Dropbox Dash

Dropbox Dash Security Whitepaper

Contents

Introduction

Dash is a productivity platform that combines smart universal search and knowledge management with in-depth content access control. Dash is designed to help you **find**, **create**, **organize**, **share**, and **secure** essential work content from SaaS and cloud applications to streamline productivity and accelerate content creation. Admins can monitor and manage Access Control Lists (ACLs) across connected work apps from one place. Dash is built on a combination of Dropbox's trusted infrastructure and leading cloud infrastructure services.

Product overview

Dash offers four primary capabilities for end users and admins.

Universal search

Dash provides AI universal search and knowledge management across connected work apps and associated content. Connect Dash with everyday work apps, such as Dropbox, Google Workspace, Microsoft OneDrive and SharePoint, Confluence, and more, to create a central hub for all your company's information. Employees can find everything in one place and let Dash search across content to find answers in seconds. Robust access permission controls guarantee your company's content is seen only by the right people, both inside and outside Dash.

Rich Media Search

Dash supports rich media search, including images and multimedia, by leveraging semantic image search and OCR capabilities. It uses embedding models (e.g: CLIP) to map images and text into a shared semantic space, enabling users to find relevant images through text queries. The system indexes these embeddings in scalable vector search infrastructure, allowing fast and accurate retrieval. Additionally, multimodal large language models generate captions or descriptions for images to explain why a result was returned, enhancing user understanding.

The search blends results from different verticals (text, images, messages) and prioritizes them based on user intent and relevance scores. This approach supports searching across various media types, including images, videos, and PDFs with scanned documents, with ongoing work to improve coverage and quality. Security and access controls are enforced throughout the pipeline to protect data and prevent unauthorized access.

Rich media search in Dash is designed with multiple security protections to prevent unauthorized access and data exposure. Metadata used in multimedia search is treated as untrusted and is validated and sanitized downstream to prevent injection attacks. Access control lists (ACLs) are synchronized and

enforced across all data stores, including metadata indexes, blob storage, and caches, ensuring users only see content they are authorized to access. Backend services and infrastructure components have strong authentication and authorization controls, and caching mechanisms are designed to prevent unauthorized data leaks. Additionally, the system monitors for malicious content injection and resource exhaustion attacks, applying rate limiting and validation to maintain security and availability.

Dash Chat

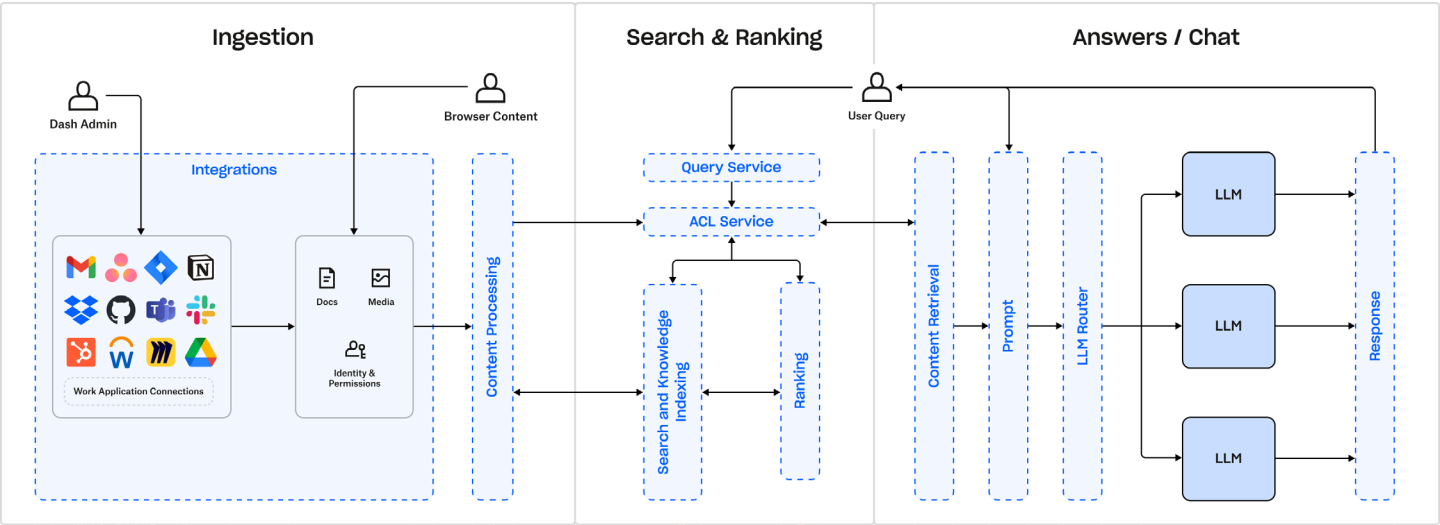
Employees can use Dash Chat to simplify getting work done. Dash enables employees to get summaries of content, ask questions and get answers about work, plus generate insights and new content based on company content and context.

