Dropbox for Business security

A Dropbox whitepaper

Dropbox

Contents

Introduction

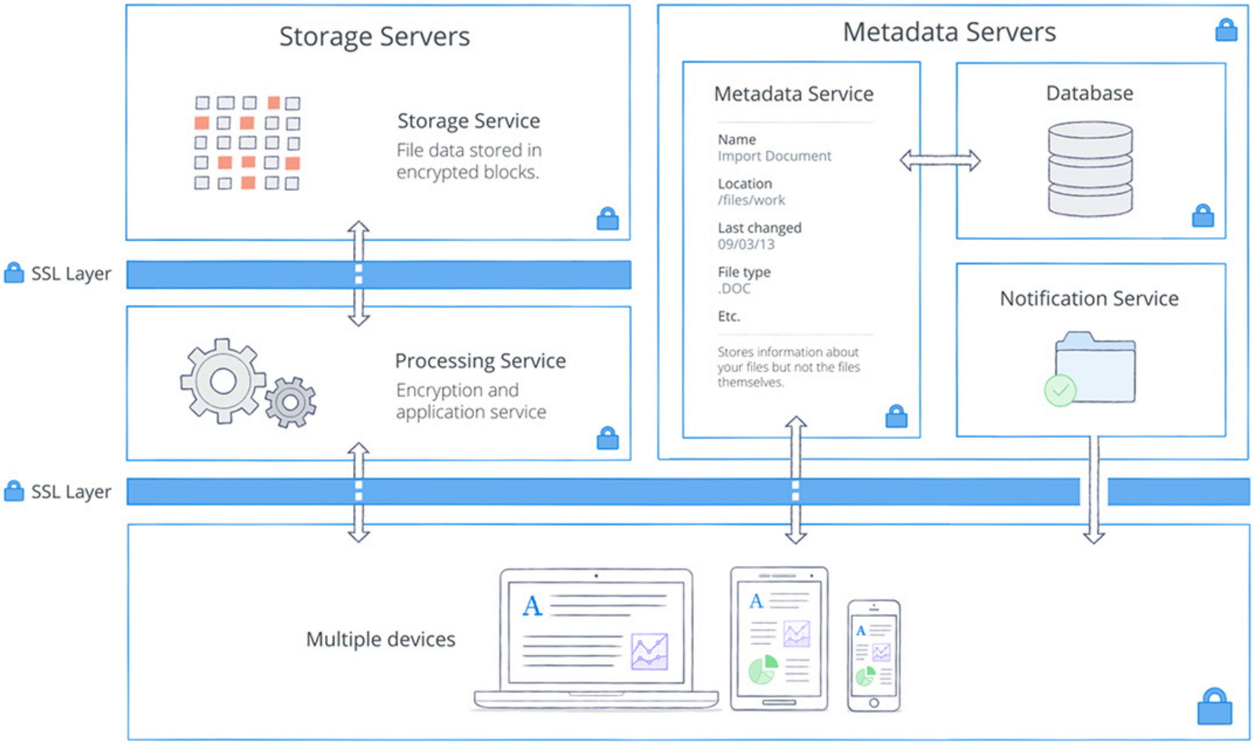
Millions of users trust Dropbox to easily and reliably store, sync, and share photos, videos, docs, and other files across devices. Dropbox for Business brings that same simplicity to the workplace, with advanced features that help teams share instantly across their organizations and give admins the visibility and control they need. But more than just an easy-to-use tool for storage and sharing, Dropbox for Business is designed to keep important work files secure. To do this, we've created a sophisticated infrastructure onto which account administrators can layer and customize policies of their own. In this paper, we'll detail the back-end policies, as well as options available to admins, that make Dropbox the secure tool for getting work done.

Under the hood

Dropbox's easy-to-use interfaces are backed by an infrastructure working behind the scenes to ensure fast, reliable uploads and downloads. To make this happen, we're continually evolving our product and architecture to speed data transfer, improve reliability, and adjust to changes in the environment. In this section, we'll explain how data is transferred, stored, and processed securely.

Architecture

Dropbox is designed with multiple layers of protection, covering data transfer, encryption, network configuration, and application-level controls, all distributed across a scalable, secure infrastructure.



