Dropbox Business

Security with Dropbox Business

At Dropbox, the security of your data is our highest priority. We've earned the trust of over 500 million users by keeping data safe while providing best-in-class performance and usability. For over 200,000 companies, Dropbox pairs the benefits of widespread adoption with the controls and certifications IT needs to protect employees and their data. The result: a truly unique security offering for the enterprise.

Built on a strong foundation
Dropbox is built with multiple layers of protection across a distributed, reliable infrastructure. With 1.2 billion files synced each day, our infrastructure is optimized for performance at a massive scale and backed by a world-class security organization.

Compliance to meet your business requirements
Dropbox combines the most accepted standards—like ISO 27001 and SOC 2—with compliance measures geared to our customers' specific industries. We provide reports from third-party auditors to help you verify our security practices.

Adoption–the ultimate security advantage
At Dropbox, we know that real security starts by bringing users onto a sanctioned platform. Dropbox Enterprise leverages ease-of-use and adoption to centralize company data, resulting in greater visibility and control.

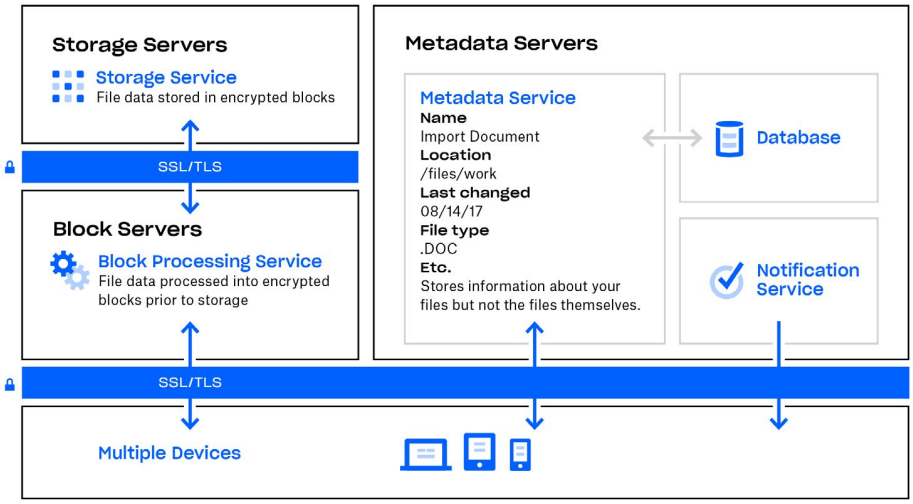
For more detail on Dropbox security features and policies, please review the Dropbox Business Security Whitepaper or contact sales@dropbox.com

Architecture

With over 1.2 billion files saved every day, Dropbox was built to secure data at scale. 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.

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.

Encryption is an important component of our security protocol. 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. Dropbox files at rest are encrypted using 256-bit Advanced Encryption Standard (AES).



Dropbox stores two kinds of data: file content (file blocks) and metadata about files and users. All metadata is stored on Dropbox servers. Most file content is also stored on Dropbox servers, in a system known as Magic Pocket. This system, which consists of both proprietary software and hardware, has been designed from the ground up to be reliable and secure. A smaller portion of file content is stored by a managed service provider, Amazon Web Services (AWS). In both Magic Pocket and AWS, file blocks are encrypted at rest, and both systems meet high standards for reliability.

Reliability and durability

Dropbox's architecture, applications, and sync mechanisms work together to protect user data and make it highly available. 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. Redundant copies of file blocks are stored independently in at least two separate geographic regions and replicated reliably within each region. Both Magic Pocket and AWS are designed to provide annual data durability of at least 99.999999999%.

In the rare event of a service availability outage, Dropbox users still have access to the latest synced copies of their files in the local Dropbox folder on linked computers. Copies of files synced in the Dropbox desktop client/local folder will be accessible from a user's hard drive during downtime, outages, or when offline. Changes to files and folders will be synced to Dropbox once service or connectivity is restored.

> "I don't have to worry about data security, because of the encryption and transport layer protocols Dropbox has in place."
>
> **Robert Everett**
> Director of IT, Brandt Companies

Compliance

There are many different compliance standards and regulations that may apply to your organization. Our approach is to combine the most accepted standards—ISO 27001, SOC 2, and more—with compliance measures geared to the specific needs of our customers' businesses or industries. Dropbox, our data centers, and our managed service provider undergo regular third-party audits.

ISO certifications

The International Organization for Standardization (ISO) has developed a series of world-class standards for information and societal security to help organizations develop reliable and innovative products and services. Dropbox has certified its data centers, systems, applications, people, and processes through a series of audits by an independent third-party, Netherlands-based EY CertifyPoint.

ISO 27001 (Information security management)
ISO 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 27002. To be worthy of your trust, we're continually and comprehensively managing and improving our physical, technical, and legal controls at Dropbox. Our auditor, EY CertifyPoint, maintains its ISO 27001 accreditation from the Raad voor Accreditatie (Dutch Accreditation Council). View the Dropbox Business, Enterprise, and Education ISO 27001 certificate.

ISO 27017 (Cloud security)
ISO 27017 is a new international standard for cloud security that provides guidelines for security controls applicable to the provision and use of cloud services. Our Shared Responsibility Guide explains several of the security, privacy, and compliance requirements that Dropbox and its customers can solve together. View the Dropbox Business, Enterprise, and Education ISO 27017 certificate.