Stacks

Dash optimizes the access and flow of information within an organization and allows companies to create a centralized repository of information from multiple sources of information or SaaS solutions. Employees can organize, find, and easily share content from multiple applications using the Stacks feature.

Platform architecture

Dash uses a modern technology stack comprised of off-the-shelf and custom services hosted on our infrastructure and cloud-hosted services. This allows us to continually improve our product and architecture to increase response speed, improve reliability, and adjust to changes in the environment.



Users and devices

Dash provides support for modern operating systems and browsers, allowing admins to manage the environment and end user to initiate searches for data that has been indexed from the device or integrated applications.

Identity

Dash uses Dropbox's core Identity infrastructure. Every Dash user must have a Dropbox account provisioned for them, which will be used to match and restrict access to Dash and specific connected work app content within Dash. Authentication of these accounts can be managed by Dropbox Identity. Alternatively, admins can configure an external SAML 2.0 identity provider to handle authentication, allowing Dropbox and Dash to be accessed through a customer's chosen Single Sign-On solution.

Ingestion

Dash's work app infrastructure periodically requests new content from each configured work app. The API Key, which is retrieved from the secrets store, is used to request recent content, identity, and groups for ACLs. Dash collects content and metadata such as document titles, links, content snippets, ACLs, and usage signals like search queries and interaction patterns. The content is stored, indexed, and temporary embeddings (numerical formats that help the system understand and compare text) are created. This helps support Retrieval Augmented Generation (RAG) and to enable fast and accurate semantic search and question answering for Chat and Stacks.

These embeddings are stored in vector databases unless the document itself is deleted or user disconnects the source of data (e.g. connected work app).

Connections between content and permissions to access individual items are computed, and then engagement signals like comments and views can be collected from some content types or the Dash browser extension. This data is used to improve the search and answers experience by providing the most active and relevant content to employees.

Dash includes capabilities that let admins exclude sensitive content from certain connected work apps. With the data exclusions feature, IT teams can keep specific folders out of search results and use with Dash's AI capabilities.

Data exclusions are limited to certain connected work apps that can be added in the admin console. Data exclusions can be set during initial setup and modified at any time. Changes typically take effect within 6 to 24 hours. This level of control supports privacy and compliance while keeping Dash useful for your team. There is no limit to the number of exclusions that you can add for a supported connected work app.

Dash ingestion services log operational events and metrics, including request operations to Cloud Services, indexing status, and data purge status. Admins can view the status and monitor the health of their work apps and their deployment through the admin console. Admins can also monitor the value that Dash brings through aggregate views of employee activity.

For full details on the data Dropbox collects for Dash and its other products, please refer to our **Privacy Policy**.

Search and knowledge indexes

Once a work app has been connected, metadata and the data itself will be indexed to these databases, which are logically separated, sharded, and replicated as needed to meet performance and high availability requirements.

