

Höhere Sicherheit von PDFs mit Adobe Reader® und Adobe Acrobat®

Die Acrobat X-Familie setzt neue Maßstäbe

Inhalt

- 1: Verbesserte Anwendungssicherheit
- 4: Engere Integration mit Systemarchitekturen
- 5: Niedrigere Gesamtbetriebskosten
- 5: Einfachere Bereitstellung und Verwaltung
- 6: Inhaltssicherheit
- 6: Fazit

Die neuen Sicherheitsfunktionen in Adobe Reader X und Adobe Acrobat X reduzieren das Sicherheitsrisiko durch PDF-basierte Schad-Software.

Adobe Reader X und Adobe Acrobat X enthalten wichtige Verbesserungen zugunsten von mehr Sicherheit für Adobe PDF-Dokumente – und damit Ihre Daten. Bei der Entwicklung von Reader X und Acrobat X stand die Anwendungssicherheit im Vordergrund. Zu diesem Zweck wurde die fortschrittliche „Sandbox“-Technologie eingeführt. Neue Funktionen sorgen für feinere Steuerungsmöglichkeiten. Die Implementierung von Patches wurde optimiert, die Integration mit Microsoft® Windows® bzw. Mac OS X vertieft. Für Bereitstellung und Verwaltung stehen erweiterte Werkzeuge zur Verfügung. Damit können Anwender von Reader X und Acrobat X im Vergleich zu früheren Versionen die Gesamtbetriebskosten verringern.

Das Adobe Secure Software Engineering Team (ASSET) und das Adobe Product Security Incident Response Team (PSIRT) arbeiten gemeinsam an Funktionen, Ihre Daten bei der Verwendung von Adobe-Produkten sicher zu machen. Als Ergänzung zu unseren internen Sicherheitsbemühungen engagiert sich Adobe auch beim Microsoft Active Protections Program (MAPP). MAPP bietet Vorabinformationen über Produktschwachstellen für Anbieter von Sicherheits-Software, wie Antivirus-Programme und Lösungen zur Erkennung und Verhinderung von Angriffen.

Verbesserte Anwendungssicherheit

Geschützter Modus in Adobe Reader X

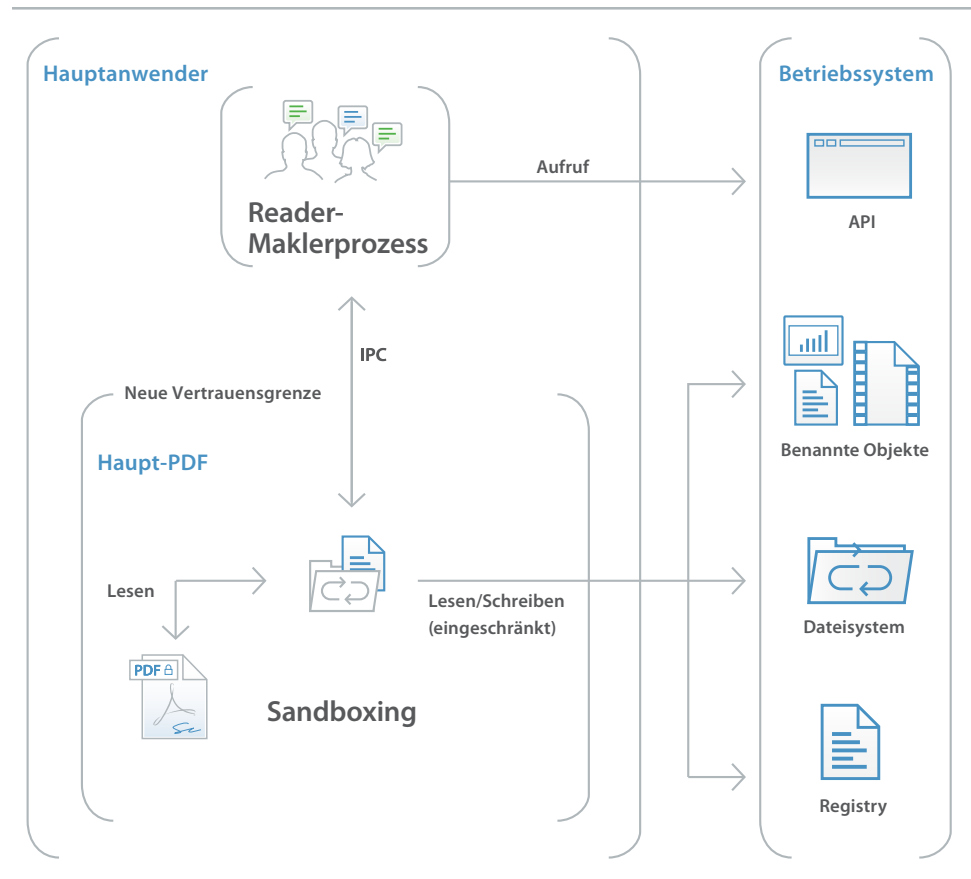
Um Sie und Ihre Organisation vor Schad-Software zu schützen, die versucht, mithilfe von PDF-Dateien das Dateisystem Ihres Computers zu manipulieren, bietet Adobe den geschützten Modus, eine Implementierung der fortschrittlichen Sandbox-Technologie.