Dropbox users can access files and folders at any time from the desktop, web, and mobile clients, or through third-party applications connected to Dropbox. All of these clients connect to secure servers to provide access to files, allow file sharing with others, and update linked devices when files are added, changed, or deleted.

Our architecture is comprised of the following services:

- **Encryption and application service.** By design, Dropbox provides a unique security mechanism that goes beyond traditional encryption to protect user data. The Encryption and Application Services process files from the Dropbox applications by splitting each into blocks, encrypting each file block using a strong cipher, and synchronizing only blocks that have been modified between revisions. When a Dropbox application detects a new file or changes to an existing file, the application notifies the encryption and application services of the change, and new or modified file blocks are processed and transferred to the storage service. For detailed information on the encryption used by these services both in transit and at rest, please see the Encryption section below.
- **Storage service.** The actual contents of users' files are stored in encrypted blocks with this service. Prior to transmission, the Dropbox client splits files into file blocks in preparation for the block storage service. The storage service acts as a Content-Addressable Storage (CAS) system, with each individual encrypted file block retrieved based on its hash value. An additional layer of encryption is provided for all files at rest using a strong cipher.
- **Metadata service.** Certain basic information about user data (including file names and types) called metadata, is kept in its own discrete storage service and acts as an index for the data in users' accounts. All Dropbox metadata is stored in a MySQL-backed database service, and is sharded and replicated as needed to meet performance and high availability requirements.
- **Notification service.** This separate service is dedicated to monitoring whether or not any changes have been made to Dropbox accounts. No files or metadata are stored here or transferred; as such, connections to this specific service are not encrypted. Each client establishes a long poll connection to the notification service and waits. When a change to any file in Dropbox takes place, the notification service signals a change to the relevant client(s) by closing the long poll connection. Closing the connection signals that the client must connect to the metadata service securely to synchronize any changes.

Both dedicated internal security teams and third-party security specialists protect these services through the identification and mitigation of risks and vulnerabilities. These groups conduct regular application, network, and other security testing and auditing to ensure the security of our back-end network.

Distributing different levels of information across these services not only makes syncing faster and more reliable, it also enhances security. The nature of the Dropbox architecture means access to any individual service cannot be used to re-create files. For information on the types of encryption used on the various services, please see the Encryption section below.

Dropbox user interfaces

The Dropbox service can be utilized and accessed through a number of interfaces. Each has security settings and features that process and protect user data while ensuring ease of access.

1. **Web.** This interface can be accessed through any modern web browser. It allows users to upload, download, view, and share their files.
2. **Desktop.** The Dropbox desktop application is a powerful sync client that stores files locally for offline access. It gives users full access to their Dropbox accounts, and runs on Windows, Mac, and Linux operating systems. Files are viewed and can be shared directly within the operating systems' respective file browsers.
3. **Mobile.** The Dropbox app is available for iOS, Android, Windows, and BlackBerry smartphones and tablets, allowing users to access all their files on the go. The mobile app also supports favoriting of files for offline access.

Our security team performs automated and manual application security testing, and works with third-party specialists, on a regular basis to identify and patch potential security vulnerabilities and bugs. In addition, our responsible disclosure policy promotes the discovery and reporting of security vulnerabilities. This policy sets forth the following guidelines to encourage participation by other industry security teams and the security research community:

- Give us reasonable time to respond before making any information about the security issue public.
- Do not access or modify user data without permission of the account owner.
- Act in good faith not to degrade the performance of our services (including denial of service).

We pledge to not sue anyone reporting issues or ask law enforcement to investigate for activities that comply with these principles. Issues can be reported by sending a detailed message to security@dropbox.com.

Reliability

A storage system is only as good as it is reliable, and to that end, we've developed Dropbox with multiple layers of redundancy to guard against data loss and ensure availability. Redundant copies of metadata are distributed across independent devices within a data center in an N+2 availability model. Hourly incremental and daily full backups are performed on all metadata. Dropbox file block storage uses systems including third-party providers that are designed to provide 99.9999999999% durability.

