

Adobe Reader® 및 Adobe Acrobat®을 통해 새로운 차원의 PDF 보안 구현

Acrobat X 제품군, 업계 보안 수준을 높이다

목차

- 1: 향상된 애플리케이션 보안
- 4: 운영 체제 아키텍처와의 긴밀한 통합
- 4: 총 소유 비용(TCO) 절감
- 5: 간편해진 배포 및 관리
- 5: 콘텐츠 보안
- 6: 결론

Adobe Reader X 및 Adobe Acrobat X의 새로운 보안 기능을 사용하면 PDF 기반의 맬웨어로 인해 발생하는 위험을 줄일 수 있습니다.

Adobe Reader X 및 Adobe Acrobat X은 데이터를 비롯한 PDF 문서의 보안을 완전히 새로운 차원으로 끌어올리는데 성공했습니다. 보안을 주안점으로 두고 설계된 Adobe Reader X 및 Adobe Acrobat X은 최첨단 '샌드박스' 기술과 보다 세밀한 제어 기능, Microsoft® Windows® 및 Apple Mac OS X 운영 체제 아키텍처와의 긴밀해진 통합, 간소화된 패치 기능, 향상된 배포 및 관리 톨 덕분에 한층 강화된 애플리케이션 보안을 제공합니다. Adobe Reader X 및 Adobe Acrobat X의 새로운 기능을 사용하면 Adobe Reader X 및 Adobe Acrobat X 제품군의 이전 버전에 대한 총 소유 비용(TCO)을 줄일 수 있습니다.

또한 ASSET(Adobe Secure Software Engineering Team) 및 Adobe PSIRT(Product Security Incident Response Team)는 고객이 Adobe 제품을 사용할 때 데이터의 안전과 보안을 유지할 수 있도록 하기 위해 협력하고 있습니다. 보안을 위한 내부적인 노력 외에도 Adobe는 MAPP(Microsoft Active Protections Program)와의 긴밀한 협력 관계를 통해 백신 프로그램 판매업체나 침투 감지 및 예방 프로그램 판매업체와 같은 보안 소프트웨어 공급업체와 제품의 취약점에 대한 고급 정보를 공유하고 있으므로 업계는 서로 협력하여 Adobe Acrobat X 및 Adobe Reader X의 취약점을 줄일 수 있습니다.

