



# 借助 Adobe Reader® 和 Adobe Acrobat® 使 PDF 安全性更上一层楼

## Acrobat X 产品系列提高了标准

### 目录

- 1: 改进后的应用程序安全性
- 3: 与操作系统架构更紧密的集成
- 3: 更低的总拥有成本
- 4: 更轻松的部署和管理
- 4: 内容安全性
- 5: 结论

Adobe Reader X 和 Adobe Acrobat X 将 PDF 文档和数据的安全性提到了一个全新高度。Adobe Reader X 和 Adobe Acrobat X 在设计时始终谨记安全性, 借助最新的“沙箱”技术以及更细化的控件、与 Microsoft® Windows® 及 Apple Mac OS X 操作系统架构更紧密的集成、简化的补丁程序功能以及经过改进的部署和管理工具实现了更高的应用程序安全性。与先前版本的 Adobe Reader X 和 Adobe Acrobat X 产品相比, Adobe Reader X 和 Adobe Acrobat X 中的新增功能使用户能体验到更低的总拥有成本 (TCO)。

Adobe 安全软件设计小组 (ASSET) 和 Adobe 产品安全应急响应小组 (PSIRT) 还联手确保使用 Adobe 产品时用户数据的安全性。作为我们内部安全工作的补充, Adobe 还加入了 Microsoft 主动保护计划 (MAPP), 这有助于促进与杀毒、入侵检测和预防供应商等安全软件提供商的产品漏洞信息共享, 使整个行业能齐心协力减少 Adobe Acrobat X 和 Adobe Reader X 中的漏洞风险。

