Dropbox Business 보안

Dropbox 백서

Dropbox

목차

개요

다양한 업계에서 디지털 트랜스포메이션이 계속 진행되는 오늘날, 장소를 불문하고 데이터와 팀, 장치를 보호할 수 있는 역량은 매우 중요합니다. Dropbox Business 같은 클라우드 솔루션을 통해 원격 근무와 분산 워크플로를 활성화한 조직은 협업을 간소화하고, 클라우드에서의 위험 요소를 사전에 관리해야 합니다. 또한, 회복력 있는 관리형 클라우드 서비스를 통해 지식재산권(IP)의 기밀성, 저장하고 공유한 데이터의 무결성, 데이터의 가용성을 보장하는 효율적인 제어 환경을 구축해야 합니다.

50만 이상의 비즈니스와 조직이 Dropbox Business를 솔루션으로 선택해 분산된 팀의 원격 근무와 안전한 협업을 지원하고 있습니다. Dropbox Business 솔루션의 중심에는 협업, 파일 동기화, 공유를 지원하는 스마트 작업 공간이 있습니다. Dropbox Business 솔루션은 업계 최고의 인프라스트럭처를 기반으로 운영되며, 고급 엔터프라이즈 보안, 팀/콘텐츠 보안, 전자 서명, 안전한 전송, 데이터 거버넌스 등의 기능을 제공합니다.

Dropbox Business의 중심에는 다계층 보안 접근 방식을 기반으로 한 통합 보안 프로그램 'Dropbox 신뢰 프로그램'이 있습니다. 이는 전 세계적으로 원격 근무가 점점 더 활발해지고 있는 오늘날 없어서는 안 될 필수 요소입니다.

이 백서에는 Dropbox Business 제품 보안 기능, Dropbox의 운영상 보안 조치, 개인정보 보호 및 투명성에 대한 약속에 더불어 Dropbox가 조직이 믿고 사용할 수 있는 안전한 솔루션임을 입증하는 백엔드 정책, 독립 기관 인증, 컴플라이언스 조치가 상세하게 기술되어 있습니다.

별도로 명시되지 않는 한 이 백서에 기술된 정보는 모든 Dropbox Business 제품(Standard, Advanced, Enterprise)과 Dropbox Education에 적용됩니다. Paper는 Dropbox Business와 Dropbox Education에서 제공되는 기능입니다.

들여다보기

Dropbox의 간편한 인터페이스는 빠르고 안정된 동기화, 공유, 협업 기능을 지원하는 인프라스트럭처를 기반으로 실행됩니다. Dropbox는 이를 위해 제품과 아키텍처를 지속적으로 개선해 데이터 전송 속도와 신뢰성을 높이며 IT 환경 변화에 대응하고 있습니다. 이 섹션에서는 데이터가 어떻게 안전하게 전송되고, 저장되고, 처리되는지 살펴보도록 하겠습니다.

파일 인프라스트럭처

Dropbox 사용자는 데스크톱, 웹, 모바일 클라이언트 또는 Dropbox에 연결된 타사 애플리케이션을 통해 언제든지 파일과 폴더에 액세스할 수 있습니다. 모든 클라이언트는 보안 서버에 연결되어 파일로의 액세스를 제공하고, 파일 공유 기능을 지원하며, 파일이 추가, 변경, 또는 삭제되었을 때 연결된 장치를 업데이트합니다.

Dropbox의 파일 인프라스트럭처는 다음과 같이 구성되어 있습니다.

- ***메타데이터 서버***

  메타데이터로 불리는 사용자 데이터에 관한 기본 정보는 자체 스토리지 서비스에 개별적으로 보관되어 사용자 계정에 있는 모든 데이터의 인덱스 역할을 합니다. 메타데이터에는 이메일 주소, 이름, 장치 이름 등과 같은 사용자 정보와 기본적인 계정 정보가 포함됩니다. 또한, 변경내용 기록, 복구, 동기화 등의 지원 기능을 위해 활용되는 파일의 기본 정보(파일 이름, 유형 등)도 메타데이터에 포함됩니다.

- ***메타데이터 데이터베이스***

  파일 메타데이터는 MySQL을 지원하는 데이터베이스 서비스에 저장되며, 필요 시 샤딩과 복제를 거쳐 성능과 고가용성 요건을 충족합니다.

- ***블록 서버***

  Dropbox는 기존의 암호화 기술의 한계를 뛰어넘은 자체 보안 메커니즘으로 데이터를 보호합니다. 블록 서버는 각 파일을 블록으로 나누고, 각 파일 블록을 강력한 암호로 암호화하며, 파일이 수정된 경우 변경된 블록만 동기화하는 방식으로 Dropbox 애플리케이션에 있는 파일을 처리합니다. 새로운 파일이나 기존 파일에 변경이 감지되면 Dropbox 애플리케이션은 이를 블록 서버에 통보하고, 새롭게 생성되거나 수정된 파일 블록은 처리를 거쳐 블록 스토리지 서버로 전송됩니다. 블록 서버는 사용자에게 파일과 미리 보기를 제공하는 역할도 합니다. 이러한 서비스에 사용되는 전송 중 데이터/저장된 데이터 암호화에 관한 자세한 내용은 아래의 암호화 섹션에서 확인할 수 있습니다.

- ***블록 스토리지 서버***

  파일의 실제 콘텐츠는 암호화된 블록 형태로 블록 스토리지 서버에 저장됩니다. Dropbox 클라이언트는 파일 콘텐츠를 전송하기 전에 파일을 블록으로 나누어 저장에 대비합니다. 블록 스토리지 서버는 내용 주소화 기억 장치(CAS) 시스템 역할을 하며 해시값을 기준으로 암호화된 개별적인 파일 블록을 검색합니다.

- ***미리 보기 서버***

  미리 보기 서버는 파일의 미리 보기를 생성하는 역할을 합니다. 미리 보기는 사용자의 장치에 빠르게 표시되도록 파일 형식을 적절하게 변환한 것을 말합니다. 미리 보기 서버는 블록 스토리지 서버에서 파일 블록을 불러와 미리 보기를 생성합니다. 파일 미리 보기 요청이 전송되면 미리 보기 서버는 미리 보기 스토리지 서버로부터 캐시로 저장된 미리 보기를 불러와 이것을 블록 서버로 전송합니다. 최종적으로 미리 보기는 블록 서버를 통해 사용자에게 전송됩니다.

- ***미리 보기 스토리지 서버***

  캐시로 저장된 미리 보기는 암호화된 형태로 미리 보기 스토리지 서버에 저장됩니다.

- ***알림 서비스***

  이 별도의 서비스는 Dropbox 계정에 변경 사항이 있는지를 모니터링하며, 이 과정에서는 어떠한 파일이나 메타데이터도 저장되거나 전송되지 않습니다. 각 클라이언트는 롱 폴링 방식으로 알림 서비스에 연결을 설정한 후 대기합니다. Dropbox 파일에 변경 사항이 생기면 알림 서비스는 롱 폴링 연결을 종료해 관련 클라이언트에 변경 사항이 있다는 것을 알립니다. 연결 종료는 클라이언트가 메타데이터 서버에 안전하게 연결되어야 파일의 변경 사항을 동기화할 수 있다는 신호입니다.

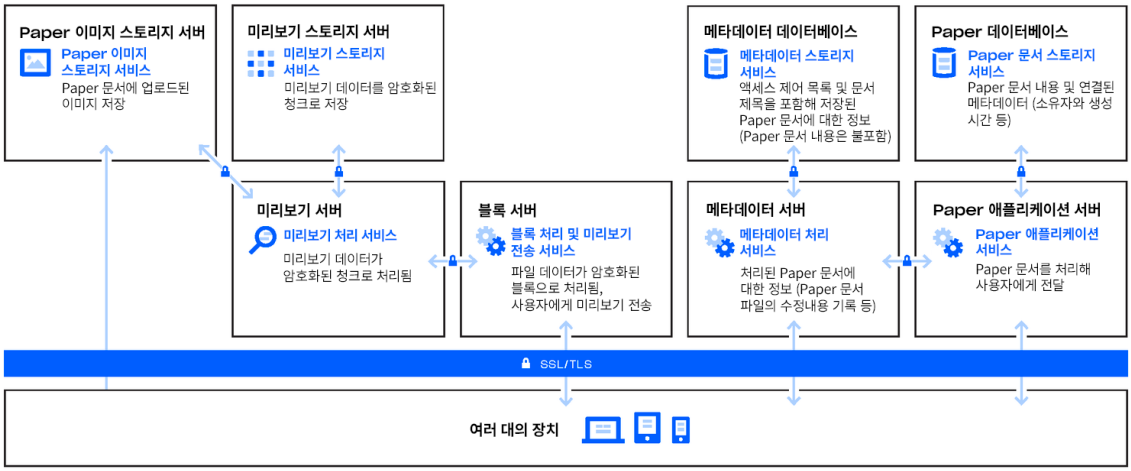
파일 데이터 저장

Dropbox는 기본적으로 2가지 데이터, 즉, 파일의 메타데이터(파일이 마지막으로 수정된 날짜와 시간 등)와 파일의 실제 콘텐츠(파일 블록)를 저장합니다. 파일 메타데이터는 Dropbox에 저장되고, 파일 블록은 Dropbox의 사내 스토리지 시스템인 Amazon Web Services(AWS)와 Magic Pocket 중 하나에 저장됩니다. Magic Pocket은 Dropbox의 독점 소프트웨어와 하드웨어로 구성되어 있으며, 초기 단계에서부터 안정성과 보안에 중점을 두고 설계되었습니다. Magic Pocket과 AWS 모두 유휴 상태에서 파일 블록을 암호화하며, 높은 수준의 신뢰성 기준을 충족합니다. 자세한 내용은 아래의 신뢰성 섹션에서 확인할 수 있습니다.

Paper 인프라스트럭처

Dropbox 사용자는 웹과 모바일 클라이언트 또는 Dropbox Paper 애플리케이션에 연결된 타사 애플리케이션을 통해 언제든지 Paper 문서에 액세스할 수 있습니다. 모든 클라이언트는 보안 서버에 연결되어 Paper 문서로의 액세스를 제공하고, 문서 공유 기능을 지원하며, 문서가 추가되거나 변경되거나 삭제되었을 때 연결된 장치를 업데이트합니다.

Dropbox Paper의 인프라스트럭처는 다음과 같이 구성되어 있습니다.



- ***Paper 애플리케이션 서버***

  Paper 애플리케이션 서버는 사용자 요청을 처리해 수정된 Paper 문서의 변경 사항을 다시 사용자에게 전송하며, 알림 서비스를 수행합니다. Paper 애플리케이션 서버가 사용자가 변경한 내용을 Paper 데이터베이스에 입력하면 이 변경 사항은 데이터베이스 내 영구 저장소에 저장됩니다. Paper 애플리케이션 서버와 Paper 데이터베이스 간의 통신은 HTTPS(Secure Hypertext Transfer Protocol)를 통해 보호됩니다.

- ***Paper 데이터베이스***

  Paper 문서와 관련된 특정한 메타데이터와 문서의 실제 콘텐츠는 Paper 데이터베이스의 영구 저장소에서 암호화됩니다. 여기에는 댓글과 작업 등 Paper 문서에 담긴 콘텐츠뿐만 아니라 제목, 소유자, 생성 날짜, 기타 정보 등과 같은 Paper 문서에 관한 정보가 포함됩니다. Paper 데이터베이스는 필요시 샤딩과 복제를 거쳐 성능과 고가용성 요건을 충족합니다.

- ***메타데이터 서버***

  Paper는 Dropbox 인프라스트럭처 도표에 설명된 메타데이터 서버를 사용해 Paper 문서 파일 버전 기록, 공유 폴더 구성원 자격과 같은 Paper 문서 정보를 처리합니다. Dropbox는 메타데이터 서버를 직접 관리하며, 이 서버는 외부업체와 공동으로 운영하는 데이터 센터에 위치해 있습니다.

- ***메타데이터 데이터베이스***

  Paper는 Dropbox 인프라스트럭처 도표에 설명된 메타데이터 데이터베이스를 사용해 공유, 권한, 폴더와 같은 Paper 문서 관련 정보를 저장합니다. Paper 문서 메타데이터는 MySQL을 지원하는 데이터베이스 서비스에 저장되며, 필요시 샤딩과 복제를 거쳐 성능과 고가용성 요건을 충족합니다.

- ***Paper 이미지 스토리지 서버***

  Paper 문서에 업로드된 이미지는 Paper 이미지 스토리지 서버에 저장되고 유휴 상태에서 암호화됩니다. Paper 애플리케이션과 Paper 이미지 스토리지 서버 간의 이미지 데이터 전송은 암호화된 세션을 통해 진행됩니다.

- ***미리 보기 서버***

  미리 보기 서버는 Paper 문서에 업로드된 이미지의 미리 보기와 문서에 삽입된 하이퍼링크의 미리 보기를 생성합니다. Paper 문서에 업로드된 이미지의 경우, 미리 보기 서버는 암호화된 경로를 통해 Paper 이미지 스토리지 서버에 저장된 이미지 데이터를 불러옵니다. Paper 문서에 삽입된 하이퍼링크의 경우, 미리 보기 서버는 소스 링크가 지정한 암호화를 사용해 이미지 데이터를 불러온 후 미리 보기를 생성합니다. 최종적으로 미리 보기는 블록 서버를 통해 사용자에게 전송됩니다.

- ***미리 보기 스토리지 서버***

  Paper는 Dropbox 인프라스트럭처 도표에 설명된 동일한 미리 보기 스토리지 서버를 사용해 캐시로 저장된 이미지 미리 보기를 저장합니다. 캐시로 저장된 미리 보기 청크는 암호화된 형태로 미리 보기 스토리지 서버에 저장됩니다.

Paper 문서 저장

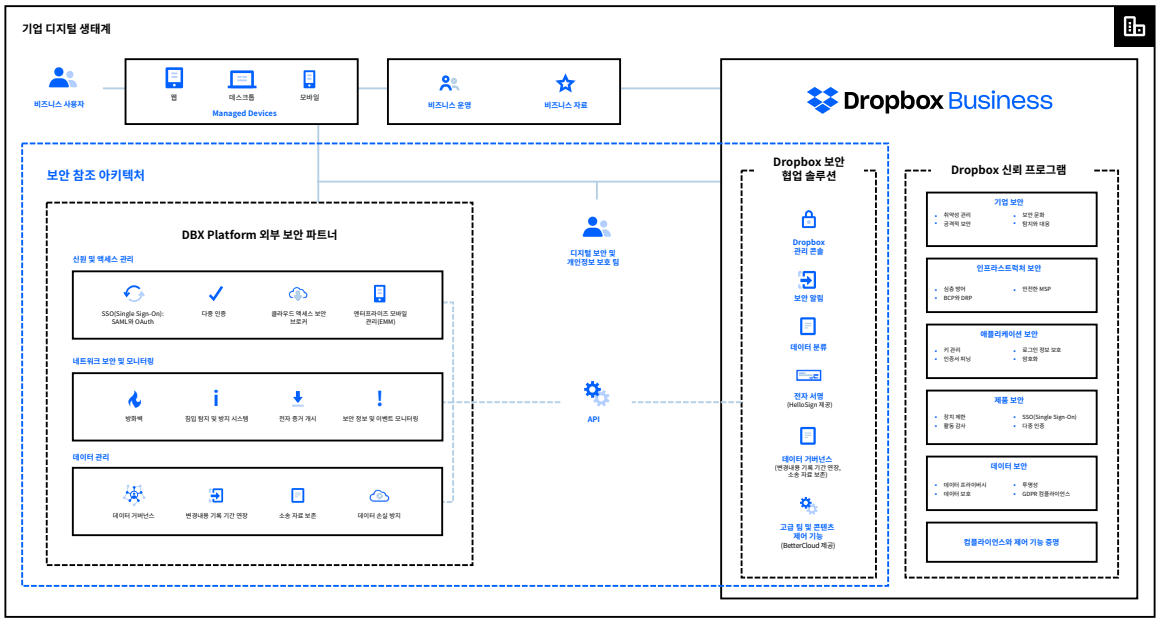
Dropbox는 기본적으로 문서의 공유 권한과 같은 Paper 문서 정보와 사용자가 문서에 입력한 실제 콘텐츠를 저장합니다. 이러한 데이터는 통칭해 Paper 문서 데이터로 불리며, Paper 문서에 업로드된 이미지는 Paper 이미지 데이터로 불립니다. 각 데이터 유형은 Amazon Web Services(AWS)에 저장됩니다. Paper 문서는 유휴 상태일 때 AWS에서 암호화되며, AWS는 높은 수준의 신뢰성 기준을 충족합니다. 자세한 내용은 아래의 신뢰성 섹션에서 확인할 수 있습니다.

Dropbox 신뢰 프로그램

신뢰는 Dropbox가 전 세계 수백만 개인·비즈니스 고객과의 관계를 형성하는 토대입니다. Dropbox는 고객의 신뢰를 소중히 여기며 사용자 정보 보호에 대한 책임을 중요하게 생각합니다. Dropbox는 보안, 개인정보 보호, 투명성, 컴플라이언스에 중점을 두고 Dropbox를 구축했고, 앞으로도 같은 방향으로 성장해 나가며 여러분의 신뢰에 보답할 것입니다.

Dropbox 신뢰 프로그램 정책은 환경적, 물리적, 사용자, 외부 업체, 관련 법률 및 규정, 계약상 요건 관련 위험을 비롯해 시스템 보안, 기밀성, 무결성, 가용성, 개인정보 보호에 영향을 줄 수 있는 기타 다양한 위험에 대처하는 위험성 평가 프로세스를 규정합니다. 성능 평가는 최소한 일 년에 한 번 이상 시행됩니다. Dropbox 신뢰 프로그램에 관한 자세한 내용은 dropbox.com/business/trust에서 확인할 수 있습니다.

Dropbox는 다계층 보안으로 조직에 영향을 미치는 엔터프라이즈, 인프라스트럭처, 애플리케이션, 제품을 보호합니다.



제품 보안

Dropbox는 제어 기능과 가시성을 통해 IT 부서와 최종 사용자 모두가 데이터를 효율적으로 관리할 수 있도록 지원합니다. Dropbox를 사용하면 도구, 콘텐츠, 공동 작업자 등 업무에 필요한 모든 것을 한 공간에서 이용할 수 있습니다. Dropbox는 단순한 보안 스토리지가 아닙니다. 기존 워크플로를 최적화하는 스마트한 업무 공간입니다.

아래에서 관리자와 사용자에게 제공되는 주요 기능과 핵심 IT 프로세스 관리를 위한 타사 앱 통합에 대해 살펴보도록 하겠습니다.

