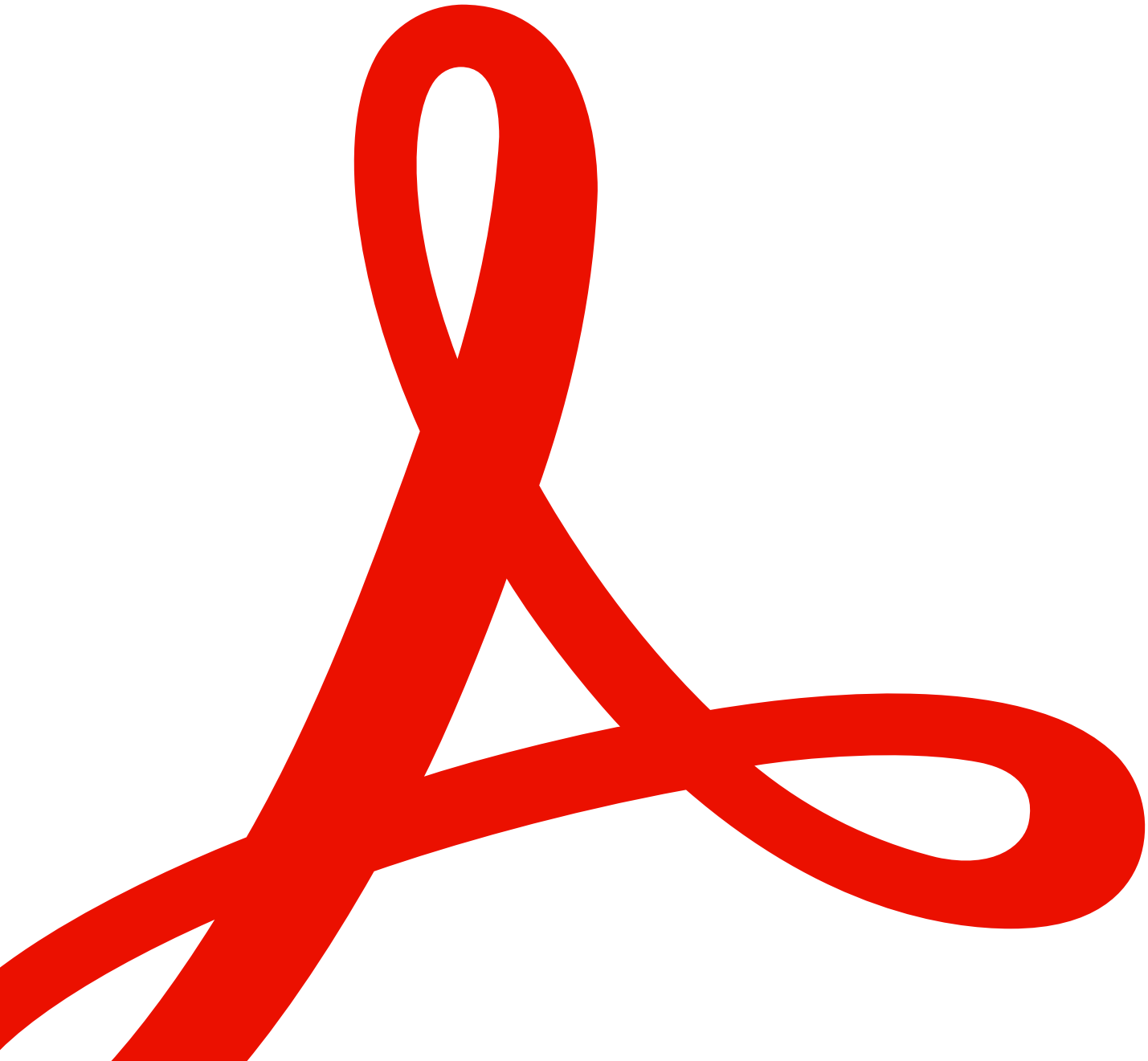
Adobe Document Cloud

Adobe

백서

Adobe Acrobat 및 Document Cloud 서비스 보안 개요



목차

Adobe 보안

Adobe는 디지털 경험에서의 보안을 중요하게 생각합니다. 보안에 관련된 관행은 Adobe의 소프트웨어 개발과 운영 프로세스 및 툴에 깊이 각인되어 있으며, Adobe의 여러 팀에서 적절한 방식으로 사고를 예방하고, 감지 및 대응하기 위해 엄격하게 준수되는 사안입니다. 또한 Adobe는 파트너, 주요 리서치 업체, 보안 연구 기관, 기타 업계 조직과 협업을 통해 최신 보안 위협과 취약점을 파악하여 Adobe의 제품 및 서비스에 첨단 보안 기술을 정기적으로 적용하고 있습니다.

본 백서에서는 Adobe Acrobat 및 Document Cloud 서비스 및 관련 데이터의 보안을 강화하기 위해 Adobe에서 구현하는 방어 중심의 접근 방식과 보안 절차를 살펴봅니다.

Acrobat 및 Document Cloud 서비스 개요

Acrobat 및 Document Cloud 서비스는 긴밀하게 연결된 멀티 디바이스 환경을 위한 완벽한 PDF 솔루션입니다. Acrobat 데스크탑 소프트웨어와 고급 모바일 기능으로 향상된 Adobe Acrobat Reader 모바일 앱 및 Document Cloud 서비스를 사용하면 조직에서 더욱 스마트한 문서 워크플로우를 구축하고, 모바일 솔루션에 대한 최종 사용자의 요구 사항을 충족하며, 디바이스 전반에서 문서를 안전하게 보호할 수 있습니다.