This feature, beyond protecting user data, provides high availability of the Dropbox service. In the event of a failed connection to Dropbox's service, a client will gracefully resume operation when a connection is re-established. Files will only be updated on the local client if they have synchronized completely and successfully validated with the Dropbox service. Load balancing across multiple servers ensures redundancy and a consistent synchronization experience for the end user.

To address information security requirements during a major crisis or disaster impacting Dropbox for Business operations, we maintain a disaster recovery plan. The Dropbox Infrastructure Team reviews this plan annually and tests selected elements at least annually. Relevant findings are documented and tracked until resolution.

Encryption

Data in transit

To protect data in transit between Dropbox apps and our servers, Dropbox uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. File data in transit between a Dropbox client (currently desktop, mobile, API, or web) and the hosted service is always encrypted via SSL/TLS. For end points we control (desktop and mobile) and modern browsers, we use strong ciphers and support perfect forward secrecy. Additionally, on the web we flag all authentication cookies as secure and enable HTTP Strict Transport Security (HSTS).

To prevent man-in-the-middle attacks, authentication of Dropbox front-end servers is performed through public certificates held by the client. An encrypted connection is negotiated before the transfer of any files and ensures secure delivery of files to Dropbox's front-end servers.

Data at rest

Dropbox files at rest are encrypted using 256-bit Advanced Encryption Standard (AES). Primary storage of Dropbox files are currently in multiple data centers, where they're stored in discrete file blocks. Each block is fragmented and encrypted using a strong cipher. Only blocks that have been modified between revisions are synchronized.

> "Dropbox for Business allows our teammates to collaborate and share content securely across the globe. As a global growth company, this is a priority for our infrastructure and Dropbox more than satisfies our enterprise security needs."
>
> Brian McManus, Senior Director of IT, Under Armour

Key management

Dropbox's key management infrastructure is designed with operational, technical, and procedural security controls with very limited direct access to keys. Encryption key generation, exchange, and storage is distributed for decentralized processing.

- **File encryption keys.** By design, Dropbox manages file encryption keys on users' behalf to remove complexity, enable advanced product features and strong cryptographic control. File encryption keys are created, stored and protected by production system infrastructure security controls and security policies.

- **Internal SSH keys.** Access to production systems is restricted with unique SSH key pairs. Security policies and procedures require protection of SSH keys. An internal system manages the secure public key exchange process, and private keys are stored securely.

Certificate pinning

Dropbox does certificate pinning on our desktop and mobile clients. Certificate pinning is an extra check to make sure that the service you're connecting to is really who they say they are, and not an imposter. We use it to guard against other ways that skilled hackers may try to spy on your activity.

Data centers

Dropbox corporate and production systems are housed at third-party subservice organization data centers and managed service providers located in the United States. All subservice organization data center SOC reports are reviewed at a minimum annually for sufficient security controls. These third-party service providers are responsible for the physical, environmental, and operational security controls at the boundaries of Dropbox infrastructure. Dropbox is responsible for the logical, network, and application security of our infrastructure housed at third-party data centers.

Dropbox's current managed service provider for processing and storage is responsible for the logical and network security of Dropbox services provided through their infrastructure. Connections are protected through the managed service provider's firewall, which is configured in a default deny-all mode. Dropbox restricts access to the environment to a limited number of IP addresses and employees.

Product features

Admin management features

As no two organizations are exactly alike, we've developed a number of tools that empower admins to customize Dropbox for Business to their teams' particular needs. Below are several control and visibility features available via the Dropbox for Business admin console.

Controls

- **User provisioning methods**
  - **Email invitation.** A tool in the Dropbox for Business admin console allows administrators to manually generate an email invitation.
  - **Active Directory.** Dropbox for Business administrators can automate the creation and removal of accounts from an existing Active Directory system. Once integrated, Active Directory can be used to manage membership.
  - **Single sign-on (SSO).** Dropbox for Business can be configured to allow team members access by signing into a central identity provider. Our SSO implementation, which uses the industry-standard Security Assertion Markup Language (SAML), makes life easier and more

secure by placing a trusted identity provider in charge of authentication and giving team members access to Dropbox without an additional password to manage.