참고: 제공되는 기능은 가입한 요금제에 따라 다릅니다. 자세한 내용은 dropbox.com/business/plans에서 확인할 수 있습니다.

콘텐츠 제어

지식재산권(IP), 개인 식별 정보(PII) 등의 민감한 비즈니스 자료를 보호하는 일은 IT팀과 데이터 보안팀의 핵심 업무입니다. Dropbox는 세분화된 콘텐츠 권한에서부터 데이터 보관 정책, 소송 자료 보존 기능까지 콘텐츠 관리, 모니터링, 보호를 위한 업계 최고의 솔루션을 제공합니다. 콘텐츠 제어를 지원하는 주요 제품과 기능은 다음과 같습니다.

세분화된 콘텐츠 권한

공유 파일과 폴더 권한

- ***공유 파일에 대한 권한***

  공유 파일을 소유한 팀원은 특정한 사용자의 액세스를 삭제하고 파일에 댓글 달기 기능을 비활성화할 수 있습니다.

- ***공유 폴더에 대한 권한***

  공유 폴더를 소유한 팀원은 특정한 사용자의 폴더 액세스를 삭제하고, 특정한 사용자의 보기/수정 권한을 변경하고, 폴더 소유권을 이전할 수 있습니다. 또한, 팀의 전체 공유 권한에 따라 각 공유 폴더의 소유자는 팀 외부 사람과의 폴더 공유, 수정 권한이 있는 구성원의 자격 관리, 폴더 외부 사람과의 링크 공유 허용 여부를 제어할 수 있습니다.

- ***공유 링크의 비밀번호***

  모든 공유 링크는 링크 소유자가 설정한 비밀번호로 보호할 수 있습니다. 액세스 제어 계층은 파일이나 폴더 데이터가 전송되기 전에 비밀번호가 올바르게 입력되었는지, 그리고 팀, 그룹, 폴더 ACL 등의 기타 요건이 충족되었는지를 확인합니다. 비밀번호가 올바르게 입력되고 기타 요건이 충족된 경우, 보안 쿠키가 사용자의 브라우저에 저장되어 입력한 비밀번호가 이전에 확인되었다는 것을 기억합니다. 관리자는 공유 제어 기능을 사용해 비밀번호 설정을 선택 사항으로 두는 대신 기본 비밀번호를 설정하여 팀의 콘텐츠를 더 강력하게 보호할 수 있습니다.

- ***공유 링크의 만료일***

  사용자는 공유 링크에 만료일을 설정해 파일이나 폴더로의 임시 액세스를 제공할 수 있습니다. 관리자는 공유 제어 기능을 사용해 만료일 설정을 선택 사항으로 두는 대신 기본 만료일을 설정하여 팀의 콘텐츠를 더 강력하게 보호할 수 있습니다.

Paper 문서와 Paper 공유 폴더 권한

- ***Paper 문서와 Paper 공유 폴더에 대한 권한***

  Paper 문서 또는 Paper 공유 폴더를 소유한 팀원은 특정한 사용자의 액세스를 삭제하고, Paper 문서를 수정하는 기능을 비활성화할 수 있습니다.

- ***Paper 문서에 대한 권한***

  Paper 문서를 소유한 팀원은 공유 패널에 등록된 특정한 사용자의 액세스를 제거할 수 있습니다. Paper 문서 소유자와 수정 권한을 가진 팀원 모두 특정한 사용자의 보기/수정 권한과 문서 링크 정책을 변경할 수 있습니다. 링크 정책은 문서를 열어볼 수 있는 사용자와 이들에게 부여된 권한을 규정합니다. 팀 관리자는 팀 전체에 적용되는 링크 정책과 문서 공유 정책을 설정할 수 있습니다.

- ***Paper 폴더에 대한 권한***

  폴더의 구성원 자격을 가진 팀원은 폴더의 공유 정책을 변경하고 폴더에 추가된 특정한 사용자의 액세스를 삭제할 수 있습니다.

파일/폴더 작업

- ***파일 저장용 팀 폴더***

  관리자는 그룹과 다른 공동 작업자들에게 적절한 콘텐츠 액세스 수준(보기 전용 또는 수정 가능)을 자동으로 부여하는 팀 폴더를 생성할 수 있습니다.

  - ***세분화된 액세스와 공유 제어 기능***

    공유 제어 기능은 회사 내외부 그룹 및 사람들이 특정한 폴더에만 액세스하도록 관리자가 최상위 또는 하위 폴더 수준에서 구성원 자격과 권한을 관리하는 기능입니다.

  - ***팀 폴더 관리 도구***

    관리자는 모든 팀 폴더를 볼 수 있고, 중심 공간에서 공유 정책을 맞춤형으로 설정해 기밀 자료가 잘못 공유되는 일을 방지할 수 있습니다.

- ***Paper 문서용 공유 폴더***

  관리자는 공동 작업자들에게 적절한 콘텐츠 액세스 수준(댓글 달기 또는 수정 가능)을 자동으로 부여하는 Paper 공유 폴더를 생성할 수 있습니다.

- ***원격 삭제***

  직원이 다른 팀으로 옮기거나 장치를 분실했을 때 관리자가 원격으로 Dropbox 데이터와 파일의 로컬 사본을 삭제할 수 있습니다. 컴퓨터와 모바일 장치가 온라인 상태가 되고 Dropbox 애플리케이션이 실행되면 파일이 컴퓨터와 모바일 장치에서 삭제됩니다.

- ***계정 이전***

  사용자 프로비전을 해제한 후(수동 작업 또는 디렉터리 서비스를 통해) 관리자는 이전 팀원이 생성한 Paper 문서의 소유권과 파일을 팀 내 다른 사용자의 계정으로 이전할 수 있습니다. 계정 이전 기능은 사용자를 삭제할 때와 사용자 계정을 삭제한 이후 언제든 사용할 수 있습니다.

다음 기능은 추가로 사용할 수 있는 부가 기능입니다(자세한 정보는 영업팀에 문의하세요).

- **콘텐츠 스캔**

  고급 팀 및 콘텐츠 제어 기능은 Dropbox에 저장된 새로운 파일과 기존 파일을 스캔해 데이터 취약성을 완화할 수 있는 부가 기능으로, Dropbox Business Advanced/Enterprise 요금제에서 제공됩니다. Dropbox Enterprise 팀은 데이터 분류 기능을 사용해 콘텐츠를 스캔하고, 민감한 콘텐츠가 외부로 공유됐을 때 알림을 받아볼 수 있습니다.

- **맞춤형 워크플로 설정과 실행**

  관리자는 고급 팀 및 콘텐츠 제어 부가 기능을 사용해 회사 정책을 위반하는 파일에 원하는 작업을 맞춤형으로 실행할 수 있습니다.

- **경고 알림 설정**

  관리자는 보안 문제를 실시간으로 모니터링해 데이터 취약성을 완화할 수 있습니다. 파일을 외부에 공유하거나 민감한 데이터를 스캔하면 경고 알림이 전송됩니다. Dropbox Enterprise 팀의 관리자는 보안 알림 기능을 사용해 민감한 콘텐츠가 외부로 공유됐을 때 알림이 전송되도록 설정할 수 있습니다.

콘텐츠 가시성

보안 알림

- **경고 및 알림**

  Dropbox Enterprise 팀 계정에서 수상한 행위, 위험한 활동, 데이터 유출 등의 잠재적 사고가 감지되면 팀 관리자에게 실시간으로 알림이 전송됩니다. 보안 기능이 모니터링하는 이벤트는 다음과 같습니다.

  - 대량의 데이터 삭제
  - 대량의 데이터 이전
  - 민감한 콘텐츠 외부 공유
  - 팀 외부에서 공유된 악성 소프트웨어
  - 팀 내부에서 공유된 악성 소프트웨어
  - 너무 많은 로그인 시도 실패
  - 고위험 국가에서의 로그인

  Dropbox는 알림 임계값 설정, 알림 수신인 변경, 민감한 파일이 보관된 파일 외부 공유 시 알림 전송 등의 기능도 제공합니다. 관리자는 알림의 상태를 검토 중, 완료, 무시로 표시할 수 있고, 대시보드 위젯에서 지난주 알림 통계와 동향을 살펴볼 수 있습니다.

외부 공유 보고서와 외부 공유 페이지

Dropbox는 외부 공유 보고서와 외부 공유 페이지로 추가적인 가시성을 제공합니다. 관리자는 인사이트 페이지나 외부 공유 페이지에서 외부 공유 보고서를 생성할 수 있습니다. 이 보고서에는 팀 외부에 공유된 모든 팀 파일과 폴더, 공유 링크가 기록되어 있습니다. 외부 공유 페이지는 관리 콘솔에 새롭게 추가된 페이지로, 관리자는 이 페이지에서 파일 유형, 공유한 사람, 링크 설정 등의 기준으로 팀이 공유한 파일과 폴더, 공유 링크를 필터링해 확인할 수 있습니다.

공유 제어 기능

공유 설정 기능은 팀 관리자에게 한층 강화된 공유 제어 기능과 팀 콘텐츠 액세스 제어 기능을 제공합니다. 관리자는 팀 전체에 기본 만료일과 비밀번호 제한이 적용되도록 설정할 수 있습니다. 관리자가 이러한 제한을 설정하면 제한 설정에 관한 책임을 사용자에게 전가하지 않아도 되어 데이터 손실의 위험성이 줄어듭니다.

데이터 분류

Dropbox Enterprise 팀은 개인정보와 민감한 데이터에 자동으로 라벨을 적용해 데이터 유출 위험성을 줄일 수 있습니다. 민감한 데이터가 보관된 팀 폴더 내 파일이나 폴더가 외부로 공유되면 이메일과 관리 콘솔로 관리자에게 데이터 손실 방지(DLP) 알림이 전송됩니다. 관리자는 공유 폴더와 팀원 개인 폴더에 저장된 민감한 데이터를 자동으로 파악해 분류하는 기능을 사용할 수 있습니다. 데이터 분류 기능은 Dropbox Enterprise 팀 관리자가 관리 콘솔에서 활성화할 수 있습니다.

데이터 거버넌스 부가 기능

데이터 거버넌스는 조직의 데이터를 관리하고 보호하는 프로세스, 기술, 팀을 통칭합니다. 여기에는 조직 데이터를 필요에 따라 저장하고, 식별하고, 검색하고, 복구하는 기능이 포함됩니다.

Dropbox 데이터 거버넌스는 조직이 더 강력하고 안전하게 데이터를 제어하는 동시에 규제와 컴플라이언스를 충족하는 데 수반되는 위험성과 비용을 줄일 수 있도록 도와주는 다양한 기능을 제공합니다. 현재 이 부가 기능에는 팀 관리자와 컴플라이언스 관리자를 위한 4가지 주요 기능이 포함되어 있습니다.

- **변경내용 기록 기간 연장**

  기본으로 제공되는 변경내용 기록 기능은 사용 중인 Dropbox 계정 유형에 따라 다릅니다. 하지만 Dropbox Business 팀의 경우, 별도로 변경내용 기록 연장(EVH) 또는 데이터 거버넌스 부가 기능을 구매해 지난 10년간 삭제되거나 변경된 모든 파일을 복구할 수 있습니다.

- **소송 자료 보존**

  팀원에게 소송 자료 보존을 걸면 팀 관리자와 컴플라이언스 관리자가 해당 팀원이 생성하거나 수정한 모든 콘텐츠를 보고, 내보낼 수 있습니다. 소송 자료 보존이 걸린 팀원에게는 이 사실이 통보되지 않으며, 팀원의 파일 생성, 수정, 삭제 권한은 계속 유지됩니다.

- **데이터 보존**

  팀 관리자와 컴플라이언스 관리자는 데이터 보존 기능으로 규정 준수에 필요한 콘텐츠를 특정한 기간 동안 보존하도록 설정해 실수로 인한 삭제를 방지할 수 있습니다. 이 기능을 설정하면 '최근 수정일'로부터 10년간 데이터가 보존됩니다.

- **데이터 처리**

  팀 관리자와 컴플라이언스 관리자는 데이터 처리 기능으로 특정한 날짜에 데이터가 영구적으로 삭제되도록 설정해 데이터 보존 및 처리 요건을 준수할 수 있습니다. 파일 삭제일이 다가오면 관리자에게 알림이 전송되어 활동 모니터링이 간편합니다.

복구와 버전 관리

Dropbox Business 고객은 삭제된 파일, Paper 문서를 복원하는 기능과 파일 이전 버전, Paper 문서를 복구하는 기능을 사용해 중요한 데이터의 변경 사항을 추적하고 되돌릴 수 있습니다.

모바일 장치에서의 데이터 보안

- **데이터 삭제**

  사용자는 비밀번호 입력 오류 10회 이후 장치에서 모든 Dropbox 데이터를 삭제하는 기능을 활성화해 보안을 강화할 수 있습니다.

- **내부 기억 장치와 오프라인 파일**

  파일은 모바일 장치의 내부 기억 장치에 저장되지 않도록 기본 설정되어 있습니다. Dropbox 모바일 클라이언트에는 개별적인 파일과 폴더를 장치에 오프라인 보기 전용으로 저장하는 기능이 있습니다. 모바일이나 웹 인터페이스에서 Dropbox 계정과 장치의 연결을 해제하면 장치에 저장되어 있던 오프라인 파일과 폴더가 자동으로 장치의 내부 기억 장치에서 삭제됩니다.

- **오프라인 Paper 문서**

  Dropbox 계정의 보안 페이지에서 Paper와 장치의 연결을 해제하면 사용자가 계정에서 로그아웃되고, 오프라인 Paper 문서가 자동으로 장치의 내부 기억 장치에서 삭제됩니다.

팀 제어

하나부터 열까지 모든 것이 똑같은 조직은 존재하지 않습니다. 그래서 Dropbox는 관리자가 팀의 환경과 특성에 따라 Dropbox Business를 맞춤형으로 설정할 수 있는 다양한 도구를 개발했습니다. Dropbox Business는 관리자를 위한 관리 도구뿐만 아니라 최종 사용자가 자신의 계정과 데이터에 대한 보안을 강화할 수 있는 도구를 갖추고 있습니다. 여러 가지 Dropbox 사용자 인터페이스를 통해 아래에 설명된 인증, 복구, 로그인, 기타 보안 기능을 이용할 수 있습니다.

아래에서 Dropbox Business 관리 콘솔에서 제공되는 제어 기능과 가시성 기능 몇 가지를 살펴보도록 하겠습니다.

세분화된 콘텐츠 권한

- ***계층적 관리자 역할***

  Dropbox는 팀을 효율적으로 관리할 수 있도록 계층적 관리자 역할을 제공합니다. 계정 관리자에게는 세 가지 수준의 액세스 중 하나를 부여할 수 있습니다. 팀당 관리자의 수에는 제한이 없으며, 팀원이라면 누구나 관리자 역할을 맡을 수 있습니다.

  - ***팀 관리자***

    팀 관리자는 팀 전체의 보안 권한과 공유 권한을 설정하고, 관리자를 만들고, 팀원을 관리할 수 있습니다. 팀 관리자에게는 Dropbox에서 제공되는 모든 관리자 권한이 주어집니다. 팀 관리자만 관리자 역할을 지정하거나 변경할 수 있기 때문에 Dropbox Business 계정에는 항상 1명 이상의 팀 관리자가 있어야 합니다.

  - ***사용자 관리자***

    관리자는 팀원 추가/삭제, 그룹 관리, 팀의 활동 피드 확인 등과 같은 대부분의 팀 관리 업무를 처리할 수 있습니다.

  - ***지원 관리자***

    지원 관리자는 삭제된 파일 복구, 2단계 인증에 실패해 계정에 액세스할 수 없는 팀원 지원과 같은 일반적인 서비스 요청을 처리할 수 있습니다. 또한, 관리자가 아닌 팀원의 비밀번호를 재설정하고, 특정한 팀원의 활동 로그를 파일로 내보낼 수 있습니다.

  - ***청구 관리자***

    청구 관리자는 관리 콘솔의 청구 페이지에 액세스할 수 있습니다.

  - ***콘텐츠 관리자***

    콘텐츠 관리자는 콘텐츠 관리 도구에서 팀 폴더를 만들어 관리할 수 있습니다.

  - ***보고서 관리자***

    보고서 관리자는 관리 콘솔에서 보고서를 생성할 수 있고, 활동 페이지에 액세스할 수 있습니다.

  - ***보안 관리자***

    보안 관리자는 보안 알림, 외부 공유, 보안 위험을 관리할 수 있습니다.

  - ***컴플라이언스 관리자*** (데이터 거버넌스 부가 기능을 사용하는 팀에서만 사용 가능)

    컴플라이언스 관리자는 데이터 거버넌스 페이지(소송 자료 보존, 데이터 보존, 데이터 처리)를 관리할 수 있고, 콘텐츠 관리 도구에 액세스할 수 있습니다.

- ***그룹***

  팀은 Dropbox에서 팀원 목록을 생성하고 관리할 수 있고, 팀원들에게 특정한 폴더로의 액세스를 제공할 수 있습니다. Active Directory 커넥터를 사용해 Dropbox와 Active Directory 그룹을 동기화할 수도 있습니다.

  - ***회사 관리 그룹***

    이 유형의 그룹은 오직 관리자만이 그룹을 생성하고, 삭제하고, 구성원을 관리할 수 있습니다. 사용자는 회사가 관리하는 그룹에 가입 요청을 하거나, 자의로 그룹을 떠날 수 없습니다.

  - ***사용자 관리 그룹***

    관리자는 사용자에게 그룹을 생성하고 관리할 권한을 줄 것인지 선택할 수 있습니다. 또한, 언제든지 사용자 관리 그룹을 회사 관리 그룹으로 변경해 그룹을 제어할 수 있습니다.

- ***컴퓨터에서 복수 계정 사용 제한***

  관리자는 팀원들이 별도의 Dropbox 계정으로 업무용 Dropbox 계정에 연결된 컴퓨터에 접속하는 것을 차단할 수 있습니다.

- ***일시 중단된 사용자 상태***

  관리자는 사용자의 계정 액세스를 비활성화하면서 계정 내 데이터를 보존하고 관계를 공유해 회사 정보를 안전하게 보호할 수 있습니다. 비활성화된 계정은 이후 관리자가 다시 활성화하거나 삭제할 수 있습니다.

- ***사용자로 로그인***

  팀 관리자는 팀원 자격으로 계정에 로그인할 수 있습니다. 팀 관리자는이 기능을 사용해 팀원 계정에 있는 파일, 폴더, Paper 문서에 직접 액세스해 팀원들을 대신해 콘텐츠를 수정하거나 공유할 수 있고, 파일 수준 이벤트에 감사를 진행할 수 있습니다. '사용자로 로그인' 이벤트는 팀의 활동 로그에 기록되며 관리자는 팀원들에게 이 이벤트에 대한 알림 전송 여부를 결정할 수 있습니다.