Query service

This service brokers requests from the user or supporting applications to initiate the search. Dash is capable of processing and responding to queries posed in everyday language form, from within the standard user interface. Dash uses aggregated information relevant to each individual user to be able to provide a curated response to queries that come up in the normal course of business, reducing time spent in looking for the correct content.

Access Control List (ACL) service

Dash is designed to only give users access to content for which they are explicitly authorized. With Dash, end users only have access to content they are authorized to view across any given company or user work app. To ensure partitioning and to maintain tenancy of the data/indices, ACLs and access are acquired when data is acquired from connected services. The ACL service contains data permission metadata that is matched and validated prior to returning a response, which ensures that only authorized results are returned to the user.

ML and LLM-powered AI

We partner with companies whose privacy policies and commitment to our customers' rights and safety align with our own. Dropbox enforces strict privacy controls with third-party LLM providers, including contractual agreements. We will not build generative AI models using customer content without consent. Retention policies vary depending on the vendor and the specific agreements in place, and are designed to comply with applicable regulatory requirements. Customer data sent to third parties is managed according to these agreements and deleted within the retention period established for each sub-processor.

If you use Dash, Dropbox may manually review snippets of the questions you ask and the responses you receive. Where possible, we will de-identify these snippets prior to review. This review helps identify nonsensical or unhelpful answers so we can improve the underlying models and reduce inaccuracies. Manual reviews are subject to role-based access control and audit logging, and are performed solely to improve system performance under strict privacy safeguards.

See our **AI FAQ** for more information.

Configuration and management

Dash provides an admin console, where customer IT professionals assign licenses, configure connected work apps, secure access to files, and enable single-sign on (SSO) if applicable. Employees with an assigned license will be invited to log into Dash and enable connected work apps that require individual consent. Employees will then be able to use Dash to search across all configured applications, organize content in Stacks, and ask questions about their current work.

Connected work apps

The admin console allows admins to configure Dash connectors, which are code implementations that enable Dash to communicate with third-party services like Google Drive, Microsoft OneDrive/SharePoint, Dropbox, Zoom, Confluence, and more. These connectors enable Dash to securely access and retrieve data, providing a seamless experience within the Dash platform.

Dash connectors follow a standardized architecture with components for secure API communication, data synchronization, and data conversion to ensure maintainability, reliability, and security. They support full and incremental syncs, are monitored through dashboards for data freshness and completeness, and are deployed and managed by admins with careful attention to performance, error handling, and operational stability.

All connectors adhere to strict security principles that enforce least-privilege access to third-party systems. By default, all authentication methods (including OAuth 2.0 and user API keys) are provisioned with read-only scopes to protect user data and reduce the risk of privilege escalation. Write access is strictly limited to tokens required for Protect and Control functionality, and only for Dash administrators performing those specific administrative tasks.

Note: Admins and users can provide API keys for personal Connectors that may have elevated privileges (e.g: write permissions) that the respective Connector does not require or use.

API keys and other credentials stored by Dash are not readable by any Dropbox employee. They are only accessible to the jobs that call cloud services on behalf of the customer.

The admin console provides operational metrics and troubleshooting documentation for each Connector, as well as insights into how employees are using Dash. When a Connector is disconnected by an admin, Dash begins purging all content from it. The status of indexing and purging is provided in the admin console for monitoring by the deployment's administrators.

Dash provides two types of connected work apps:

- **Managed by User** connectors require customers to authenticate themselves directly, giving Dash access only to their individual accounts with read-only or limited permissions.
- **Managed by Admin** connectors involve users obtaining credentials from an administrator, but these credentials do not grant them more access than they already have. They are usually integration identifiers, and not full access keys.

  Note: Admins create a centralized connection to applications that are used organization-wide. Company work apps can be set up by administrators to shared applications at the organizational level, so that employees don't need to set them up individually.

Select company work apps allow administrators to govern data within these applications, and users to view content they're authorized to see. The key difference is who controls the credentials and the level of access granted to customers through those credentials.