향상된 애플리케이션 보안

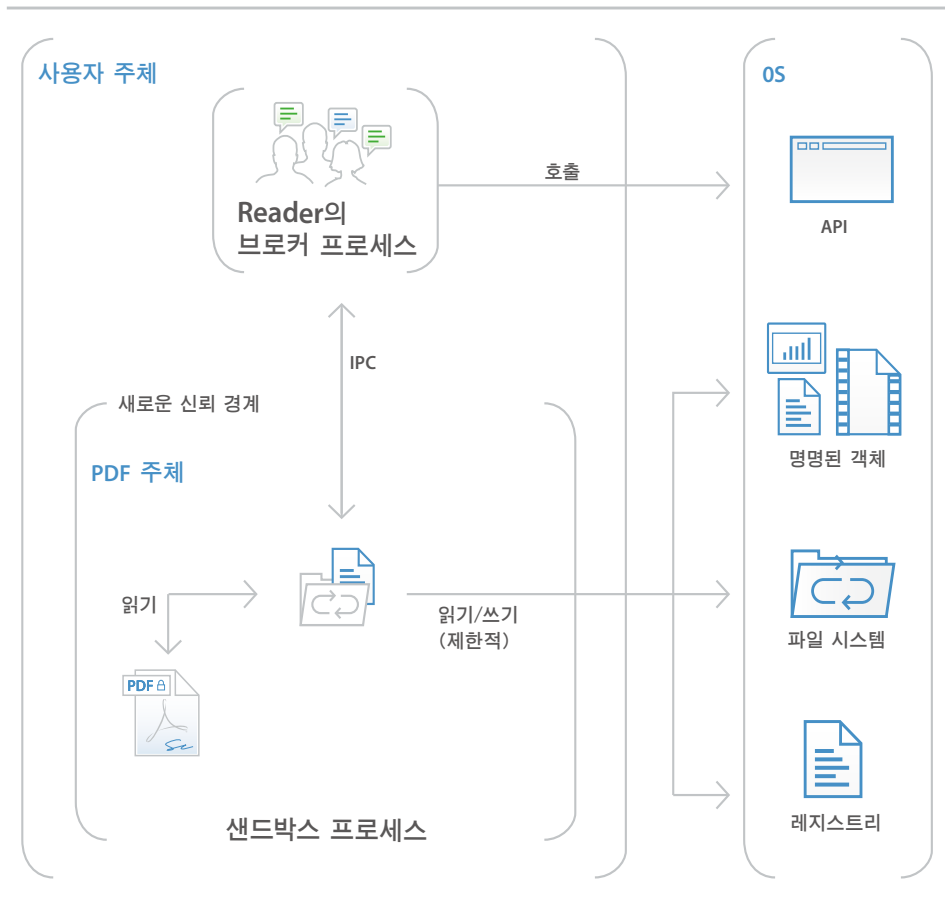
Adobe Reader X의 보호 모드

Adobe는 PDF 포맷을 악용해 컴퓨터 파일 시스템에 쓰기를 시도하는 악성 코드로부터 고객 및 고객 조직을 보호하기 위해 '샌드박스' 기술을 구현한 보호 모드를 제공합니다.

Adobe Reader X을 실행할 때마다 기본적으로 활성화되는 보호 모드는 침입자가 사용자 시스템에 맬웨어를 설치하지 못하도록 막아주므로 잠재적인 보안 위협에 따른 위험을 줄여줍니다. 특히 보호 모드는 해당 프로그램에 부여된 액세스 수준을 제한하므로 컴퓨터 파일 시스템에 쓰거나 파일을 삭제하거나 시스템 정보를 변경하려고 시도하는 악성 PDF 파일로부터 Microsoft Windows 운영 체제 기반의 시스템을 안전하게 보호합니다.

'샌드박스'란?

보안 전문가가 매우 높지 평가하는 샌드박스는 저작권 수준이나 사용 권한 수준이 낮은 프로그램을 실행하는 데 필요한 제한적인 실행 환경을 개발하는 하나의 방식입니다. 샌드박스는 실행 가능한 코드가 포함되어 신뢰할 수 없는 문서의 위협으로부터 사용자 시스템을 보호합니다. Adobe Reader의 맥락에서 이해해 보면 신뢰할 수 없는 콘텐츠란 모든 PDF는 물론이고 PDF를 호출하는 과정까지를 포괄하는 개념입니다. Adobe Reader X은 모든 PDF가 잠재적으로 손상되어 있다고 간주하여 PDF에서 호출하는 모든 처리 과정을 샌드박스로 제한합니다.



또한 Adobe SPLC(Secure Product Lifecycle) 프로세스를 통해 제품 라이프사이클의 모든 단계에 보안 기능을 통합하기 위한 노력의 일환으로 Adobe는 기존 코드를 정기적으로 검토하여 필요하다고 판단되는 경우 이를 보강하는 방식으로 Adobe 제품을 사용할 때 애플리케이션 보안과 데이터 안전을 한층 강화해 나가고 있습니다.

Adobe Acrobat X의 보호 뷰

Adobe Reader의 보호 모드와 유사한 보호 뷰는 풍부한 Adobe Acrobat 기능을 위해 샌드박스 기술을 구현한 것으로 Acrobat X 버전 10.1에서 제공됩니다. 보호 모드와 마찬가지로 보호 뷰도 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 쓰지 못하도록 합니다.

보호 뷰는 사용자가 파일을 신뢰할 수 있다고 특별히 지정하지 않는 경우 모든 PDF 파일이 잠재적으로 악성 파일이라고 간주하여 프로세스를 샌드박스로 제한합니다. 보호 뷰는 사용자가 독립 실행형 Adobe Acrobat X 애플리케이션과 브라우저에서 PDF 문서를 열 때 지원되지만 이때 사용자 경험은 약간 다릅니다.

독립 실행형 Adobe Acrobat X 애플리케이션의 보호 뷰에서 잠재적으로 해로운 파일을 열면 Acrobat의 보기 창 상단에 노란색 메시지 막대(YMB: Yellow Message Bar)가 표시됩니다. 이 막대는 파일이 신뢰할 수 없으며 사용자가 보호 뷰에 있다는 것을 나타냅니다. 즉, 많은 Acrobat 기능이 비활성화되고 파일과의 인터랙션이 제한됩니다. 기본적으로 파일은 읽기 전용 모드이며 보호 뷰는 임베드되었거나 태그로 된 악성 콘텐츠로 인한 시스템 손상을 막아줍니다. 파일을 신뢰하고 모든 Adobe Acrobat X 기능을 사용하기 위해 노란색 메시지 막대에서 "모든 기능 사용" 버튼을 클릭하면 Adobe Acrobat은 보호 뷰를 종료하고 파일을 Acrobat의 사용 권한이 부여된 목록에 추가하여 파일에 대한 영구적인 신뢰를 제공합니다. 이후 신뢰할 수 있는 PDF를 열면 보호 뷰 제한 기능이 비활성화됩니다.