- **Sharing permissions.** Dropbox for Business account administrators can control whether team members are able to share items with people outside the team, and set different rules for shared folders and shared links. If sharing outside the team is enabled, members will still be able to make individual folders or links "team only" as needed. Admins can also set shared links to be visible to team members only by default.
- **Password reset.** As a proactive security measure, admins can reset passwords for the entire team or on a per-user basis.
- **Web sessions.** Active browser sessions can be tracked and terminated from both the admin console and individual users' account settings.
- **App access.** Admins have the ability to view and revoke third-party app access to user accounts.
- **Unlink devices.** Computers and mobile devices connected to user accounts can be unlinked by the admin through the admin console or the user through individual account security settings. On computers, unlinking removes authentication data and provides the option to delete local copies of files the next time the computer comes online (see Remote wipe). On mobile devices, unlinking removes files marked as favorites, cached data, and login information. If two-step verification is enabled, users must re-authenticate any device upon relinking. Additionally, users' account settings provide the option to send a notification email automatically when any devices are linked.
- **Two Dropboxes.** Each user can choose to connect a personal and a work Dropbox across all devices to enable clear separation of business and personal data. Admins can enable or block desktop client access to this feature for team members.

> "Dropbox for Business gives our employees a clear separation of work and personal data, and our IT team can deploy the appropriate safeguards to ensure our company data is kept safe."
>
> Benjamin Hasselgren, IT Procurement Manager, Spotify

- **Remote wipe.** When employees leave the team or in the event of device loss, admins can remotely delete Dropbox data and local copies of files from both computers and mobile devices.
- **Account transfer.** After deprovisioning a user (either manually or via directory services), admins can transfer files from that user's account to another user on the team.

Visibility

- **User activity reports.** Dropbox for Business admins can generate activity reports at any time for several types of events, filtered by date range. Reports are available for individual users or entire team accounts and can be downloaded in CSV (comma-separated values) format for analysis with SIEM (security information and event management) tools. The following information is available to admins in user activity reports:

- **Passwords.** Changes to password or two-step verification settings. Admins do not have visibility into users' actual passwords.
- **Logins.** Successful and failed sign-ins to the Dropbox website
- **Admin actions.** Changes to settings in the admin console, such as shared folder permissions
- **Apps.** Linking of third-party apps to Dropbox accounts
- **Devices.** Linking of computers or mobile devices to Dropbox accounts
- **Sharing.** Events for both shared folders and shared links, including creating/joining shared folders and sending/opening shared links to documents. In many cases, reports will specify whether actions involve non-team members.
- **Membership.** Additions to and removals from team

Additionally, individual file and folder events (edits, deletions, and shared folder membership) can be tracked from each user's Events page.

- **Technical support identity verification.** Before any troubleshooting or account information is provided by Dropbox Support, the account admin must provide a one-time use, randomly-generated security code to validate his or her identity. This PIN is only available through the admin console.

User management features

Dropbox for Business also includes tools for end users to further protect their accounts and data. The authentication, recovery, logging, and other security features below are available through the various Dropbox user interfaces.

Recovery and version control. All Dropbox for Business customers have the ability to restore lost files and recover unlimited previous versions of files, ensuring changes to important data can be tracked and retrieved.

Two-step verification. This optional — but highly recommended — security feature adds an extra layer of protection to a user's Dropbox account. Once two-step verification is enabled, Dropbox will require a six-digit security code in addition to a password upon sign-in or when linking a new computer, phone, or tablet.

- Account administrators can track which team members have two-step verification enabled.
- Dropbox two-step authentication codes can be received via text message or apps which conform to the Time-based One-Time Password (TOTP) algorithm standard. In the event a user cannot receive security codes via these methods, they may opt to use a 16-digit, one-time-use emergency backup code. Alternately, they may use a secondary phone number to receive a backup code via text message.
- Once a user enables two-step verification, admins can mandate that they keep it enabled on their accounts. Additionally, admins can generate a reminder email for users with the service disabled, prompting them to enable it.