- ***공유 권한***

  팀 관리자는 다음과 같은 광범위한 팀 공유 권한을 제어할 수 있습니다.

  - 팀원이 파일과 폴더를 팀 외부 사람과 공유할 수 있는 권한
  - 팀원이 팀 외부 사람 소유의 폴더를 수정할 수 있는 권한
  - 팀원이 생성한 공유 링크에 팀 외부 사람이 액세스할 수 있는 권한
  - 팀원이 파일 요청을 생성해 팀원 또는 팀 외부 사람으로부터 파일을 수집할 수 있는 권한
  - 다른 사람이 팀 소유의 파일을 보고 댓글을 달 수 있는 권한
  - 팀원이 Paper 문서와 Paper 폴더를 팀 외부와 공유할 수 있는 권한

- ***영구 삭제 권한***

  Dropbox Business 계정의 팀 관리자는 팀 관리자만이 파일과 Paper 문서를 영구적으로 삭제할 수 있도록 권한을 제한할 수 있습니다.

온보딩과 사용자 프로비전

- ***사용자 프로비전과 계정 관리 방법***
  - ***이메일 초대장***

    관리자는 Dropbox Business 관리 콘솔에 있는 도구를 사용해 이메일 초대장을 수동으로 생성할 수 있습니다.

  - ***Active Directory***

    Dropbox Business 관리자는 Dropbox의 Active Directory 커넥터 또는 외부 ID 공급업체를 통해 기존의 Active Directory에 있는 계정의 생성과 삭제 작업을 자동화할 수 있습니다. Active Directory를 통합하면 Active Directory를 사용해 구성원 자격을 관리할 수 있습니다.

  - ***SSO(Single Sign-On)***

    Dropbox Business의 경우 팀원들이 중앙 ID 공급업체 로그인을 통해 계정에 액세스하도록 설정할 수 있습니다. Dropbox의 SSO(Single Sign-On) 구축 기능은 업계 표준 SAML 2.0(Security Assertion Markup Language 2.0)을 사용합니다. 신뢰할 수 있는 ID 공급업체가 인증을 책임지고, 팀원들이 별도로 비밀번호를 관리하지 않아도 Dropbox에 액세스할 수 있어 프로비전이 훨씬 간편하고 안전해집니다. 또한,

Dropbox는 업계를 선도하는 여러 계정 관리 공급업체와 제휴해 사용자를 자동으로 프로비전/프로비전 해제하는 기능을 제공합니다. 자세한 내용은 아래의 Dropbox Business API 통합 섹션에서 확인할 수 있습니다.

- ***API***

  Dropbox Business API를 사용하면 고객이 직접 맞춤형 사용자 프로비전 솔루션과 계정 관리 솔루션을 구축할 수 있습니다. 자세한 내용은 아래의 Dropbox Business API 통합 섹션에서 확인할 수 있습니다.

- ***2단계 인증***

  Dropbox가 강력하게 권장하는 이 보안 기능은 사용자의 Dropbox 계정에 보안 계층을 한 겹 더 추가합니다. 2단계 인증이 활성화되면 Dropbox에 로그인할 때와 새로운 컴퓨터, 휴대폰, 태블릿을 Dropbox에 연결할 때 비밀번호에 더불어 별도의 6자리 보안 코드를 입력해야 합니다.

  - 관리자는 2단계 인증을 팀 전체에 적용할지, 특정한 팀원에게만 적용할지 선택할 수 있습니다.
  - 계정 관리자는 어떤 팀원이 2단계 인증을 활성화했는지 추적할 수 있습니다.
  - Dropbox의 2단계 인증 코드는 시간 기반 일회용 비밀번호(TOTP) 알고리즘 표준을 지원하는 문자메시지나 앱을 통해 전송됩니다.
  - 문자메시지나 앱으로 보안 코드가 전송되지 않을 경우, 16자리 일회용 긴급 백업 코드를 사용하거나, 보조 휴대폰 번호를 사용해 문자메시지로 백업 코드를 전송받을 수 있습니다.
  - Dropbox는 개방형 인증 표준 FIDO U2F(Universal Second Factor)도 지원합니다. 이를 통해 사용자는 6자리 코드 대신 사용자가 설정한 USB 보안 키로 인증할 수 있습니다.

- ***엔터프라이즈 설치 관리자***

  프로비전 확장이 필요한 경우, 관리자가 Windows용 엔터프라이즈 설치 관리자의 관리형 소프트웨어 솔루션과 배포 메커니즘을 통해 Dropbox 데스크톱 클라이언트를 원격으로 설치할 수 있습니다.

관리 장치와 로그인

- ***엔터프라이즈 모바일 관리(EMM)***

  Enterprise 요금제를 사용 중인 Dropbox Business 팀의 관리자는 Dropbox와 외부 EMM 공급업체를 통합해 팀원들이 모바일 장치에서 Dropbox를 사용하는 방식을 보다 강력하게 제어할 수 있습니다. 관리자는 관리 장치(회사에서 제공한 장치 또는 개인 장치)로만 Dropbox Enterprise 계정을 사용할 수 있도록 제한하고, 앱 사용 현황(남은 용량, 액세스 위치 등)을 확인하고, 분실하거나 도난당한 장치를 원격으로 삭제할 수 있습니다. Paper 모바일 앱은 EMM으로 관리할 수 없습니다.

- ***장치 승인***

  Advanced/Enterprise 요금제를 사용 중인 Dropbox Education과 Dropbox Business 팀의 관리자는 사용자당 Dropbox에 동기화할 수 있는 장치의 수를 제한하고, 장치 승인의 주체가 사용자인지 관리자인지 선택할 수 있습니다. 또한, 동기화할 수 있는 장치 수의 제한을 받지 않는 예외 사용자 목록을 만들 수도 있습니다. Paper 모바일 앱은 장치 승인에 포함되지 않습니다.

- ***2단계 인증 요건***

  관리자는 2단계 인증을 팀 전체에 적용할지, 특정한 팀원에게만 적용할지 선택할 수 있습니다. 팀 SSO 구축을 통해 다른 다중 인증 요건도 적용할 수 있습니다.

- ***비밀번호 제어***

  Education, Advanced, Enterprise 팀의 관리자는 팀원들이 강력하고 복잡한 비밀번호를 사용하도록 설정할 수 있습니다. 이 기능이 활성화되면 모든 웹 세션에서 팀원들의 계정이 로그아웃되고, 다시 로그인할 때는 새로운 비밀번호를 생성하라는 요청이 표시됩니다. 기능에 내장된 도구가 사용자가 입력한 비밀번호를 흔히 사용되는 단어, 이름, 패턴, 숫자를 수집해 놓은 데이터베이스와 비교해 비밀번호의 강도를 분석합니다. 사용자가 흔히 사용되는 비밀번호를 입력할 경우에는 더 독특하고 추측하기 어려운 비밀번호를 입력하라는 메시지가 표시됩니다. 또한, 관리자는 팀 전체의 비밀번호와 개별적인 사용자의 비밀번호를 재설정할 수 있습니다.

- ***도메인 관리***

  Dropbox는 조직이 사용자 온보딩 프로세스와 Dropbox 사용 제어 방식을 단순하게 개선해 시간을 절약할 수 있는 다양한 도구를 제공합니다.

  - ***도메인 인증***

    회사는 회사 도메인에 대한 소유권을 주장할 수 있고, 다른 도메인 관리 도구를 사용할 수 있습니다.

  - ***초대를 통한 의무 이전***

    관리자는 회사의 Dropbox 팀에 초대된 Dropbox 개인 사용자에게 팀 계정으로 이전하라고 요구하거나, 개인용 계정에서 사용 중인 이메일 주소를 변경하라고 요구할 수 있습니다.

  - ***도메인 통계***

    관리자는 회사 이메일 주소를 사용 중인 Dropbox 개인용 계정의 수 등의 주요 정보를 확인할 수 있습니다.

  - ***계정 캡처***

    관리자는 회사 이메일 주소를 사용 중인 모든 Dropbox 사용자가 회사 팀 계정에 합류하거나, 개인용 계정에서 사용 중인 이메일 주소를 변경하도록 강제할 수 있습니다.

- ***웹 세션 제어***

  관리자는 팀원들이 dropbox.com에 로그인되어 있는 시간을 제어할 수 있고, 모든 웹 세션과 유휴 상태 세션의 지속 시간을 제한할 수 있습니다. 제한 시간이 지난 세션은 자동으로 로그아웃됩니다. 또한, 관리자는 개별 사용자의 웹 세션을 추적하거나 종료할 수도 있습니다.

- ***앱 액세스***

  관리자는 사용자 계정으로의 타사 앱 액세스를 확인하고 철회할 수 있습니다.

- ***장치 연결 해제***

  사용자 계정에 연결된 컴퓨터와 모바일 장치는 관리자가 관리 콘솔에서 연결을 해제하거나, 사용자가 직접 개인 계정의 보안 설정에서 연결을 해제할 수 있습니다. 컴퓨터를 사용할 경우, 연결을 해제하면 인증 데이터가 삭제되며, 다음번에 컴퓨터가 온라인 상태가 되었을 때 파일의 로컬 사본을 삭제할 수 있는 옵션이 표시됩니다(원격 삭제 참조). 모바일 장치를 사용할 경우, 연결을 해제하면 즐겨찾기에 추가된 파일, 캐시로 저장된 데이터, 로그인 정보가 삭제됩니다. 또한, Paper 모바일 애플리케이션에 저장되어 있던 오프라인 Paper 문서가 삭제됩니다. 2단계 인증이 활성화된 경우, 장치를 다시 연결했을 때 반드시 재인증을 받아야 합니다. 또한, 사용자 계정 설정의 옵션을 사용해 장치가 연결되었을 때 자동으로 이메일 알림이 전송되도록 설정할 수 있습니다.

- ***네트워크 제어***

  Enterprise 요금제를 사용 중인 Dropbox Business 팀의 관리자는 회사 네트워크에서 Dropbox를 사용할 수 있는 계정을 Enterprise 팀 계정으로만 제한할 수 있습니다. 이 기능을 회사 네트워크의 보안 서비스 공급업체와 통합하면 특정 레지스트리 키가 있는 컴퓨터에서 승인된 계정을 제외한 모든 트래픽을 차단할 수 있습니다. 현재 Paper는 네트워크 제어 기능으로 관리할 수 없습니다.

모바일 보안

- ***지문 스캔***

  사용자는 Dropbox 모바일 앱의 잠금을 해제하는 방식으로 iOS 장치의 경우 Touch ID/Face ID, Android 장치의 경우 지문으로 잠금 해제(해당할 경우)를 활성화할 수 있습니다.

액세스 가시성

- ***기술 지원 신원 확인***

  Dropbox 지원팀이 문제를 해결하거나 계정 정보를 제공하기에 앞서 계정 관리자는 임의로 생성된 일회용 보안 코드를 제공해 본인의 신원을 확인해야 합니다. 이 PIN 코드는 관리 콘솔을 통해서만 생성할 수 있습니다.

사용자 계정 활동

모든 사용자는 다음과 같은 계정 설정 페이지에서 본인의 계정 활동에 관한 최신 정보를 확인할 수 있습니다.

- ***공유 페이지***

  이 페이지에는 현재 사용자의 Dropbox에 있는 공유 폴더와 사용자가 추가할 수 있는 공유 폴더가 표시됩니다. 사용자는 폴더와 파일의 공유를 해제하거나 공유 권한을 설정할 수 있습니다(아래 설명 참조).

- ***파일 페이지***

  이 페이지에는 사용자에게 공유된 파일과 각 파일을 통해 공유된 데이터가 표시됩니다. 사용자는 원할 경우 파일로의 액세스를 삭제할 수 있습니다. 다른 사람이 본인과 공유한 Paper 문서를 확인하려면 Paper 문서의 탐색 인터페이스에 있는 '나와 공유됨' 페이지로 이동하면 됩니다.

- ***링크 페이지***

  이 페이지에는 사용자가 생성한 모든 활성 공유 링크와 각 링크의 생성일, 다른 사람이 사용자와 공유한 모든 링크가 표시됩니다. 사용자는 링크를 비활성화하거나 권한을 변경할 수 있습니다(아래 설명 참조).

- ***이메일 알림***

  사용자는 새로운 장치나 앱이 본인의 Dropbox 계정으로 연결됐을 때 이메일 알림이 전송되도록 설정할 수 있습니다.

사용자 계정 권한

- ***연결된 장치***

  계정 보안 설정의 장치 섹션에는 사용자 계정에 연결된 모든 컴퓨터와 모바일 장치가 표시됩니다. 또한, 각 컴퓨터의 IP 주소와 국가, 최근 활동이 발생한 대략적인 시간이 표시됩니다. 사용자는 원하는 장치의 연결을 해제할 수 있고, 다음번에 컴퓨터가 온라인 상태가 됐을 때 연결된 컴퓨터의 파일을 삭제할 것인지 선택할 수 있습니다.

- ***활성화된 웹 세션***

  세션 섹션에는 현재 사용자 계정에 로그인되어 있는 모든 웹 브라우저가 표시됩니다. 또한, 각 브라우저의 IP 주소와 국가, 가장 최근 세션의 로그인 시간, 최근 활동이 발생한 대략적인 시간이 표시됩니다. 사용자는 계정 보안 설정에서 원하는 웹 세션을 원격으로 종료할 수 있습니다.

- ***연결된 앱***

  연결된 앱 섹션에는 사용자의 계정에 액세스할 수 있는 모든 타사 앱과 각 앱에 부여된 액세스 수준이 표시됩니다. 사용자는 본인의 Dropbox에 액세스할 수 있는 앱의 액세스 권한을 취소할 수 있습니다.

활동 피드

Dropbox Business의 관리자는 관리 콘솔의 활동 피드에서 파일 작업 기록을 확인할 수 있습니다. 활동 피드에는 관리자가 특정한 계정이나 파일, Paper 문서를 지정해 활동을 조사할 수 있는 유연한 필터링 옵션이 있습니다. 예를 들어, 하나의 파일 또는 Paper 문서를 지정해 이에 관한 모든 기록과 사용자 활동을 살펴보거나, 특정한 기간을 지정해 이 기간에 발생한 모든 팀 활동을 확인할 수 있습니다. 활동 피드는 CSV 형식의 다운로드 가능한 보고서로 내보낼 수 있고, 타사 파트너 솔루션을 통해 보안 관제 시스템(SIEM) 제품이나 기타 분석 도구에 직접 통합할 수도 있습니다. 활동 피드에 기록되는 활동은 다음과 같습니다.

- **파일, 폴더, 링크 공유**

  팀 외부 사람이 연관된 활동이 있을 경우 보고서에 표시됩니다.

  #### *공유 파일*

  - 팀원 또는 팀 외부 사람 추가 또는 삭제
  - 팀원 또는 팀 외부 사람의 권한 변경
  - 그룹 추가 또는 삭제
  - 사용자의 Dropbox에 공유 파일 추가
  - 파일 또는 폴더 초대를 통해 공유된 파일 콘텐츠 보기
  - 사용자의 Dropbox로 공유 콘텐츠 복사
  - 공유 콘텐츠 다운로드
  - 파일에 댓글 달기
  - 댓글 완료 또는 완료 취소
  - 댓글 삭제
  - 댓글 알림 수신 또는 수신 해제
  - 팀 소유 파일로의 초대 수락
  - 팀 소유 파일로의 액세스 요청
  - 파일 공유 해제

  #### *공유 폴더*

  - 새로운 공유 폴더 생성
  - 팀원, 팀 외부 사람, 그룹의 추가 또는 삭제
  - 사용자의 Dropbox로 공유 폴더 추가, 또는 사용자가 직접 본인의 공유 폴더 액세스 삭제
  - 링크를 통해 공유 폴더 추가
  - 팀원 또는 팀 외부 사람의 권한 변경
  - 폴더 소유권을 다른 사용자에게 이전
  - 폴더 공유 해제
  - 공유 폴더 구성원 자격 수락
  - 공유 폴더로의 액세스 요청
  - 구성원 자격을 요청한 사용자를 공유 폴더에 추가
  - 팀 외부 사람을 폴더에 추가하는 기능을 차단 또는 차단 해제
  - 폴더에 구성원을 추가할 수 있는 권한을 팀원 전체 또는 소유자에게만 허용
  - 공유 폴더로의 그룹 액세스 변경

공유 링크

- 링크의 생성 또는 삭제
- 링크의 콘텐츠를 볼 수 있는 권한을 링크를 받은 사람 누구나 또는 팀원 전용으로 설정
- 링크의 콘텐츠에 비밀번호 설정
- 링크에 만료일 설정 또는 삭제
- 링크 보기
- 링크의 콘텐츠 다운로드
- 링크의 콘텐츠를 사용자의 Dropbox로 복사
- API 앱으로 파일 링크 생성
- 팀원, 팀 외부 사람, 그룹과 링크 공유
- 팀 외부 사람의 공유 폴더 내 파일 링크 보기를 차단 또는 차단 해제
- 앨범 공유

파일 요청

- 파일 요청의 생성, 변경, 종료
- 파일 요청에 사용자 추가
- 파일 요청 기한 추가 또는 삭제
- 파일 요청 폴더 변경
- 파일 요청을 통해 파일 수신

파일 활동 개별적인 파일과 폴더에 관한 활동

- Dropbox에 파일 추가
- 폴더 생성
- 파일 보기
- 파일 수정
- 파일 다운로드
- 파일 또는 폴더 복사
- 파일 또는 폴더 이동
- 파일 또는 폴더의 이름 변경
- 파일을 이전 버전으로 되돌리기
- 파일의 변경 사항 롤백
- 삭제된 파일 복구
- 파일 또는 폴더 삭제
- 파일 또는 폴더 영구 삭제

로그인 Dropbox 로그인 성공과 실패

- 로그인 시도 성공 또는 실패
- SSO(Single Sign-On)를 통한 로그인 시도 실패 또는 오류
- EMM을 통한 로그인 시도 실패 또는 오류
- 로그아웃
- 웹 세션의 IP 주소 변경

비밀번호 비밀번호 변경 또는 2단계 인증 설정 변경(관리자는 사용자의 실제 비밀번호를 볼 수 없음)

- 비밀번호 변경 또는 재설정
- 2단계 인증의 활성화, 재설정, 비활성화
- SMS나 모바일 앱 사용을 위한 2단계 인증 설정 또는 변경
- 2단계 인증을 위한 백업 휴대폰 추가, 변경, 삭제
- 2단계 인증을 위한 보안 키 추가 또는 삭제