브라우저에서 PDF 파일을 열면 보호 뷰는 노란색 메시지 막대가 없는 간소화된 경험을 제공합니다. 브라우저 환경에서는 모든 Adobe Reader 기능을 사용할 수 있을 뿐만 아니라 문서 작성자가 Acrobat을 사용하여 기존 양식 필드에 서명, 새 서명 필드 추가, 양식 데이터 저장 등과 같은 기능을 Reader 사용자가 이용할 수 있도록 확장하는 경우 활성화되는 기능도 사용할 수 있습니다.

Adobe JavaScript 제어 기능

Adobe JavaScript 제어 기능을 사용하면 다음을 수행할 수 있습니다.

- JavaScript 엔진 설정 또는 해제
- JavaScript에서 호출한 URL의 활성화 또는 비활성화
- 다른 사용 권한과 상관없이 권한 수준이 높은 JavaScript의 실행 제어
- 인증된 문서에서 권한 수준이 높은 JavaScript 활성화

Adobe는 파일, 폴더, 호스트 등 신뢰할 수 있는 위치에 대해서는 이러한 제한 사항을 선택적으로 우회할 수 있는 유연성을 제공합니다.

JavaScript 실행

Adobe Acrobat X 제품군은 Windows 및 Mac OS X 환경에서 JavaScript 실행을 관리하는 데 필요한 세밀하고 정밀한 제어 기능을 제공합니다. Adobe JavaScript Blacklist Framework는 비즈니스 워크플로우의 일부로 JavaScript 사용을 허용하는 동시에 특정 JavaScript API 호출을 대상으로 하는 공격으로부터 사용자와 시스템을 보호합니다.

특정 JavaScript API 호출을 블랙리스트에 추가하면 JavaScript를 완전히 비활성화시키지 않고도 이 호출이 실행되지 못하도록 할 수 있습니다. 또한 개별 사용자가 특정 JavaScript API 호출을 차단하려는 의사 결정을 재정의하지 못하게 하여 회사 전체를 악성 코드로부터 보호할 수 있습니다. Windows 환경의 경우 블랙리스트는 Windows 레지스트리에 보관되고 Mac OS X 환경의 경우 Mac OS X FeatureLockdown 파일에 저장됩니다.

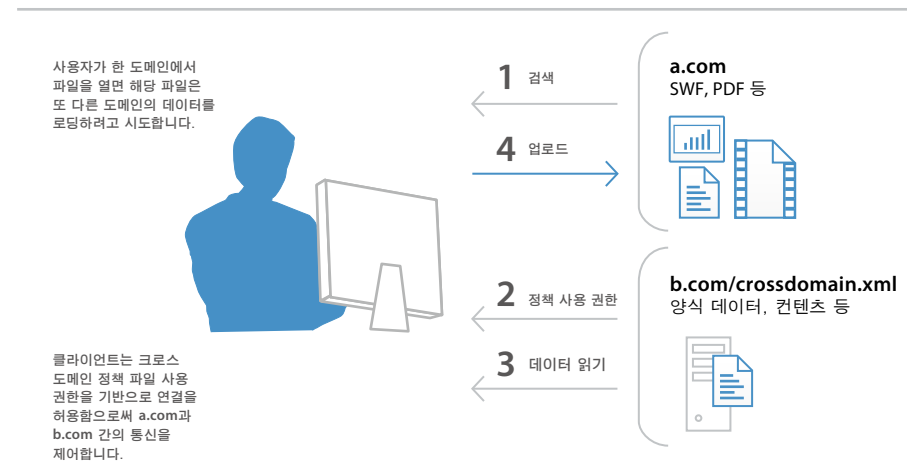
크로스 도메인 구성

기본적으로 Adobe Acrobat X 제품군은 Microsoft Windows 및 Mac OS X 클라이언트에 대한 무제한 크로스 도메인 액세스를 비활성화시킴으로써 리치 PDF 파일을 악용해 또 다른 도메인의 리소스에 액세스하려는 침입자의 시도를 봉쇄합니다.

