso di domande.

Trasparenza

Dropbox si impegna a garantire la massima trasparenza nella gestione delle richieste di applicazione della legge per le informazioni degli utenti, oltre al numero e ai tipi di tali richieste. Esaminiamo tutte le richieste di dati per assicurarci che siano legittime e ci impegniamo ad avvisare gli utenti quando i loro account sono identificati in una richiesta di applicazione della legge, a meno che ciò non ci sia proibito per legge.

Tale impegno sottolinea la nostra volontà di tutelare la privacy dei nostri utenti, nonché quella dei loro dati. A tal fine, mettiamo a disposizione un rapporto sulla trasparenza e abbiamo definito un insieme di Principi relativi alle richieste da parte delle forze dell'ordine. I principi che seguono regolano le nostre azioni nel momento in cui riceviamo, analizziamo e rispondiamo alle richieste delle autorità sui dati dei nostri utenti:

- ***Essere trasparenti***

  Crediamo che ai servizi online debba essere consentito di pubblicare il numero e la tipologia delle richieste governative ricevute e di informare i soggetti interessati in merito alla richiesta di informazioni che li riguardano. Questo tipo di trasparenza aiuta gli utenti a comprendere meglio le istanze e i modelli di rischio con gli enti pubblici. Continueremo a pubblicare informazioni dettagliate su queste richieste e a difendere il diritto di fornire sempre più importanti informazioni di questo tipo.

- ***Rifiutare richieste di portata globale***

  Le richieste di dati da parte di enti governativi devono essere limitate a persone specifiche e legittime indagini. Ci opporremo a qualsiasi richiesta di portata eccessivamente ampia.

- ***Proteggere tutti gli utenti***

  Le norme che garantiscono alle persone tutele diverse in base al luogo in cui vivono o alla loro cittadinanza sono obsolete e non riflettono la natura globale dei servizi online. Continueremo a sostenere la riforma di queste leggi.

- ***Fornire servizi affidabili***

  La pubblica autorità non deve mai installare backdoor nei servizi online o violare l'infrastruttura per ottenere i dati degli utenti. Continueremo a lavorare per proteggere i nostri sistemi e per cambiare le leggi affinché sia chiaro che questo tipo di attività è da considerarsi illegale.

I nostri rapporti sulla trasparenza sono disponibili alla pagina dropbox.com/transparency.

Certificazioni sulla privacy, attestazioni e conformità normativa

Ogni giorno persone e organizzazioni affidano a Dropbox i loro file di lavoro più importanti. Per questo motivo, è nostra responsabilità proteggere questi file e garantirne la riservatezza. Il nostro impegno nei confronti della tua privacy è al centro di ogni decisione che prendiamo.

ISO/IEC 27018 (Codice di condotta per la protezione dei dati personali nel cloud) e ISO/IEC 27701 (Estensione di ISO/IEC 27001 e ISO/IEC 27002 per la gestione delle informazioni sulla privacy)

Tra i principali fornitori di servizi cloud, Dropbox Business è stato uno tra i primi ad aver ottenuto la certificazione ISO/IEC 27018 e ISO/IEC 27701.

ISO/IEC 27018 è uno standard globale per la protezione della privacy e dei dati nel cloud ed è stato pubblicato nell'agosto del 2014 per affrontare nello specifico la protezione della privacy e dei dati degli utenti.

ISO/IEC 27701 è stato il primo standard globale certificabile per la gestione delle informazioni sulla privacy ed è stato pubblicato nel 2019 per fornire un quadro normativo per estendere il sistema di gestione della sicurezza (ISMS) da ISO/IEC 27001 a un sistema di gestione delle informazioni sulla privacy (PIMS) includendo considerazioni sulla privacy dei dati.

Tali standard prevedono numerosi requisiti relativi a come Dropbox utilizzerà o meno le informazioni della tua organizzazione:

- ***È la tua organizzazione ad avere il controllo dei dati***

  Utilizziamo solo le informazioni personali che ci fornisci affinché possiamo offrirti i servizi per i quali ti sei registrato. Puoi aggiungere, modificare o eliminare i file e documenti di paper da Dropbox all'occorrenza.