User account activity. Each user can view the following pages from their account settings to obtain up-to-date information regarding their own account activity:

- **Sharing page.** This page shows a user all folders they are currently a member of, as well as any shared folders they have left (with the option to rejoin). A user who owns shared folders can view all members of the folder, revoke folder access for specific users, and transfer folder ownership from this page. Each shared folder's owner can also control whether it can be shared with people outside the team, if others with edit permissions can manage membership, and if files within the folder can be shared with people outside the folder.
- **Links page.** Here, a user can view all active sharing links and the creation dates for each. It also allows a user to track all links shared from others, and disable currently active links.
- **Events page.** A running log of all individual file and folder edits, additions, and deletions is available on this page. Shared folder activity including membership and changes from other members of the folder can be tracked here as well.
- **Email notifications.** A user can opt in to receive an email notification immediately when a new device or app is linked to their Dropbox account.

User account permissions

- **Linked devices.** The Devices section of a user's account security settings displays all computers and mobile devices linked to the user's account. For each computer, the IP address, country, and approximate time of most recent activity is displayed. A user can unlink any device, with the option to have files on linked computers deleted the next time it comes online.
- **Active web sessions.** The Sessions section shows all web browsers currently logged into a user's account. For each, the IP address, country, and login time of the most recent session, as well as the approximate time of most recent activity, is displayed. A user can terminate any session remotely from the user's account security settings.
- **Linked apps.** The Apps linked section provides a list of all third-party apps with access to a user's account, and the type of access each app holds. A user can revoke any app's permission to access the user's Dropbox.

Mobile security

- **Passcode lock.** As an extra layer of access protection for the Dropbox mobile app, a user can require a four-digit passcode be entered anytime the app is launched or resumed. A user is prompted for the passcode immediately after launching or returning to the Dropbox app.
- **Erase data.** For additional security, a user can enable the option to erase all Dropbox data from the device after 10 failed passcode attempts.
- **Internal storage and favorited files.** By default, files are not stored on the internal storage of mobile devices. Dropbox's mobile clients feature the ability to mark individual files as favorites, saving them to the device for offline viewing. When a device is unlinked from a Dropbox account, via either the mobile or web interface, favorites are automatically deleted from the device's internal storage.

Shared file and folder permissions

- **View-only permissions for shared folders.** This access allows members of a shared folder to always see the latest versions of the files without having the ability to edit them.
- **Passwords for shared links.** Any shared link can be protected to ensure only collaborators with an owner-defined password can access shared files or folders.
- **Expirations for shared links.** Users can set an expiration for any shared link to provide temporary access to files or folders.

Apps for Dropbox

The Dropbox Platform is composed of a robust ecosystem of developers who build on top of our flexible Application Programming Interface (API). There are currently over 300,000 active apps built for document editing, communication, productivity, and more.

The Dropbox API

The three different types of Dropbox APIs include:

- **Sync API.** A powerful way for mobile apps to store and sync files with Dropbox.
- **Datastore API.** Helps keep structured data in sync.
- **Core API.** Supports advanced functionality like search, revisions, and restoring files, and is suited for server-based apps.

App permissions

- **Drop-ins.** The Chooser and Saver Drop-ins allow uploading from and downloading to a user's Dropbox, respectively. In essence, they take the place of traditional Open and Save dialog boxes, and restrict an app's access to only the files and/or folders the user specifically selects on a one-off basis.
- **Datastores only.** Datastore-only apps can access data through the Datastore API or by requesting file/folder access via Drop-ins. Datastores are special data structures which are stored separately from the file system. The app is not able to access any files in a user's Dropbox (aside from those specifically authorized by the user through Drop-ins) with this permission.
- **App folder.** A dedicated folder named after the app is created within the Apps folder of a user's Dropbox. The app receives read and write access to this folder only and users can provide content to the app by moving files into this folder. In addition, the app may also create its own datastore and/or request file/folder access via Drop-ins.

> "Dropbox for Business gives us a secure, unified place to store all of our work, and helps reverse the friction that can come with having hundreds of computers in one company."
>
> Bill O'Donnell, Chief Architect and SVP of Mobile Products, Kayak

- **File type.** The file type permission gives apps access to all files of a specific type (such as text or image files) across a user's entire Dropbox. In addition, the app may also create its own datastore and/or request file/folder access via Drop-ins.
- **Full Dropbox.** The app receives full access to all the files and folders in a user's Dropbox, as well as permission to read and write datastores using the Datastore API and request file/folder access via Drop-ins.