Acrobat 및 Document Cloud 서비스를 통해 거의 모든 콘텐츠를 다른 사람과 공유할 수 있는 전자 문서로 변환하고 Acrobat 클라우드 서비스, 데스크탑 애플리케이션 또는 모바일 앱에서 PDF 파일의 생성, 편집, 변환을 손쉽게 자동화할 수 있습니다.

Acrobat 사용자 경험

고객은 Document Cloud 서비스를 통해 다양한 Acrobat 사용자 경험을 할 수 있습니다.

- Acrobat Pro — 노트북 및 데스크탑 사용자를 위한 데스크탑 애플리케이션
- Acrobat 온라인 — Chrome, Microsoft Edge, Firefox, Safari를 비롯한 데스크탑 및 모바일 디바이스가 지원하는 브라우저 내의 웹 앱
- Acrobat Reader 모바일 클라이언트 — Apple App Store와 Google Play에서 무료로 다운로드할 수 있는 모바일 및 태블릿 사용자용 앱

Adobe는 Acrobat을 여러 Microsoft 생산성 툴에 통합하여 독립 실행형 Acrobat과 다른 문서 저장 방식을 제공합니다. 이러한 통합에 대한 자세한 보안 정보는 'Acrobat Microsoft 통합' 섹션을 참조하십시오.

Document Cloud 서비스

Adobe Document Cloud 서비스에 포함된 기능은 다음과 같습니다.

- PDF 전송 — 이메일 클라이언트를 사용하여 수신자에게 PDF 전송
- PDF 구성 — PDF에서 페이지 삽입, 삭제, 순서 변경 또는 회전
- PDF 작성 — Word, Excel, PowerPoint 문서, 이미지 또는 사진을 PDF 파일로 변환
- PDF 내보내기 — PDF를 편집 가능한 Microsoft Word, Excel, PowerPoint 또는 RTF 파일로 변환
- PDF 편집 — 모바일 디바이스 또는 노트북에서 PDF를 손쉽게 편집
- PDF 결합 — 여러 파일을 하나의 PDF로 결합 및 어디에서나 문서 패키지 취합
- 채우기 및 서명 — 양식 작성 및 서명 추가
- Adobe Scan — 무엇이든 캡처한 다음, 검색 가능한 고품질 PDF로 변환
- Adobe Acrobat Sign — 간단한 서명에서 클라우드의 디지털 서명에 이르기까지 모든 최신 디바이스에서 신뢰할 수 있는 전자 서명을 위한 문서 준비 및 전송

Adobe는 Document Cloud 서비스에 새로운 솔루션을 지속적으로 추가하고 있습니다. 모든 Document Cloud 서비스의 최신 목록은 Adobe.com에서 확인하실 수 있습니다.

Acrobat 문서 보안 기능

교정

Adobe Document Cloud 서비스에는 교정 툴셋이 포함되어 있어, 문서를 배포하기 전에 문서에 포함된 텍스트 및 그래픽 이미지를 영구 삭제하는 등 민감한 정보나 기밀 정보를 보호하기 위한 여러 기능을 사용할 수 있습니다. 또한 전화번호, 신용카드 번호 및 이메일 주소와 같은 패턴을 기반으로 정보를 검색하여 교정할 수도 있습니다. 선택한 정보는 다른 툴 또는 방법에서처럼 단순히 가려지는 것이 아니라 파일에서 완전히 제거됩니다. 문서의 기밀 정보 가리기 기능을 사용하면 PDF에 포함된 메타데이터와 같은 숨겨진 정보와 그래픽이 아닌 개체도 제거할 수 있습니다.

파일 공유

클라우드에 저장된 Document Cloud 파일에는 자동으로 '비공개' 레이블이 지정되므로, 콘텐츠는 업로드한 최종 사용자만이 볼 수 있습니다. 따라서 콘텐츠를 공유하기 위해서는 최종 사용자가 조치를 취해야 하며, 그렇지 않으면 비공개로 유지됩니다. Document Cloud 파일의 콘텐츠를 공유할 때는 Document Cloud 콘텐츠에 대한 URL 링크를 수신자에게 전송하면 됩니다.

Document Cloud 서비스 사용자는 두 가지 옵션(보기 전용 또는 검토)을 통해 파일을 공유할 수 있습니다. 사용자가 보기 전용으로 제한된 링크를 전송하면 수신자는 해당 콘텐츠를 읽기 전용 문서로만 볼 수 있습니다. 또는 사용자가 검토용으로 문서를 전송하면 수신자는 해당 문서에 주석을 추가할 수 있지만, 문서를 편집하거나 변경할 수는 없습니다. 링크는 이메일, 문자 메시지 또는 모든 공동 작업 소프트웨어를 통해 수신자에게 전송될 수 있습니다.

