A DROPBOX WHITEPAPER

Dropbox Dash

Overview

Dropbox Dash is AI-powered universal search that helps speed up the way you work across all your applications. Dash learns and evolves with you, getting better the more you use it.

Dash’s intelligent connection to your applications allows you to find, organize, and take action on content and information. Finding content is easy via the web or the Dash application installed on your Windows or MacOS device. Flexible organization of your content from any connected applications allows you to group items into Stacks, matching how you work versus the rigid file structures and data silos of the past. Dash will provide smart recommendations based on topic and usage to help with Stack creation and curation.

As content is found via Dash or organized with Stacks, both solutions become an easy platform to launch right to that referenced content or solution. Natural language queries will provide rich answers based upon the aggregate context of your information.
Dropbox Dash is backed by an infrastructure designed to ensure fast, reliable search and secure protection of your content. To make this happen, we continually improve our product and architecture to speed responses, improve reliability, and adjust to changes in the environment. Dash uses a modern stack comprised of off-the-shelf and custom services hosted on Amazon Web Services (AWS) infrastructure.

Dropbox Dash's infrastructure is comprised of the following major components:

**Connector platform**

To allow search across all your applications, Dash has pre-built integrations for modern productivity and business applications, such as Google Workspace, Salesforce, Microsoft Outlook, etc. These integrations are HTTP/REST-based, encrypted API connections and are authorized either via API keys or an OAuth 2.0 authorization flow that grants Dash access to acquire and index data associated to the application. The connector platform optimizes content retrieval from multiple sources through efficient connection pooling. It intelligently prioritizes the connectors based on their significance or specific criteria, ensuring efficient content access.
Search and metadata databases

Once an integration has been established to an application, metadata and the data itself, will be ingested to these databases, which are logically separated, sharded, and replicated as needed to meet performance and high availability requirements.

AI / ranking service

In order to provide relevant returns for queries from the user, Dash will utilize AI to rank metadata and content on multiple categories and dimensions. Dash constructs a knowledge graph based on the content the user has access to and their interactions, enabling it to construct valuable insights and patterns. The Dash AI models leverage the user’s knowledge graph and personalized engagement to rank and score the results. The ranking will be based on recency, relationship between content, and usage patterns of the users and team members. Our AI Principles guide our teams as we develop AI products and features responsibly.

ACL service

To ensure partitioning and to maintain tenancy of the data/indices, permission 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.

Query service

This service brokers requests from the user or supporting applications to initiate the search.

Users & devices

Dash provides support for modern operating systems and browsers allowing the end user to initiate searches for data that has been indexed from the device or integrated applications. A browser extension, which is installed with the Dash client, allows browsing history to be intelligently surfaced along with other relevant content on a browser start page.
Dash uses off-the-shelf and custom services hosted on Dropbox and AWS infrastructure. AWS is operated with shared responsibility between Dropbox and AWS. Logical and network security of AWS infrastructure is provided by AWS.

Currently, all AWS infrastructure used for Dash is located within the United States and is distributed across multiple availability zones. As product development progresses for Dash and as customer demand expands, additional worldwide regions may be added to support data residency requirements.

Trust is the foundation of our relationship with millions of people and businesses around the world. We value the confidence you’ve put in us and take the responsibility of protecting your information seriously. To be worthy of your trust, we built and will continue to grow Dropbox with an emphasis on security, privacy, transparency, and compliance.

The Dropbox Trust Program establishes a risk assessment process, which is designed to address environmental, physical, user, third party, applicable laws and regulations, contractual requirements, and various other risks that may affect system security, confidentiality, integrity, availability, or privacy. Performance reviews occur at least annually. More information on the Dropbox Trust Program website.

We follow a multilayered approach to secure the enterprise, infrastructure, applications, and products that impact your organization.

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 Dropbox 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.