Dropbox uses OAuth, an industry-standard protocol for authorization, to allow users to grant apps account access without exposing their account credentials. We support both OAuth 2.0 and 1.0 for authenticating all API requests.

Dropbox developers

We provide a number of guidelines and practices to help developers create API apps that respect and protect user privacy while enhancing users' Dropbox experience.

- **App keys.** For each distinct app a developer writes, a unique Dropbox app key must be used. In addition, if an app provides services or software that wrap the Dropbox Platform for other developers to use, each developer must also sign up for their own Dropbox app key.
- **App review process**
  - **Development status.** When a Dropbox API app is first created, it is given development status. The app functions the same as any production status app, except that it can only be accessed by 100 or fewer users. In order for the app to become accessible to the general public, developers must apply for production status.
  - **Production status and approval.** In order to receive production status approval, all API apps must adhere to our developer branding guidelines and Terms & Conditions, which include prohibited uses of the Dropbox Platform. These uses include: promoting IP or copyright infringement, creating file sharing networks, and downloading content illegally. Developers are first prompted for additional information regarding their app's functionality, and how it uses the Dropbox API before submitting for review. Once the app is approved for production status, any number of Dropbox users can link to the app.

Dropbox information security

Dropbox has established an information security management framework describing the purpose, direction, principles, and basic rules for how we maintain trust. This is accomplished by assessing risks and continually improving the security, confidentiality, integrity, and availability of the Dropbox for Business systems. We regularly review and update security policies, provide security training, perform application and network security testing (including penetration testing), monitor compliance with security policies, and conduct internal and external risk assessments.

Our policies

We've established a thorough set of security policies covering the areas of Information security, Physical security, Incident response, Logical access, Physical production access, Change management, and Support. These policies are reviewed and approved at least annually, and are enforced by the Dropbox security team. Employees, interns, and contractors participate in mandatory security training when joining the company and ongoing security awareness education.

- **Information security.** Policies pertaining to user and Dropbox information, with key areas including device security; authentication requirements; data and systems security; restrictions on and guidelines for employee use of resources; and handling of potential issues
- **Physical security.** How we maintain a safe and secure environment for people and property at Dropbox (see Physical security section below)
- **Incident response.** Our requirements for responding to potential security incidents, including assessment, communication, and investigation procedures
- **Logical access.** Policies for securing Dropbox systems, user information, and Dropbox information, covering access control to corporate and production environments
- **Physical production access.** Our procedures for restricting access to the physical production network, including management review of personnel and de-authorization of terminated personnel
- **Change management.** Policies for code review and managing changes that impact security by authorized developers to application source code, system configuration, and production releases
- **Support.** User metadata access policies for our support team regarding viewing, providing support for, or taking action on accounts

Employee policy and access

Employee access to the Dropbox environment is maintained by a central directory and authenticated using a combination of strong passwords, passphrase protected SSH keys, two-factor authentication, and OTP tokens. Remote access requires the use of VPN protected with two-factor authentication, and any special access is reviewed and vetted by the security team.

Access between networks is strictly limited to the minimum number of employees and services. For example, production network access is SSH key-based and restricted to engineering teams requiring access as part of their duties. Firewall configuration is tightly controlled and limited to a small number of administrators.

In addition, our internal policies require employees accessing production and corporate environments to adhere to best practices for the creation and storage of SSH private keys.

Employee onboarding and offboarding policies require background checks, security policy acknowledgement, communicating updates to security policy, and non-disclosure agreements. All employee access is promptly removed when an employee leaves the company.

Dropbox employs technical access controls and internal policies to prohibit employees from arbitrarily accessing user files and to restrict access to metadata and other information about users' accounts.

In order to protect end user privacy and security, only a small number of engineers responsible for developing Dropbox's core services have access to the environment where user files are stored.

As Dropbox becomes an extension of our customers' infrastructure, they can rest assured that we are responsible custodians of their data. See the Privacy section below for more details.

Network security

Dropbox diligently maintains the security of our back-end network. Dropbox identifies and mitigates risks via regular application, network, and other security testing and auditing by both dedicated internal security teams and third-party security specialists.