- ***I tuoi dati vengono utilizzati con la massima trasparenza***

  Saremo trasparenti su dove vengono ubicati i dati nei nostri server. Inoltre, ti informeremo su chi sono i nostri partner fidati. Ti spiegheremo che cosa accade quando chiudi un account o elimini un file o un documento di Paper. Infine, ti faremo sapere se vengono apportate modifiche a una qualsiasi delle funzionalità di Dropbox.

- ***I tuoi dati sono al sicuro e protetti***

  ISO/IEC 27018 e ISO/IEC 27701 sono stati concepiti per migliorare ed estendere ISO/IEC 27001, uno degli standard di sicurezza delle informazioni più accettati al mondo. Abbiamo ricevuto il rinnovo della certificazione ISO/IEC 27001 nell'ottobre del 2021.

- ***Le nostre pratiche vengono revisionate regolarmente***

  L'adesione agli standard ISO/IEC 27018, ISO/IEC 27701 e ISO/IEC 27001 prevede che, per poter mantenere tali certificazioni, vengano effettuati annualmente audit da parte di terze parti indipendenti. Le nostre certificazioni ISO sono disponibili qui.

Trasferimenti di dati

Nel trasferire dati dall'Unione Europea, dallo Spazio economico europeo, dal Regno Unito e dalla Svizzera, Dropbox si affida a una serie di meccanismi legali, inclusi i contratti con i propri clienti e affiliati, le Clausole contrattuali standard e le decisioni di adeguatezza della Commissione europea in merito a determinati Paesi, a seconda dei casi.

Dropbox è conforme alle normative dello Scudo UE-USA e Svizzera-USA per la privacy come stabilito dal Dipartimento del commercio degli Stati Uniti d'America per quanto riguarda la raccolta, l'utilizzo e la conservazione dei dati personali provenienti dall'Unione Europea, dallo Spazio economico europeo, dal Regno

Unito e dalla Svizzera e trasferiti agli Stati Uniti, sebbene Dropbox non utilizzi lo Scudo UE-USA né lo Scudo Svizzera-USA come base giuridica per i trasferimenti di dati personali. Dropbox ha certificato al Dipartimento del Commercio degli Stati Uniti la propria adesione ai principi dello Scudo per la privacy per quanto riguarda tali dati. Per ulteriori informazioni sullo Scudo per la privacy, consulta la pagina https://www.privacyshield.gov.

Eventuali reclami e controversie relativi alla nostra conformità allo Scudo per la privacy vengono esaminati e risolti tramite JAMS, una terza parte indipendente. Per ulteriori informazioni, vedere le nostre Norme sulla privacy (dropbox.com/privacy).

Regolamento generale sulla protezione dei dati (GDPR)

Il Regolamento generale sulla protezione dei dati (GDPR)) è un regolamento europeo del 2018 che stabilisce un accordo quadro completo sulla gestione e sulla protezione dei dati personali.

Dropbox si impegna a garantire la sicurezza e la protezione dei dati dei nostri utenti in qualsiasi momento, in conformità ai requisiti legali e alle best practice. In linea con il nostro impegno verso i nostri utenti, lavoriamo duramente per garantire che Dropbox sia conforme al GDPR; a tale proposito, abbiamo designato un responsabile per la protezione dei dati, ristrutturato il nostro programma sulla privacy per assicurare che gli utenti potessero esercitare i propri diritti in qualità di soggetti interessati, e documentato i nostri processi interni in caso di violazioni del sistema di sicurezza. Continuiamo ad apportare miglioramenti per garantire che, a mano a mano che continuano a emergere nuove linee guida da parte delle autorità per la protezione dei dati, i nostri processi e le nostre pratiche soddisfino o addirittura superino gli elementi specifici delle nuove norme.

Codice di condotta UE per il cloud

Il Codice di condotta UE per il cloud è uno strumento volontario che consente a un fornitore di servizi cloud come Dropbox di dimostrare il proprio impegno verso la conformità al GDPR. Dropbox Business, che comprende i piani Standard, Advanced, Enterprise ed Education per team, è stato dichiarato aderente al Codice di condotta UE per il cloud e ha ricevuto un marchio di conformità di "Livello 2"; ciò significa che questi servizi hanno implementato misure tecniche, organizzative e contrattuali in linea con i requisiti del Codice. Per ulteriori informazioni sul Codice di condotta dell'UE per il cloud e sulla conformità di Dropbox al codice, visita il sito ufficiale del codice.