구성원 자격 팀 구성원 추가와 삭제

- 팀원 초대
- 팀 가입
- 팀원 삭제
- 팀원 계정 일시 중단 또는 일시 중단 해제
- 삭제된 팀원 복구
- 계정 도메인을 기준으로 팀 가입 요청
- 계정 도메인을 기준으로 팀 가입 요청 승인 또는 거절
- 기존의 도메인 계정에 도메인 초대장 발송
- 계정 캡처에 응해 팀 가입
- 계정 캡처에 응해 팀 탈퇴
- 팀원의 새로운 팀원 추천 차단 또는 차단 해제
- 새로운 팀원 추천

앱 Dropbox 계정에 타사 앱 연결

- 애플리케이션의 승인 또는 삭제
- 팀 애플리케이션의 승인 또는 삭제

장치 Dropbox 계정으로 컴퓨터 또는 모바일 장치 연결

- 장치 연결 또는 연결 해제
- 원격 삭제 기능으로 파일 전체 삭제 성공 또는 일부 파일 삭제 실패
- 데스크톱 컴퓨터 또는 모바일 장치의 IP 주소 변경

관리자 활동 관리 콘솔에서 공유 폴더 권한 등의 설정 변경

- **인증과 SSO(Single Sign-On)**
  - 팀원의 비밀번호 재설정
  - 모든 팀원의 비밀번호 재설정
  - 팀원의 2단계 인증 비활성화 차단 또는 차단 해제
  - SSO(Single Sign-On) 활성화 또는 비활성화
  - SSO(Single Sign-On)를 통한 로그인을 필수로 설정
  - SSO(Single Sign-On) URL 변경 또는 삭제
  - SSO(Single Sign-On) 인증 업데이트
  - SSO(Single Sign-On) 계정 모드 변경
- **구성원 자격**
  - 계정 도메인을 기준으로 사용자의 가입 요청 차단 또는 차단 해제
  - 팀원 자격 요청 시 자동 승인 또는 관리자 수동 승인 설정
- **팀원 계정 관리**
  - 팀원 이름 변경
  - 팀원 이메일 주소 변경
  - 관리자 상태 정보 제공 또는 삭제, 또는 관리자 역할 변경
  - 팀원으로 로그인 또는 로그아웃
  - 삭제된 팀원 계정의 콘텐츠 이전 또는 삭제
  - 삭제된 팀원 계정의 콘텐츠 영구 삭제

- **전체 공유 설정**
  - 팀원이 팀 외부 사람 소유의 공유 폴더를 추가하는 기능 차단 또는 차단 해제
  - 팀원이 팀 외부 사람과 폴더 공유하는 기능 차단 또는 차단 해제
  - 팀원이 팀 외부 사람과 폴더를 공유하기 전에 경고 메시지 전송
  - 팀 외부 사람의 공유 링크 보기 차단 또는 차단 해제
  - 공유 링크를 팀 전용으로 기본 설정
  - 파일에 댓글 달기 차단 또는 차단 해제
  - 팀원의 파일 요청 생성 차단 또는 차단 해제
  - 공유 링크 페이지의 로고 추가, 변경, 삭제
  - 팀원이 팀 외부 사람과 Paper 문서 및 Paper 폴더 공유하는 기능 차단 또는 차단 해제
- **팀 폴더 파일 관리**
  - 팀 폴더 생성
  - 팀 폴더 이름 변경
  - 팀 폴더 보관 또는 보관 취소
  - 팀 폴더 영구 삭제
  - 팀 폴더를 공유 폴더로 다운그레이드
- **도메인 관리**
  - 도메인 인증 시도, 도메인 인증 성공, 또는 도메인 삭제
  - Dropbox 지원팀의 도메인 인증 또는 삭제
  - 도메인 초대장 발송 활성화 또는 비활성화
  - '신규 사용자 자동 초대' 활성화 또는 비활성화
  - 계정 캡처 모드 변경
  - Dropbox 지원팀의 계정 캡처 허용 또는 허용 철회
- **엔터프라이즈 모바일 관리(EMM)**
  - 테스트 모드(선택 사항) 또는 배포 모드(필수 사항)에 EMM 활성화
  - EMM 토큰 새로 고침
  - EMM에서 제외된 사용자 목록으로 팀원 추가 또는 삭제
  - EMM 비활성화
  - EMM 사용 예외 목록 보고서 생성
  - EMM 모바일 앱 사용 현황 보고서 생성
- **기타 팀 설정 변경**
  - 팀 병합
  - 팀을 Dropbox Business로 업그레이드 또는 무료 버전으로 다운그레이드
  - 팀 이름 변경
  - 팀 활동 보고서 생성
  - 팀원이 컴퓨터 한 대당 한 개 이상의 계정 연결하는 기능 차단 또는 차단 해제
  - 팀원 전체 또는 관리자만 그룹 만들기 허용
  - 팀원이 파일 영구 삭제하는 기능 차단 또는 차단 해제
  - 리셀러의 Dropbox 지원 세션 시작 또는 종료

그룹 그룹 만들기, 그룹 삭제, 그룹 구성원 정보

- 그룹 생성, 이름 변경, 이동, 삭제
- 구성원 추가 또는 삭제
- 그룹 구성원의 액세스 유형 변경
- 팀 관리 또는 관리자 관리로 그룹 변경
- 그룹 외부 ID 변경

- **Paper 활동 로그**

  관리자는 활동 로그에서 Paper 활동의 유형을 선택하거나, 모든 활동이 기록된 보고서를 다운로드할 수 있습니다. 로그에 기록되는 Paper 활동은 다음과 같습니다.

  - Paper 활성화 또는 비활성화
  - Paper 문서 생성, 수정, 내보내기, 보관, 영구 삭제, 복구
  - Paper 문서에 댓글 달기 및 댓글 완료
  - 팀원과 팀 외부 사람에게 Paper 문서 공유 및 공유 해제
  - 팀원과 팀 외부 사람의 Paper 문서 액세스 요청
  - Paper 문서에서 팀원과 팀 외부 사람 멘션
  - 팀원과 팀 외부 사람의 Paper 문서 보기
  - Paper 문서 팔로우
  - Paper 문서에 대한 구성원 권한 변경(수정, 댓글, 보기 전용)
  - Paper 문서 외부 공유 정책 변경
  - Paper 폴더 생성, 보관, 영구 삭제
  - Paper 문서를 폴더에 추가 또는 폴더에서 삭제
  - Paper 폴더 이름 변경
  - Paper 문서와 폴더 이전

애플리케이션 보안

Dropbox 사용자 인터페이스

Dropbox 서비스는 다양한 인터페이스로 액세스해 사용할 수 있습니다. 각 서비스는 사용자 데이터를 처리하고 보호하면서 간편한 액세스를 제공하는 보안 설정과 기능을 갖추고 있습니다.

- ***웹***

  이 인터페이스는 모든 최신 웹 브라우저를 통해 액세스할 수 있습니다. 사용자는 웹에서 파일을 업로드하고, 다운로드하고, 보고, 공유할 수 있으며, 컴퓨터에 설치된 기본 애플리케이션으로 기존의 로컬 버전 파일을 열어볼 수 있습니다.

- ***데스크톱***

  Dropbox 데스크톱 애플리케이션은 파일을 로컬 장치에 저장해 오프라인 액세스를 제공하는 강력한 동기화 클라이언트입니다. 이 애플리케이션은 사용자에게 Dropbox 계정으로의 전체 액세스를 제공하며, Windows와 Mac 운영체제에서 지원됩니다. 파일은 운영체제의 각 파일 브라우저에서 바로 확인하고 공유할 수 있습니다.

- ***모바일***

  Dropbox 앱은 iOS, Android 장치에서 지원됩니다. 사용자는 Dropbox 앱을 통해 이동 중에도 모든 파일에 액세스하고, 오프라인으로도 파일에 액세스할 수 있습니다.

- ***API***

  Dropbox API는 맞춤형 설정을 통해 파일 검색, 수정, 복구와 같은 고급 기능에 액세스하고, Dropbox 계정에서 콘텐츠를 읽고 쓸 수 있는 기능을 제공합니다. API는 Dropbox Business 계정의 사용자 수명 주기를 관리하고, 팀원 전체에 일괄 작업을 실행하고, Dropbox Business 관리자 기능으로의 액세스를 활성화하는 데 사용할 수 있습니다.

Paper 사용자 인터페이스

Paper 서비스는 다양한 인터페이스로 액세스해 사용할 수 있습니다. 각 서비스는 사용자 데이터를 처리하고 보호하면서 간편한 액세스를 제공하는 보안 설정과 기능을 갖추고 있습니다.

- ***웹***

  이 인터페이스는 모든 최신 웹 브라우저를 통해 액세스할 수 있습니다. 사용자는 웹 인터페이스를 통해 Paper 문서를 생성하고, 보고, 수정하고, 다운로드하고, 공유할 수 있습니다.

- ***모바일***

  Paper 모바일 애플리케이션은 iOS, Android 모바일 장치와 태블릿에서 지원되어 이동 중에도 모바일 애플리케이션을 통해 모든 Paper 문서에 액세스할 수 있습니다. 모바일 애플리케이션은 자연어 코드(iOS 또는Android)가 내부의 웹 뷰 브라우저를 감싸고 있는 구조의 하이브리드 애플리케이션입니다 .

- ***API***

  위에서 설명한 Dropbox API에는 Dropbox Paper에 저장된 문서와 폴더를 관리하는 엔드포인트와 데이터 유형이 포함되어 있습니다. 여기에는 권한 관리, 압축 보관, 영구 삭제 등의 기능 지원이 포함됩니다.

암호화

전송 중 데이터

Dropbox는 데이터 전송 시 보안 소켓 계층(SSL)/전송 계층 보안(TLS) 프로토콜을 활용해 Dropbox 앱과 서버 사이에 전송되는 데이터를 보호하며, 128bit 이상의 고급 암호 표준(AES) 알고리즘으로 보호되는 보안 터널을 생성합니다. Dropbox 클라이언트(현재 기준으로 데스크톱, 모바일, API, 웹)와 호스팅된 서비스 사이에 전송되는 파일 데이터는 SSL/TLS를 통해 암호화됩니다. 마찬가지로, Paper 클라이언트(현재 기준으로 모바일, API, 웹)와 호스팅된 서비스 사이에 전송되는 Paper 문서 데이터도 SSL/TLS를 통해 암호화됩니다. 엔드포인트 보안을 위해 Dropbox는 (데스크톱, 모바일)과 최신 브라우저를 제어하며, 강력한 암호를 사용해 완전 순방향 비밀성과 인증서 피닝을 지원합니다. 또한, 인증된 모든 쿠키를 웹에서 안전한 것으로 표시하고, 활성화된 includeSubDomains로 HSTS(HTTP Strict Transport Security)를 활성화합니다.

참고: Dropbox는 취약성이 발견된 SSLv3 사용을 중단하고 TLS를 단독으로 사용합니다. TLS는 흔히 'SSL/TLS'로 통용되며, 이러한 이유로 이 백서에서는 TLS 대신 SSL/TLS라는 용어를 사용했습니다.

Dropbox의 프런트 엔드 서버 인증은 중간자 공격을 방지하기 위해 클라이언트가 소유한 공개 인증서를 통해 실행됩니다. 모든 파일과 Paper 문서는 전송되기 전에 암호화된 연결 상태로 전환되어 Dropbox의 프런트 엔드 서버로 안전하게 전송됩니다.

저장된 데이터

사용자가 업로드한 Dropbox 파일은 저장된 상태에서 256bit 고급 암호 표준(AES)을 통해 암호화됩니다. 파일은 개별적인 파일 블록으로 나뉘어 복수의 데이터 센터에 저장됩니다. 각 블록은 강력한 암호를 사용해 분리되고 저장되며, 최신 버전에서 수정된 블록만 동기화됩니다. Paper 문서 역시 저장된 상태에서 256bit 고급 암호 표준(AES)을 통해 암호화되며, 외부 시스템을 통해 복수의 가용 영역에 저장됩니다.

키 관리

Dropbox의 키 관리 인프라스트럭처는 키에 대한 직접적인 액세스를 최소한으로 제한해 운영상·기술적·절차상 보안을 유지하도록 설계되었습니다. 암호화 키 생성, 교환, 저장은 분산 처리를 위해 여러 곳에 나뉘어 저장됩니다.

- ***파일 암호화 키***

  Dropbox는 복잡성을 제거하고, 고급 제품 기능을 지원하고, 암호를 철저히 통제할 수 있도록 사용자를 대신해 파일 암호화 키를 관리하도록 설계되었습니다. 파일 암호화 키는 운영 체계 인프라스트럭처 보안 제어 장치와 보안 정책에 따라 생성되고, 저장되고, 보호됩니다.

- ***내부 SSH 키***

  운영 체계로의 액세스는 고유의 SSH 키 쌍을 가진 사람으로만 제한됩니다. 보안 정책과 절차는 SSH 키로 보호됩니다. 내부 시스템이 보안 공개 키 교환 프로세스를 관리하고, 비공개 키는 안전하게 저장됩니다. 별도의 2차 인증 요소가 없는 경우 내부 SSH 키를 사용해 운영 체계로 액세스할 수 없습니다.

- ***키 분배***

  Dropbox는 자동화된 방식으로 운영에 필요한 시스템 키를 분배하고 관리합니다.

인증서 피닝

Dropbox는 대부분의 시나리오와 구축에서 HTTP Public Key Pinning(HPKP) 사양을 지원하는 최신 브라우저와 Dropbox의 데스크톱/모바일 클라이언트에 인증서 피닝 기술을 사용합니다. 인증서 피닝은 사용자가 연결하려는 서비스가 진짜임을 확인하기 위해 시행하는 추가 점검입니다. Dropbox는 인증서 피닝을 통해 숙련된 해커가 사용자 활동을 염탐하는 다양한 경로를 방어합니다.

인증 데이터 보호

Dropbox는 일반적인 해싱을 뛰어넘는 기술로 사용자의 로그인 정보를 보호합니다. 업계의 우수 사례에 발맞춰 모든 패스워드는 임의로 생성된 고유의 일회성 솔트로 솔팅 처리되며, 반복 해싱을 사용해 계산의 속도를 늦춥니다. 이러한 방법은 무작위 대입 공격, 사전 공격, 레인보우 공격을 방어하는 데 유용합니다. Dropbox는 추가 예방을 위해 데이터베이스에서 따로 저장된 키로 해시를 암호화해 데이터베이스가 공격을 받았을 때도 비밀번호를 안전하게 보호합니다.

악성 소프트웨어 스캔

Dropbox는 악성 소프트웨어가 Dropbox의 공유 링크 기능에 침투하는 것을 방지하는 자동 스캔 시스템을 개발했습니다. 이 시스템은 Dropbox 독점 기술과 업계 표준 바이러스 탐지 엔진을 모두 사용합니다.

인프라스트럭처 보안

네트워크 보안

Dropbox는 백엔드 네트워크의 보안을 철저히 유지합니다. Dropbox의 네트워크 보안 및 감시 기술은 여러 계층의 보호와 방어를 제공하도록 설계되었습니다. Dropbox는 방화벽, 네트워크 취약성 점검, 네트워크 보안 감시, 침입 탐지 시스템 등의 업계 표준 보호 기술을 적용해 악성이 아닌 트래픽만 Dropbox의 인프라스트럭처에 접근할 수 있게 합니다.

Dropbox의 내부 비공개 네트워크는 사용 현황과 위험 수준에 따라 세그먼트화됩니다. 주요 네트워크는 다음과 같습니다.

- 인터넷 방향 DMZ
- 우선순위 인프라스트럭처 DMZ
- 운영 네트워크
- 기업 네트워크

운영 환경으로의 액세스는 승인된 IP 주소로만 제한되며, 운영 환경에 액세스하려면 모든 엔드포인트에서 다중 인증을 거쳐야 합니다. 액세스 권한을 가진 IP 주소는 기업 네트워크나 승인된 Dropbox 인력과 연결되어 있습니다. Dropbox는 이러한 IP 주소를 분기별로 검토해 운영 환경의 보안을 유지합니다. IP 주소 목록을 변경할 수 있는 사람은 승인된 인력으로만 제한됩니다.

운영 네트워크에 접근하는 인터넷 트래픽은 여러 계층의 방화벽과 프록시로 보호됩니다.

내부 Dropbox 네트워크와 공개 인터넷 간에는 엄격한 제한이 유지됩니다. 운영 네트워크를 오가는 인터넷 방향의 트래픽은 전용 프록시 서비스로 철처하게 통제되며, 방화벽 제한 규정의 보호를 받습니다.

Dropbox는 정교한 도구를 사용해 Mac, Windows 운영체제를 지원하는 노트북, 데스크톱의 악성 이벤트를 감시합니다. 보안 로그는 포렌식과 사고 대응을 위해 업계 표준 보존 정책에 따라 중앙 위치로 수집됩니다.

Dropbox는 내부 보안팀과 외부 보안 전문가를 통한 네트워크 보안 테스트와 감사를 정기적으로 시행해 위험성을 파악하고 이를 완화합니다.

인터넷 접속 거점(PoP)

Dropbox는 외부 콘텐츠 전송 네트워크(CDN)와 전 세계 31곳의 자체 운영 인터넷 접속 거점(PoP)을 사용해 웹사이트 성능을 최적화합니다. PoP에서는 그 어떤 사용자 데이터도 캐시로 저장되지 않으며 전송 중인 모든 사용자 데이터는 SSL/TLS로 암호화됩니다. Dropbox가 운영하는 PoP로의 물리적·논리적 액세스는 승인된 Dropbox 직원에게만 허용됩니다. Dropbox는 전송 계층(TCP)과 응용 계층(HTTP) 모두에서 최적화 작업을 실행합니다.

피어링(대등 접속)

Dropbox는 피어링 정책을 공개적으로 개방하며, 누구든 Dropbox와 피어링하는 것을 환영합니다. 자세한 내용은 dropbox.com/peering에서 확인할 수 있습니다.

안정성

스토리지 시스템은 신뢰할 수 있을 때만 그 가치를 발휘합니다. 이를 위해 Dropbox는 데이터 손실을 막고 가용성을 보장하는 다중 리던던시 시스템으로 설계되었습니다.

파일 메타데이터

메타데이터의 여분 사본은 최소한 N+2 방식의 가용성 모델이 적용된 데이터 센터 내부의 개별적인 장치에 분산되어 저장되며, 증분 백업은 1시간마다, 전체 백업은 3일에 1번씩 실행됩니다. 메타데이터는 미국 Dropbox가 운영하는 서버에 저장되고, 미국 Dropbox에 의해 관리됩니다.