Employee access management processes

Upon hire, each Dropbox employee is required to complete a background check, sign a security policy acknowledgement and non-disclosure agreement, and receive security training. Only individuals that have completed these procedures are granted physical and logical access to the corporate and production environments, as required by their job responsibilities. In addition, all employees are required to complete annual
security training, and they receive regular security awareness training via informational emails, talks and presentations, and resources available on our intranet.

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 user accounts. In order to protect end user privacy and security, only a small number of engineers responsible for developing core Dropbox services have access to the environment where user files are stored. Employee access is promptly removed when an employee leaves the company.

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

**Vulnerability management**

Our security team carries out regular automated security testing and patch management, and works with third-party specialists to identify and remediate potential security vulnerabilities and bugs.

As a necessary component of our information security management system, findings and recommendations that result from all of these assessments are communicated to Dropbox management, evaluated, and appropriate action is taken, as determined to be necessary. Issues with high severity are documented, tracked, and resolved by assigned security engineers.

**Change management**

All development, issue remediation, and patch processes follow our formal Change Management Policy, which is defined by the Dropbox Engineering team to ensure that system changes have been tested and authorized prior to implementation in the production environments. Source code changes are initiated by developers who want to make an improvement to the Dropbox application or service. 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. 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. Changes released into production
are logged and archived, and alerts are automatically sent to Dropbox Engineering team management.

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

**Scanning and security penetration testing (internal and external)**

Our security team performs automated and manual application security testing on a regular basis to identify and patch potential security vulnerabilities and bugs on our desktop, web, and mobile applications.

Additionally, Dropbox contracts with third-party vendors to perform periodic penetration and vulnerability tests on the production environment. We work with third-party specialists, other industry security teams, and the security research community to keep our applications secure. We also leverage automatic analysis systems to identify vulnerabilities. This process includes systems that we develop internally, open source systems we modify for our needs, as well as external vendors we hire for continuous automated analysis.

**Bug bounties**

While we work with professional firms for penetration testing engagements and conduct our own testing in-house, bug bounties (or vulnerability rewards programs) tap into the expertise of the broader security community. Our bug bounty program provides an incentive for researchers to identify and responsibly disclose software bugs. This involvement of the external community provides our security team with independent scrutiny of our applications to help keep users safe. We strive to be among the industry leaders in bounty rewards, as well as response and remediation times.

Dash will be included in the Bug Bounty program soon. Check the Bugcrowd Web site [bugcrowd.com/dropbox](http://bugcrowd.com/dropbox) for updates.
Physical security

Infrastructure

Physical access to sub-service organization facilities where production systems reside is 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, an authorized member of the infrastructure team will contact the appropriate sub-service organization to request access for the approved individual. The sub-service 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.

Corporate offices

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

- Visitor and access policy
  Physical access to corporate facilities, other than public entrances and lobbies, is restricted to authorized Dropbox personnel and registered visitors who are accompanied by Dropbox personnel. A badge access system ensures only authorized individuals have access to restricted areas within the corporate facilities.

- Server access
  Access to areas containing corporate servers and network equipment 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.
Incident response

We have incident response policies and procedures to address service availability, integrity, security, privacy, and confidentiality issues. As part of our incident response procedures, we have designated teams who are trained to:

- Promptly respond to alerts of potential incidents.
- Determine the severity of the incident.
- If necessary, execute mitigation and containment measures.
- Communicate with relevant internal and external stakeholders, including notification to affected customers to meet breach or incident notification contractual obligations and to comply with relevant laws and regulations.
- Gather and preserve evidence for investigative efforts.
- Document a postmortem and develop a permanent triage plan.

The incident response policies and processes are audited as part of our SOC 2 attestation engagement.

Network security

Dropbox diligently maintains the security of our back-end network. 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 vulnerability scanning, network security monitoring, and intrusion detection systems to ensure only eligible and non-malicious traffic is able to reach our infrastructure.