Der geschützte Modus wird standardmäßig beim Starten von Adobe Reader X aktiviert und trägt dazu bei, Angreifer zu hindern, Schad-Software auf dem Anwendersystem zu installieren, wodurch das Risiko von Sicherheitsbedrohungen reduziert wird. Insbesondere schränkt der geschützte Modus die Zugriffsrechte für das Programm ein, sodass Systeme, die mit dem Windows-Betriebssystem laufen, vor böswilligen PDF-Dateien geschützt werden, die gegebenenfalls versuchen, in das Dateisystem des Computers zu schreiben, Dateien zu löschen oder auf andere Weise Systemdaten zu verändern.

Darüber hinaus führt Adobe im Rahmen seiner Bemühungen, mithilfe von Adobe Secure Product Lifecycle (SPLC) Sicherheit auf jeder einzelnen Stufe der Produktlebensdauer zu integrieren, regelmäßig Prüfungen des bestehenden Codes durch und schottet ihn gegebenenfalls ab, um die Anwendungssicherheit noch weiter zu verbessern und die Sicherheit Ihrer Daten zu erhöhen, wenn Sie mit Adobe-Produkten arbeiten.

Was ist „Sandboxing“?

„Sandboxing“ wird von Sicherheitsfachleuten hoch geschätzt. Es handelt sich um eine Methode, eine abgegrenzte Umgebung mit eingeschränkten Rechten für die Ausführung von Programmen zu schaffen. Sandboxing schützt das System des Anwenders vor Angriffen von nicht vertrauenswürdigen Dokumenten, die ausführbaren Code enthalten. Im Kontext von Adobe Reader gelten alle PDF-Dateien und die Prozesse, die sie aufrufen, als nicht vertrauenswürdige Inhalte. Adobe Reader X behandelt alle Adobe PDF-Dokumente als potenziell schädlich und beschränkt alle Prozesse, die die Adobe PDF-Datei aufruft, auf die Sandbox.



Geschützte Ansicht in Adobe Acrobat X

Ähnlich wie der geschützte Modus in Adobe Reader ist die geschützte Ansicht in Acrobat X Version 10.1 eine Implementierung der Sandbox-Technologie. Sie beschränkt die Ausführung nicht vertrauenswürdiger Programme (z. B. eine Adobe PDF-Datei mit von ihr aufgerufenen Prozessen) auf eine isolierte Umgebung – die „Sandbox“ –, um zu verhindern, dass schädlicher Code in der Datei den Rechner beeinträchtigt.

Bei der geschützten Ansicht wird davon ausgegangen, dass alle Adobe PDF-Dateien potenziell schädlich sind. Daher wird jede Ausführung auf die Sandbox beschränkt, es sei denn, Sie haben eine Datei als vertrauenswürdig gekennzeichnet. Dieser Schutz beim Öffnen von Adobe PDF-Dokumenten steht sowohl in Adobe Acrobat X als auch im Browser zur Verfügung; das Anwendererlebnis ist jedoch unterschiedlich.