파일 블록

파일 블록의 여분 사본은 최소 2개의 지역에 개별적으로 저장되며 각 지역에서 안전하게 복제됩니다. (참고: 독일, 호주, 일본 인프라스트럭처에 파일이 저장되도록 선택한 경우 파일 블록은 각 지역에서만 복제됩니다. 자세한 내용은 아래의 데이터 센터 및 관리 서비스 제공업체 섹션에서 확인할 수 있습니다.) Magic Pocket과 AWS는 모두 최소 99.999999999%의 연간 데이터 지속성을 제공하도록 설계되었습니다.

Dropbox는 아키텍처, 애플리케이션, 동기화 메커니즘을 결합해 사용하며 사용자 데이터를 보호하고 높은 데이터 가용성을 제공합니다. 드물기는 하지만 간혹 서비스 사용이 불가능한 상황이 발생하더라도 사용자는 연결된 컴퓨터의 로컬 Dropbox 폴더에 동기화되어 있는 파일의 최신 사본에 액세스할 수 있습니다. Dropbox 데스크톱 클라이언트/로컬 폴더에 동기화된 파일 사본은 다운 타임, 운영 중단, 오프라인 시에도 하드 드라이브를 통해 액세스할 수 있습니다. 그사이 변경된 파일과 폴더는 서비스 또는 연결이 복원되는 즉시 Dropbox에 동기화됩니다.

Paper 문서

Paper 문서 데이터의 여분 사본은 N+1 방식의 가용성 모델이 적용된 데이터 센터 내부의 개별적인 장치에 분산되어 저장되며, 매일 Paper 문서 데이터의 전체 백업이 실행됩니다. Dropbox는 Paper 문서 저장소로 최소 99.999999999%의 연간 데이터 지속성을 유지하도록 설계된 미국 내 AWS 인프라스트럭처를 사용합니다. 드물기는 하지만 간혹 서비스 사용이 불가능한 상황이 발생하더라도 사용자는 모바일 애플리케이션에서 가장 최근에 동기화된 Paper 문서의 사본에 '오프라인' 모드로 액세스할 수 있습니다.

파일 동기화

Dropbox는 업계가 인정하는 동종 최고의 파일 동기화 기능을 제공합니다. Dropbox의 동기화 메커니즘은 파일의 빠르고 즉각적인 전송을 보장하며, 어디서나 다양한 장치로 데이터에 액세스할 수 있도록 합니다. Dropbox 동기화 기능은 회복력도 뛰어납니다. Dropbox 서비스로의 연결이 끊긴 경우, 클라이언트는 연결이 복구된 후 파일 전송을 자동으로 재개합니다. 파일은 동기화가 완료되거나 Dropbox 서비스의 인증을 받은 경우에만 로컬 클라이언트에 업데이트됩니다. 데이터가 복수의 서버에 분산되어 저장되기 때문에 가외성이 보장되며 최종 사용자는 일관성 있는 동기화 기능을 경험할 수 있습니다.

델타 동기화

델타 동기화를 사용하면 파일에서 변경된 부분만 다운로드/업로드됩니다. Dropbox는 업로드된 파일을 각각 암호화된 블록에 개별적으로 저장하고, 변경된 블록만 업데이트합니다.

스트리밍 동기화

스트리밍 동기화는 파일 완전히 업로드될 때까지 기다리지 않고 첫 번째 장치에서 모든 블록이 업로드되기 전에 두 번째 장치에 동기화된 블록의 다운로드를 시작합니다. 이 동기화 방식은 동일한 Dropbox 계정에 컴퓨터 여러 대가 연결되어 있거나, 여러 개의 계정이 하나의 폴더를 공유할 때 자동으로 적용됩니다.

스마트 동기화

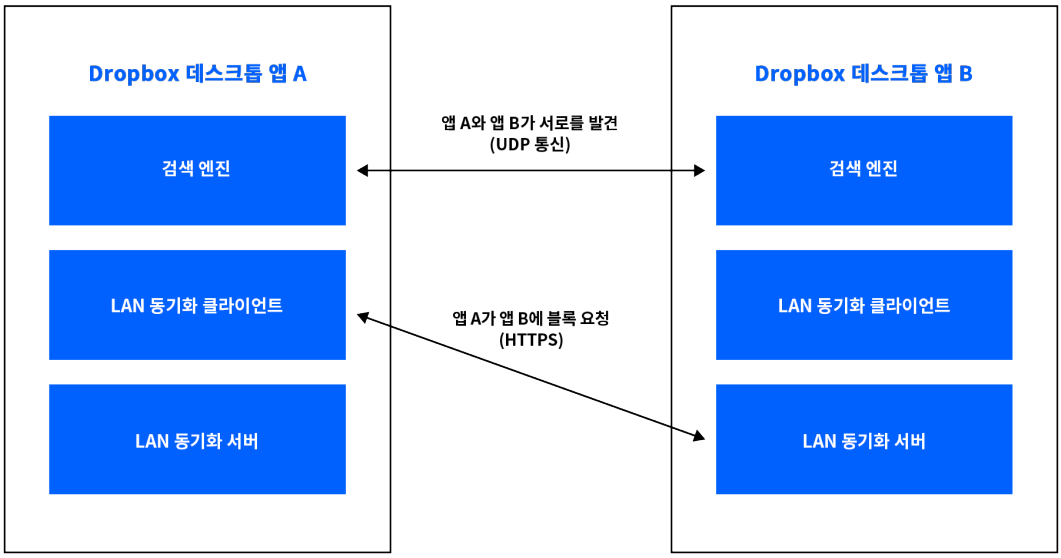
스마트 동기화는 사용자가 원하는 파일만 하드 드라이브로 동기화해 컴퓨터의 저장 용량을 확보할 수 있는 기능입니다. 스마트 동기화는 로컬 하드 드라이브에 있는 파일과 폴더를 클라우드로 옮겨 컴퓨터 용량을 확보하고, 모든 콘텐츠를 사용자의 dropbox.com 계정과 연결된 클라우드에 보관합니다. 또한, 일정 기간 동안 액세스하지 않은 파일과 폴더를 자동으로 사용자의 하드 드라이브에서 클라우드로 옮겨 저장 용량을 추가로 확보합니다.

LAN 동기화

LAN 동기화가 활성화되면 동일한 근거리 통신망(LAN)에 연결된 다른 컴퓨터에서 새로운 파일과 업데이트된 파일의 다운로드가 시작되어 Dropbox 서버에서 파일을 다운로드할 때보다 시간과 대역폭이 절약됩니다.

아키텍처

데스크톱 앱에서 실행되는 LAN 동기화 시스템은 세 가지 주요 요소(검색 엔진, 서버, 클라이언트)로 구성되어 있습니다. 검색 엔진은 네트워크에서 동기화할 컴퓨터를 찾는 역할을 하며, 이때 동기화할 수 있는 컴퓨터는 동일한 Dropbox 개인/공유 폴더로 액세스가 허용된 컴퓨터로만 제한됩니다. 서버는 네트워크에 있는 다른 컴퓨터가 보낸 요청을 처리해 요청된 파일 블록을 제공하고, 클라이언트는 네트워크에 파일 블록을 요청합니다.



검색 엔진

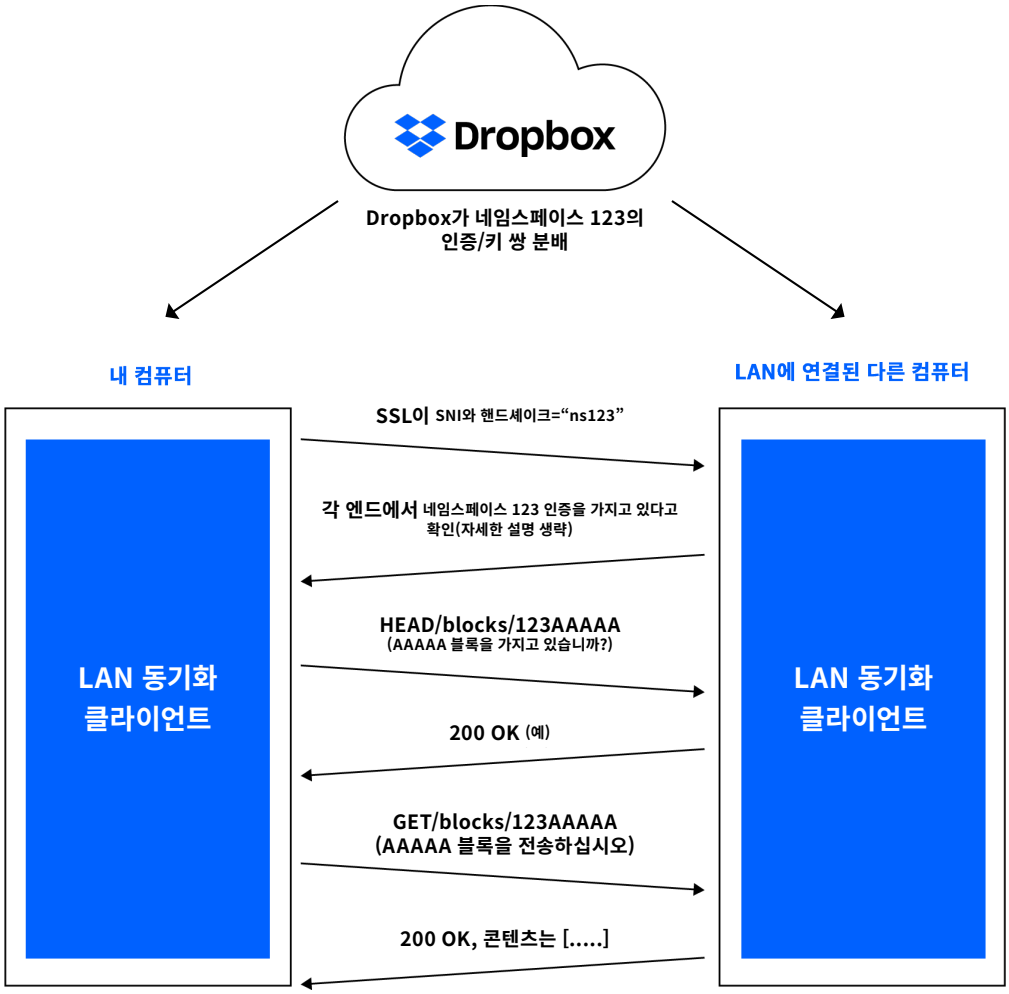
LAN에 연결된 각 컴퓨터는 인터넷 할당 번호 관리 기관(IANA)이 LAN 동기화 전용으로 지정한 17500번 포트를 통해 주기적으로 UDP 동보 패킷을 송수신합니다. 동보 패킷에는 컴퓨터에 사용된 프로토콜 버전, 지원되는 Dropbox 개인/공유 폴더, 서버 운영에 사용되는 TCP 포트(이 포트가 지원되지 않을 경우 포트 번호가 17500이 아닐 수 있음), 컴퓨터 임의 식별자가 포함되어 있습니다. 패킷이 감지되면 각각의 개인/공유 폴더 목록에 컴퓨터 IP 주소가 추가되며 잠재적인 타깃이 됩니다.

프로토콜

실질적인 파일 블록은 HTTPS를 통해 전송됩니다. 각 컴퓨터는 엔드포인트로 HTTPS 서버를 작동합니다. 클라이언트는 복수의 피어를 폴링해 파일 블록의 유무를 확인한 후 1개의 서버에서만 블록을 다운로드합니다.

Dropbox는 모든 데이터를 안전하게 보관하기 위해 폴더의 인증을 받은 클라이언트만 파일 블록을 요청할 수 있게 하고, 컴퓨터가 제어할 수 없는 폴더의 서버 행세를 할 수 없게 합니다. 이를 위해 Dropbox는 모든 개인/공유 폴더에 SSL 키-인증 쌍을 생성합니다. 이 키-인증 쌍은 Dropbox의 서버에서 폴더의 인증을 받은 사용자의 컴퓨터로 분산되고, 공유 폴더에서 누군가가 삭제된 경우와 같이 구성원 자격이 변경될 때마다 순환됩니다. Dropbox는 HTTPS에 연결된 양쪽 엔드 모두 동일한 인증서(Dropbox 또는 공유 폴더의 인증서)의 인증을 받도록 해 연결의 양쪽 엔드 모두 인증을 받았음을 확인합니다.

Dropbox는 HTTPS에 연결할 때 서버 이름 표시(SNI)를 사용해 서버에 어떤 개인용 Dropbox 또는 폴더가 연결을 시도 중인지 알려줍니다. 서버는 이 정보를 통해 어떤 인증서를 사용할 것인지 결정합니다.



서버/클라이언트

위에 설명된 프로토콜처럼 서버에 필요한 정보는 현재 존재하는 블록과, 블록을 찾을 수 있는 위치뿐입니다.

클라이언트는 검색 엔진의 검색 결과를 토대로 각 Dropbox 개인/공유 폴더의 피어 목록을 보관합니다. LAN 동기화 시스템이 파일 블록 다운로드 요청을 받으면 시스템은 해당 Dropbox 개인/공유 폴더에서 찾은 피어 목록 중 임의의 피어 샘플에 요청을 전송하며, 블록을 보유하고 있다고 응답한 피어 중 가장 먼저 응답한 피어에 블록을 요청합니다.

Dropbox는 속도 지연을 최소화하기 위해 연결 풀에서 이미 시작된 연결을 재사용합니다. 필요할 때까지는 연결을 열지 않고, 연결을 연 후에는 다시 필요한 경우를 대비해 연결 상태를 유지합니다. 또한, 피어마다 연결 수를 제한합니다.

파일 블록을 찾지 못한 경우나 다운로드에 실패한 경우, 연결이 너무 느린 경우에는 블록을 Dropbox 서버에서 다운로드합니다.

데이터 센터와 관리 서비스 제공업체

Dropbox의 기업 체계와 운영 체계는 미국 여러 지역에 위치한 외부 하청 서비스 업체 데이터 센터와 관리 서비스 제공업체에 보관되어 있습니다. 보안 제어를 위해 하청 서비스 업체 데이터 센터의 SOC 보고서와 공급업체 보안 설문지, 계약상 의무는 최소한 일 년에 한 번씩 검토됩니다. 이러한 외부 서비스 제공업체는 Dropbox 인프라스트럭처가 제어할 수 없는 영역의 물리적, 환경적, 운영상 보안 제어를 담당합니다. Dropbox는 외부 데이터 센터에 보관된 Dropbox 인프라스트럭처의 논리적 보안, 네트워크 보안, 애플리케이션 보안을 담당합니다.

Dropbox의 데이터를 처리하고 저장하는 관리 서비스 제공업체 Amazon Web Services(AWS)는 자체 인프라스트럭처를 통해 제공된 Dropbox 서비스의 논리적 보안과 네트워크 보안을 담당합니다. 연결은 AWS의 디폴트 전체 차단 모드로 설정된 방화벽에 의해 보호되며, Dropbox는 제한된 수의 IP 주소와 직원들에게만 보안 환경으로의 액세스를 허용합니다.

독일, 호주, 일본, 영국 내 인프라스트럭처

Dropbox는 일정한 자격을 갖춘 고객에게 미국 이외 지역에 위치한 파일 블록 스토리지를 제공합니다. Dropbox의 인프라스트럭처는 독일, 호주, 일본, 영국에 위치한 Amazon Web Services(AWS)에 의해 운영되며, 각 지역에서 복제되어 리던던시를 보장하고 데이터 손실을 방지합니다. 파일 메타데이터는 미국 내 Dropbox 전용 서버에 저장됩니다. 현재 모든 고객의 Paper 문서와 미리 보기는 미국에 저장되어 있습니다.

사고 대응

Dropbox는 서비스 가용성, 무결성, 보안, 개인정보 보호, 기밀성과 관련된 문제에 대응하기 위한 사고 대응 정책과 절차를 갖추고 있습니다. 사고 대응 절차의 일환으로 사고 대응 전담팀은 다음과 같은 교육을 받습니다.

- 잠재적 사고 알림에 신속하게 대응
- 사고의 심각도 결정
- 필요한 경우 완화 조치와 억제 조치 실행
- 관련된 내외부 이해 당사자에게 연락(피해를 입은 고객에게 통보해 위반 또는 사고 알림에 관한 계약상 의무를 이행하고, 관련된 법과 규정 준수하기 위한 목적)
- 조사를 위해 관련 증거를 수집하고 보존
- 사고 후 결과를 기록하고 영구적인 데이터 분류 계획 구축

Dropbox는 SOC 2+, ISO/IEC 27001, 기타 보안 평가의 일환으로 사고 대응 정책과 프로세스에 대한 감사를 실행합니다.

업무 연속성

Dropbox는 비즈니스 운영에 필수적인 프로세스와 활동에 지장이 생겼을 때 사용자에게 서비스를 지속적으로 제공하거나, 서비스를 재개하고, 기업으로서 어떻게 기능해야 하는지 대처하기 위해 업무 연속성 관리 체계(BCMS)를 구축해 놓았습니다. Dropbox는 다음 단계에 따라 순환 프로세스를 실행합니다.

- ***비즈니스 영향과 위험성 평가***

  Dropbox는 최소한 일 년에 한 번씩 비즈니스 영향 평가(BIA)를 실시해 Dropbox 운영에 필수적인 프로세스를 파악하고, 운영에 지장이 생겼을 때 잠재적인 영향을 평가하며, 복구를 위해 우선적으로 처리해야 할 업무를 시간별로 계획하고, 주요 종속성과 공급업체를 식별합니다. 또한, 최소한 일 년에 한 번씩 기업 전반에 걸쳐 위험성 평가를 시행합니다. 위험성 평가는 Dropbox 운영에 지장을 주는 사고의 위험성을 체계적으로 파악하고, 분석하고, 평가하도록 도와줍니다. BIA와 위험성 평가는 업무 연속성 계획(BCP)에 필요한 완화 및 복구 전략과 업무 연속성 활동의 우선순위 파악에 중요한 요소로 활용됩니다.

- ***업무 연속성 계획***

  BIA에서 Dropbox의 업무 연속성에 꼭 필요하다고 파악된 팀은 이 정보를 활용해 팀의 주요 프로세스에 필요한 BCP를 개발합니다. 이러한 계획을 통해 팀은 응급상황 발생 시 프로세스를 재개하는 사람이 누구인지, 운영이 중단된 상황에서 다른 지점 누구에게 팀의 프로세스를 인계해야 하는지, 어떤 방법으로 연락할 것인지 알 수 있습니다. 또한, BCP는 계획을 실행해야 하는 경우와 그 방법, 연락처, 회의 정보, 주요 앱, 복구 전략 등의 복구 계획과 기타 주요 정보를 중앙 집중화해 사고 발생에 대응할 수 있도록 도와줍니다. Dropbox의 연속성 계획은 Dropbox 위기관리팀과 사고대응팀이 수립한 위기관리 계획(CMP)과 연계되어 있습니다.