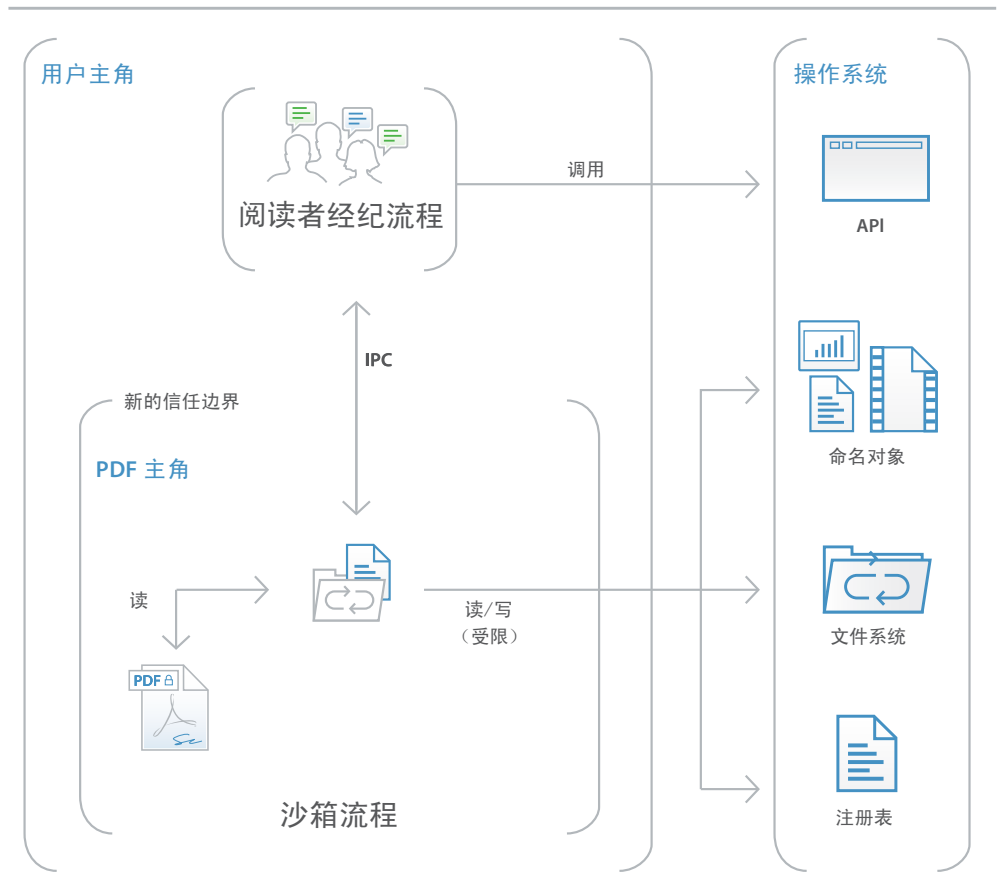
### 改进后的应用程序安全性

Adobe Reader X 和 Adobe Acrobat X 中新增的安全功能有助于降低基于 PDF 的恶意软件造成的风险。

#### Adobe Reader X 中的保护模式

恶意代码会试图使用 PDF 格式写入计算机的文件系统, 为了保护您和贵组织避免这些破坏, Adobe 提供保护模式, 它采用了“沙箱”技术。

每当您启动 Adobe Reader X 时都会默认启用这一模式, 它有助于防止攻击者在用户系统上安装恶意软件, 从而降低了潜在安全威胁造成的风险。具体而言, 保护模式限制了授予程序的访问级别, 保护运行 Microsoft Windows 操作系统的系统避开恶意 PDF 文件, 这些文件可能会试图写入计算机的文件系统、删除文件或通过其他方式修改系统信息。



什么是“沙箱”？

沙箱在安全专业人士中备受青睐，它是一种创建有限执行环境的方法，用户可以在该环境中以较低的权限运行程序。沙箱可以保护用户的系统免遭包含可执行代码的不信任文档的破坏。在 Adobe Reader 环境中，不信任内容可以是任何 PDF 及其调用的进程。Adobe Reader X 将所有 PDF 视为可能受损并将 PDF 调用的所有处理限制在沙箱中。

此外，作为公司通过 Adobe 安全产品生命周期 (SPLC) 流程将安全性集成到产品生命周期的每个阶段的不懈努力的一部分，Adobe 会定期评估现有代码并酌情固化，从而进一步提高了应用程序安全性以及使用 Adobe 产品时的数据安全性。

### Adobe Acrobat X 中的保护视图

与 Adobe Reader 中的保护模式相似，保护视图也采用针对丰富的 Adobe Acrobat 功能集的沙箱技术，Acrobat X 版本 10.1 开始提供此视图。与保护模式一样，保护视图将不可信程序（如，它调用的任何 PDF 文件和进程）的执行限制在沙箱内，防止使用 PDF 格式的恶意代码写入计算机文件系统。

保护视图认为所有 PDF 文件都可能是恶意文件，它将处理操作限制在沙箱中，直至您指出某个文件是可信的。虽然当用户在独立的 Adobe Acrobat X 应用程序和浏览器中打开 PDF 文档时，两者都支持保护视图，但是这两种情况下的用户体验略有不同。

在独立的 Adobe Acrobat X 应用程序中，当您在保护视图中打开一个潜在恶意文件时，Acrobat 会在查看窗口顶部显示一个黄色消息栏 (YMB)。它表示此文件不可信，同时提醒您目前处于保护视图模式，因此会禁用许多 Acrobat 功能并限制用户与此文件的交互。文件基本上处于只读模式，并且保护视图会防止任何嵌入式或随标记一起的恶意内容篡改系统。要信任此文件并启用所有 Adobe Acrobat X 功能，您可以单击 YMB 中的“启用所有功能”按钮，此时 Adobe Acrobat 将退出保护视图，通过将这个文件加入 Acrobat 的特权位置列表为它提供永久信任。之后每次打开信任的 PDF 文件时都会解除保护视图限制。

在浏览器中打开 PDF 文件时，保护视图提供一种不需要黄色消息栏的简化体验。浏览器环境提供所有 Adobe Reader 功能以及文档作者使用 Acrobat 将功能扩展到 Reader 用户时的功能，其中包括签署现有表单字段、添加新的签名字段、保存表单数据等。