ISO 27018 (Cloud privacy and data protection)
ISO 27018 is an emerging international standard for privacy and data protection that applies to cloud service providers like Dropbox who process personal information on behalf of their customers and provides a basis for which customers can address common regulatory and contractual requirements or questions. View the Dropbox Business, Enterprise, and Education ISO 27018 certificate.

ISO 22301 (Business continuity management)
ISO 22301 is an international standard for business continuity that guides organizations on how to decrease the impact of disruptive events and respond to them appropriately if they occur by minimizing potential damage. The Dropbox business continuity management system (BCMS) is part of our overall risk management strategy to protect people and operations during times of crises. View the Dropbox Business, Enterprise, and Education ISO 22301 certificate.

SOC reports

The Service Organization Controls (SOC) reports, known as either the SOC 1, SOC 2, or SOC 3, are frameworks established by the American Institute of Certified Public Accountants (AICPA) for reporting on internal controls implemented within an organization. Dropbox has certified its operations, processes, and technology by an independent third-party auditor, Ernst & Young LLP.

SOC 3 for Security, Confidentiality, Integrity, Availability, and Privacy
The SOC 3 assurance report covers all five Trust Service Principles of Security, Confidentiality, Integrity,Availability, and Privacy (TSP Section 100). The Dropbox general-use report is an executive summary of the SOC 2 report and includes the independent third-party auditor's opinion on the effective design and operation of our controls. View the Dropbox Business, Enterprise, and Education SOC 3 examination.

SOC 2 for Security, Confidentiality, Integrity, Availability, and Privacy
The SOC 2 report provides customers with a detailed level of controls-based assurance, covering all five Trust Service Principles of Security, Confidentiality, Processing Integrity, Availability, and Privacy (TSP Section 100). The SOC 2 report includes a detailed description of Dropbox's processes and the more than 100 controls in place to protect your stuff. In addition to our independent third-party auditor's opinion on the effective design and operation of our controls, the report includes the auditor's test procedures and results for each control. The SOC 2 examination of Dropbox Business, Enterprise, and Education is available upon request through the sales team or the account management team.

SOC 1 / SSAE 16 / ISAE 3402 (formerly SAS 70)
The SOC 1 report provides specific assurances for customers who determine that Dropbox Business, Enterprise, or Education is a key element of their internal controls over financial reporting (ICFR) program. These specific assurances are primarily used for our customers' Sarbanes-Oxley (SOX) compliance. The independent third-party audit is conducted in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standard on Assurance Engagements No. 3402 (ISAE 3402). These standards have replaced the deprecated Statement on Auditing Standards No. 70 (SAS 70). The SOC 1 examination of Dropbox Business, Enterprise, and Education is available upon request through the sales team or the account management team.

HIPPA/HTECH

Dropbox will sign business associate agreements (BAAs) with Dropbox Business, Enterprise, and Education customers who require them in order to comply with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). Learn more by visiting our Getting Started with HIPAA guide and Help Center article.

Dropbox makes available a third-party assurance report evaluating our controls for the HIPAA/HITECH Security, Privacy, and Breach Notification rules, as well as a mapping of our internal practices and recommendations for customers who are looking to meet the HIPAA/HITECH Security and Privacy rule requirements with Dropbox Business, Enterprise, and Education.

Cloud Security Alliance

Security, Trust, and Assurance Registry (CSA STAR)
The CSA Security, Trust & Assurance Registry (STAR) is a free, publicly-accessible registry that offers a security assurance program for cloud services, thereby helping users to assess the security posture of cloud providers they currently use or are considering contracting with. Dropbox Business, Enterprise, and Education have received the CSA STAR Level 2 Certification, a third-party independent assessment of our security controls by EY CertifyPoint based on the requirements of ISO 27001 and the CSA Cloud Controls Matrix (CCM) v.3.0.1, a set of criteria that measures the capability levels of cloud services. Dropbox Business has also completed the CSA STAR Level 1 Self-Assessment, a rigorous survey based on CSA's Consensus Assessments Initiative Questionnaire (CAIQ), which aligns with the CCM, and provides answers to almost 300 questions a cloud customer or a cloud security auditor may wish to ask. View our CSA STAR Level 1 Self-Assessment and Level 2 Certification on the CSA website.

Adoption: the key to true enterprise security

Encryption, secure protocols, and compliance are a given for anything in your IT suite—but in order to realize the value of a secure solution, adoption is critical. At the same time, bringing new technology into an organization can be a major challenge. At Dropbox, we believe that user-friendly tools provide IT with a unique opportunity to centralize data onto a sanctioned platform—the first step to gaining real visibility and control.

Dropbox has approached this by becoming employees' go-to tool for productivity, whether they're working together at the office, out in the field, or with their network of partners, vendors, and customers. As an industry leader in both performance and usability, Dropbox gains widespread adoption when brought into organizations. Additionally, Dropbox Business helps IT bring prior Dropbox usage—and all of its data—into the company domain. By pairing unparalleled adoption with the controls IT needs, Dropbox Business delivers greater value and security than traditional solutions.

For more information on the visibility and control features available on Dropbox Business, please read our Admin Guide.

"As we procure more highprofile clients, we need to be able to assure them that every system we use is completely secure. Dropbox Business is perfect for that."

Buzz Osborne,
Director of UX, Campaign Monitor