Per ulteriori informazioni sulle nostre pratiche e norme sulla privacy, consulta il nostro libro bianco in materia di protezione della privacy e dei dati.

Compliance

Esistono molti requisiti normativi e specifici di settore in materia di sicurezza e privacy che la tua organizzazione potrebbe essere tenuta a soddisfare. Il nostro approccio consiste nel combinare gli standard più ampiamente accettati con provvedimenti sulla compliance personalizzati in base alle specifiche esigenze delle attività o dei settori dei nostri clienti.

ISO

La International Organization for Standardization (ISO) ha sviluppato una serie di standard di livello mondiale per la sicurezza delle società e delle informazioni, al fine di aiutare le organizzazioni a sviluppare prodotti e servizi affidabili e innovativi. Dropbox vanta data center, sistemi, applicazioni, persone e processi certificati acquisiti tramite una serie di audit condotti da EY CertifyPoint, una terza parte indipendente con sede nei Paesi Bassi e accreditamenti ISO emessi dalla Raad voor Accreditatie (Consiglio di accreditamento olandese).

ISO/IEC 27001 (sicurezza delle informazioni)

ISO/IEC 27001 è riconosciuto come il più importante standard per la gestione della sicurezza delle informazioni al mondo. Lo standard sfrutta inoltre le best practice delineate in ISO/IEC 27002. Per guadagnarci la tua fiducia, presso Dropbox gestiamo in maniera continuativa e completa i nostri controlli legali, tecnici e fisici.

Visualizza il certificato ISO/IEC 27001 di Dropbox Business e Dropbox Education.

ISO/IEC 27017 (sicurezza del cloud)

ISO/IEC 27017 è uno standard internazionale per la sicurezza del cloud che fornisce linee guida per i controlli di sicurezza applicabili al provisioning e all'utilizzo di servizi cloud. Numerosi altri requisiti di sicurezza, privacy e compliance ai quali Dropbox e i suoi clienti possono rispondere insieme sono illustrati nella nostra Guida alla responsabilità condivisa.

Visualizza il certificato ISO/IEC 27017 di Dropbox Business e Dropbox Education.

ISO/IEC 27018 (protezione di dati e privacy nel cloud)

ISO/IEC 27018 è uno standard internazionale per la privacy e la protezione dei dati che si applica ai fornitori di servizi cloud come Dropbox, che elaborano informazioni personali per conto dei propri clienti e fornisce la base su cui i clienti possono affrontare le questioni o i requisiti normativi e contrattuali più frequenti.

Visualizza il certificato ISO/IEC 27018 di Dropbox Business e Dropbox Education.

ISO/IEC 22301 (continuità aziendale)

ISO/IEC 22301 è uno standard internazionale per la continuità aziendale, che indica alle organizzazioni come ridurre le probabilità di eventi imprevisti e quali risposte approntare nel caso in cui questi ultimi si verifichino, riducendo al minimo i danni. Il sistema di gestione della continuità aziendale (BCMS) di Dropbox Business fa parte della nostra strategia generale di gestione dei rischi per proteggere le persone e le operazioni in momenti di crisi.

Visualizza il certificato ISO/IEC 22301 di Dropbox Business e Dropbox Education.

ISO/IEC 27701 (Gestione delle informazioni sulla privacy)

ISO 27701 è uno standard internazionale per la gestione delle informazioni sulla privacy. Lo standard fornisce un quadro normativo per migliorare ed estendere il sistema di gestione della sicurezza delle informazioni disciplinato da ISO 27001 a un sistema di gestione delle informazioni sulla privacy. Dropbox Business e Dropbox Education hanno ricevuto questa certificazione in quanto responsabili delle informazioni di identificazione personale.

Visualizza il certificato ISO 27701 di Dropbox Business e Dropbox Education.

SOC

I report dei Service Organization Controls (SOC), noti rispettivamente come SOC 1, SOC 2 o SOC 3, sono disposizioni stabilite dall'American Institute of Certified Public Accountants (AICPA) per la segnalazione dei controlli interni implementati in un'organizzazione. Sistemi, applicazioni, persone e processi di Dropbox sono stati certificati tramite una serie di audit condotti da Ernst & Young LLP, una società terza di audit indipendente.