에셋 설정 및 공유 제한

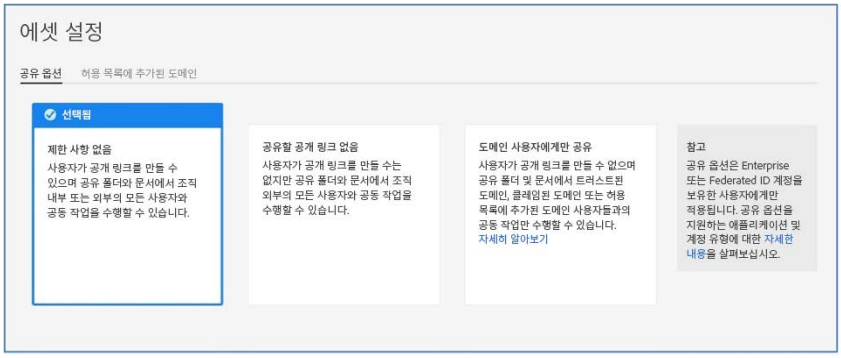


그림 1. Document Cloud 서비스 에셋 설정

Adobe Admin Console의 에셋 설정 기능을 통해 Document Cloud에 저장된 콘텐츠의 공유 제한을 활성화할 수도 있습니다. 이를 통해 기업 IT 관리자는 공개 링크 공유 기능을 비활성화하고, 기업이 요청한 도메인과 화이트리스트에 등록된 도메인에서만 Document Cloud 공동 작업이 가능하도록 할 수 있습니다. 공유 제한이 활성화되면 수신자는 로그인이 필요합니다. '도메인 사용자에게만 공유'가 활성화되어 있으면, 사용자는 조직 내의 다른 사용자나 신뢰할 수 있는 기타 도메인의 사용자에 한해서만 콘텐츠를 공유할 수 있으며 외부 공유는 완전히 비활성화됩니다.

Microsoft Purview Information Protection

Microsoft Purview Information Protection(MPIP)은 Microsoft 저작권 관리 솔루션입니다. Azure Information Protection과 기타 Microsoft Purview Information Protection 솔루션 사용자는 Acrobat 또는 Acrobat Reader를 사용하여 레이블이 지정되고 보호된 콘텐츠를 읽을 수 있습니다. 최신 데스크탑 버전의 Acrobat Pro/Standard(버전 22.003.20258 이상)에서는 플러그인이나 별도의 설치 없이도 Information Protection 민감도 레이블 및 정책을 PDF에 기본적으로 적용하고 편집할 수 있습니다.

보호 모드

Adobe는 PDF 포맷을 악용해 컴퓨터 파일 시스템에서 쓰기 또는 읽기를 시도하는 악성 코드로부터 고객을 보호하기 위해 최첨단 샌드박스 기술을 구현한 보호 모드를 제공합니다.

Adobe Reader의 보호 모드는 컴퓨터 시스템에 악성 코드를 설치하려고 시도하는 침입자로부터 보호할 뿐만 아니라 컴퓨터 또는 기업 네트워크에서 민감한 데이터와 지적 재산권에 액세스하여

추출하려는 악의적인 사용자를 차단합니다. 보호 모드는 사용자가 Acrobat Reader를 실행할 때마다 기본적으로 활성화되고 해당 프로그램에 부여된 액세스 수준을 제한하므로 컴퓨터 파일 시스템에서 읽고 쓰거나, 파일을 삭제하거나, 시스템 정보를 변경하려고 시도하는 악성 PDF 파일로부터 Microsoft Windows 기반의 시스템을 안전하게 보호합니다.

Acrobat Reader 보호 모드(Windows 8.1 이상)는 AppContainer에서 단독으로 실행됩니다.

제한된 보기

샌드박스는 저작권 수준이나 사용 권한 수준이 낮은 프로그램을 실행할 때 필요한 제한적인 실행 환경을 구현하는 데 사용하는 신뢰도가 높은 보안 방법으로, 실행 가능한 코드가 포함되어 신뢰할 수 없는 문서의 위협으로부터 사용자 시스템을 보호합니다. Acrobat Reader의 맥락에서 이해해 보면 신뢰할 수 없는 콘텐츠란 모든 PDF 파일은 물론 PDF 파일을 호출하는 과정까지 포괄하는 개념입니다. Reader는 모든 PDF 파일이 잠재적으로 손상되어 있다고 간주하여 PDF 파일에서 호출하는 모든 처리 과정을 샌드박스로 제한합니다. Acrobat Reader의 보호 모드와 유사한 제한된 보기는 Acrobat의 기능 강화를 위해 샌드박스 기술을 구현한 것입니다.

Acrobat에서 Adobe는 PDF 파일 포맷을 사용하여 컴퓨터 시스템에서 악성 코드를 실행하려는 쓰기 기반의 공격뿐만 아니라 PDF 파일을 통해 민감한 데이터나 지적 재산권을 도용하려는 읽기 기반의 공격까지 차단하도록 제한된 보기 기능을 확장합니다. 보호 모드와 마찬가지로 제한된 보기도 신뢰할 수 없는 프로그램(예: 모든 PDF 파일 및 PDF 파일에서 호출하는 프로세스)의 실행을 제한된 샌드박스로 한정하여 PDF 포맷을 사용하는 악성 코드가 컴퓨터의 파일 시스템에 쓰거나 파일 시스템을 읽지 못하도록 합니다. 제한된 보기는 신뢰할 수 있다고 지정한 특정 파일은 제외하고 모든 PDF 파일을 잠재적인 악성 파일로 간주하여 프로세스를 샌드박스로 제한합니다.