In Adobe Acrobat X wird oben im Anzeigefenster eine gelbe Meldungsleiste eingeblendet, sobald Sie eine potenziell schädliche Datei in der geschützten Ansicht öffnen. Diese Leiste weist darauf hin, dass eine nicht vertrauenswürdige Datei in der geschützten Ansicht geöffnet wurde, in der viele Acrobat-Funktionen deaktiviert und die Möglichkeiten der Interaktion mit der Datei eingeschränkt sind. Die Datei ist schreibgeschützt. Eingebettete oder verknüpfte schädliche Inhalte können in Ihr System nicht eindringen. Um die Datei als vertrauenswürdig zu kennzeichnen und alle Funktionen von Adobe Acrobat X zu aktivieren, klicken Sie auf „Alle Funktionen aktivieren“ in der Meldungsleiste. Adobe Acrobat schaltet daraufhin die geschützte Ansicht aus und fügt die Datei zur Liste vertrauenswürdiger Quellen bzw. Elemente hinzu. Ab dem nächsten Öffnen dieser Datei gelten nicht mehr die Einschränkungen der geschützten Ansicht.

Wenn Sie eine Adobe PDF-Datei in der geschützten Browser-Ansicht öffnen, ist die gelbe Meldungsleiste dank einer optimierten Oberfläche überflüssig. Stattdessen stehen im Browser alle Adobe Reader-Funktionen sowie diejenigen Funktionen zur Verfügung, die der Ersteller ggf. in Adobe Acrobat für Reader-Anwender aktiviert hat. Dazu zählen das Ausfüllen von Unterschriftsfeldern, das Hinzufügen neuer Unterschriftsfelder, das Speichern von Formulardaten u. v. m.

Adobe JavaScript-Steuerelemente

Mit den Adobe JavaScript-Steuerelementen haben Sie außerdem folgende Möglichkeiten:

- die JavaScript-Engine ein- oder ausschalten
- per JavaScript aufgerufene URLs aktivieren oder deaktivieren
- die Ausführung von JavaScript mit Berechtigungen von hoher Priorität überwachen, unabhängig von anderen Berechtigungen
- JavaScripte mit Berechtigungen von hoher Priorität in zertifizierten Dokumenten aktivieren

Adobe bietet Ihnen die Flexibilität, diese Einschränkungen für vertrauenswürdige Standorte, Dateien, Ordner und Hosts selektiv zu umgehen.

Ausführung von JavaScript

Die Acrobat X-Familie bietet erweiterte Steuerungen für die Ausführung von JavaScript unter Windows und Mac OS. Mithilfe des Adobe JavaScript Blacklist Framework kann JavaScript in Geschäftsabläufen verwendet werden, während Anwender und Systeme vor Angriffen geschützt bleiben, die auf bestimmte JavaScript-API-Aufrufe ausgerichtet sind.

Wenn ein bestimmter JavaScript-API-Aufruf der „schwarzen Liste“ hinzugefügt wird, können Sie ihn sperren, ohne JavaScript vollständig deaktivieren zu müssen. Sie können auch einzelne Anwender daran hindern, Ihre Entscheidung, einen bestimmten JavaScript-API-Aufruf zu sperren, aufzuheben, sodass der Schutz vor Schad-Software für Ihr gesamtes Unternehmen erhöht wird. In Windows-Umgebungen wird die „schwarze Liste“ in der Windows-Registry geführt, unter Mac OS X wird sie in der Datei FeatureLockdown gespeichert.