SOC 3 per sicurezza, riservatezza, integrità, disponibilità e privacy

La relazione SOC 3 copre tutti e cinque i Trust Service Criteria di sicurezza, riservatezza, integrità, disponibilità e privacy (TSP Section 100). La relazione generale di Dropbox è un riassunto esecutivo del report SOC 2 e include l'opinione della società terza incaricata dell'audit sulla progettazione e sull'effettiva attuazione dei nostri controlli.

Visualizza l'esame SOC 3 di Dropbox Business e Dropbox Education.

SOC 2 per sicurezza, riservatezza, integrità, disponibilità e privacy

Il report SOC 2 fornisce ai clienti un livello avanzato di garanzia basata su controlli che coprono tutti e cinque i Trust Service Criteria di sicurezza, riservatezza, integrità, disponibilità e privacy (TSP Section 100). Il report SOC 2 include una descrizione dettagliata dei processi di Dropbox e di oltre 100 controlli che effettuiamo per la protezione dei dati dei clienti. Oltre all'opinione della società terza incaricata dell'audit sulla progettazione e sull'effettiva attuazione dei nostri controlli, il report include le procedure di test della società di audit e i risultati di ciascun controllo. Il nostro report SOC 2 (talvolta definito report SOC 2+) include anche una mappatura sottoposta ad audit dei nostri controlli in base agli standard ISO summenzionati, per offrire ai clienti una trasparenza ancora maggiore. L'esame SOC 2 per Dropbox Business e Dropbox Education è disponibile su richiesta.

SOC 1/SSAE 18/ISAE 3402 (in precedenza SSAE 16 o SAS 70)

Il report SOC 1 fornisce garanzie specifiche per i clienti che determinano come Dropbox Business o Education sia un elemento fondamentale del proprio programma di controlli interni sui report finanziari (ICFR). Queste garanzie specifiche sono utilizzate principalmente per la compliance Sarbanes-Oxley (SOX) dei nostri clienti. L'audit di società terza indipendente è condotto secondo quanto previsto dallo Statement on Standards for Attestation Engagements No. 18 (SSAE 18) e dall'International Standard on Assurance Engagements No. 3402 (ISAE 3402), che hanno sostituito gli ormai obsoleti Statement on Standards for Attestation Engagement No. 16 (SSAE16) e Statement on Auditing Standards No. 70 (SAS 70). L'esame SOC 1 di Dropbox Business ed Education è disponibile su richiesta.

CSA

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

Il CSA Security, Trust & Assurance Registry (STAR) è un registro gratuito e pubblico che offre un programma di garanzia della sicurezza per servizi cloud. Aiuta gli utenti a valutare il livello di sicurezza cloud dei fornitori dei servizi che utilizzano al momento o con i quali hanno intenzione di stipulare un contratto.

Dropbox Business e Dropbox Education hanno ottenuto la CSA STAR Level 2 Certification e la Level 2 Attestation. La CSA STAR Level 2 richiede una valutazione da parte di una società terza indipendente dei nostri controlli di sicurezza, effettuata da EY CertifyPoint (Certification) e da Ernst & Young (Attestation) in base ai requisiti ISO 27001, SOC 2 Trust Services Criteria e CSA Cloud Controls Matrix (CCM) v.4.0.2.

Visualizza il nostro CSA STAR Level 2 Certification and Attestation sul sito web del CSA.

HIPAA/HITECH

Dropbox intende stipulare dei contratti di società in affari (BAA) con i clienti Dropbox Business o Dropbox Education che ne facciano richiesta per conformarsi all'Health Insurance Portability and Accountability Act (HIPAA) e all'Health Information Technology for Economic and Clinical Health Act (HITECH). Vedi Dropbox e HIPAA/HITECH per altre informazioni.

Dropbox rende disponibile un report di garanzia di terze parti che valuta i nostri controlli di conformità alle norme HIPAA/HITECH in materia di sicurezza, privacy e violazione, oltre a una mappatura delle nostre pratiche e raccomandazioni interne per i clienti che necessitano di soddisfare i requisiti HIPAA/HITECH Security e Privacy Rule con Dropbox Enterprise, Enterprise o Education.