제한된 보기는 사용자가 독립 실행형 Acrobat 애플리케이션과 브라우저에서 PDF 문서를 열 때 모두 지원됩니다. Windows 8 이상의 경우 제한된 보기가 AppContainer에서 항상 실행되며, 이를 통해 제한된 보기 기능을 사용하는 고객에게 더욱 강력한 보안 환경을 제공합니다. 제한된 보기에서 잠재적인 악성 파일을 열면 Acrobat의 보기 창 상단에 노란색 메시지 막대(YMB: Yellow Message Bar)가 표시됩니다. YMB에 현재 파일을 신뢰할 수 없으며 제한된 보기 기능이 실행되고 있다는 메시지가 나타나며, 여러 Acrobat 기능이 비활성화되고 파일과의 상호 작용이 제한됩니다. 즉, 파일은 '읽기 전용' 모드 상태가 되고 제한된 보기가 임베드되었거나 태그로 된 악성 콘텐츠로 인한 시스템 손상을 막아줍니다.

파일을 신뢰하고 모든 Acrobat 기능을 활성화하려면 YMB에서 '모든 기능 사용' 버튼을 클릭합니다. 그러면 제한된 보기가 종료되고, Acrobat의 권한 위치 목록에 해당 파일을 추가하여 파일에 대한 신뢰를 영구적으로 부여합니다. 이후 신뢰할 수 있는 PDF 파일을 열면 제한된 보기의 각종 제한이 해제됩니다.

Adobe Document Cloud 서비스 보안

사용자 인증

관리자는 Adobe Admin Console에서 지정된 사용자 라이선스를 통해 Adobe Document Cloud에 대한 최종 사용자의 액세스 권한을 부여할 수 있습니다. Acrobat 및 Document Cloud 서비스는 Adobe ID, Business ID, Enterprise ID, Federated ID 등 4가지 유형의 사용자 지정 라이선스를 지원합니다. 이러한 ID 유형 및 Adobe ID 관리 서비스에 대한 자세한 내용은 Adobe ID 관리 서비스 보안 개요를 참조하십시오.

문서 및 사용자 생성 콘텐츠 저장

Adobe Document Cloud 서비스는 멀티테넌트 스토리지를 활용합니다. 사용자 생성 콘텐츠와 문서는 다수의 데이터 센터와 각 데이터 센터의 여러 디바이스에 중복으로 저장됩니다. 모든 네트워크 트래픽은 체계적인 데이터 인증과 검사값 계산을 거쳐 데이터 손상을 방지하고 데이터 무결성을 보장합니다. 마지막으로, 저장된 콘텐츠는 고객의 지역에 있는 다른 데이터 센터 시설에 동시에 자동 복제되므로 데이터 손실이 발생하더라도 두 위치에 저장된 데이터의 무결성이 유지됩니다.

Document Cloud에 업로드된 사용자 생성 콘텐츠와 문서는 일반적으로 ID 유형에 상관없이 데이터를 업로드한 사용자와 관련된 국가 코드에 해당하는 지역 데이터 센터에 저장됩니다.

- 북미, 중미 또는 남미 국가 코드를 가진 사용자의 경우 스토리지는 미국 버지니아에 있습니다.
- 유럽 또는 아프리카 국가 코드를 가진 사용자의 경우 스토리지는 아일랜드 더블린에 있습니다.
- 아시아 태평양 또는 중동 국가 코드를 가진 사용자의 경우 스토리지는 일본 도쿄에 있습니다.

관리자가 Adobe Admin Console을 통해 일부 Enterprise ID와 Federated ID 계정에 개별 클라우드 스토리지를 할당할 수 있지만, Document Cloud 서비스 스토리지에 저장된 모든 최종 사용자 문서나 콘텐츠에 직접 액세스할 수는 없습니다. 그러나 관리자가 사용자 계정에 대한 소유권을 관리하고 있으므로 사용자의 이용 권한을 취소할 수 있습니다. 공유 서비스 스토리지를 이용 중인 이러한 계정 유형을 삭제하면 최종 사용자는 클라우드 스토리지에 있는 모든 데이터에 액세스할 수 없게 되며, 해당 데이터는 90일 후에 삭제됩니다.

또한 관리자는 Admin Console을 사용해 Adobe ID 계정에 스토리지를 할당할 수 있으며, 관리자는 Adobe ID 계정을 제어할 수는 없지만, 계정을 삭제하는 방식으로 최종 사용자 계정에 부여된 엔터프라이즈 스토리지 할당량과 애플리케이션 및 서비스에 대한 액세스 권한을 취소할 수 있습니다. 이때도 데이터는 90일 이후에 삭제됩니다.

데이터 암호화

기본적으로 Document Cloud 서비스 사용자 생성 콘텐츠 및 문서는 HTTPS TLS 1.2 암호화를 통해 전송 중에 암호화됩니다. Document Cloud 서비스 콘텐츠는 저장되는 과정에서 각 고객과 각 고객의 도메인에 고유한 AES 256비트 대칭 보안키로 암호화됩니다. 이러한 암호화 방법은 영구 및 임시 문서 스토리지에 모두 적용됩니다.