Adobe Acrobat X 및 Adobe Reader X는 서버 기반의 크로스 도메인 정책 파일을 기본으로 지원하므로 여러 도메인에 있는 데이터를 처리할 수 있습니다. XML 문서로 된 크로스 도메인 정책 파일은 원격 도메인에서 호스팅되어 소스 도메인에 대한 액세스 권한을 부여하고 Adobe Acrobat X 또는 Adobe Reader X에 트랜잭션을 계속 수행할 수 있도록 허용합니다.

다음의 경우 Adobe 크로스 도메인 지원을 활성화해야 합니다.

- 선별적 크로스 도메인 액세스가 필요하고 디지털 인증을 기반으로 하는 인식과 같은 다른 기능을 활용하려는 경우
- 서버 기반의 단일 위치의 크로스 도메인 액세스 사용 권한을 중앙에서 관리하는 경우
- 양식 데이터, SOAP 요청, 스트리밍 미디어 참조 및 Net.HTTP 요청을 반환하기 위해 여러 도메인의 데이터 요청을 포함하고 있는 워크플로우를 구현하는 경우



사용자에게 친숙한 보안 경고

Adobe Acrobat X 제품군은 비침입형 노란색 메시지 막대(YMB)를 통해 사용자에게 친숙한 보안 경고 방식을 구현합니다. YMB는 페이지에서 콘텐츠를 보기 어렵게 만드는 기존의 대화 상자를 대체하는 것으로, 사용자는 간편하게 보안 경고를 확인하고 이에 응답할 수 있습니다.

Adobe Acrobat X 또는 Adobe Reader X 클라이언트에서 YMB는 문서 상단에 경고 또는 오류 메시지와 함께 표시됩니다. 사용자는 해당 문서를 "한 번" 또는 "항상" 신뢰할 수 있도록 선택합니다. "항상"을 선택하면 애플리케이션의 사용 권한이 있는 문서 목록에 해당 문서가 추가됩니다.

강화된 보안 기능이 활성화되었으나 PDF 파일이 아직 사용 권한이 부여된(예: 신뢰할 수 있는) 위치로 설정되어 있지 않은 경우 PDF가 다음과 같이 잠재적으로 위험한 동작을 실행하려고 할 때 YMB가 표시됩니다.

- 크로스 도메인 액세스 호출
- JavaScript 실행
- JavaScript에서 호출한 URL 호출
- 블랙리스트에 추가된 JavaScript API 호출
- 데이터 삽입
- 스크립트 삽입
- 임베드된 이전 멀티미디어 재생

사용자는 '옴션' 버튼으로 한 번 또는 항상 신뢰하도록 신속하게 설정할 수 있습니다. 전사적으로 파일, 폴더 및 호스트의 신뢰 수준을 미리 구성하여 신뢰할 수 있는 엔터프라이즈 워크플로우에 YMB가 절대로 표시되지 않도록 할 수도 있습니다.

운영 체제 아키텍처와의 긴밀한 통합

실시간 보안

Adobe Acrobat X 제품군은 Microsoft Windows 및 Mac OS X 운영 체제에서 기본으로 제공하는 실시간 보안 보호 기능을 활용하여 데스크탑 시스템을 제어하거나 메모리를 손상시키려는 공격에 대해 한층 두터운 보안 층을 형성합니다.

- DEP(Data Execution Prevention)은 데이터 또는 위험한 코드가 Windows 운영 체제에서 "보호"하도록 정의된 메모리 위치에 침투하는 것을 막아줍니다. Apple도 64비트 Safari 브라우저에서 Mac OS X 10.6을 위해 이와 유사한 실행 가능한 보호 기능을 제공하고 있습니다.
- ASLR(Address Space Layout Randomization)은 시스템 구성 요소의 메모리 및 페이지 파일 위치를 숨김으로써 침입자가 이러한 구성 요소를 찾아 공격하는 것을 차단합니다. Windows와 Mac OS X 10.6은 모두 ASLR를 사용합니다.

레지스트리 레벨 및 plist 구성

Adobe Acrobat X 제품군은 레지스트리 레벨(Windows) 및 plist(Macintosh) 환경 설정을 비롯하여 보안 설정을 관리할 수 있는 다양한 툴을 제공합니다. 이러한 설정을 활용하면 배포 전후에 클라이언트를 구성하여 다음을 수행할 수 있습니다.