### Adobe JavaScript 控件

您还可以使用 Adobe JavaScript 控件：

- 开启或关闭 JavaScript 引擎
- 启用或禁用 JavaScript 调用的 URL
- 控制高特权 JavaScript 的执行（无论其他权限如何）
- 启用认证文档中的高特权 JavaScript

Adobe 使您能为包括文件、文件夹和主机在内的信任位置灵活选择跳过这些限制。

### JavaScript 执行

Adobe Acrobat X 产品系列为管理 Windows 和 Mac OS X 环境中的 JavaScript 执行提供了精良、细化的控制。Adobe JavaScript Blacklist Framework 允许将 JavaScript 用作业务工作流程的一部分，同时保护用户和系统免遭针对特定 JavaScript API 调用的攻击。

通过将特定 JavaScript API 调用加入黑名单，您无需完全禁用 JavaScript 就可以阻止这些调用的执行。您还可以防止个别用户覆盖阻止特定 JavaScript API 调用的决策，这有助于保护整个企业免受恶意代码的攻击。在 Windows 环境中，通过 Windows 注册表维护黑名单；在 Mac OS X 环境中，黑名单存储在 Mac OS X FeatureLockdown 文件中。

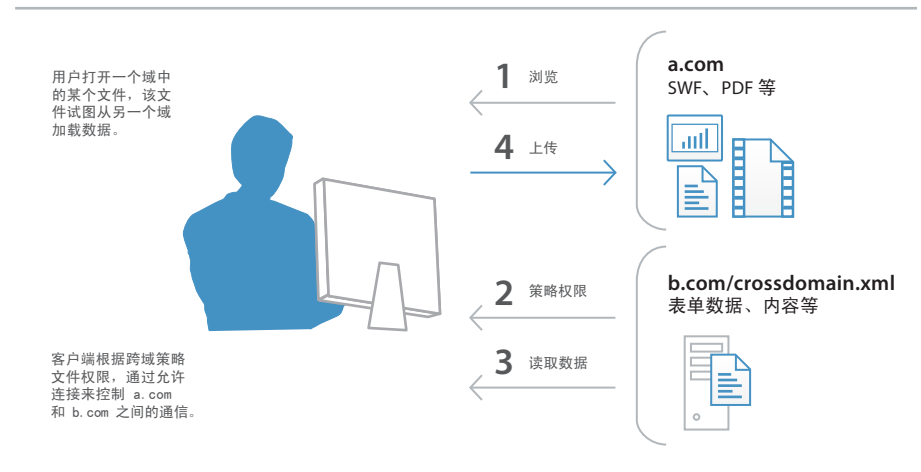
### 跨域配置

默认情况下，Adobe Acrobat X 产品系列会禁止 Microsoft Windows 和 Mac OS X 客户端不受限制的跨域访问，从而防止攻击者利用各种 PDF 文件访问另一个域中的资源。

利用服务器端跨域策略文件的内建支持，您可以允许 Adobe Acrobat X 和 Adobe Reader X 跨域处理数据。这个跨域策略文件是一个 XML 文档，它存储在远程域中，该文件将授予对源域的访问权并允许 Adobe Acrobat X 或 Adobe Reader X 继续事务。

在以下情况下，您希望启用 Adobe 跨域支持：

- 需要选择性跨域访问并希望利用基于数字证书的认识等其他功能；
- 需要从一个基于服务器的位置集中管理跨域访问权限；
- 采用的工作流程包含多个域返回表单数据、SOAP 请求、流媒体引用和 Net.HTTP 请求的数据请求。



## 用户友好型安全警报

Adobe Acrobat X 系列通过一种非侵入式的黄色消息栏 (YMB) 采用用户友好型安全警报方法。YMB 取代了传统的对话框, 因为对话框会遮挡住页面内容, 而 YMB 使用户能更轻松地查看警报并采取措施。

在 Adobe Acrobat X 或 Adobe Reader X 客户端中, YMB 在文档顶部显示警报或错误消息。用户可以选择“一次”或“始终”信任文档。选择“始终”会将文档加入应用程序的特权文档列表。