I clienti interessati a richiedere questi documenti o che desiderano maggiori informazioni sull'acquisto di Dropbox Business o Dropbox Education, sono pregati di contattare il nostro team di vendita. Se sei un amministratore team corrente di Dropbox Business o Dropbox Education, puoi firmare elettronicamente un BBA dalla pagina Account nella Console amministratore.

Si noti che la possibilità di firmare un BAA elettronico tramite la Console amministratore è disponibile solo per i clienti con sede negli Stati Uniti.

NIST 800-171

Il National Institute of Standards and Technology (NIST) statunitense promuove e mantiene gli standard e le linee guida per aiutare a proteggere i sistemi informativi. La NIST Special Publication (SP) 800-171 Revision 2 (R2) fornisce le linee guida sulla protezione delle Informazioni non classificate controllate nelle organizzazioni e nei sistemi non federali. Qualsiasi entità che elabori o memorizzi Informazioni non classificate controllate del governo statunitense, quali istituti di ricerca e il settore dell'istruzione, dovrebbe essere conforme al NIST SP 800-171 R2. I sistemi, i processi e i controlli delle Informazioni non classificate controllate sono stati convalidati da un revisore indipendente di terze parti, Ernst & Young LLP.

Il report NIST SP 800-171 R2 per Dropbox Business e Dropbox Education è disponibile su richiesta tramite il nostro team di vendita o (per i clienti Dropbox Business esistenti) tramite il nostro supporto.

Si noti che Dropbox Paper non è incluso nell'ambito del report NIST SP 800-171 R2.

FERPA e COPPA (studenti e minori)

Dropbox Business e Dropbox Education permettono ai clienti di utilizzare i servizi in ottemperanza agli obblighi dei rivenditori imposti dal Family Education Rights and Privacy Act (FERPA). Anche gli istituti scolastici con studenti di età inferiore ai 13 anni possono utilizzare Dropbox Business o Dropbox Education in conformità al Children's Online Privacy Protection Act (COPPA), a condizione che accettino specifiche norme contrattuali che richiedono all'istituto di ottenere il consenso dei genitori in relazione all'uso dei nostri servizi.

FDA 21 CFR Part 11

Il Titolo 21 del Code of Federal Regulations (CFR) disciplina i prodotti alimentari e farmaceutici negli Stati Uniti per la Food and Drug Administration (FDA), la Drug Enforcement Administration e l'Office of National Drug Control Policy. La parte 11 del Title 21 stabilisce i criteri in base ai quali la FDA ritiene i registri elettronici e le firme attendibili, affidabili e in genere equivalenti a quelli cartacei e alle firme olografe apposte su carta.

Vedere il nostro Libro bianco Dropbox and FDA 21 CFR Part 11 e l'articolo del centro assistenza per ulteriori informazioni su come Dropbox può aiutare le aziende a raggiungere la conformità a 21 CFR Part 11.

PCI DSS

Dropbox è conforme ai Payment Card Industry Data Security Standard (PCI DSS). Tuttavia, Dropbox Business, Dropbox Education e Dropbox Paper non nascono con l'obiettivo di elaborare o archiviare dati sulle transazioni con carta di credito. Dropbox mette a disposizione dei clienti una AoC (Attestation of Compliance) PCI su richiesta.

Per altre informazioni sulla conformità di Dropbox Business e Dropbox Education, visita dropbox.com/business/trust/compliance.

App per Dropbox

La piattaforma DBX è costituita da un ecosistema affidabile di sviluppatori che creano i loro progetti sfruttando le nostre flessibili API. Sulla piattaforma Dropbox oltre 750.000 sviluppatori hanno creato applicazioni e servizi per produttività, collaborazione, sicurezza, amministrazione e altro.

Componenti pronti all'uso

Chooser, Saver ed Embedder sono componenti predefiniti Web e per dispositivi mobili che agevolano l'accesso a Dropbox da app o siti di terze parti in poche righe di codice.

- Chooser consente la selezione di file da Dropbox.
- Saver consente agli utenti di salvare file direttamente in Dropbox.
- Embedder consente agli utenti di visualizzare file e cartelle da Dropbox.