- ***계획의 테스트와 실행***

  Dropbox는 업무 연속성 계획 중 일부 요소를 선별해 최소한 일 년에 한 번씩 테스트를 시행합니다. 이러한 테스트는 BCMS의 범위 및 목표와 맥락을 같이하고, 적절한 시나리오를 바탕으로 하며, 명확하게 규정된 목표를 토대로 정교하게 설계됩니다. 테스트의 범위는 모의 훈련에서부터 실제 사고를 재현한 대규모 시뮬레이션까지 다양합니다. 팀은 테스트 결과와 실제 사고에 대한 경험을 바탕으로 계획을 수정하고 개선해 문제 해결 능력과 대응력을 강화합니다.

- ***BCMS의 검토와 승인***

  Dropbox 경영진은 Dropbox 신뢰 프로그램 점검의 일환으로 최소한 일 년에 한 번씩 BCMS를 검토합니다.

재해 복구

Dropbox는 Dropbox Business의 운영에 영향을 미치는 중대한 위기나 재해가 발생할 경우 정보 보안 요건에 대처할 수 있도록 재해 복구 계획을 수립해 놓았습니다. Dropbox 신뢰팀이 매년 이 계획을 검토하며, 최소한 일 년에 한 번씩 선별된 요소를 테스트합니다. 검토와 테스트를 통해 발견된 결과는 문서로 기록하고, 문제가 해결될 때까지 추적합니다.

Dropbox의 재해 복구 계획(DRP)은 재해의 내구성과 가용성을 다룹니다. 내구성과 가용성은 다음과 같이 분류할 수 있습니다.

- **내구성 재해: 다음 항목 중 1개 이상 발생 시**
  - 메타데이터가 저장된 핵심 데이터 센터 또는 파일 블록이 저장된 복수의 데이터 센터의 완전하거나 영구적인 상실
  - 메타데이터가 저장된 핵심 데이터 센터 또는 파일 콘텐츠가 저장된 복수의 데이터 센터에 보관된 데이터와의 통신 또는 처리 능력 상실
- **가용성 재해: 다음 항목 중 1개 이상 발생 시**
  - 10일 이상 지속된 운영 중단
  - 메타데이터가 저장된 스토리지 서비스/데이터 센터 또는 파일 블록이 저장된 복수의 스토리지 서비스/데이터 센터에 보관된 데이터와의 통신 또는 처리 능력 상실

Dropbox는 복구 목표 시간(RTO: 재해 발생 후 비즈니스 프로세스 또는 서비스를 복구하는 데 허용된 시간 및 서비스 수준)과 복구 목표 시점(RPO: 서비스 중단으로 손실된 데이터를 복구하는 데 허용된 최대 시간)을 분명하게 규정하고 있습니다. 또한, 최소한 일 년에 한 번씩 재해 복구 테스트를 시행해 실제 복구 시간(RTA)을 측정합니다.

Dropbox의 사고 대응, 업무 연속성, 재해 복구 계획에 대한 테스트는 정기적으로 시행되며, 중대한 조직상·환경적 변화가 생겼을 때도 시행됩니다.

내부 보안 사례

Dropbox는 정보 보안 관리 체계를 수립해 Dropbox가 신뢰를 유지하는 목적과 방향, 원칙, 기본 규정을 명시해 놓고, Dropbox Business 시스템의 보안, 기밀성, 무결성, 가용성, 개인정보 보호를 지속적으로 개선하고 위험성을 평가하며 이를 유지합니다. Dropbox는 정기적으로 보안 정책을 검토해 업데이트하고, 보안 교육을 제공하며, 모의 해킹을 비롯한 애플리케이션 테스트와 네트워크 보안 테스트를 시행합니다. 또한, 보안 정책 준수 현황을 감시하고, 내외부적으로 위험성 평가를 시행합니다.

Dropbox의 정책

Dropbox는 상세한 보안 정책을 수립해 Dropbox 보안팀의 주도하에 정책을 실행합니다. 모든 보안 정책은 최소한 일 년에 한 번씩 검토를 거쳐 승인됩니다. 모든 직원과 인턴, 협력업체는 업무를 시작하기에 앞서 필수 보안 교육을 받아야 하고, 정기적으로 보안 인식 교육을 받습니다.

- ***정보 보안***

  사용자와 Dropbox의 정보를 안전하게 보관
- ***인증***

  Dropbox 직원들이 정보 체계와 데이터에 액세스하기 위해 인증을 거치는 방식 설명
- ***장치 보안***

  회사 정보에 액세스하는 데 사용된 모바일 장치에 관한 최소한의 보안 요건
- ***논리적 액세스 제어***

  Dropbox 시스템, 사용자, 정보로의 액세스를 안전하게 유지. 기업 환경과 운영 환경으로의 액세스 제어 설명
- ***데이터 보안***

  Dropbox가 특정한 저장, 액세스, 사용 요건을 통해 데이터를 보호하는 방식 설명
- ***출장 보안***

  Dropbox 직원들이 해외로 출장을 가기 전에 취해야 할 조치 설명
- ***영업과 고객 경험(CX) 보안 지침***

  사용자 정보를 안전하게 유지하고, 직원들을 보호하고, 사용자에게 지원 제공
- ***물리적 보안***

  Dropbox의 인력과 시설 보호를 위한 안전한 환경 유지
- ***운영에 관한 물리적 보안 지침***

  운영 시설로의 물리적 액세스 관리
- ***사고 대응***

  여러 가지 유형의 사고 발생 시 Dropbox가 보안, 개인정보 보호, 사이트 이벤트, 문서 사고 대응 계획을 처리하는 방식 설명
- ***승인되지 않은 저작권 자료***

  직원들이 승인되지 않은 콘텐츠를 저장하거나 공유할 때 Dropbox 또는 Dropbox 시스템을 사용하는 것을 금지

- ***변경 사항 관리***

  운영 체계의 변경 사항 관리 운영 체계에 액세스할 수 있는 모든 Dropbox 직원, 협력업체, 인턴에 적용
- ***사용자 개인정보 보호***

  개인정보처리방침에 따라 Dropbox에서 사용자 정보와 사용자 데이터를 보호하고 처리
- ***업무 연속성 정책과 비상 상황 관리***

  인력(Dropbox 직원), 시설, 프로세스(업무 프로세스)의 보존과 보호, 안전
- ***Dropbox 개인정보 보호 프로그램***

  Dropbox 개인정보 보호 프로그램의 목적, 원칙, 책임
- ***Dropbox 신뢰 프로그램***

  Dropbox의 운영 방식과 Dropbox를 신뢰할 수 있는 이유 설명
- ***결제 환경 보안***

  Dropbox에서 신용카드 결제를 승인하는 데 사용되는 전용 결제 환경의 보안과 관리

직원 정책과 액세스

Dropbox의 직원은 입사 시 신원 조사를 받고, 보안 정책 확인서와 비밀 유지 서약서에 서명하고, 보안 교육을 받아야 합니다. 직무상 책임에 규정된 바에 따라 이러한 절차를 완료한 직원만이 기업 및 배포 환경에 대한 물리적·논리적 액세스를 제공받을 수 있습니다. 또한, 모든 직원은 의무적으로 연례 보안 교육을 받아야 하며, 정보성 이메일과 강연, 프레젠테이션, 인트라넷에 있는 자료를 통해 주기적으로 보안 인식 교육을 받습니다.

직원들의 Dropbox 환경 액세스는 중앙 디렉터리에서 관리되며, 강력한 암호와 패스프레이즈 암호가 설정된 SSH 키, 2단계 인증, OTP 토큰을 거쳐 인증됩니다. 원격으로 액세스하려면 2단계 인증이 설정된 VPN을 사용해야 하고, 모든 특별 액세스는 보안팀의 검토와 심사를 거칩니다.

기업 네트워크와 운영 네트워크로의 액세스는 규정된 정책에 따라 엄격하게 제한됩니다. 예를 들어, 운영 네트워크로의 액세스는 SSH 키를 통해 인증되며, 업무의 일환으로 액세스가 필요한 엔지니어링팀만 여기에 액세스할 수 있습니다. 방화벽 환경 설정에는 소수의 관리자만이 액세스할 수 있고, 이 소수의 관리자에 의해 철저하게 관리됩니다.

또한, Dropbox의 내부 정책에 따라 운영 환경과 기업 환경에 액세스하는 직원은 SSH 비공개 키를 생성하고 저장할 때 우수 사례를 준수해야 합니다.

데이터 센터, 서버 환경 설정 지원 프로그램, 운영 서버, 소스 코드 개발 지원 프로그램과 같은 기타 자료에 액세스하려면 담당 경영진의 명시적인 승인을 받아야 합니다. 경영진은 액세스 요청, 정당한 요청 사유, 승인을 기록으로 남기며, 이 기록에 액세스하려면 관련 담당자의 승인을 받아야 합니다.

Dropbox는 기술적 액세스 제어와 내부 정책을 통해 직원들이 임의로 사용자 파일에 액세스하는 것을 금지하고, 사용자 계정에 관한 메타데이터와 기타 정보에 액세스하는 것을 제한합니다. 사용자의 개인정보 보호와 보안을 위해 사용자 파일이 저장된 환경으로의 액세스는 Dropbox의 핵심 서비스를 개발하는 소수의 엔지니어에게만 허용되며, 퇴사한 직원의 액세스는 즉시 삭제됩니다.

Dropbox는 고객 인프라스트럭처의 연장선상과도 같습니다. Dropbox를 책임감 있는 데이터 관리자로 생각하고 안심하고 사용하세요. 자세한 내용은 아래의 개인정보 보호 섹션에서 확인할 수 있습니다.

취약성 관리

Dropbox의 보안팀은 정기적으로 자동/수동 애플리케이션 보안 테스트와 패치 관리를 시행하며, 외부 전문가들과 협력해 잠재적인 보안상 취약점과 버그를 식별하고 완화합니다.

Dropbox 정보 보안 관리 시스템의 필수 요소로서 모든 평가 결과와 권고 사항을 Dropbox 경영진에게 보고하며, 경영진의 평가를 거쳐 필요하다고 판단될 경우 적절한 조치를 취합니다. 심각한 수준의 문제는 담당 보안 엔지니어가 문서로 남기고, 추적하고, 해결합니다.

변경 관리

모든 개발, 문제 완화, 패치 프로세스는 Dropbox 엔지니어링팀이 수립한 공식적인 변경 관리 정책을 따르며, 이 정책에 따라 시스템 변경 사항은 승인을 받은 후에야 운영 환경에 배포될 수 있습니다. 소스 코드 변경은 Dropbox 애플리케이션 또는 서비스를 개선하고자 하는 개발자들이 주도합니다. 변경 사항은 버전 관리 시스템에 저장되고, 자동화된 품질 관리(QA) 테스트를 거쳐 보안 요건 충족 여부를 확인합니다. QA 절차가 성공적으로 완료되면 변경 사항을 적용하는 단계로 넘어가며, QA를 통과한 변경 사항은 자동으로 운영 환경에 적용됩니다. 개발자는 Dropbox의 소프트웨어 개발 수명 주기(SDLC)에 따라 안전한 코딩 지침을 준수하고, Dropbox의 QA와 수동 검토 프로세스를 통해 코드 변경 사항에 잠재적인 보안 문제가 내포되어 있는지 점검해야 합니다.

운영 환경에 적용된 변경 사항은 문서로 기록되고 보관됩니다. 또한, Dropbox 엔지니어링팀 임원들에게 자동으로 알림이 전송됩니다.

Dropbox 인프라스트럭처를 변경할 수 있는 권한은 승인된 직원에게만 주어집니다. Dropbox 보안팀은 인프라스트럭처의 보안을 유지하고, 서버와 방화벽, 기타 보안 관련 설정을 업계 표준에 따라 최신으로 유지하는 역할을 합니다. 방화벽 규정과 운영 서버에 액세스할 수 있는 직원은 정기적으로 심사를 거칩니다.

스캔과 보안 모의 해킹(내부 및 외부)

Dropbox의 보안팀은 정기적으로 자동·수동 애플리케이션 보안 테스트를 실시해 Dropbox 데스크톱, 웹(Dropbox와 Paper), 모바일(Dropbox와 Paper) 애플리케이션의 잠재적인 보안상 취약점과 버그를 식별하고 보완합니다.

또한, 외부 공급업체와 계약을 맺고 기업 환경과 운영 환경에 대한 보안 모의 해킹과 취약성 테스트를 주기적으로 시행합니다. Dropbox는 애플리케이션의 안전한 보호를 위해 외부 전문가, 기타 업계 보안팀, 보안 연구 커뮤니티와 협력합니다.

또한, Dropbox는 자동 분석 시스템을 활용해 취약성을 식별합니다. 이 프로세스에는 자체적으로 개발한 시스템과 Dropbox가 필요에 따라 수정하는 오픈 소스 시스템, 지속적인 자동 분석을 위해 고용한 외부 공급업체가 포함됩니다.

유해 콘텐츠 차단

Dropbox는 Dropbox에서 유해한 콘텐츠를 저장하고 공유하는 것을 방지하는 스캔 기능을 갖추고 있습니다. 이 스캔 기능은 자체 기술에 Microsoft, Google과 같은 파트너의 첨단 기술을 결합해 Dropbox를 고객이 안심하고 사용할 수 있는 공간으로 만듭니다.

버그 포상금

Dropbox는 전문 기업과 협력해 모의 해킹을 시행하고, 자체적으로 내부 테스트를 시행하는 것에 더불어

광범위한 보안 커뮤니티의 전문 지식을 활용하는 버그 포상금 프로그램(또는 보안 취약점 보상 프로그램)을 진행하고 있습니다. Dropbox의 버그 포상금 프로그램은 소프트웨어의 버그를 발견해 신고한 사람에게 포상금을 제공합니다. 이러한 외부 커뮤니티의 참여는 Dropbox 보안팀에 Dropbox 애플리케이션에 대한 독립적인 조사 결과를 제공한다는 점에서 사용자를 안전하게 보호하는 데 도움이 됩니다. Dropbox는 포상금뿐만 아니라 대응 시간과 문제 완화 속도에서도 업계 최고가 되기 위해 노력하고 있습니다.

Dropbox는 보안상 취약점의 발견과 신고를 촉진하고 사용자 보안을 향상하는 책임감 있는 공개 정책을 실행하는 것에 더불어 적격한 신고 요건과 적용되는 Dropbox 애플리케이션의 범위를 규정해 놓았습니다. 이 정책에는 다음과 같은 지침이 포함됩니다.

- Dropbox에 보안 문제를 상세하게 전달해야 합니다.
- Dropbox의 기존 애플리케이션을 존중해야 합니다. 자동화된 취약성 스캐너를 사용해 무작위로 양식을 전송하는 것은 프로그램의 범위를 명백하게 벗어나는 행위로, 이 경우 어떠한 포상금이나 보상도 받을 수 없습니다.
- 보안 문제를 대중에 공개하기 전에 Dropbox에 충분한 대응 시간을 제공해야 합니다.
- 계정 소유자의 승인 없이 사용자 데이터에 액세스하거나 데이터를 변경하면 안 됩니다.
- 데이터를 보거나, 변경하거나, 저장하거나, 전송하거나, 그 외 다른 방식으로 액세스해서는 안 되며, 취약성을 Dropbox에 신고하는 즉시 로컬 장치에 저장된 모든 정보를 삭제해야 합니다.
- 개인정보를 침해하거나, 데이터를 파기하거나, Dropbox 서비스를 방해하거나 폄하하려는 의도가 아니라 선의를 가진 행동이어야 합니다(서비스 거부 포함).

보안 관련 문제는 HackerOne(hackerone.com/dropbox)에서 신고할 수 있습니다.

물리적 보안

인프라스트럭처

운영 체계가 위치한 하청 서비스 업체 시설로의 물리적 액세스는 직무상 역할 수행에 필요해 Dropbox로부터 승인을 받은 인력으로만 제한됩니다. 운영 환경 시설로의 추가적인 액세스가 필요한 사람은 담당 경영진의 명시적인 승인을 받아야 합니다.

경영진은 액세스 요청, 정당한 요청 사유, 승인을 기록으로 남기며, 이 기록에 액세스하려면 관련 담당자의 승인을 받아야 합니다. 승인을 받은 후에는 권한이 있는 인프라스트럭처팀 직원이 해당 하청 서비스 업체에 연락해 승인된 직원의 액세스를 요청합니다. 하청 서비스 업체는 사용자 정보를 자체 시스템에 입력한 후 승인된 Dropbox 직원에게 배지 액세스와 가능한 경우 생채 인증 액세스를 제공합니다. 액세스 승인이 완료된 후 운영 환경으로의 액세스를 승인된 사람들로만 제한하는 것에 대한 책임은 데이터 센터에 있습니다.

기업 사무실

- ***물리적 보안***

  물리적 보안 정책을 집행하고 Dropbox 사무실의 보안을 감독하는 역할은 Dropbox의 물리적 보안팀이 담당합니다.

- ***방문자 및 액세스 정책***

  공공 출입구와 로비 이외의 기업 시설에 대한 물리적 액세스는 승인된 Dropbox 직원, Dropbox 직원과 동행하는 등록 방문객으로만 제한됩니다. Dropbox는 배지 액세스 시스템을 통해 승인된 사람만 기업 시설 내 제한 구역에 액세스하도록 허용하고 있습니다.

- ***서버 액세스***

  기업 서버와 네트워크 장치가 있는 구역으로의 액세스는 배지 액세스 시스템을 통해 상급자가 승인한 직원으로만 제한됩니다. 기업 환경과 운영 환경으로의 물리적 액세스를 승인받은 직원의 목록은 최소한 분기별로 한 번씩 점검을 거칩니다.

개인정보 보호와 투명성

많은 개인과 조직이 매일 Dropbox를 사용해 중요한 업무를 처리합니다. 그리고 이러한 정보를 보호하고 비공개로 유지하는 것은 Dropbox의 책임입니다.

개인정보처리방침

Dropbox의 개인정보처리방침은 dropbox.com/privacy에서 확인할 수 있습니다. Dropbox의 개인정보처리방침, Business 계약, 서비스 약관, 사용 제한 정책에는 다음과 같은 약관이 명시되어 있습니다.

- 수집하는 데이터의 유형과 데이터 수집의 목적
- 정보 공유 대상
- 데이터 보호 방식과 데이터 보존 기간
- 데이터를 저장하고 전송하는 위치
- 정책 변경 또는 고객 문의 절차

투명성

Dropbox는 사용자 정보에 관한 법률 집행 요청과 이와 유사한 성격의 모든 요청을 처리하는 데 있어 투명성을 유지할 것을 약속합니다. Dropbox는 모든 데이터 요청을 면밀히 검토해 이러한 요청이 적법한 것인지 확인하며, 법이 허용하는 한 법률 집행 요청에 포함된 계정의 소유주에게 이 사실을 통보할 것입니다.