当启用增强安全性并且 PDF 尚未设置为特权 (如信任) 位置, 则 PDF 试图执行可能存在风险的操作时会显示 YMB, 包括:

- 调用跨域访问
- 运行 JavaScript
- 调用 JavaScript 调用的 URL
- 调用黑名单中的 JavaScript API
- 注入数据
- 注入脚本
- 播放嵌入的旧版多媒体

“选项”按钮允许用户设置信任, 共有实时、一次或始终三个选项。在企业中, 您还可以预先配置文件、文件夹和主机的信任级别, 这样 YMB 始终不会出现在信任的企业工作流程中。

## 与操作系统架构更紧密的集成

### 始终开启的安全性

为了进一步抵御试图控制桌面系统或破坏内存的攻击, Adobe Acrobat X 产品系列充分利用了 Microsoft Windows 和 Mac OS X 操作系统中始终开启的内建安全保护。

- 数据执行保护 (DEP) 可以防止将数据或危险代码放入 Windows 操作系统定义为“受保护的”内存位置。Apple 在 64 位 Safari 浏览器中为 Mac OS X 10.6 提供相似的可执行文件保护。
- 地址空间布局随机化 (ASLR) 可以隐藏系统组件的内存和页面文件位置, 使攻击者难以找到并瞄准那些组件。Windows 和 Mac OS X 10.6 都使用 ASLR。

### 注册表级别和 plist 配置

Adobe Acrobat X 产品系列提供各种用于管理安全性设置的工具, 其中包括注册表级别 (Windows) 和 plist (Macintosh) 首选项。借助这些设置, 您可以通过在部署前后配置客户端实现以下目的:

- 开启或关闭增强的安全性
- 开启或关闭特权位置
- 指定预先定义的特权位置
- 锁定特定功能并禁用应用程序 UI, 使最终用户无法更改设置
- 禁用、启用和以其他方式配置几乎任何其他安全性相关功能

## 降低总拥有成本

### 增强软件安全性

Adobe Reader 保护模式和 Acrobat 保护视图等安全性增强只是 Adobe 大力投资设计、增强 Acrobat 产品系列在当前和新兴威胁抵御能力的两个例子。通过提高软件对攻击尝试的抵御能力, Adobe 可以减少、甚至消除计划外安全更新的需求并降低定期更新的紧迫性。所有这些提高了操作灵活性, 降低了总拥有成本, 对于安全要求较高的大型环境尤为如此。

## Microsoft SCCM/SCUP 支持

借助 Adobe Acrobat X 产品系列,您可以通过 Microsoft System Center Configuration Manager (SCCM) 高效导入和发布更新,确保受管 Windows 桌面始终使用最新的安全补丁程序和更新。

新增的 Microsoft System Center Updates Publisher (SCUP) 目录支持使您能在整个组织内实现 Adobe Acrobat X 和 Adobe Reader X 软件的自动更新并简化最初软件部署。SCUP 可以在第一时间自动导入 Adobe 发布的任何更新,令 Adobe Acrobat X 和 Adobe Reader X 部署更新更轻松、高效。新增的 SCCM/SCUP 集成有助于降低 Adobe 软件的总拥有成本,因为补丁程序可以更简单、更快地在整个组织中推广。

## Apple Package Installer 和 Apple Remote Desktop 支持

在 Adobe Acrobat X 产品系列中,Adobe 已采用 Mac OS X 提供的标准 Apple Package Installer,不再使用专用的 Adobe Installer。这使得在企业中将 Adobe Acrobat 和 Acrobat Reader 软件部署到 Macintosh 桌面变得更轻松,因为您现在可以使用 Apple Remote Desktop 管理软件从一个中央位置管理最初的软件部署以及后续升级和补丁程序。