전용 암호화 키

내장된 표준 암호화 기능 외에도 관리자는 고객 조직의 일부 또는 전체 도메인에 대한 전용 암호화 키를 사용하여 저장된 문서에 대한 또 다른 제어 및 보안 레이어를 추가할 수 있습니다. 그런 다음 해당 전용 암호화 키를 사용하여 저장된 Document Cloud 서비스 콘텐츠를 암호화할 수 있으며, 필요한 경우 Admin Console에서 취소할 수 있습니다. 암호화 키를 취소하면 모든 최종 사용자는 해당 키로 암호화된 모든 콘텐츠에 액세스할 수 없고 암호화 키가 다시 활성화될 때까지 콘텐츠를 업로드하거나 다운로드할 수 없습니다.

참고: 전용 암호화 키를 사용하여 Adobe Document Cloud 파일을 암호화할 수 있지만, 메타데이터는 암호화할 수 없습니다.

전용 키를 이용한 암호화 관리에 대한 자세한 내용은 Adobe.com을 참조하십시오.

전자 서명 및 디지털 서명

Document Cloud 서비스를 이용하면 서명을 통해 안전하게 작업할 수 있는 다양한 툴을 사용할 수 있습니다.

- **채우기 및 서명 툴** — 사용자가 PDF를 열어 양식 필드를 채우고 문서에 전자 서명할 수 있습니다.
- **인증서 툴** — 사용자가 서명 필드에 암호화 방식으로 바인딩된 디지털 인증서를 통해 문서에 전자 서명할 수 있습니다. 각 디지털 인증서(또는 디지털 ID)는 서명자를 고유하게 식별하며 Adobe AATL(Adobe Approved Trust List) 또는 EUTL(European Union Trusted List)에 나열된 TSP(Trust Service Provider) 또는 인증 기관(CA)에서 발급합니다. 인증서 툴을 사용하면 문서에 타임스탬프를 추가하고 위변조 방지 봉인을 통해 문서를 인증할 수 있습니다.

Acrobat Microsoft 통합

Adobe는 Microsoft와의 파트너십을 통해 주요 생산성 툴을 통합하여 다음 솔루션 내에서 기본적으로 Acrobat 및 Document Cloud 서비스에 액세스할 수 있습니다.

- Microsoft SharePoint 및 OneDrive
- Microsoft Teams
- Microsoft Word, Excel 및 PowerPoint(PDF 작성 및 보호만 해당)

이러한 통합을 통해 Adobe는 PDF 문서의 임시 사본만 만들고 사용자로부터 고객 정보나 개인 식별 정보를 수집하지 않습니다.

SharePoint 및 OneDrive용 Acrobat

SharePoint 및 OneDrive용 Acrobat을 통해 사용자는 Microsoft 365 내의 PDF 워크플로우에 액세스할 수 있으며 클라우드에서 PDF를 열람, 작성, 수정할 수 있습니다.

이 통합 버전의 Acrobat을 사용하면 문서가 SharePoint 또는 OneDrive의 원래 위치에 저장됩니다. 열람, 주석 추가, 검색과 같은 작업은 사용자의 기기에서 진행됩니다. 사용자가 문서를 변경하면 해당 문서가 SharePoint 또는 OneDrive 계정에 다시 저장됩니다.

사용자가 문서를 생성, 구성, 결합 또는 내보내는 경우, 임시 처리를 위해 사용자 국가 코드에 해당하는 지역의 Adobe Document Cloud 서버로 전송되며 24시간 이내에 삭제됩니다. 이 프로세스에서 문서는 전송 및 저장 시 모두 암호화된 상태로 유지됩니다('데이터 암호화' 섹션 참조). 수정된 문서는 사용자의 SharePoint 또는 OneDrive 계정에 다시 저장됩니다.

SharePoint 및 OneDrive용 Acrobat의 특정 기능에 대한 자세한 내용은 Adobe.com를 참조하십시오.

Microsoft Teams용 Acrobat

Microsoft Teams용 Acrobat을 통해 사용자는 Microsoft Teams 내의 PDF 워크플로우에 액세스할 수 있으며 클라우드에서 PDF를 열람, 작성, 수정할 수 있습니다. 고객은 Microsoft Teams용 Acrobat을 개인 탭, 봇, 탭, 메시지 작업 또는 메시지 확장 툴로 사용할 수 있습니다.

Microsoft Teams 채팅 또는 채널에서 공유된 모든 PDF는 기본적으로 사용자의 OneDrive 또는 SharePoint에 저장됩니다. 그러나 Microsoft Teams용 Acrobat을 사용하여 PDF를 공유한 다음 공동 작업(공유 주석 추가)을 하는 경우, 문서는 임시 처리를 위해 사용자 국가 코드에 해당하는 지역의 Adobe Document Cloud 서버로 전송되며 24시간 이내에 삭제됩니다. 이 프로세스에서 문서는 전송 및 저장 시 모두 암호화된 상태로 유지됩니다('데이터 암호화' 섹션 참조). 수정된 문서는 원래 위치에 다시 저장됩니다.

고객의 관리자가 Document Cloud 서비스를 비활성화하면, 최종 사용자는 자신의 문서를 미리 보고 주석을 추가할 수는 있지만 공유 주석 추가 기능을 사용하여 공동 작업할 수는 없습니다.

Microsoft Teams 통합으로 사용할 수 있는 Acrobat의 특정 기능에 대한 자세한 내용은 Adobe.com을 참조하십시오.