이러한 노력은 사용자의 개인정보와 데이터를 보호하겠다는 Dropbox의 헌신을 반영합니다. 이를 위해 Dropbox는 정부의 정보 요청에 대한 원칙을 수립해 놓았고, 투명성 보고서를 꾸준하게 관리하고 있습니다. 다음의 원칙은 정부로부터 정보 요청을 받았을 때, 이를 검토할 때, 이에 대응할 때 Dropbox가 따라야 할 행동을 규정합니다.

- ***투명성 유지***

  Dropbox는 온라인 서비스가 정부의 개인정보 요청 횟수와 유형을 공개하는 것이 허용되어야 한다고 생각하며, 정보 요청 대상에게 이 사실을 통보하는 것이 옳다고 생각합니다. 이러한 투명성은 정부의 과도한 요청 사례와 패턴을 알려 사용자에게 더 많은 권한을 부여하기 위한 것입니다. Dropbox는 계속해서 이러한 요청에 관한 자세한 정보를 공개할 것이고, 이 중요한 정보를 더 자세하게 제공할 권리를 지지할 것입니다.

- ***광범위한 요청 거부***

  정부의 개인정보 요청은 특정한 인물과 적법한 조사로 제한되어야 합니다. Dropbox는 지나치게 광범위하고 포괄적인 요청을 거절할 것입니다.

- ***모든 사용자 보호***

  거주지나 국적에 따라 다른 수준의 보호를 제공하는 법은 낡은 법이며, 전 세계에 적용되는 온라인 서비스의 본질을 반영하지 못합니다. Dropbox는 계속해서 이러한 낡은 법의 개혁을 지지할 것입니다.

- ***신뢰할 수 있는 서비스 제공***

  정부는 온라인 서비스 공급업체에 백도어 프로그램을 설치하거나, 사용자 데이터를 얻기 위해 업체의 인프라스트럭처를 침투해서는 안 됩니다. Dropbox는 계속해서 Dropbox의 시스템을 보호하고 이러한 정부의 활동이 불법이라는 것이 법에 분명하게 명시될 수 있도록 노력하고 있습니다.

Dropbox의 투명성 보고서는 dropbox.com/transparency에서 확인할 수 있습니다.

개인정보 보호 인증, 증명, 규정 컴플라이언스

매일 수많은 개인과 조직이 Dropbox를 사용해 중요한 업무를 처리합니다. 그리고 이들의 파일을 보호하고 비공개로 유지하는 것은 Dropbox의 책임입니다. 개인정보 보호에 대한 헌신은 Dropbox가 내리는 모든 결정의 중추로 작용합니다.

클라우드 개인정보 보호에 관한 ISO/IEC 27018, 개인정보 보호 관리에 관한 ISO/IEC 27701(ISO/IEC 27001 및 ISO/IEC 27002 확장판)

Dropbox Business는 가장 먼저 ISO/IEC 27018 인증과 ISO/IEC 27701 인증을 획득한 주요 클라우드 서비스 공급업체 중 하나입니다.

ISO/IEC 27018은 클라우드 개인정보 및 데이터 보호에 관한 국제 표준입니다. 2014년 8월에 발표된 이 표준은 사용자 개인정보와 데이터 보호에 관한 지침을 세부적으로 규정합니다.

ISO/IEC 27701은 개인정보 보호 관리에 관한 최초의 국제 표준 인증입니다. 2019년에 발표된 이 표준은 ISO/IEC 27001에 개인정보 보호에 관한 고려사항을 추가해 정보보호관리체계(ISMS)를 개인정보보호관리체계(PIMS)로 확장하는 프레임워크를 제공합니다.

이 표준에는 Dropbox가 조직의 정보를 사용할 수 있는 경우와 사용할 수 없는 경우의 요건이 다양하게 명시되어 있습니다.

- ***여러분의 데이터에 대한 통제권은 여러분의 조직이 갖고 있습니다.***

  Dropbox는 서비스를 제공할 때 사용자가 제공한 개인정보만을 사용합니다. 사용자는 필요에 따라 Dropbox에 저장된 파일과 Paper 문서를 추가하고, 수정하고, 삭제할 수 있습니다.

- ***Dropbox는 언제나 데이터 투명성을 유지합니다.***

  Dropbox는 사용자의 데이터가 어느 서버에 저장되어 있는지 투명하게 공개합니다. 또한, 사용자들에게 Dropbox와 협력하는 파트너가 누구인지, 계정을 닫거나 파일/Paper 문서를 삭제했을 때 데이터가 어떻게 처리되는지를 공개합니다. 마지막으로, 이 중 하나라도 변경될 경우 사용자들에게 변경된 사항을 통보합니다.

- ***여러분의 데이터는 안전하게 보호됩니다.***

  ISO/IEC 27018과 ISO/IEC 27701은 전 세계에서 가장 일반적으로 통용되는 정보 보안 표준인 ISO/IEC 27001을 보완한 확장판입니다. Dropbox는 2020년 10월에 ISO/IEC 27001 인증을 갱신했습니다.

- ***Dropbox는 정기적으로 운영 사례를 점검합니다.***

  Dropbox는 ISO/IEC 27018, ISO/IEC 27701, ISO/IEC 27001 준수의 일환으로 매년 독립적인 외부 기관의 감사를 받아 인증을 유지하고 있습니다. Dropbox가 획득한 모든 ISO 인증은 여기에서 확인할 수 있습니다.

데이터 전송

Dropbox는 유럽연합, 유럽경제지역, 스위스에서 다른 지역으로 데이터를 전송할 때 고객, 제휴사와 맺은 계약서, 표준계약조항(SCC), 유럽연합 집행위원회가 규정한 국가별 결정 사항 등의 여러 가지 합법적 메커니즘을 근거로 사용합니다.

Dropbox는 유럽연합, 유럽경제지역, 영국, 스위스에서 미국으로 전송되는 개인정보의 수집, 사용, 보존과 관련해 미국 상무부가 규정한 유럽연합-미국/스위스-미국 프라이버시 실드 규정을 준수하지만, 이러한 규정을 개인정보 전송의 법적 근거로 사용하지는 않습니다. Dropbox의 프라이버시 실드 인증은 www.privacyshield.gov/list에서 확인할 수 있고, 프라이버시 실드에 관한 자세한 내용은 www.privacyshield.gov에서 확인할 수 있습니다.

Dropbox의 프라이버시 실드를 준수와 관련된 고소와 분쟁은 독립적인 외부 기관 JAMS의 조사를 거쳐 해결됩니다. 자세한 내용은 Dropbox의 개인정보처리방침(dropbox.com/privacy)에서 확인할 수 있습니다.

유럽연합 개인정보보호법(GDPR)

개인정보보호법(GDPR) 2016/679는 유럽연합 시민의 개인정보 처리에 관한 기존의 프레임워크를 대폭 수정한 유럽연합의 새로운 개인정보 보호 규정입니다. GDPR에는 Dropbox처럼 개인정보를 처리하는 기업에 적용되는 강력한 규정이 새롭게 도입되었습니다. GDPR은 2018년 5월 25일부터 시행되고 있으며, 기존의 유럽연합 개인정보보호지침(EU Directive 95/46 EC)을 대체합니다.

Dropbox는 언제나 법률적 요건과 우수 사례에 따라 사용자 데이터의 보안을 유지하고 보호하기 위해 최선을 다하고 있습니다. Dropbox는 데이터 보호 책임자를 임명하고, 사용자가 데이터 주체로서의 권리를 행사할 수 있도록 개인정보 보호 프로그램을 재편하며, 데이터 처리 활동을 문서화하고, 보안 위반 시 취해야 할 내부 프로세스를 강화하는 등 GDPR을 준수하기 위해 많은 노력을 기울였습니다. Dropbox는 데이터 보호 당국이 발표하는 추가 지침에 따라 이러한 프로세스와 사례가 새로운 법에 규정된 구체적인 요소를 충족하거나 초과 달성할 수 있도록 계속해서 이를 조정해 나갈 것입니다.

Cloud Security Alliance(CSA): Code of Conduct for GDPR Compliance

CSA Code of Conduct for GDPR Compliance는 Dropbox와 같은 클라우드 서비스 공급업체가 자발적인 책임 이행과 전반적인 투명성 제고를 통해 클라우드 서비스를 사용하는 고객들에게 유럽연합 개인정보보호법(GDPR)의 핵심 규정을 어떻게 준수하고 있는지 입증할 수 있는 도구입니다. Dropbox Business는 외부 감사기관의 엄격한 감사가 수반되는 CSA Code of Conduct for GDPR Compliance 자체 평가를 거쳐 규정 준수 마크 'Declared'를 획득했습니다. CSA Code of Conduct for GDPR Compliance와 이와 관련된 Dropbox의 컴플라이언스 현황에 대한 자세한 정보는 CSA 웹사이트에서 확인할 수 있습니다.

Dropbox의 개인정보 보호 사례와 정책에 관한 자세한 내용은 개인정보 및 데이터 보호 백서에서 확인할 수 있습니다.

컴플라이언스

각 조직이 준수해야 하는 보안 요건과 개인정보 보호 요건은 업계에 따라 차이가 있습니다. Dropbox는 가장 일반적으로 통용되는 표준과 고객의 비즈니스나 업종에 특화된 컴플라이언스 방안을 결합해 비즈니스의 규정 준수를 지원합니다.

ISO/IEC

국제 표준화 기구(ISO)는 세계 최고 수준의 정보 보안 및 사회 안보 관련 표준을 개발해 조직이 혁신적이면서 믿을 수 있는 제품과 서비스를 개발하도록 지원합니다. Dropbox는 네덜란드에 위치한 독립적인 외부 감사기관 EY CertifyPoint의 감사를 통해 데이터 센터와 시스템, 애플리케이션, 직원, 프로세스를 검증받았습니다. EY CertifyPoint는 Raad voor Accreditatie(네덜란드 인증 위원회)로부터 ISO 인가를 받은 기관입니다.

ISO/IEC 27001(정보 보안)

ISO/IEC 27001은 세계 최고의 정보 보호 관리 체계(ISMS) 표준으로 인정받고 있습니다. 이 표준은 ISO/IEC 27002에 설명된 보안 우수 사례를 활용합니다. Dropbox는 고객의 신뢰에 보답하기 위해 끊임없이 Dropbox의 물리적, 기술적, 법적 제어를 철저하게 관리하고 있습니다.

Dropbox Business와 Dropbox Education의 ISO/IEC 27001 인증 보기

ISO/IEC 27017(클라우드 보안)

ISO/IEC 27017은 프로비전과 클라우드 서비스 사용에 적용되는 보안 제어 지침을 제공하는 클라우드 보안 부문 국제 표준입니다. Dropbox의 공동 책임 안내서에는 Dropbox와 고객이 함께 노력해야 할 보안, 개인정보 보호, 컴플라이언스 요건이 다양하게 설명되어 있습니다.

Dropbox Business와 Dropbox Education의 ISO/IEC 27017 인증 보기

ISO/IEC 27018(클라우드 개인정보 및 데이터 보호)

ISO/IEC 27018은 Dropbox처럼 고객을 대신해 개인정보를 처리하는 클라우드 서비스 공급업체에 적용되는 개인정보 및 데이터 보호 부문 국제 표준입니다. 이 표준은 고객이 일반적인 규정상·계약상 요건이나 문의에 대처하는 방법에 관한 근거를 제시합니다.

Dropbox Business와 Dropbox Education의 ISO/IEC 27018 인증 보기

ISO/IEC 22301(업무 연속성)

ISO/IEC 22301은 잠재적인 위험을 최소화해 운영 중단의 가능성을 줄이고, 운영 중단 상황이 발생했을 시 이에 적절하게 대응하는 방법을 제시하는 업무 연속성 부문 국제 표준입니다. Dropbox는 위기 상황에서 인력과 비즈니스 운영을 보호하는 통합 위기관리 전략의 일환으로 업무 연속성 관리 체계(BCMS)를 구축해 놓았습니다.

Dropbox Business와 Dropbox Education의 ISO/IEC 22301 인증 보기

ISO/IEC 27701(개인정보 보호 관리)

ISO 27701은 개인정보 보호 관리에 관한 국제 표준입니다. 이 표준은 ISO 27001에 규정된 정보보호관리체계(ISMS)를 보완해 개인정보보호관리체계(PIMS)로 확장한 것으로, 개인정보 보호에 관한 통합적인 프레임워크를 제공합니다. Dropbox Business와 Dropbox Education은 개인 식별 정보(PII) 처리업체 자격으로 이 인증을 획득했습니다.

Dropbox Business와 Dropbox Education의 ISO 27701 인증 보기

SOC

흔히 SOC 1, SOC 2, SOC 3으로 불리는 SOC(Service Organization Controls) 보고서는 미국 공인 회계사 협회(AICPA)가 조직의 내부 제어 환경을 평가하기 위해 개발한 프레임워크입니다. Dropbox는 독립적인 외부 감사기관 Ernst & Young LLP의 감사를 거쳐 시스템, 애플리케이션, 인력, 프로세스를 인증받았습니다.

보안, 기밀성, 무결성, 가용성, 개인정보 보호에 관한 SOC 3

SOC 3 검증 보고서는 보안, 가용성, 절차상 무결성, 기밀성, 개인정보 보호로 구성된 5대 신뢰 서비스 기준을 모두 다룹니다(TSP 섹션 100). Dropbox 일반 사용 보고서는 SOC 2 보고서를 종합적으로 요약한 것으로, 여기에는 디자인의 실용성과 제어 환경 운영에 관한 독립 외부 감사기관의 의견도 포함되어 있습니다.

Dropbox Business와 Dropbox Education의 SOC 3 검증 보기

보안, 기밀성, 무결성, 가용성, 개인정보 보호에 관한 SOC 2

SOC 2 보고서는 보안, 가용성, 절차상 무결성, 기밀성, 개인정보 보호로 구성된 5대 신뢰 서비스 기준을 모두 다루며 제어 환경에 관한 상세한 검증 결과를 제공합니다(TSP 섹션 100). SOC 2 보고서에는 Dropbox가 고객의 자료를 보호하기 위해 실행 중인 프로세스와 100가지 이상의 제어 기능이 상세하게 설명되어 있습니다. 또한, 디자인의 실용성과 제어 환경 운영에 관한 독립 외부 감사기관의 의견에 더불어 감사기관의 테스트 절차와 각 제어 기능에 대한 감사 결과가 포함되어 있습니다. SOC 2 보고서(또는 SOC 2+ 보고서)에는 위에 언급된 ISO 국제 표준에 관한 Dropbox의 제어 환경을 감사한 결과가 포함되어 있어 Dropbox의 고객은 이를 통해 한층 강화된 투명성을 확보할 수 있습니다. Dropbox Business와 Dropbox Education의 SOC 2 검증 보고서는 요청 시 확인할 수 있습니다.

SOC 1/SSAE 18/ISAE 3402(구 SSAE 16 또는 SAS 70)

SOC 1 보고서는 Dropbox Business 또는 Dropbox Education을 내부 재무 보고 관리(ICFR) 프로그램의 핵심 요소인 고객에게 상세한 검증 결과를 제공합니다. 이 검증은 주로 사베인스-옥슬리법(SOX) 규정 준수에 사용됩니다. 독립적인 외부 기관의 감사는 SSAE 18(Statement on Standards for Attestation Engagements No. 18)과 ISAE 3402(International Standard on Assurance Engagements No. 3402)에 따라 시행되며, 이러한 규정은 이제는 사용이 중단된 SSAE 16(Statement on Standards for Attestation Engagement No.16)과 SAS 70(Statement on Auditing Standards No. 70)을 대체합니다. Dropbox Business와 Dropbox Education의 SOC 1 검증 보고서는 요청 시 확인할 수 있습니다.

CSA

CSA STAR(Cloud Security Alliance: 보안, 신뢰, 보장, 위험성 등록)

CSA STAR는 클라우드 서비스 보안 보증 프로그램을 제공하는 무료 공개 등록부로, 사용자는 이를 참조해 현재 사용 중이거나 계약을 검토 중인 클라우드 서비스 공급업체의 보안 환경을 평가할 수 있습니다.

Dropbox Business와 Dropbox Education은 CSA START 레벨 2 인증과 레벨 2 증명을 획득했습니다. CSA STAR 레벨 2를 획득하려면 ISO/IEC 27001, SOC 2 신뢰 서비스 기준, CSA CCM(Cloud Controls Matrix) v3.0.1 요건을 토대로 독립적인 외부 감사기관 EY CertifyPoint(인증 부문)와 Ernst & Young LLP(증명 부문)의 보안 제어 환경 평가를 거쳐야 합니다. Dropbox의 CSA STAR 레벨 2 인증과 증명은 CSA 웹사이트에서 확인할 수 있습니다.

HIPAA/HITECH

Dropbox는 HIPAA(Health Insurance Portability and Accountability Act)와 HITECH(Health Information Technology for Economic and Clinical Health Act) 규정을 준수해야 하는 Dropbox Business/Dropbox Education 고객과 BAA(Business Associate Agreement)를 체결합니다. 자세한 내용은 'HIPAA 시작하기' 안내서와 도움말 센터 게시물에서 확인할 수 있습니다.

Dropbox는 Dropbox Business나 Dropbox Education을 사용해 HIPAA/HITECH 보안 및 개인정보 보호 규정 요건을 준수하고자 하는 고객에게 Dropbox의 HIPAA/HITECH 보안, 개인정보 보호, 개인정보 침해 통보 규정 제어 현황을 평가한 외부 기관의 검증 보고서와 다양한 내부 사례, 권장 사항을 제공합니다.

이 문서를 요청하려거나 Dropbox Business 구매에 관해 자세한 정보를 알고 싶은 고객은 Dropbox 영업팀으로 문의하시기 바랍니다. Dropbox Business나 Dropbox Education의 팀 관리자인 경우, 관리 콘솔 계정 페이지에서 전자 BAA를 체결할 수 있습니다.

현재 관리 콘솔에서 전자 BAA를 체결하는 기능은 미국에 거주하는 고객에게만 제공됩니다.

독일 BSI C5 증명 보고서

C5(Cloud Computing Compliance Controls Catalog)는 독일 연방정보기술보안청(BSI)이 클라우드 서비스 프로비전에 적용되는 보안 제어 환경을 평가하기 위해 개발한 프레임워크입니다. C5 증명은 조직이 BSI가 규정한 '클라우드 공급업체를 위한 보안 권장 사항'을 준수하는 정보 보안 환경을 구축하고 있다는 것을 의미합니다. C5는 ISO/IEC 27001, CSA STAR 등 현존하는 국제 보안 표준을 토대로 개발되었습니다. Dropbox는 독일에 위치한 독립적인 외부 감사기관 Ernst & Young GmbH로부터 시스템과 프로세스, 제어 환경을 검증받아 C5 증명 보고서를 취득했습니다. 외부 기관의 감사는 International Standard on Assurance Engagements No. 3000(ISAE 3000과 IDW PS 860)을 기준으로 시행됩니다.