L'autorizzazione a questi componenti avviene interamente tramite Dropbox. Le app possono accedere ai file selezionati per mezzo dei link condivisi tramite Dropbox o con link di download di breve durata. Questi componenti predefiniti possono essere usati singolarmente o in combinazione con l'API descritta in seguito.

Integrazioni API Dropbox Business

L'API pubblica di Dropbox consente a sviluppatori di terze parti di accedere a Dropbox e interagire all'interno delle applicazioni. Sono incluse le interazioni con file e metadati, con le funzionalità di condivisione e del team.

Autorizzazioni

Dropbox utilizza OAuth, un protocollo standard di settore per l'autorizzazione, per consentire agli utenti di concedere alle applicazioni l'accesso all'account, senza dover mostrare le credenziali dell'account stesso. Supportiamo OAuth 2.0 per l'autenticazione di tutte le richieste API; le richieste vengono autenticate tramite il sito web o l'app per dispositivi mobili di Dropbox. Il supporto delle best practice di OAuth include token di accesso di breve durata e PKCE per le applicazioni distribuite.

Autorizzazioni utente

Le applicazioni che usano l'API Dropbox possono essere create con il seguente livello di accesso ai contenuti da parte degli utenti finali Dropbox:

- ***Cartella dell'applicazione.***
  All'interno della cartella delle applicazioni di un utente Dropbox viene creata una cartella dedicata a cui è attribuito il nome dell'applicazione. L'applicazione riceve l'accesso in lettura e scrittura solo per questa cartella e gli utenti possono fornire contenuti all'applicazione spostando i file all'interno di questa cartella. Inoltre, l'applicazione può anche richiedere l'accesso a file/cartelle attraverso Chooser o Saver.

- ***Dropbox completo.***
  L'applicazione riceve l'accesso completo a tutti i file e le cartelle presenti nel Dropbox di un utente e può richiedere l'accesso a file/cartelle attraverso Chooser e Saver.

Le applicazioni possono inoltre richiedere ambiti specifici, restringendo i loro comportamenti tramite l'accesso a sottoinsiemi di endpoint API. Ad esempio, è possibile restringere l'accesso alle applicazioni in sola lettura dei file o consentendo di caricare contenuti ma non di crearli.

Autorizzazioni del team

Gli amministratori di Dropbox Business possono autorizzare le applicazioni alla funzionalità di amministrazione nella Console amministratore del team. Gli ambiti delle azioni eseguibili dalle applicazioni collegate al team possono essere ristrette specificando le impostazioni del team che l'applicazione può leggere o gestire.

Le combinazioni degli ambiti più comuni includono:

- ***Informazioni sul team***
  Informazioni di sola lettura sul team e relative all'utilizzo generale.

- ***Audit del team***
  Accesso in sola lettura alle informazioni sul team e ai registri dettagliati degli eventi.

- ***Accesso ai file dei membri del team***
  La possibilità di eseguire azioni per conto degli utenti del team, come gestire i loro file e cartelle.

- ***Gestione dei membri del team***
  Aggiunta e rimozione di membri del team.

Webhook

I Webhook sono un modo per le applicazioni eb di ottenere notifiche in tempo reale sulle modifiche apportate nell'account Dropbox di un utente. Una volta registrato un URI per la ricezione di webhook, sarà inviata una richiesta HTTP a tale URI ogni volta che verrà apportata una modifica a uno degli utenti registrati all'applicazione. Utilizzando l'API di Dropbox Business, i webhook possono anche essere utilizzati per generare notifiche sulle modifiche all'appartenenza al team. Molte app di sicurezza utilizzano i webhook per aiutare gli amministratori a monitorare e a gestire le attività del team.

Estensioni

Le applicazioni possono registrare URI di estensione, consentendo la visualizzazione delle azioni nei menu "Condividi" e "Apri" nell'interfaccia utente di Dropbox. Le estensioni consentono agli utenti di avviare flussi di lavoro personalizzati di terze parti direttamente da un file in Dropbox. Una volta attivata un'azione, Dropbox reindirizzerà gli utenti all'URI specificato, convalidando un identificatore file che può essere usato con l'API per eseguire qualsiasi operazione sui file. Perché un'estensione registrata sia visibile all'utente, l'applicazione deve essere autorizzata. Possiamo promuovere una serie di integrazioni specifiche di estensioni nei menu "Condividi" e "Apri", anche se queste applicazioni non avranno accesso ai contenuti fino all'autorizzazione dell'utente.