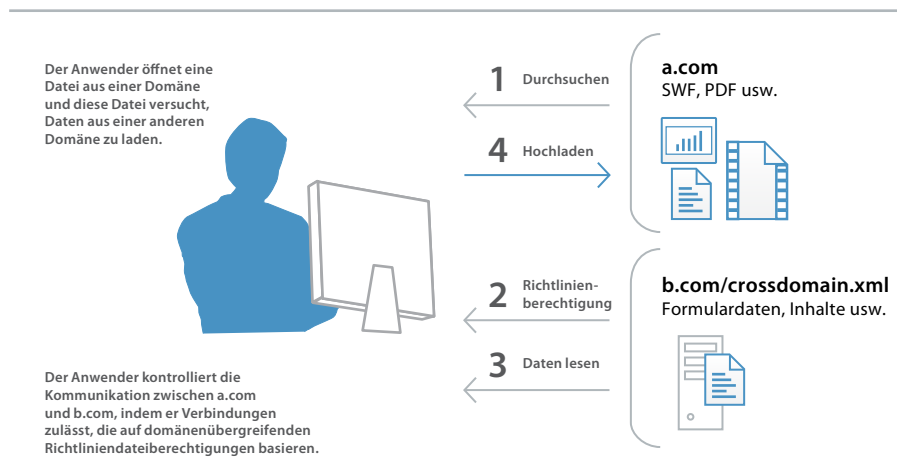
Domänenübergreifende Konfiguration

Standardmäßig wird bei der Adobe Acrobat X-Produktfamilie der uneingeschränkte domänenübergreifende Zugriff für Microsoft Windows- und Mac OS X-Clients eingeschränkt, damit Angreifer Multimedia-PDF-Dateien nicht dazu nutzen können, auf Ressourcen in einer anderen Domäne zuzugreifen.

Durch Nutzung der integrierten Unterstützung für Server-basierte domänenübergreifende Richtliniendateien können Sie den domänenübergreifenden Datenzugriff für Adobe Acrobat X und Adobe Reader X zulassen. Diese Datei ist ein XML-Dokument, enthält die Richtlinien für domänenübergreifenden Zugriff und befindet sich in der entfernten Domäne. Die Datei gewährt Zugriffsrechte auf die Ausgangsdomäne und gestattet es Acrobat oder Reader, die Transaktion fortzuführen.

In den folgenden Situationen sollten Sie die domänenübergreifende Unterstützung von Adobe aktivieren:

- Wenn domänenübergreifender Zugriff erforderlich ist und sonstige Funktionen genutzt werden sollen, etwa die Erkennung aufgrund eines digitalen Zertifikats
- Wenn domänenübergreifende Zugriffsrechte von nur einem Server-basierten Standort aus verwaltet werden sollen
- Wenn Sie Workflows implementieren, die Datenanforderungen aus mehreren Domänen zur Rückgabe von Formulardaten, SOAP-Anforderungen, Bezugnahmen auf Stream-Medien sowie Net.HTTP-Anforderungen enthalten



Benutzerfreundliche Sicherheitsmeldungen

Die Adobe Acrobat X-Produktfamilie implementiert eine benutzerfreundliche Methode mit Sicherheitsmeldungen über eine unaufdringliche gelbe Meldungsleiste. Diese Leiste ersetzt die herkömmlichen Dialogfelder, die den Seiteninhalt verdeckt haben, wodurch der Anwender den Überblick behält und besser auf eine Meldung reagieren kann.

In Acrobat und Reader erscheint die Leiste im oberen Dokumentbereich mit einer Warnung beziehungsweise Fehlermeldung. Der Anwender kann auswählen, ob er dem Dokument „Einmal“ oder „Immer“ vertrauen möchte. Wenn Sie „Immer“ wählen, wird das Dokument der Liste privilegierter Dokumente hinzugefügt.

Wenn die erweiterte Sicherheit aktiviert ist und die PDF-Datei nicht schon als privilegiert eingestuft wurde (zum Beispiel „vertrauenswürdig“), erscheint die Leiste, wenn die Datei versucht, eine möglicherweise riskante Aktion auszuführen, z. B.:

- Domänenübergreifenden Zugriff aufrufen
- JavaScript ausführen
- Eine von JavaScript aufgerufene URL aufrufen
- Eine in die „schwarze Liste“ eingetragene JavaScript-API aufrufen
- Daten einfügen
- Skripte einfügen
- Eingebettete Multimedia-Elemente wiedergeben

Wenn Anwender eine Datei erhalten, können sie die Stufe der Vertrauenswürdigkeit über die Schaltfläche „Optionen“ einrichten. Unternehmensweit können Sie die Vertrauenswürdigkeit für Dateien, Ordner und Hosts vorab konfigurieren, sodass die Meldungsleiste in einem vertrauenswürdigen Unternehmens-Workflow nie angezeigt wird.

Engere Integration mit Systemarchitekturen

Permanent aktive Sicherheit

Die Adobe Acrobat X-Produktfamilie nutzt mithilfe einer weiteren Verteidigungsebene gegen Angriffe, die versuchen, die Kontrolle über Desktop-Systeme zu übernehmen oder den Arbeitsspeicher zu beschädigen, integrierte, permanent aktivierte Sicherheitsmaßnahmen unter Microsoft Windows und Mac OS X.