Word, Excel 및 PowerPoint용 Acrobat

사용자는 PDF 작성 추가 기능을 사용하여 Microsoft 365 문서를 고품질 PDF로 손쉽게 변환하고, PDF를 OneDrive에 저장하거나 개인 하드 드라이브에 다운로드할 수 있습니다. 또한 사용자는 문서에 대한 무단 액세스를 방지하기 위해 암호를 추가하여 PDF를 보호할 수 있습니다.

Adobe 보안 프로그램 개요

Adobe의 통합 보안 프로그램은 5개의 COE(Center of Excellence)로 구성되어 있으며, 각 COE는 자동화, 인공 지능(AI), 머신 러닝과 같은 신기술을 활용하여 위험을 감지하고 예방하는 방법을 지속적으로 반복하고 발전시킵니다.

그림 2. 5개의 COE(Center of Excellence)

Adobe 보안 프로그램의 COE는 다음과 같습니다.

- **애플리케이션 보안** — 제품 코드의 보안에 중점을 두고 위협 연구 수행, 보안 취약점 신고 포상제(bug bounty) 구현
- **운영 보안** — 시스템, 네트워크, 프로덕션 클라우드 시스템 모니터링 및 보호
- **엔터프라이즈 보안** — Adobe 기업 환경에 대한 보안 액세스 및 인증에 집중
- **규정 준수** — 보안 거버넌스 모델, 감사 및 규정 준수 프로그램, 위험 분석 감독
- **사고 대응** — 연중무휴 운영되는 24시간 보안 운영 센터와 위협 대응 요원

Adobe의 제품 및 서비스 보안에 집중할 수 있도록 COE는 현재의 모든 보안 노력을 조율하고 Adobe에서 보안 기술의 진화에 대한 비전을 개발하는 최고 보안 책임자(CSO)가 직접 관리합니다.

Adobe 보안 조직

투명하고, 책임감 있으며, 정보를 기반으로 하는 의사 결정 플랫폼을 토대로, Adobe 보안 조직은 단일 거버넌스 모델에 전체 보안 서비스를 통합했습니다. CSO는 최고정보책임자(CIO) 및 최고 개인정보 보호 책임자(CPO)등 고위 경영진과 긴밀하게 협력하여 보안 전략 및 운영을 조율합니다.

위에서 설명한 COE 외에도 Adobe는 법무, 개인 정보 보호, 마케팅, PR 부서의 팀원들을 보안 조직에 포함시켜, 모든 보안 관련 결정이 투명하고 책임감 있게 이루어지도록 합니다.

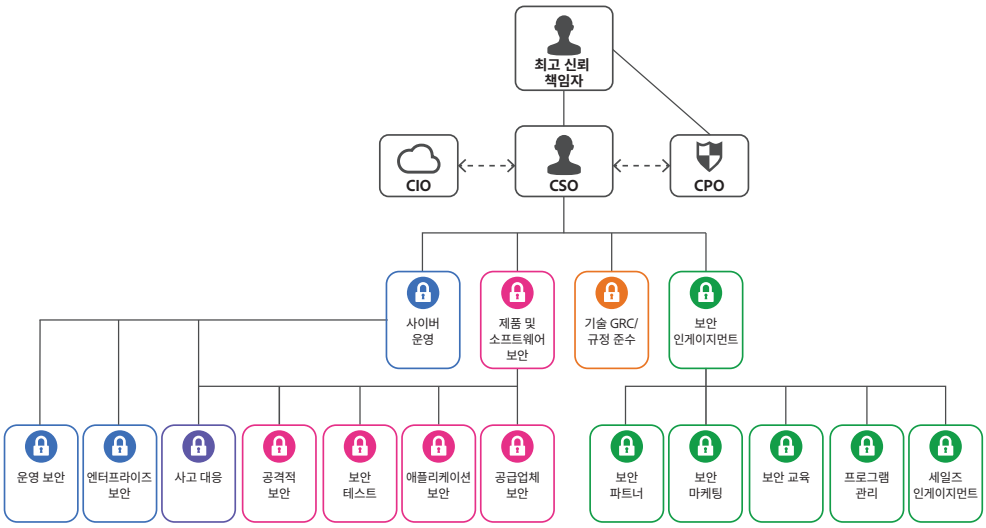


그림 3. Adobe 보안 조직

Adobe는 전사적 보안 문화의 일환으로 모든 직원이 Adobe의 보안 인식 및 교육 트레이닝을 수료해야 합니다. 매년 수료하고 재인증을 받아야 하는 트레이닝을 통해 모든 Adobe 직원이 당사의 기업 에셋뿐만 아니라 고객 및 직원 데이터를 주도적으로 보호하도록 합니다. 채용 시 엔지니어링 및 기술 운영 팀을 비롯한 기술 직원은 직책별로 마련된 심층 '도제식' 교육 프로그램에 자동 등록됩니다. Adobe의 보안 문화 및 트레이닝 프로그램에 대한 자세한 내용은 Adobe 보안 방식 백서를 참조하십시오.