Dash accesses only the data your organization chooses to connect.
The admin controls which work apps and data sources are integrated with Dash. Additionally, Dash offers data exclusion capabilities that allow admins to exclude specific files, folders, user drives, or sites from being ingested or appearing in search results for certain company work apps. This ensures sensitive or proprietary content remains outside of Dash. Data exclusions can be set during initial setup and modified at any time. This level of control supports privacy and compliance while keeping Dash useful for your team.

These connected apps are REST-based, encrypted API connections and are authorized either via API keys or an OAuth 2.0 authorization flow that grants Dash access to either acquire and index data or fetch data in real time that is associated to the application. The work app platform optimizes content retrieval from multiple sources through efficient connection pooling. It intelligently prioritizes the work apps based on their significance or specific criteria, ensuring efficient content access.

Once this integration is complete, the Dash work app platform connects to the integrated SaaS application to acquire content based on a known data schema for the service. ACLs for that content are acquired and this metadata is stored in our ACL service. A periodic refresh of both content and ACLs is performed to ensure freshness of the index and secure control of query results related to the content.

For a current listing of supported apps, see **What types of content does Dash support?**

Model Context Protocol (MCP) Server

The MCP server is a standardized API gateway that provides a unified interface for AI applications to connect to external systems, access relevant context, and perform actions. It acts as a protocol implementation layer that handles authentication, authorization, rate limiting, and request routing, enabling AI assistants to interact with data sources like Dropbox files and services through the Model Context Protocol (MCP).

MCP servers expose tools, prompts, and resources that AI assistants discover and invoke. Tool handlers call backend services to fulfill requests, while the MCP server translates between the MCP protocol (JSON-RPC over HTTP) and those underlying service APIs. This architecture allows teams to focus on building functionality while the MCP server handles common platform concerns like logging, metrics, and error handling.

MCP servers must follow strict security requirements including OAuth-based authentication and least-privilege authorization controls with granular scopes enforced by Dropbox's authorization service. They must validate access tokens on every request, enforce tool-level scopes, and reject tokens that lack the required permissions. Servers operate statelessly — each request is independently authenticated — and include detailed telemetry for audit and incident response.

Additionally, MCP servers enforce request size limits and rate limiting to prevent abuse, and implement structured audit logging that captures request metadata without storing raw sensitive payloads. Customer-facing MCP servers provide transparency through published OAuth metadata and tool annotations that describe operational characteristics such as whether a tool is read-only, destructive, or idempotent. Together, these requirements help ensure MCP deployments support Dropbox's security, compliance, and audit objectives while maintaining developer velocity.

For more information, see **How to connect the Dropbox Dash MCP server.**

Account security and authorization

As an admin, you can monitor and configure security settings to control how members access Dropbox Dash. You can configure security settings to control how members access Dash, including:

- Filtering, viewing, and downloading account activity.
- Enabling single sign-on (SSO) to configure access settings.
- Choosing which email domains users can use to log in to Dash.
- Verifying ownership and getting insights on your company domain.
- Enabling public sharing of Stacks.

For more information, see: **How to manage team security in Dropbox Dash.**

Protect and control

Through the Protect and Control feature in the admin console, administrators have full visibility into ACLs across all documents, folders, and drives within linked company work apps showing who has access to company content. Admins are able to quickly identify document access and mitigate risks across company content. This visibility and control exist in one place, eliminating the need for manual scripts or multiple admin consoles.

Dash provides the following advanced data access governance capabilities across select platforms (e.g: Dropbox, Google Workspace, Microsoft 365). Dash provides the following advanced data access governance capabilities across select platforms.

Granular content access controls:

- Set ACLs at the document and folder level.
- Ensure sensitive information is only seen by authorized users.
- Quickly adjust access settings as roles and needs change.