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

- Internet-facing DMZ
- Priority infrastructure DMZ
- Production network
- Corporate network
- Dropbox services and applications are isolated via containers when possible
Access to the production environment is restricted to authorized IP addresses and requires multi-factor authentication on all endpoints. 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.

Traffic from the internet destined to our production network is protected using multiple layers of firewalls and proxies.

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

Dropbox instruments sophisticated tool sets to monitor laptops and desktops with Mac and Windows operating systems, and production systems, for malicious events. Security logs are collected in a centralized location for forensic and incident response following the industry standard retention policy.

Dropbox identifies and mitigates risks via regular network security testing and auditing by both dedicated internal security teams and third-party security specialists.

**Reliability**

A storage system is only as good as it is reliable and, to that end, we’ve developed Dash with multiple layers of redundancy to guard against data loss and ensure availability.

**Connector data storage**

Data is stored on AWS infrastructure and leverages redundancies built into AWS. Our connector infrastructure leverages RDS, with multi-AZ redundancy and failover within a region and full data snapshots are created daily. Additional, non-critical data is stored in AWS S3, which has 11 9’s of durability.

**Data centers and managed service providers**

Dropbox corporate and production systems are housed at third-party sub-service organization data centers and managed service providers located in different regions of the United States. Sub-service organization data center SOC reports and / or vendor security questionnaires and contractual obligations 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.

Our managed service provider for processing and storage, Amazon Web Services (AWS), is responsible for the logical and network security of Dash services provided through their infrastructure. Connections are protected through their 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. Dash’s intelligent data analysis and decisioning capabilities are powered by the ElasticSearch platform, which provides a complete managed SaaS solution with security demonstrated through their ISO certification and SOC attestation reports.

Reliability

A storage system is only as good as it is reliable and, to that end, we’ve developed Dash with multiple layers of redundancy to guard against data loss and ensure availability.

Business continuity

Dropbox has established a business continuity management system (BCMS) to address how to resume or continue providing services to users—as well as how to function as a company—if business-critical processes and activities are disrupted. We conduct a cyclic process consisting of the following phases:

- **Business impact and risk assessments**
  We conduct a business impact assessment (BIA) at least annually to identify processes critical to Dropbox, assess the potential impact of disruptions, set prioritized timeframes for recovery, and identify our critical dependencies and suppliers. We also conduct a company-wide risk assessment at least annually. The risk assessment helps us systematically identify, analyze, and evaluate the risk of disruptive incidents to Dropbox. Together, the risk assessment and BIA inform continuity priorities, and mitigation and recovery strategies for business continuity plans (BCPs).

- **Review and approval of BCMS**
  At least annually, our executive staff reviews the BCMS as part of reviewing Dropbox’s Trust Program.
Dash user interfaces

Dash can be utilized and accessed through a desktop application and a Web browser extension. Each has security settings and features that process and protect user data while ensuring ease of access.

Web browser extension

The Dash browser extension is currently supported by Chrome and Edge browsers. It allows users to easily re-retrieve content and has smart stacks which intelligently groups related content together and makes suggestions so users always have the right content, at the right time.

Desktop

The Dash desktop application is a powerful universal search client enabling users to seamlessly search through their data across multiple platforms. It runs on Windows and Mac operating systems, and allows users to connect a variety of data sources and use a highly customizable interface to locate content.

Secure development lifecycle

Security training & awareness

We empower our software development teams with the best practices and techniques for building secure applications. In an ever-evolving digital landscape, ensuring the security of our software is of paramount importance, and we are committed to equipping our teams with the knowledge and skills needed to safeguard our products and protect our users.

Design reviews

The security team at Dash integrates security review into the product roadmap, so every major release has undergone threat models and design reviews in order to deliver a secure experience for our users.