- 강화된 보안 기능의 실행 또는 해제
- 사용 권한이 부여된 위치의 실행 또는 해제
- 사용 권한이 부여되도록 미리 정의된 위치 지정
- 사용자가 설정을 변경하지 못하도록 특정 기능 잠금 설정 및 애플리케이션 UI 비활성화
- 거의 모든 다른 보안 관련 기능을 비활성화, 활성화 또는 구성

총 소유 비용(TCO) 절감

소프트웨어 보안 강화

Adobe Reader 보호 모드 및 Acrobat 보호 뷰와 같은 향상된 보안 기능은 Adobe가 이미 출현한 위협과 앞으로 나타나게 될 위협으로부터 Acrobat 제품군을 보호하기 위해 단행한 광범위한 엔지니어링 투자의 두 가지 예에 불과합니다. 어떠한 공격에도 안전한 소프트웨어를 만들면 Adobe는 대역외 보안 업데이트에 대한 필요성을 줄이거나 없앨 수 있으며 정기적으로 업데이트를 제공해야 하는 절박감도 낮출 수 있습니다. 이 모든 것은 결과적으로 운영 유연성을 높이고 TCO를 줄이는 효과를 가져오며 특히 보안 요구 사항이 높은 대규모 환경에서 그 효과는 더욱 빛을 발할 것입니다.

Microsoft SCCM/SCUP 지원

Adobe Acrobat X 제품군에서는 Microsoft SCCM(System Center Configuration Manager)을 통해 업데이트를 효율적으로 가져오고 게시함으로써 관리 대상인 Windows 데스크탑에 항상 최신 보안 패치와 업데이트가 설치될 수 있도록 할 수 있습니다.

Microsoft SCUP(System Center Updates Publisher) 카탈로그에 대한 새로운 지원을 활용하여 조직 전체에 Adobe Acrobat X과 Adobe Reader X 소프트웨어를 자동으로 업데이트할 뿐만 아니라 초기 소프트웨어 배포를 간소화할 수도 있습니다. SCUP는 Adobe에서 업데이트를 제공하는 대로 바로 자동으로 가져오므로 Adobe Acrobat X 및 Adobe Reader X 배포를 보다 간편하고 효율적으로 업데이트할 수 있습니다. 패치는 전사적으로 보다 빠르고 간단하게 제공되므로 SCCM/SCUP와의 새로운 통합 기능을 사용하면 Adobe 소프트웨어의 TCO를 줄이는 데 도움이 됩니다.

Apple Package Installer 및 Apple Remote Desktop 지원

Adobe는 Adobe Acrobat X 제품군에서 독점적인 Adobe 설치 프로그램이 아니라 Mac OS X에서 제공하는 표준 Apple Package Installer를 구현했습니다. 이제 Apple Remote Desktop 관리 소프트웨어를 사용하여 중앙에서 초기 소프트웨어 배포와 이후 업그레이드 및 패치를 관리할 수 있기 때문에 기업에서 사용되고 있는 Macintosh 데스크탑에 Adobe Acrobat 및 Reader 소프트웨어를 훨씬 간편하게 배포할 수 있게 되었습니다.

간편해진 배포 및 관리

정기적으로 제공되는 누적 업데이트 및 패치

소프트웨어를 최신 상태로 유지하기 위해 Adobe는 기능 업그레이드와 보안 픽스가 모두 포함되어 있는 업데이트를 정기적으로 제공하고 있습니다. 또한 제로데이 공격에 발 빠르게 대처하기 위해 필요한 경우 비정기적인 패치를 제공합니다. 뿐만 아니라 Adobe는 시스템을 최신 상태로 유지하는 데 필요한 노력과 비용을 줄이기 위해 누적 패치를 가능한 한 많이 활용하고 있으며 출시 전에 보안 패치를 철저히 테스트함으로써 기존 설치된 제품 및 워크플로우와의 호환성을 보장하기 위해 노력하고 있습니다.

또한 Adobe는 다음 보안 웹 사이트 및 알림 서비스를 제공합니다.

Adobe 제품에 대한 최신 보안 게시판 및 권고 조치를 살펴보려면 www.adobe.com/kr/support/security를 참조하십시오.

최신 보안 장애 보고서 및 취약점 수정 사항을 확인하려면 Adobe PSIRT 블로그(blogs.adobe.com/psirt/)를 참조하십시오.

Adobe 제품 및 보안 기능에 대한 자세한 내용은 Adobe Security Library(www.adobe.com/go/learn_acr_appsecurity_en)를 참조하십시오.

Adobe 사용자 정의 마법사 및 AIM

전사적 배포에 대한 보다 높은 수준의 제어를 위해 Adobe는 다음과 같은 툴을 제공합니다.