Full visibility into content access settings:

- Get a complete view of how much exposure exists.
- See which documents have public or company links and who has access.
- Identify internal and external accounts and domains with access to documents.

User-friendly content ACL management:

- Bulk update ACLs for any amount of assets in seconds.
- Simplify controlling access, even in complex environments.
- Enable seamless collaboration without compromising security.

Admins can view, control, and monitor who has access to files, helping organizations protect sensitive information, respond quickly to access issues, and keep accurate records of permission changes.

Note: Admins can see files shared through specific connected apps, but Dash doesn't provide access to user's local files or browser history.

Policies

In Protect and Control, admins can automatically detect and fix potential data risks across their organization. Daily scans run for conditions like files with open links, externally shared content, or inactive accounts.

Policies help teams simplify governance and prove compliance without slowing collaboration, enabling teams to:

- See who has access to company files across all connected apps.
- Identify and close risky exposure points like public links or personal accounts.
- Automate cleanup to reduce repetitive manual work.
- Enforce consistent sharing rules across tools.
- Track and audit every change with detailed logs for compliance.
- Keep data secure and governance effortless over time.

When applied well, policies do more than protect, they build trust. Teams can share confidently, knowing sensitive data stays contained.

To see the full workflow, from spotting exposure to enforcing policies at scale with automation, see: **How to use Policies in Dropbox Dash**

There are two ways to use policies after you've set up your requirements:

- **Send an alert:** Sends admins an email every 24 hours at 8:00 UTC that summarizes matching policies that need manual review.
- **Automatically fix it:** Performs automatic fixes daily on matching items at 8:00 UTC, with changes logged in **Action history**.

Note: Depending on the size of your organization, automatic fixes can take a few hours to complete.

For more information about how to enforce policies, see: **How admins can enforce policies in Dropbox Dash with Protect and Control.**

Reports

In Protect and Control, reports give admins a clear view of how files, folders, and shared drives are owned and shared across connected apps. These reports make it easier to surface items with broad access, uncover stale or abandoned

content, and identify where action may be needed. They're especially helpful for leaders who want a quick, high-level look at how information is shared across the organization, and where potential risks may exist.

With these reports, admins can:

- Spot files with overly broad access.
- Detect aging or unused content.
- Understand sharing trends across apps.
- Review past actions and confirm whether issues have already been addressed.
- Prioritize folders or drives for review.
- Support audits and compliance efforts.

For more information, see: **View Protect and Control reports in Dash.**

Filters

In Protect and Control, you can use filters to quickly find documents based on specific criteria, such as last modified date, file type, application, sharing status, and more. Preset filters make it easy to view common permission groupings, like files shared with personal accounts.

Audit and activity logging

A select set of activities are logged into the Dropbox audit log, and accessible to admins who have access to the audit log. These activities include adding, removing, enabling, or disabling work apps; creating, deleting, or adding/removing/modifying a link to a stack; granting or removing user access to Dash; and modifying the company logo, team name, or email allow list.

This level of visibility of how Dash is being used in your company's environment can also be exported for quick analysis or integrated with SIEM solutions for centralized monitoring and alerting.

Managed deployments

Setup is easy with simple standard deployment solutions in your environment for Windows, macOS clients, and browser extensions. An MSI for Windows and a PKG for macOS can be deployed and managed via device management services. The browser extension can be deployed via managed browser consoles or device management tools.

User interfaces

Dash can be utilized and accessed through the dash.ai website, a browser extension, desktop application for Windows and macOS, and mobile applications for iOS and Android.

Web application

Dash is supported in any browser at dash.ai. It allows users to easily retrieve content and has Stacks which intelligently group related content together and makes suggestions so users always have the right content, at the right time.

Web browser extension

The Dash browser extension is currently supported by Chrome, Edge and Safari. It makes it easy to retrieve content, intelligently groups related content together through Stacks, and it also makes suggestions so users always have the right content, at the right time. The extension enables searching within Stacks, surfaces related Stacks, provides a view into all Stacks, and gives users the ability to both create and add items to Stacks. It also allows browsing history to be AI-powered surfaced along with other relevant content on a browser start page.