Adobe 보안 제품 수명 주기

Adobe의 모든 보안 기능은 설계 및 개발에서 품질 보증, 테스트 및 배포에 이르기까지, 제품 수명 주기의 여러 단계에 통합된 Adobe 보안 제품 수명 주기(SPLC)를 기반으로 합니다. 소프트웨어 개발 작업, 프로세스, 툴을 위한 수백 가지의 보안 활동을 포괄하는 Adobe SPLC는 개발 팀이 제품 및 서비스에 보안을 구축하고 최신 업계 모범 사례를 도입하도록, 지속적인 발전에 도움이 되는 명확하고 반복 가능한 프로세스를 정의합니다.

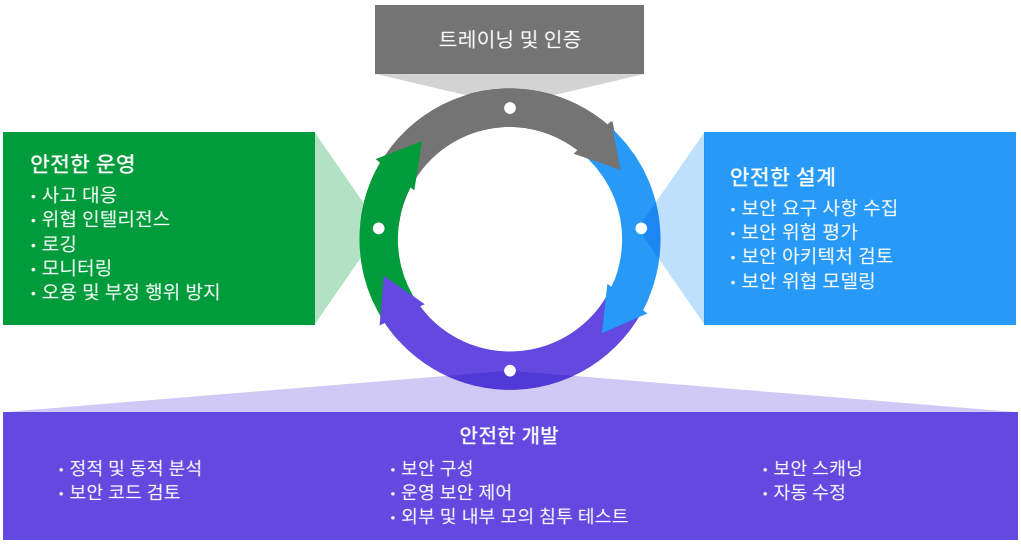


그림 4. Adobe 보안 제품 수명 주기

Adobe는 요청 시 검토할 수 있는 공개된 SPLC 표준을 유지합니다. Adobe SPLC의 구성 요소에 대한 자세한 내용은 Adobe 애플리케이션 보안 개요를 참조하십시오.

Adobe 애플리케이션 보안

Adobe에서 '강력한 보안'을 갖춘 애플리케이션을 구축하는 작업은 Adobe 애플리케이션 보안 스택에서 시작됩니다. 연구 결과와 경험에 기초한 명확하고 반복 가능한 작업에서 일관성을 유지하면서 보안 통제를 보장할 수 있도록 프로세스 자동화를 구현한 Adobe 애플리케이션 보안 스택은 개발자의 효율성을 높이고 보안상의 실수 위험을 최소화하는 데 도움이 됩니다. 자주 사용하는 코딩 패턴과 블록을 처음부터 개발할 필요가 없도록 테스트를 통과하고 사전 승인된 안전한 코딩 블록을 활용하여 개발자는 코드의 보안에 대한 우려 없이 자신의 전문 분야에 집중할 수 있습니다. 테스트, 전문 툴, 모니터링과 더불어, Adobe 애플리케이션 보안 스택은 소프트웨어 개발자가 기본적으로 안전한 코드를 생성하도록 지원합니다.

그림 5. Adobe 애플리케이션 보안 스택

또한, Adobe는 공용 클라우드 인프라 사용과 관련된 작업을 위한 표준을 포함하여 애플리케이션 보안을 다루는 여러 건의 공개 표준을 유지합니다. 이 표준은 요청 시 열람할 수 있습니다. Adobe 애플리케이션 보안에 대한 자세한 내용은 Adobe 애플리케이션 보안 개요를 참조하십시오.

Adobe 운영 보안

모든 Adobe 제품 및 서비스가 처음부터 보안 모범 사례를 염두에 두고 설계되도록 운영 보안 팀은 Adobe 운영 보안 스택(OSS)을 만들었습니다. OSS는 제품 개발자와 엔지니어가 보안 태세를 강화하고 Adobe와 고객 모두에 대한 위험을 줄이는 동시에 Adobe가 전사적으로 규정 준수, 개인 정보 보호 및 기타 거버넌스 프레임워크를 준수하도록 돕는 통합 툴 세트입니다.