Linee guida per gli sviluppatori di Dropbox

Mettiamo a disposizione numerose linee guida e istruzioni pratiche per aiutare gli sviluppatori a creare applicazioni basate sulle API che rispettino e proteggano la riservatezza dell'utente, migliorando al tempo stesso l'esperienza degli utenti Dropbox.

- ***Chiavi dell'applicazione***

  Per ogni singola app scritta da uno sviluppatore, è necessario utilizzare una chiave app Dropbox unica. Inoltre, se un'app mette a disposizione servizi o software che comprendono l'uso della DBX Platform da parte di altri sviluppatori, ciascuno di essi dovrà richiedere la propria chiave app Dropbox.

- ***Autorizzazioni delle applicazioni***

  Agli sviluppatori è stato spiegato che un'applicazione dovrebbe utilizzare il minor numero di autorizzazioni con privilegi possibile. Quando uno sviluppatore invia un'applicazione per l'approvazione dello stato di produzione, verifichiamo che l'applicazione non richieda un numero inutilmente spropositato di autorizzazioni sulla base delle funzionalità fornite dall'applicazione.

- ***Processo di revisione delle applicazioni***

  - **Stato di sviluppo.**
    Nel momento in cui un'applicazione basata sull'API di Dropbox viene creata, le viene attribuito uno stato di sviluppo. L'applicazione funziona come una qualsiasi applicazione in stato di produzione, salvo il numero totale di utenti Dropbox che possono essere associati, uguale a 500. Una volta collegati 50 utenti Dropbox a un'applicazione, lo sviluppatore dispone di due settimane di tempo per richiedere e ricevere l'approvazione dello stato di produzione prima che venga bloccata la possibilità dell'applicazione di collegare utenti Dropbox aggiuntivi.

  - **Stato di produzione e approvazione.**
    Per ricevere l'approvazione dello stato di produzione, tutte le app API devono rispettare le nostre linee guida sul branding per gli sviluppatori e i nostri Termini e condizioni, che includono gli utilizzi vietati di DBX Platform. Tra essi vi sono la promozione di violazioni dell'IP o del copyright, la creazione di reti per la condivisione di file e il download illegale di contenuti. Prima di esaminare l'app, agli sviluppatori viene richiesto di fornire ulteriori informazioni in relazione alle funzionalità dell'app e a come questa utilizza l'API Dropbox. Una volta approvata, l'app potrà passare allo stato di produzione e non vi sarà limite al numero di utenti che potranno collegarsi a essa.

Amministrazione dell'app del team

All'interno della Console amministratore del team, gli amministratori di Dropbox Business possono gestire le applicazioni collegate e le integrazioni per il loro team.

Partnership tra API

Dropbox ha collaborato fianco a fianco con i nostri partner tecnologici per aiutarli a sviluppare integrazioni con i più popolari pacchetti software. Questi partner hanno creato applicazioni usando le API Dropbox, lavorando insieme agli architetti di Dropbox per seguire le best practice relative a sicurezza ed esperienza utente. Queste includono una varietà di applicazioni per la produttività degli utenti finali, come anche strumenti di sicurezza e gestione, quali:

- ***Gestione delle informazioni e degli eventi di sicurezza (SIEM) e dati analitici***

  Collega il tuo account Dropbox Business a SIEM e a strumenti di analisi per monitorare e valutare la condivisione degli utenti, i tentativi di accesso, le azioni amministratore e altro ancora. Accedi e gestisci registri delle attività dei dipendenti e dati relativi alla sicurezza tramite lo strumento di gestione registri centralizzato.

- ***Data Loss Prevention (DLP)***

  Scansiona automaticamente metadati e contenuti di file per attivare avvisi, rapporti e azioni quando nel tuo account Dropbox Business vengono effettuate modifiche importanti. Applica le norme aziendali alla tua implementazione Dropbox Business e aiuta a soddisfare i requisiti di conformità previsti dalle norme.