In addition, the extension includes Dash Chat, which enables users to ask questions about anything visible on a single browser tab. Users have the option to quickly create a summary and highlights, a task list, a quick draft, or follow-up tasks.

Desktop application

The Dash desktop application is a powerful universal search client enabling users to seamlessly search through their data across multiple platforms, via a simple keyboard shortcut. It uses the local file system search APIs on Windows and macOS, so that files on the device can be used in search results.

Mobile application

The Dash mobile client is a companion app designed to extend Dash's productivity features to mobile devices, enabling users to perform quick searches, get context-aware, AI-powered responses, and manage work content on the go. It integrates deeply with mobile OS features like voice commands to provide seamless, daily utility without disrupting desktop workflows.

Security and trust

Dash is secure by design. When you use Dash, you get the same experienced team and security management practices as Dropbox file sync and share, trusted by over 700 million registered users and 575,000 teams with their most important information. We have extensive history in soundly implementing security controls and policies that govern the secure storage of your data in the cloud. Dash includes the same level of monitoring and scrutiny.

At Dropbox, we follow a multi-layered approach to secure the enterprise, infrastructure, applications, and products that impact your organization. This approach also includes infrastructure-as code controls, which require security peer review for modification.

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, availability, and privacy of the Dash systems. We regularly review and update security policies, provide security training, perform application and network security testing (including penetration testing via multiple third-party providers), monitor compliance with security policies, and conduct internal and external risk assessments.

AI security

Dash follows **AI principles** developed by Dropbox to promote responsible AI. We will not build generative AI models using customer content without consent. We may use other types of data—like data related to your usage of or interactions with the product—to improve and fine-tune Dash. To respect your privacy, Dash provides controls that let you opt out of having data used for these purposes. Our trusted AI partners don't train on or retain your data beyond their contractual retention window. Dash ensures that LLMs access only the data authorized by users and the organization, while protecting sensitive information.

We use **Lakera Guard**, a third-party solution that detects malicious attempts to extract personal data from training sets—whether from Dropbox-managed data or from data used by foundational model providers.

For **open-source foundation models**, we check that datasets are properly licensed and not collected through unauthorized scraping. We also take steps to reduce the risk of processing sensitive information, such as:

- removing or masking personally identifiable information (PII), where possible.
- excluding sensitive sites (e.g: financial or medical) from the browser extension.
- minimizing human review.

For **non-open-source foundation models**, we work with providers who commit to training on legally sourced data. Our contracts also require them to implement strong technical and organizational safeguards to protect data and address security risks.

Additional safeguards include:

- automated checks that detect unusual or restricted content, such as patterns linked to sensitive data.
- human oversight during design and testing to help prevent harmful outputs.
- regular evaluations to assess accuracy and alignment with privacy and security standards.

To learn more, refer to our blog post titled **How Lakera Guard Helps Secure Fine-Tuned LLMs**.

See Dropbox's **AI principles**, our **AI FAQ**, and our **AI Transparency Resource** for more information.

Data protection

Dash encrypts all data both in transit and at rest. This encryption is included in the scope of our SOC 2 Type II audit and is independently assessed. Content stored is encrypted transparently at the disk level for all Dropbox database technologies, while cloud-hosted storage services are encrypted using FIPS 140-2, Level 3 cryptographic services, with key management processes handled by Dropbox.

All Requests between Dash backend services and the public internet (including calls from Dash clients and calls to Cloud Service providers for Data Acquisition) are mediated by HTTPS. Requests between internal components of the Dash backend are encrypted using mutual TLS.

Dash is a multi-tenant, Software as a Service application, meaning that all customer data is stored in the same data stores. These data stores share the same mature security tooling used by Dropbox file sync and share, which includes extensive security auditing, monitoring and alerting as well as strict production access controls. A multi-layered approach is taken to controls, including infrastructure-as-code controls, which require security peer review for modification.