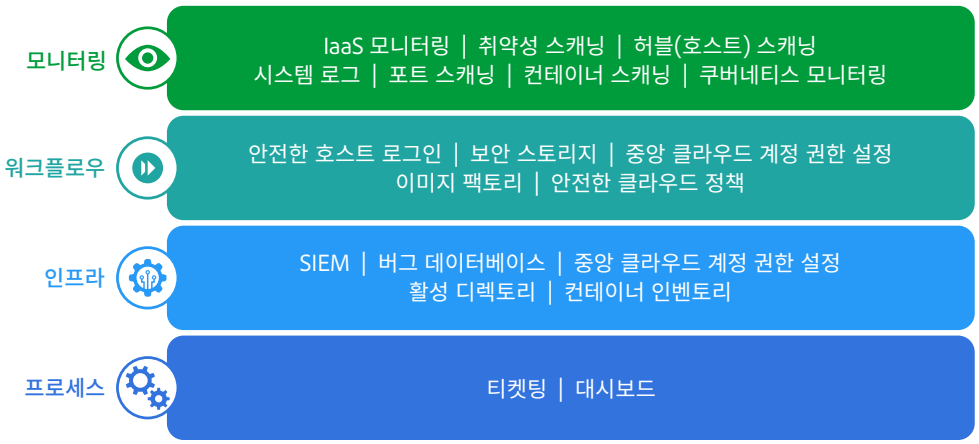


그림 6. Adobe 운영 보안 스택

Adobe는 지속적인 클라우드 운영을 다루는 몇 건의 공개 표준을 유지하며, 요청 시 열람할 수 있습니다. Adobe OSS 및 Adobe 전체에서 사용되는 특정 툴에 대한 자세한 설명은 Adobe 운영 보안 개요를 참조하십시오.

Adobe 엔터프라이즈 보안

Adobe는 제품, 서비스, 클라우드 호스팅 운영을 보호하는 것과 더불어 내부 네트워크 및 시스템, 기업 소재지, 직원, 고객 데이터의 보안을 보장하기 위해 다양한 내부 보안 제어 기능을 사용합니다.

이러한 제어를 위해 개발된 엔터프라이즈 보안 제어 및 표준에 대한 자세한 내용은 Adobe 엔터프라이즈 보안 개요를 참조하십시오.

Adobe 규정 준수

모든 Adobe 제품과 서비스는 Adobe CCF(Common Controls Framework)를 준수합니다. Adobe CCF는 보안 활동 및 규정 준수를 위한 제어 프레임워크로서 Adobe 제품 운영 팀 외에도 인프라 및 애플리케이션 팀의 다양한 업무 분야에 적용됩니다. Adobe는 최첨단 자동화 프로세스를 활용하여 규정 위반 가능성이 있는 상황을 관련 부서에 알리고 신속하게 완화 및 재정비 조치를 취하도록 지원합니다.

Adobe 제품 및 서비스는 해당 법적 표준을 충족하거나 고객이 서비스 제공업체 이용과 관련된 법적 의무를 다할 수 있도록 지원하는 방식으로 사용될 수 있습니다. 고객은 문서, 데이터 및 워크플로우에 대한 제어를 유지하며 유럽 연합의 개인 정보 보호 규정(GDPR)과 같은 해당 지역 또는 국가의 규제를 준수할 최선의 방법을 선택할 수 있습니다.

또한 Adobe는 요청 시 검토할 수 있는 규정 준수 트레이닝 및 관련 표준을 유지합니다. Adobe CCF 및 주요 인증에 대한 자세한 내용은 Adobe 규정 준수, 인증 및 표준 목록을 참조하십시오.

사고 대응

Adobe는 위험 요인과 취약점 관리, 사고 대응, 완화 및 해결 프로세스를 더욱 정확하고 신속하게 만들기 위해 위해 노력하고 있습니다. 지속적으로 위협 지형을 모니터링하고 전 세계 보안 전문가와 정보를 공유하며, 사고가 발생하는 즉시 해결하고 해당 정보를 개발 팀에 전달하여 모든 Adobe 제품 및 서비스에 최고 수준의 보안을 제공하기 위해 최선을 다하고 있습니다.

또한 요청 시 볼 수 있는 사고 대응 및 취약성 관리에 대한 내부 표준을 유지합니다. Adobe의 사고 대응 및 알림 프로세스에 대한 자세한 내용은 Adobe 사고 대응 개요를 참조하십시오.

비즈니스 연속성 및 재해 복구

Adobe 비즈니스 연속성 및 재해 복구(Business Continuity and Disaster Recovery, BCDR) 프로그램은 Adobe 제품 및 서비스의 지속적인 가용성과 지원을 보장하는 Adobe 비즈니스 연속성 계획(BCP)과 제품별 재해 복구(DR) 계획으로 구성됩니다. ISO 22301 인증을 받은 Adobe의 BCDR 프로그램은 예상치 못한 중단에 대응하고, 그 영향을 완화하며, 이를 복구하는 능력을 향상합니다. 자세한 내용은 Adobe 비즈니스 연속성 및 재해 복구 프로그램 개요를 참조하십시오.

결론

본 문서에서 설명한 보안에 대한 선제적 접근 방식과 철저한 보안 절차를 사용하면 Acrobat 및 Document Cloud 서비스와 고객의 기밀 데이터를 안전하게 보호할 수 있습니다. Adobe는 디지털 경험 데이터의 보안을 무엇보다 중요하게 생각하며 끊임없이 변화하는 위협 상황을 지속적으로 모니터링함으로써 악성 코드 침투를 예방하고, 고객 데이터를 철저하게 보호하기 위해 최선을 다하고 있습니다.

Adobe 보안에 관한 자세한 내용은 Adobe Trust Center를 참조하십시오.

이 문서에 포함된 정보는 예고 없이 변경될 수 있습니다. Adobe 솔루션, 제어 기능, 라이선스 옵션에 대한 자세한 내용은 Adobe 세일즈 담당자에게 문의하십시오.

Adobe

8/23