- ***eDiscovery e conservazione ai fini giudiziari***

  Rispondi a controversie, arbitrati e indagini legali con dati dal tuo account Dropbox Business. Cerca e raccogli informazioni importanti archiviate in formato elettronico e preserva i tuoi dati tramite il processo di eDiscovery, consentendo alla tua azienda di risparmiare tempo e denaro.

- ***Gestione dei diritti digitali (DRM)***

  Aggiungi la protezione dei contenuti di terze parti per dati sensibili o protetti da copyright archiviati negli account dei dipendenti. Ottieni l'accesso a potenti funzioni DRM, tra cui crittografia lato client, filigrana, registri di controllo, revoca dell'accesso e blocco di utenti/dispositivi.

- ***Migrazione dati e backup in loco***

  Migra i dati da server o altre soluzioni basate su cloud esistenti a Dropbox, risparmiando tempo, denaro e lavoro. Automatizza i backup dal tuo account Dropbox Business a server locali.

- ***Gestione dell'identità e accesso singolo (Single sign-on, SSO)***

  Automatizza i processi di provisioning e deprovisioning e velocizza l'ingresso nel team per i nuovi dipendenti. Semplifica la gestione e rafforza la sicurezza integrando Dropbox Business in un sistema di identità esistente.

- ***Flussi di lavoro personalizzati***

  Crea app interne che integrano Dropbox nei processi aziendali esistenti per ottimizzare i flussi di lavoro interni.

Consulta la pagina delle Integrazioni per le applicazioni di Dropbox per un elenco completo dei partner tecnologici. Gli utenti finali possono scoprire le applicazioni e le integrazioni di Dropbox e di terze parti nell'App Center.

Integrazioni di Dropbox

Abbiamo anche collaborato con alcuni dei nostri migliori partner tecnologici per creare integrazioni presenti sulle piattaforme di Dropbox. Queste profonde integrazioni sono state sviluppate in collaborazione da Dropbox e dai partner. Sono incluse:

Dropbox Extensions

Queste integrazioni ti consentono di usare varie tipologie di estensioni per applicazioni per eseguire azioni senza interruzioni, come pubblicare un video, aggiungere file a email e chat, inviare un file per la firma elettronica e molto altro, direttamente da Dropbox. Da un lato, sono state create dai partner, dall'altro Dropbox agevola la scoperta di partner selezionati per le estensioni tramite i menu "Apri con" e "Condividi con".

Slack, Zoom e Trello

Queste integrazioni sono create da Dropbox e consentono agli utenti di avviare conservazioni in Slack, iniziare riunioni e creare attività in Dropbox. Gli utenti finali autenticano questi strumenti tramite OAuth.

Microsoft Office per Web e dispositivi mobili

Le nostre integrazioni con Microsoft Office consentono agli utenti di aprire file di Word, Excel e PowerPoint archiviati in Dropbox, effettuare modifiche nelle app mobili o web di Office e salvare tali modifiche direttamente in Dropbox. Agli utenti viene richiesto di concedere l'accesso al primo tentativo di apertura di un file Dropbox in ogni app mobile di Office o qualsiasi app web di Office. Gli avvii successivi conserveranno questi link.

Adobe Acrobat e Acrobat Reader

Le nostre integrazioni con le versioni desktop e mobile (Android e iOS) di queste applicazioni consentono agli utenti di visualizzare, modificare e condividere i PDF archiviati nel proprio Dropbox. Agli utenti viene richiesto di concedere l'accesso al primo tentativo di apertura di un file di Dropbox in ciascuna applicazione. Le modifiche apportate ai PDF vengono salvate automaticamente in Dropbox.

Riepilogo

Dropbox Business offre strumenti intuitivi per aiutare i team a collaborare in modo efficiente, fornendo al tempo stesso le misure di sicurezza e le certificazioni richieste dalle aziende. Grazie a un approccio a più livelli, che combina un'infrastruttura back-end sicura con una serie di norme personalizzabili, siamo in grado di fornire alle aziende una soluzione potente che può essere adeguata alle loro esigenze specifiche. Per ulteriori informazioni su Dropbox Business, contattataci all'indirizzo sales@dropbox.com.