- Adobe 사용자 정의 마법사 - 배포하기 전에 Acrobat 설치 프로그램을 원하는 대로 변경하고 애플리케이션 기능을 구성할 수 있으며 무료로 다운로드하여 사용하는 유틸리티입니다.
- AIM(Administrator's Information Manager) - Preference Reference가 포함되어 있고 원하는 대로 변경할 수 있으며 자동으로 업데이트되는 Adobe AIR® 애플리케이션입니다. AIM에는 엔터프라이즈 관리자에게 유익한 리소스 목록이 포함되어 있습니다.

컨텐츠 보안

Adobe는 애플리케이션 보안 외에도 디지털 서명, 저작권 관리, 문서 모범 사례 등 PDF 문서에 저장되는 정보를 안전하게 보호하고 인증할 수 있도록 다양한 업계 표준의 메커니즘을 지원합니다.

디지털 서명

디지털 서명은 "잉크" 서명에 비해 시간 및 비용 절감 효과가 있을 뿐만 아니라 문서 작성자 및 수신자는 이를 통해 문서 내용의 무결성과 진정성을 보장받을 수 있습니다. Adobe Reader X 및 Adobe Acrobat X을 사용하면 문서에 표준 기반의 디지털 서명을 손쉽게 추가할 수 있고 해당 서명의 진위를 검사할 수 있으며 사용 권한과 제약 사항을 추가하여 서명 워크플로우를 제어할 수 있습니다.

저작권 관리

Adobe Acrobat X 제품군은 Adobe LiveCycle® Rights Management ES2 소프트웨어와의 연동을 통해 기밀 데이터 또는 기타 중요한 정보가 조직 외부로 유출되거나 악의적인 사용자에게 넘어가는 것을 방지할 수 있는 저작권 관리 기능을 제공합니다. 이 기능을 통해 문서 액세스, 인쇄, 복사, 편집 등을 문서, 사용자 또는 그룹 레벨로 제어할 수 있으며 문서가 이용되는 동안 언제든지 이 정책을 동적으로 변경할 수 있습니다. 뿐만 아니라 Adobe Reader 사용자는 이 콘텐츠를 안전하게 액세스할 수 있으므로 추가 제품 또는 플러그인을 구입하거나 다운로드하지 않고도 보호 대상 문서를 손쉽게 볼 수 있습니다.

일관된 모범 사례

Adobe Acrobat X의 새로운 동작 마법사 기능을 사용하면 문서 프로세스를 스크립트로 손쉽게 작성하여 조직 전체에 배포할 수 있으므로 공개 문서를 준비하고 보호할 때 모든 사용자가 모범 사례에 따라 수행할 수 있습니다.

중요한 정보 관리

사용자는 하나의 버튼으로 실행할 수 있는 문서의 기밀 정보 가리기 툴과 향상된 교정 툴을 사용하여 파일에서 중요한 정보를 신속하게 제거할 수 있습니다. 또한 표준 기반의 강력한 암호화 기술을 통해 모든 PDF 문서에 대한 액세스를 제어하거나 변경을 금지할 수 있는 암호 및 사용 권한을 설정할 수 있습니다.

결론

Adobe는 Adobe Acrobat X 제품군을 통해 새로운 차원의 PDF 문서 및 데이터 보안 기능을 제공합니다. 향상된 애플리케이션 보안에서부터 보다 세밀한 제어 기능, 운영 체제와의 긴밀해진 통합에 이르기까지 Adobe Acrobat X 및 Adobe Reader X은 보안에 주안점을 두고 개발된 제품입니다. Adobe Reader X 및 Adobe Acrobat X 사용자는 향상된 애플리케이션 보안, 운영 체제와의 긴밀해진 통합, 간소화된 패치 기능, 향상된 배포 및 관리 툴 덕분에 이전 버전의 Adobe Reader 및 Adobe Acrobat 제품과 비교해 크게 줄어든 TCO를 경험할 수 있습니다.

또한 Adobe Acrobat X 및 Adobe Reader X은 Adobe의 제품 보안 전문가 팀인 ASSET(Adobe Secure Software Engineering Team)의 지원을 받고 있습니다. ASSET은 사용자가 Adobe 제품을 사용할 때 데이터의 안전과 보안을 유지할 수 있도록 하기 위해 Adobe PSIRT(Product Security Incident Response Team)와 협력하고 있습니다.

자세한 내용

솔루션 세부 정보: www.adobe.com/kr/security