Our network security and monitoring techniques are designed to provide multiple layers of protection and defense. We employ industry-standard protection techniques, including firewalls, network security monitoring, and intrusion detection systems to ensure only eligible traffic is able to reach our infrastructure.

> "By moving our employees to Dropbox for Business, we've been able to take over central management so that IT can fulfill our security needs while offering our users the solution that they were asking for. That's a win-win for us."
>
> Karl Ma, Global Security & Compliance, BCBGMAXAZRIAGROUP

Dropbox's internal private network is segmented according to use and risk level. The primary networks are:

- Internet-facing DMZ
- VPN front-end DMZ
- Production network
- Corporate network

Access to the production environment is restricted to only authorized IP addresses. IP addresses with access are associated with the corporate network or approved Dropbox personnel. Authorized IP addresses are reviewed on a quarterly basis to ensure a secure production environment. Access to modify the IP address list is restricted to authorized individuals.

Strict limitation is maintained between Dropbox's internal network and the public Internet. All Internet-bound traffic to and from the production network is carefully controlled through a dedicated proxy service and those, in turn, are protected by a restrictive firewall rules.

Change management

A formal Change Management Policy has been defined by the Dropbox Engineering team to ensure that all application changes have been authorized prior to implementation into the production environments. Source code changes are initiated by developers that would like to make an enhancement to the Dropbox application or service. All changes are stored in a version control system and are required to go through automated Quality Assurance (QA) testing procedures to verify that security requirements are met. Successful completion of QA procedures leads to implementation of the change. All QA-approved changes are automatically implemented in the production environment. Our software development lifecycle (SDLC) requires adherence to secure coding guidelines, as well as screening of code changes for potential security issues via our QA and manual review processes.

All changes released into production are logged and archived, and alerts are sent to Dropbox Engineering team management automatically.

Changes to Dropbox infrastructure are restricted to authorized personnel only. The Dropbox Security team is responsible for maintaining infrastructure security and ensuring that server, firewall, and other security-related configurations are kept up-to-date with industry standards. Firewall rule sets and individuals with access to production servers are reviewed on a periodic basis.

Compliance

Dropbox, our data centers, and our managed service provider undergo regular third-party audits. As part of our promise to continually improve the security of customers' data, we've achieved certification under ISO 27001, recognized as the premier information security standard around the world. This certification uses the ISO/IEC 27001:2013 revision of the standard, which was designed with cloud computing in mind. Our ISO 27001 certificate, issued by a leading independent third party in the Netherlands and recognized in all countries with IAF membership, can be viewed at www.dropbox.com/static/business/resources/dropbox-certificate-iso-27001.pdf.

We also undergo the following Service Organization Control (SOC) examinations, conducted by Ernst & Young LP. A report is available for each:

- **SOC 3.** This audit covers the Security, Confidentiality, and Processing Integrity Trust Services Principles, and provides customers with the American Institute of Certified Public Accountants (AICPA) SysTrust Seal of assurance. The report generated as part of this audit is an executive summary of our SOC 2 report and includes our independent third-party auditor's opinion on the effective design and operation of our controls. It can be viewed at cert.webtrust.org/soc3_dropbox.html.
- **SOC 2 Type 2.** This audit provides customers with a detailed level of controls-based assurance and covers the Security, Confidentiality, Processing Integrity, and Availability Trust Services Principles. Our SOC 2 report includes a detailed description of our processes and the nearly 100 controls we have in place to protect customer data. This report is available upon request.
- **SOC 1 / SSAE 16 / ISAE 3402 (formerly SAS 70).** This audit assists customers with internal controls over financial reporting (ICFR) programs, and is primarily used for customers' Sarbanes-

Oxley (SOX) compliance. The independent third-party examination for this report is conducted in accordance with Standards for Attestation Engagements No. 16 (SSAE 16) and International Standard on Assurance Engagements No. 3402 (ISAE 3402), which have replaced the previous Statement on Auditing Standards No. 70 (SAS 70) standard. This report is available upon request.

We will continue to participate in regular compliance audits, and current SOC reports will be made available as they are completed.