이 보고서에는 Dropbox의 시스템, 애플리케이션, 프로세스, 제어 환경에 더불어 외부 감사기관의 테스트 절차와 각 제어 기능에 대한 감사 결과가 상세하게 설명되어 있습니다. Dropbox Business와 Dropbox Education에 관한 C5 보고서는 요청 시 확인할 수 있습니다.

Dropbox Paper는 C5 보고서 평가 범위에 포함되지 않습니다.

NIST 800-171

미국 국립표준기술원(NIST)은 정보 체계 보호에 관한 표준과 지침을 규정하고 관리하는 기관입니다. NIST SP 800-171 2차 개정판(R2)은 연방 정보 체계와 조직이 아닌 곳에서의 미분류 제어 정보(CUI) 보호에 관한 지침을 제공합니다. 연구기관과 교육기관처럼 미국 정부의 CUI를 처리하거나 저장하는 모든 기관은 NIST SP 800-171 R2를 준수해야 합니다. Dropbox의 CUI 시스템, 프로세스, 제어 환경은 독립적인 외부 감사기관 Ernst & Young LLP를 통해 그 유효성을 입증받았습니다.

Dropbox Business와 Dropbox Education에 관한 NIST SP 800-171 R2 보고서는 Dropbox 영업팀 또는 (기존 Dropbox Business 고객의 경우) 지원팀에 요청 시 확인할 수 있습니다.

Dropbox Paper는 NIST SP 800-171 R2 보고서 평가 범위에 포함되지 않습니다.

FERPA와 COPPA(학생과 아동)

Dropbox Business와 Dropbox Education 고객은 미국 FERPA(Family Education Rights and Privacy Act)에 규정된 공급업체의 의무를 준수하며 서비스를 사용할 수 있습니다. 만 13세 이하의 학생들을 가르치는 교육기관도 부모로부터 서비스 이용에 관한 동의를 얻어야 하는 계약상 조항에 동의할 경우 COPPA(Children's Online Privacy Protection Act)를 준수하며 Dropbox Business 또는 Dropbox Education을 사용할 수 있습니다.

영국 디지털 마켓플레이스 G-Cloud

Dropbox Business는 영국 디지털 마켓플레이스 정부 클라우드 조달 부문에 등록되어 있습니다. 영국 디지털 마켓플레이스 웹사이트에서 Dropbox Business Standard 요금제, Dropbox Business Advanced 요금제, Dropbox Enterprise 요금제가 등록된 것을 확인할 수 있습니다.

Dropbox Paper는 영국 디지털 마켓플레이스 G-Cloud 목록에 포함되어 있지 않습니다.

FDA 21 CFR Part 11

미국 연방규정집(CFR) Title 21은 미국 식품의약국(FDA), 마약단속국(DEA), 마약통제정책국(ONDCP)이 따라야 할 미국 내 식품 및 의약품에 관한 규정입니다. Title 21 Part 11에는 FDA가 서면 기록, 문서에 한 수기 서명과 일반적으로 동일한 것으로 인정하는 신뢰할 수 있는 전자 기록과 전자 서명의 기준이 명시되어 있습니다.

Dropbox가 FDA 21 CFR Part 11 컴플라이언스에 어떤 도움이 되는지는 Dropbox 및 FDA 21 CFR Part 11 백서와 도움말 센터 게시글에서 자세히 확인할 수 있습니다.

PCI DSS

Dropbox는 지불 카드 보안 표준(PCI DSS)을 준수하는 전자상거래 업체이지만, Dropbox Business와 Dropbox Education, Dropbox Paper는 신용카드 거래를 처리하거나 저장하지 않습니다. Dropbox의 업체 상태에 관한 PCI 컴플라이언스 증명(AoC)은 요청 시 확인할 수 있습니다.

Dropbox Business와 Dropbox Education 컴플라이언스에 관한 자세한 정보는 다음에서 확인할 수 있습니다.

Dropbox.com/business/trust/compliance 방문하기

Dropbox 앱

DBX Platform은 Dropbox의 유연한 응용 프로그램 인터페이스(API)를 기반으로 애플리케이션을 제작하는 개발자들이 모인 활발한 생태 공간입니다. 이미 75만 이상의 개발자가 DBX Platform에서 생산성, 협업, 보안, 관리 등 다양한 부문의 애플리케이션과 서비스를 개발했습니다.

사전 구축된 구성 요소

Chooser, Saver, Embedder는 사전 구축된 웹/모바일 구성 요소로, 이러한 구성 요소를 사용해 몇 줄의 코드만으로 타사 앱/사이트에서 Dropbox로 간편하게 액세스할 수 있습니다.

- Chooser는 Dropbox에 저장된 파일을 활성화합니다.
- Saver는 사용자가 파일을 Dropbox에 바로 저장할 수 있게 합니다.
- Embedder는 사용자가 Dropbox에 있는 파일과 폴더를 볼 수 있게 합니다.

이 구성 요소를 승인하는 작업은 Dropbox를 통해서만 가능합니다. Chooser를 구축하면 앱에 Dropbox 공유 링크나 단발성 다운로드 링크를 통해 활성화된 파일에 액세스할 수 있는 권한이 부여됩니다. 이러한 사전 구축 구성 요소는 개별적으로 사용할 수도 있고, 아래에 설명된 API와 함께 사용할 수도 있습니다.

Dropbox Business API 통합

Dropbox 공개 API는 외부 개발자에게 직접 개발한 애플리케이션에서 Dropbox에 액세스하고 Dropbox와 상호 교류할 수 있는 기능을 제공합니다. 여기에는 파일 및 메타 데이터 교환, 공유, 팀 기능이 포함됩니다.

인증

Dropbox는 업계 표준 인증 프로토콜인 OAuth를 사용하며, 이를 통해 사용자는 본인의 계정 정보를 노출하지 않고도 앱 계정으로의 액세스를 승인할 수 있습니다. Dropbox는 OAuth 2.0으로 API 요청 인증을 처리하며, 이러한 요청은 Dropbox 웹사이트나 모바일 앱을 통해 인증됩니다. Dropbox는 분산된 앱에서 사용할 수 있는 단발성 액세스 토큰과 PKCE 등의 OAuth 우수 사례를 지원합니다.

사용자 권한

Dropbox API를 사용해 개발된 앱은 다음과 같은 콘텐츠 액세스 수준을 통해 최종 사용자의 Dropbox에 액세스할 수 있습니다.

- ***앱 폴더***

  앱 이름과 동일한 이름의 이 전용 폴더는 사용자 Dropbox의 Apps 폴더에 생성됩니다. 이 앱에는 Apps 폴더에서의 읽기 액세스와 쓰기 액세스만 제공되며, 사용자는 Apps 폴더에 파일을 옮겨 앱에 콘텐츠를 제공할 수 있습니다. 또한, 앱은 Chooser 또는 Saver를 통해 파일/폴더 액세스를 요청할 수 있습니다.

- ***Dropbox 전체***

  앱에 사용자 Dropbox의 모든 파일과 폴더로의 전체 액세스가 제공됩니다. 앱은 Chooser나 Saver를 사용해 파일/폴더로의 액세스를 요청할 수 있습니다(아래 설명 참조).

애플리케이션이 특정한 범위를 요청해 API 엔드포인트 일부에만 액세스하며 작업을 제한하는 것도 가능합니다. 예를 들어, 애플리케이션의 액세스를 파일 읽기나 콘텐츠 업로드만으로 제한하고, 공유 기능을 사용하는 것은 허용하지 않을 수 있습니다.

팀 권한

Dropbox Business 팀의 관리자는 애플리케이션이 팀 관리 콘솔에 있는 관리 기능에 액세스하도록 승인할 수 있습니다. 앱이 읽거나 관리할 수 있는 팀 설정의 범위를 지정해 팀에 연결된 앱이 실행할 수 있는 작업을 특정한 범위로 제한할 수 있습니다.

일반적으로 결합해 사용하는 범위는 같습니다.

- ***팀 정보***

  팀과 사용량이 많은 정보에 관한 읽기 전용 액세스

- ***팀 감사***

  팀 정보와 상세한 이벤트 로그로의 읽기 전용 액세스

- ***팀원 파일 액세스***

  팀원을 대신해 파일, 폴더 관리 등의 작업을 실행하는 기능

- ***팀원 관리***

  팀원 추가 및 제거

웹훅

웹훅은 사용자의 Dropbox에 변경 사항이 생겼을 때 웹 앱에 실시간으로 알림을 전송하는 데 사용됩니다. URI를 등록해 웹훅을 수신할 수 있는 상태가 되면 앱에 등록된 사용자에게 변경 사항이 생길 때마다 HTTP 요청이 해당 URI로 전송됩니다. Dropbox Business API를 사용하면 팀원 자격 변경에 관한 알림을 생성할 때도 웹훅을 사용할 수 있습니다. 많은 보안 앱이 웹훅을 사용해 관리자가 팀 활동을 추적하고 관리할 수 있도록 지원합니다.

확장 프로그램

앱 개발자는 확장 프로그램 URI를 등록해 Dropbox UI의 '공유' 메뉴와 '열기' 메뉴에 작업을 표시할 수 있습니다. 확장 프로그램을 사용하면 사용자가 Dropbox 작업 공간에서 바로 맞춤형 외부 워크플로를 사용할 수 있습니다. 작업이 실행되면 Dropbox는 파일을 실행할 때 API와 함께 사용되는 파일 식별자를 전달해 사용자를 지정된 URI로 리디렉션합니다. 등록된 앱 확장 프로그램은 승인을 받은 후에 사용자 화면에 표시됩니다. Dropbox는 확장 프로그램 통합(아래 설명 참조)을 엄선해 공유' 메뉴와 '열기' 메뉴로 승격할 수 있으며, 앱은 사용자가 액세스를 승인할 때까지 콘텐츠에 액세스할 수 없습니다.

Dropbox 개발자 지침

Dropbox는 개발자들이 사용자의 개인정보를 보호하면서 사용자 경험을 향상하는 API 앱을 제작할 수 있도록 다양한 지침과 사례를 제공합니다.

- ***앱 키***

  개발자는 앱을 코딩할 때 고유의 Dropbox 앱 키를 사용해야 합니다. 또한, 앱이 DBX Platform을 통해 다른 개발자들이 사용할 수 있는 서비스나 소프트웨어를 제공할 경우, 각 개발자는 고유의 Dropbox 앱 키를 신청해야 합니다.

- ***앱 권한***

  개발자는 앱에 허용되는 최소한의 특권만을 사용해야 합니다. 개발자가 배포 상태를 승인받기 위해 앱을 제출하면 Dropbox는 앱이 제공하는 기능에 비해 불필요하게 광범위한 권한을 요청하지 않았는지 검토합니다.

- ***앱 검토 프로세스***

  - ***개발 상태***

    Dropbox API 앱 개발이 완료되면 앱에는 개발 상태가 부여됩니다. 개발 상태의 앱은 연결할 수 있는 Dropbox 사용자 수가 최대 500명이라는 점을 제외하면 배포 상태의 앱과 동일하게 기능합니다. 앱에 연결한 사용자 수가 50명에 도달하면 개발자는 2주 이내에 배포 상태를 신청하고 승인받아야 합니다. 그렇지 않으면 더 이상 앱에 사용자를 연결할 수 없습니다.

  - ***배포 상태와 승인***

    모든 API 앱은 DBX Platform 사용 시 금지되는 사항이 명시되어 있는 Dropbox 개발자 브랜딩 지침서와 이용 약관을 준수해야 배포 상태를 승인받을 수 있습니다. DBX Platform 사용 시 금지되는 사항에는 지식재산권 홍보, 저작권 침해, 파일 공유 네트워크 생성, 콘텐츠 불법 다운로드 등이 포함됩니다. 개발자는 앱을 제출해 심사를 받기 전에 먼저 앱의 기능과 앱의 Dropbox API 활용 방식에 관한 추가 정보를 제공해야 합니다. 배포 상태가 승인되면 무제한의 Dropbox 사용자가 앱에 연결할 수 있습니다.

팀 앱 관리

Dropbox Business 팀의 관리자는 팀 관리 콘솔에서 연결된 앱과 팀의 통합(아래 설명 참조) 기능 사용을 관리할 수 있습니다.

API 파트너십

Dropbox는 기술 파트너들과 긴밀하게 협력해 파트너가 업체의 인기 소프트웨어 패키지를 Dropbox와 통합할 수 있게 합니다. 이러한 파트너는 Dropbox API를 사용해 앱을 개발하며, Dropbox 아키텍트와 협력해 우수 보안 사례와 UX 사례를 따릅니다. 이렇게 개발된 앱에는 다음과 같은 다양한 생산성 앱과 보안 도구, 관리 도구가 포함됩니다.

- ***보안 관제 시스템(SIEM)과 분석***

  Dropbox Business 계정을 SIEM과 분석 도구에 연결해 사용자 공유 현황과 로그인 시도, 관리자 활동 등을 감시하고 평가할 수 있습니다. 중앙 로그 관리 도구를 통해 직원들의 활동 로그와 보안 관련 데이터에 액세스하고 관리할 수 있습니다.

- ***데이터 손실 방지(DLP)***

  이 도구는 파일 메타데이터와 콘텐츠를 자동으로 스캔해 Dropbox 계정에 중요한 변경 사항이 생길 시 알림, 보고, 작업을 실행합니다. Dropbox Business 배포에 회사 정책을 적용하면 컴플라이언스 요건을 더 효율적으로 준수할 수 있습니다.

- ***전자 증거 개시와 소송 자료 보존***

  이 도구는 Dropbox Business 계정에 저장된 데이터에 관한 소송, 중재, 조사에 대응하는 데 유용합니다. 전자 증거 개시 프로세스를 통해 온라인에 저장된 정보 중 관련된 것을 검색·수집하고 데이터를 보존할 수 있어 업무상 시간과 비용이 절약됩니다.

- ***디지털 저작권 관리(DRM)***

  타사 콘텐츠 보호 도구를 추가해 직원의 계정에 저장된 데이터 중 민감한 데이터 또는 저작권이 있는 데이터를 보호할 수 있습니다. DRM은 클라이언트 측 암호화, 워터마크 표시, 감사 추적, 액세스 철회, 사용자/장치 차단 등의 강력한 기능을 제공합니다.

- ***데이터 이전과 온프레미스 백업***

  더 적은 시간과 비용, 노력으로 기존의 서버나 다른 클라우드 기반 솔루션에서 Dropbox로 데이터를 이전할 수 있습니다. Dropbox Business 계정에서 온프레미스 서버로 백업을 자동화할 수 있습니다.

- ***계정 관리와 SSO(Single Sign-On)***

  프로비전과 프로비전 해제 프로세스를 자동화해 신규 직원의 온보딩 시간을 단축할 수 있습니다. Dropbox Business를 기존의 계정 관리 시스템과 통합해 관리를 간소화하고 보안을 강화할 수 있습니다.

- ***맞춤형 워크플로***

  Dropbox를 기존의 비즈니스 프로세스와 통합하는 사내 앱을 구축해 조직의 워크플로를 향상할 수 있습니다.

Dropbox 공개 API를 사용해 애플리케이션과 서비스를 개발한 기술 파트너 목록은 Dropbox 앱 통합 페이지에서 확인할 수 있습니다. 최종 사용자는 App Center에서 엄선된 Dropbox 자체, 타사 앱과 통합 기능을 살펴볼 수 있습니다.

Dropbox 통합

Dropbox는 일부 일류 기술 파트너들과 협력해 Dropbox 작업 공간에 파트너의 소프트웨어를 통합할 수 있는 기능을 개발했습니다. 이러한 심층 통합은 Dropbox와 파트너가 공동 개발한 것으로, 여기에는 다음과 같은 심층 통합이 포함됩니다.

Dropbox Extensions

이 통합은 다양한 유형의 앱 확장 프로그램을 사용해 Dropbox에서 바로 동영상을 게시하고, 이메일과 채팅으로 파일을 추가하고, 파일을 전송해 전자 서명을 요청하는 것과 같은 작업을 원활하게 실행할 수 있도록 합니다. 애플리케이션의 개발은 파트너가 담당하며, Dropbox는 파트너를 엄선해 '다음으로 열기', '다음으로 공유' 메뉴에 표시합니다.

Slack, Zoom, Trello

Dropbox가 자체적으로 개발한 이 통합 기능을 통해 Dropbox에서 Slack 대화를 시작하고, 회의를 진행하고, 업무를 생성할 수 있습니다. 최종 사용자는 OAuth 인증을 통해 이러한 도구에 액세스할 수 있습니다.

모바일/웹용 Microsoft Office

Dropbox와 Microsoft Office의 통합을 통해 사용자는 Dropbox에 저장된 Word, Excel, PowerPoint 파일을 열어 보고 Office 모바일 앱이나 웹 앱에서 파일을 수정할 수 있습니다. 수정한 파일의 변경 사항은 Dropbox에 다시 저장됩니다. Dropbox와 Microsoft Office를 통합한 후 Office 모바일 앱 또는 웹 앱에서 처음으로 Dropbox 파일을 열면 액세스 승인 여부를 묻는 메시지가 표시되며, 이후에 파일을 열 때는 연결 상태가 유지됩니다.

Adobe Acrobat/Acrobat Reader

Dropbox와 Adobe Acrobat/Acrobat Reader의 데스크톱 버전 및 모바일 버전(Android와 iOS)을 통합하면 사용자는 Dropbox에 저장된 PDF 파일을 보고, 편집하고, 공유할 수 있습니다. 통합 후 각 앱에서 처음으로 Dropbox 파일을 열면 액세스 승인 여부를 묻는 메시지가 표시됩니다. PDF 파일의 변경 사항은 자동으로 Dropbox에 다시 저장됩니다.

마무리

Dropbox Business는 팀의 효율적인 협업을 지원하는 쉽고 간편한 도구와 함께 조직에 필요한 컴플라이언스 인증과 보안 조치를 제공합니다. Dropbox는 강력한 백엔드 인프라스트럭처와 맞춤형 정책을 결합한 다계층 보안 접근 방식을 사용해 비즈니스에 각 조직의 필요에 따라 맞춤형으로 설계할 수 있는 강력한 솔루션을 제공합니다. Dropbox Business에 관한 자세한 내용은 Dropbox 영업팀(sales@dropbox.com)에 문의할 수 있습니다.