Penetration testing

The security team also regularly conducts “open-box” tests on Dash features being released, ensuring flaws and bugs are discovered and patched before reaching the hands of our users.
DROPBOX DASH SECURITY

Secure deployment

As part of our software development lifecycle, whenever new Dash web application features are added to our codebase, the code is first analyzed and scanned for code quality and security flaws. Features must pass this review process, including peer evaluation, before it is deemed ready for release.

Data in transit

To protect data in transit between Dash clients, integrated applications and our infrastructure, Dash uses Transport Layer Security (TLS) for data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. For the Dash client and modern browsers, we use strong ciphers and on the web we flag all authentication cookies as secure and enable HTTP Strict Transport Security (HSTS) with include SubDomains enabled.

Data at rest

Data that is transferred from the Dash client or integrated applications is encrypted at rest using 256-bit Advanced Encryption Standard (AES).

Key management

Databases that store content from the Dash client or integrated applications are encrypted using cryptographic processes provided by AWS Key Management Service (KMS) and key management processes built and managed by Dropbox. Key management services are designed with operational, technical, and procedural security controls.

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.

Dropbox Dash contains and uses AI components, which helps get the information that you need and provides more context about that information. The privacy and protection of that information is paramount to Dropbox’s commitment to “Be Worthy of Trust”. Our AI Principles guide our teams as we develop AI products and features responsibly.

We currently support users’ ability to request access or deletion of their personal data via software processes that are automated and verified.
for accuracy. Users can also correct their personal data via engagement with our account and CX teams. Lastly, we systematically look for opportunities to apply retention policies that can govern the period of time data is retained and securely destroyed.

Dash uses AI, which is supported by the third-party service, OpenAI. Individual users have the ability to control both which apps they integrate with Dash and what data is shared with Dash. Data sent to OpenAI is never used to train OpenAI models, and is deleted after 30 days.

Data transfers

**Note:** Dropbox Dash is currently available in only the United States and data is stored within the United States.

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, vendors and affiliates, other legally recognized transfer mechanisms, and the European Commission’s adequacy decisions about certain countries, as applicable in the circumstances.

**EU general data protection regulation (GDPR)**

The General Data Protection Regulation (GDPR) is a 2018 European Union regulation that establishes a comprehensive framework for handling and protecting personal data. Dropbox is committed to the security and protection of our users’ data in line with legal requirements and best practices at all times. In line with our commitment to our users, we have implemented measures to ensure that Dropbox is GDPR compliant, including appointing a Data Protection Officer; architecting our privacy program to ensure that users can exercise their data subject rights; documenting our data processing activities; and bolstering our internal processes in the event of a security breach. We continue to make adjustments to ensure that, as further guidance continues to emerge from data protection authorities, our process and practices meet or exceed the requirements of applicable law.

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.

Dropbox Dash is currently in development, and we are working in parallel
on compliance audits for SOC 2. We are actively considering obtaining additional compliance certifications and attestations, such as ISO 27001, HIPAA and others, in the future. Available reports for Dropbox Dash are available upon request.

Dropbox Dash has created and partnered with solution providers to create a library of connectors that allow you to integrate modern SaaS applications and other information resources. Generally, each connector uses public APIs of those applications and authorization to the APIs is granted by an administrator or a user via OAuth 2.0. Certain applications will allow an administrator for Dash to create the integration from a future version of the Dropbox Dash Admin Console. Applications like Gmail and Outlook require that individual users create the integration, which can be done during initial Dash setup or from the Dropbox Dash client on Windows or MacOS.

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

When the Dropbox Dash client is installed on Windows or MacOS, a browser extension is also installed and can be enabled for Chrome and Edge browsers. This extension works in conjunction with the Dropbox Dash connector platform to provide recent browser activity to Dash.

The Dropbox Dash client also contains a component that utilizes the local file system search APIs on Windows and MacOS, so that files on your device can be used in search results.

As the Dash connector platform acquires content from the integrated SaaS and local information resources; de-duplication, enrichment, and content protections are applied to content as it is committed to the Search Index and Metadata Graph databases.