Dropbox also reviews SOC reports for all subservice organizations. In the event a SOC report is unavailable, we perform security site visits at new facilities to verify applicable physical, environmental, and operational security controls satisfy control criteria and contractual requirements. Procedures for the identification and resolution of security breaches are reviewed as well. We will evaluate additional certifications and compliance standards, and share updates as we receive them.

Dropbox is a Payment Card Industry Data Security Standard (PCI DSS) compliant merchant. However, Dropbox for Business is not meant to process or store credit card transactions. Dropbox provides customers with a PCI Attestation of Compliance (AoC) for our merchant status.

Dropbox is also a member of the Cloud Security Alliance (CSA), a non-profit organization that promotes and provides education around cloud security best practices. The Dropbox for Business security self-assessment is now available on the CSA's Security, Trust & Assurance Registry (STAR), a publicly available registry that details the security controls, assurance requirements, and maturity levels of various cloud computing services. Our Level 1 Self-Assessment documents how our security practices map to the CSA's best practices and industry-accepted standards. It can viewed at cloudsecurityalliance.org/star-registrant/dropbox-inc.

Physical security

Infrastructure

Physical access to subservice organization facilities where production systems reside are restricted to personnel authorized by Dropbox, as required to perform their job function. Any individuals requiring additional access to production environment facilities are granted that access through explicit approval by appropriate management.

A record of the access request, justification, and approval are recorded by management, and access is granted by appropriate individuals. Once approval is received, a responsible member of the infrastructure team will contact the appropriate subservice organization to request access for the approved individual. The subservice organization enters the user's information into their own system and grants the approved Dropbox personnel badge access and, if possible, biometric scan access. Once access is granted to approved individuals, it is the data center's responsibility to ensure that access is restricted to only those authorized individuals.

Office

- **Physical security.** The Dropbox Physical Security Team is responsible for enforcing physical security policy and overseeing the security of the office.

> "I would rather have [data] in a secure, encrypted, redundant system like Dropbox, than put it in my office and risk losing local data."
>
> Richard Wetzel, Partner, Centric Projects

- **Visitor and access policy.** Physical access to corporate facilities is restricted to authorized Dropbox personnel. A badge access system ensures only authorized individuals can have corporate facilities access.
- **Server access.** Access to areas containing corporate servers such as server rooms is restricted to authorized personnel via elevated roles granted through the badge access system. The lists of authorized individuals approved for physical access to corporate and production environments are reviewed at least quarterly.

Privacy

Guarding users' privacy and that of their business data is something we take seriously, so we work hard to protect user information from unauthorized access. Our privacy policy is available at www.dropbox.com/privacy.

Dropbox complies with the U.S.–E.U. and U.S.–Swiss Safe Harbor frameworks regarding personal data. Adhering to the seven Safe Harbor Principles ensures an organization provides adequate privacy protection under the EU data protection directive. Complaints and disputes related to Dropbox's Safe Harbor compliance are investigated and resolved through TRUSTe, an independent third party.

Both our privacy and Safe Harbor policies can be applied to data protection requirements in most countries worldwide.

Dropbox is committed to transparency in handling law enforcement requests for user information, as well as the number and types of those requests. We scrutinize all data requests to make sure they comply with the law and are committed to giving users notice, as permitted by law, when their accounts are identified in a law enforcement request.

These efforts underscore our commitment to guarding the privacy of our users and their data. To this end, we maintain a transparency report at www.dropbox.com/transparency and have established a set of Government Request Principles. The following principles govern our actions when receiving, scrutinizing, and responding to government requests for our users' data:

- Be transparent
- Fight blanket requests
- Protect all users
- Provide trusted services

Summary

Dropbox for Business offers easy-to-use tools to help teams collaborate effectively, while providing the security measures and compliance certifications organizations require. With a multi-layered approach that combines a robust back-end infrastructure with a customizable set of policies, we provide businesses a powerful solution that can be tailored to their unique needs. To learn more about Dropbox for Business, contact our sales team at sales@dropbox.com.

About Dropbox for Business

Dropbox lets you bring your docs, photos, and videos anywhere and share them easily. Keep files up to date across multiple devices and stay in sync with your team — effortlessly. Dropbox for Business also offers administrative tools, phone support, and as much space as you need.