## 更轻松的部署和管理

### 累积、定期更新和补丁程序

为了帮助您确保软件处于最新状态,Adobe 主动提供包含功能升级和安全修复的定期更新。为了对零日攻击作出快速回应,Adobe 可以根据需要提供临时补丁程序。Adobe 还通过尽可能地利用累积补丁减少保持系统最新所需的工作和成本,同时在发布前积极测试安全补丁程序,帮助用户确保它们与现有安装及工作流程的兼容性。

Adobe 还提供以下安全性网站和通知服务:

要查看 Adobe 产品的最新安全公告和建议,请访问 [www.adobe.com/cn/support/security/](http://www.adobe.com/cn/support/security/)

您可以访问 Adobe PSIRT 博客 ([blogs.adobe.com/psirt/](http://blogs.adobe.com/psirt/)) 了解最新安全事故报告和漏洞修复

有关 Adobe 产品和安全性功能的进一步详细信息,请访问 Adobe 安全库 ([www.adobe.com/go/learn\\_acr\\_appsecurity\\_cn](http://www.adobe.com/go/learn_acr_appsecurity_cn))

### Adobe 自定义向导和 AIM

为了增强对企业内部部署的控制,Adobe 提供以下工具:

- Adobe 自定义向导—这是一个可下载的自由实用程序,它允许您在部署前自定义 Acrobat Installer 和配置应用程序功能;
- 管理员信息管理器 (AIM)—这是一个自动更新、可自定义、包含首选项参考的 Adobe AIR® 应用程序。AIM 还包含一个企业管理员感兴趣的其他资源的列表,这个列表不断扩大。

## 内容安全性

除了应用程序安全性,Adobe 还支持一套行业标准机制,它们有助于确保和认证 PDF 文档中存储的信息,包括数字签名、版权管理和文档最佳做法。

### 数字签名

与“原始”签名相比,数字签名省时省钱,并且可以帮助文档作者及接收方确保接收到完整、真实的文档内容。借助 Adobe Reader X 和 Adobe Acrobat X,您可以将基于标准的数字签名轻松添加到文档中,通过检查签名核对有效性,通过添加权限和限制控制签名工作流程。

### 版权管理

Adobe Acrobat X 产品系列可与 Adobe LiveCycle® Rights Management ES2 软件一起提供版权管理功能,使您能防止机密数据或其他敏感信息泄漏到组织以外或落入坏人之手。您可以借助它在文档、用户或组级别控制访问、打印、复制和编辑,并在文档的整个生命周期内动态更改那些策略。此外,因为使用 Adobe Reader 的任何用户可以安全访问这些内容,所以查看受保护的文档更简单并且接收方不需要购买或下载其他产品或插件。

### 一致的最佳做法

Adobe Acrobat X 中新增的“操作向导”功能使您能轻松编写文档流程并在整个组织内部署它们,这有助于确保所有用户在准备和保护对外文档时都遵循最佳做法。

## 管理敏感信息

用户可以使用一键式清理和增强的修订工具一致、快速地删除文件中的敏感信息。功能强大、基于标准的加密技术使最终用户能通过设置密码和权限控制任何 PDF 文档的访问或阻止用户更改它们。

## 结论

借助 Adobe Acrobat X 产品系列, Adobe 将 PDF 文档以及您的数据的安全性提到了一个全新高度。从改进的应用程序安全性和更细化的控制, 到更紧密的操作系统集成, Adobe Acrobat X 和 Adobe Reader X 在设计过程中时刻谨记安全性。由于更高的应用程序安全性、更紧密的操作系统集成、简化的补丁功能以及经过改进的部署和管理工具, Adobe Reader X 和 Adobe Acrobat X 用户可以体验到比先前版本的 Adobe Reader 和 Adobe Acrobat 产品更低的总拥有成本。

并且, Adobe Acrobat X 和 Adobe Reader X 得到 Adobe 产品安全专家小组 Adobe 安全软件工程小组 Team (ASSET) 的支持。ASSET 与 Adobe 产品安全事故响应小组 (PSIRT) 携手确保使用 Adobe 产品时用户数据的安全性。

## 有关更多信息

解决方案详细信息: [www.adobe.com/cn/security](http://www.adobe.com/cn/security)