Data Execution Prevention (DEP) verhindert die Platzierung von Daten oder gefährlichem Code an Stellen im Arbeitsspeicher, die vom Windows-Betriebssystem als geschützt definiert sind. Apple bietet einen ähnlichen Schutz vor ausführbaren Dateien für Mac OS X 10.6 im 64-Bit-Safari-Browser.

Address Space Layout Randomization (ASLR) verbirgt Arbeitsspeicher und die Speicherorte der Dateien von Systemkomponenten. So wird es für Angreifer schwieriger, diese Komponenten zu finden. Windows und Mac OS X 10.6 verwenden ASLR.

Registrierungsebene und Plist-Konfiguration

Die Acrobat X-Produktfamilie bietet Ihnen eine Reihe von Werkzeugen zur Verwaltung der Sicherheitseinstellungen, etwa Voreinstellungen für die Registrierungsebene (Windows) und für die Plist (Mac OS). Mit diesen Voreinstellungen können Sie Clients konfigurieren, sowohl vor als auch nach der Bereitstellung, um Folgendes zu erreichen:

- Erweiterte Sicherheit aktivieren oder deaktivieren
- Vertrauenswürdige Sites aktivieren oder deaktivieren
- Vordefinierte vertrauenswürdige Sites angeben
- Bestimmte Funktionen sperren und die Benutzerschnittstelle der Anwendung deaktivieren, sodass die Endanwender die Voreinstellungen nicht ändern können
- Nahezu sämtliche anderen sicherheitsrelevanten Funktionen deaktivieren, aktivieren und auf andere Weise konfigurieren

Niedrigere Gesamtbetriebskosten

Höhere Software-Sicherheit

Der geschützte Modus von Adobe Reader und die geschützte Ansicht von Acrobat sind nur zwei Beispiele für die umfangreiche Entwicklungsarbeit an der Acrobat-Produktfamilie zum Schutz vor aktuellen und künftigen Bedrohungen. Durch den höheren Schutz gegen Fremdeinwirkung werden die Anzahl außerplanmäßiger Sicherheits-Updates verringert und die Dringlichkeit geplanter Updates herabgesetzt. All diese Punkte erhöhen die Flexibilität und senken die Gesamtbetriebskosten, insbesondere in Umgebungen mit hohen Anforderungen an die Sicherheit.

Unterstützung für Microsoft SCCM und SCUP

Sie können über den Microsoft System Center Configuration Manager (SCCM) Aktualisierungen effizient importieren und veröffentlichen, damit gewährleistet ist, dass die von Ihnen verwalteten Windows-Desktops immer auf dem neuesten Sicherheitsstand sind.

Über Microsoft System Center Publisher-Kataloge (SCUP) lässt sich die Aktualisierung aller Acrobat X- und Reader X-Installationen innerhalb einer Organisation automatisieren. Außerdem erleichtern sie die Erstimplementierung von Adobe-Software. SCUP kann automatisch Updates von Adobe importieren, sobald sie verfügbar sind, damit die Aktualisierung Ihrer Acrobat- und Reader-Implementierungen vereinfacht wird. Die neue Integration mit SCCM/SCUP verringert die Gesamtbetriebskosten für Adobe-Produkte, da Patches in der gesamten Organisation einfacher und schneller installiert werden können.

Unterstützung für das Apple Package-Installationsprogramm und für Apple Remote Desktop

Adobe hat das standardmäßige Apple Package-Installationsprogramm aus dem Lieferumfang von Mac OS X anstelle des eigenen Adobe-Installationsprogramms implementiert. Dadurch wird es einfacher, Acrobat und Reader auf Macintosh-Desktops im Unternehmen zu installieren, weil Sie mit Apple Remote Desktop die Erstimplementierung und die nachfolgenden Upgrades und Patches zentral verwalten können.