As product development progresses for Dash, and as customer demand expands, additional worldwide regions may be added to support data customer residency requirements, but currently Dash does does not offer an option for data storage outside of the US.

Privacy

Every day, people and organizations trust Dropbox with their most important data. Because of this, it's our responsibility to protect this data and keep it private. Our commitment to your privacy is at the heart of every decision we make.

We support users' right to request access or deletion of their personal data. Users can make these requests through their admins, who can work with their account managers or contact **privacy@dropbox.com** for help with the request.

Dropbox systematically applies retention policies that govern the period of time personal data is retained. We also apply the principles of data minimization and purpose limitation to only keep data for as long as we have use for it.

Sub-processors

To enable provision of our Dash Services, Dropbox may engage sub-processors with access to customer personal data. Before we engage with sub-processors, Dropbox performs due diligence on sub-processor privacy, security, and confidentiality practices and executes appropriate contractual measures regarding protection of personal data.

For more information, including a full list of sub-processors, refer to our **Sub-processor List** for Dash.

Data transfers

When transferring data from the European Union, the European Economic Area, the United Kingdom, and Switzerland, Dropbox relies upon a variety of legal mechanisms, such as contracts with our customers and affiliates, Standard Contractual Clauses, the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, and the European Commission's adequacy decisions about certain countries, as applicable.

For more information about Dropbox's privacy practices and processes, visit **Privacy and Data Protection**.

Compliance

Customers all over the world trust Dropbox with their most sensitive data. Dash was built with the same priority on security to meet the highest industry standards. There are various regulatory and industry-specific requirements for security and privacy that your organization may be required to comply with. Our approach is to combine the most accepted standards with compliance measures geared to the specific needs of our customers' businesses or industries, underscoring our commitment to industry standards and the protection of our client's data.

SOC 2 Type II

Dash meets the Trust Services Criteria for Security, underscoring our commitment to industry standards and the protection of our clients' data. The SOC 2 report provides a thorough description of Dropbox's processes and the controls in place to protect your data, including the independent third-party auditor's opinion on the operational effectiveness of these controls over a specified period. The current SOC 2 report can be requested through the **Trust Center**.

ISO/IEC 27001

ISO/IEC 27001 is recognized as the premier information security management system (ISMS) standard around the world. The standard also leverages the security best practices detailed in ISO/IEC 27002. To be worthy of your trust, we're continually and comprehensively managing our physical, technical, and legal controls at Dropbox. View the **Dash ISO/IEC 27001 certificate**.

EU General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a 2018 European Union regulation that marked a significant change to the previous framework for processing personal data of EU data subjects. The GDPR introduced a series of new or enhanced requirements that applies to companies like Dropbox, which handle personal data. Dash adheres to GDPR so that customers can use Dash to facilitate their GDPR compliance.

California Consumer Privacy Act (CCPA)

Dropbox is committed to safeguarding the security and privacy of our users' data and is in compliance with CCPA.

EU - US Data Privacy Frameworks (DPF)

Dropbox complies with the EU-U.S. and Swiss-U.S. Data Privacy Frameworks, as well as the UK Extension to the EU-U.S. DPF. Reports for Dash are available upon request.

Learn more

View our compliance reports and further information on our security, compliance, and privacy practices so you can see how Dash's security stacks up to competitors. Access the latest security policies in real time and stay up to date about how we keep your company data and information secure. For more information, see the **Trust Center**.

Please note: Dropbox Dash and Dash for Business are now referred to as Dash. It remains the same product as scoped in our audit reports and certifications.

Reporting issues

Help Dash stay secure. If you believe you have found a security vulnerability in Dash's product offering, please email your findings to **dash-security@dropbox.com**.

We also have a bug bounty program that provides an incentive for researchers to identify and responsibly disclose software bugs. For more information, see the **Trust Center**.