Einfachere Bereitstellung und Verwaltung

Kumulative, regelmäßige Updates und Patches

Damit Ihre Software immer auf dem neuesten Stand ist, stellt Adobe in regelmäßigen Zeitabständen Updates mit Funktions-Upgrades und Bugfixes bereit. Im Bedarfsfall werden außerplanmäßige Patches veröffentlicht. Adobe setzt möglichst oft kumulative Patches ein, um den Arbeits- und Zeitaufwand für die Systemaktualisierungen zu minimieren. Alle Sicherheits-Patches werden intensiv getestet, bevor sie freigegeben werden, damit die Kompatibilität mit vorhandenen Installationen und Abläufen gewährleistet ist.

Adobe bietet auch die folgenden Sicherheits-Websites und Benachrichtigungsdienste:

- Die neuesten Sicherheitsbulletins und -hinweise über Adobe-Produkte finden Sie unter www.adobe.com/de/support/security.
- Die neuesten Sicherheitsberichte und Bugfixes finden Sie unter blogs.adobe.com/psirt.
- Detaillierte Hinweise zu Adobe-Produkten und Sicherheitsfunktionen finden Sie in der Adobe Security Library unter www.adobe.com/go/learn_acr_appsecurity_de.

Adobe Customization Wizard und AIM

Für eine bessere Kontrolle über Ihre unternehmensweiten Installationen liefert Adobe die folgenden Werkzeuge:

- **Adobe Customization Wizard** – Unterstützt IT-Experten bei der Anpassung des Acrobat-Installationsprogramms und der Anwendungsfunktionen vor der Bereitstellung.
- **Administrator's Information Manager (AIM)** – In dieser Adobe AIR®-Anwendung werden Voreinstellungen von Adobe-Anwendungen ausführlich erklärt. Die Anwendung wird automatisch aktualisiert und lässt sich beliebig anpassen. Der AIM enthält außerdem eine ständig gepflegte Liste mit weiteren Ressourcen für Administratoren in Unternehmen und Organisationen.

Inhaltssicherheit

Neben der Anwendungssicherheit unterstützt Adobe eine Reihe von branchenüblichen Lösungen für den Schutz und die Authentifizierung von Informationen, die in Adobe PDF-Dokumenten gespeichert sind, darunter digitale Signaturen, Zugriffsrechte und Best Practices.

Digitale Signaturen

Digitale Signaturen sparen Zeit und Geld. Mit ihrer Hilfe lassen sich die Integrität und Authentizität der Inhalte eines Dokuments sicherstellen. In einem Dokumenten-Workflow auf Basis von Adobe Reader X und Adobe Acrobat X können Sie intuitiv eine standardbasierte digitale Signatur hinzufügen, die Gültigkeit einer Signatur verifizieren und Zugriffsrechte vergeben.

Verwaltung von Zugriffsrechten

Die Acrobat X-Produktfamilie arbeitet mit LiveCycle® Rights Management ES2 zusammen und bietet Rechteverwaltungsfunktionen, mit deren Hilfe Sie verhindern können, dass vertrauliche oder andere wichtige Informationen nach außen oder in falsche Hände geraten. Sie können Zugriffsrechte, Druck-, Kopier- und Bearbeitungsvorgänge auf Dokument-, Anwender- oder Gruppenebene steuern. Außerdem können Sie diese Richtlinien während der gesamten Laufzeit des Dokuments dynamisch ändern. Da jede beliebige Person mit Adobe Reader sicher auf diese Inhalte zugreifen kann, können geschützte Dokumente ohne Probleme angezeigt werden und der Empfänger braucht keine zusätzlichen Produkte oder Plug-ins.

Best Practices

Mithilfe des neuen Aktionsassistenten von Acrobat X lassen sich Dokumentenprozesse auf Skriptbasis automatisieren und organisationsweit implementieren. So können Sie sicherstellen, dass alle Mitarbeiter beim Vorbereiten und Schützen von Dokumenten für die Öffentlichkeit nach bewährten Verfahren vorgehen.

Umgang mit vertraulichen Informationen

Endanwender können vertrauliche Informationen mithilfe von Bereinigungs- und Schwärzungswerkzeugen konsistent und rasch entfernen. Leistungsstarke, standardbasierte Verschlüsselungstechnologien ermöglichen außerdem die Vergabe von Kennwörtern und Zugriffsberechtigungen bzw. verhindern die unbefugte Änderung eines Adobe PDF-Dokuments.

Fazit

Bei der Adobe Acrobat X-Produktfamilie hat Sicherheit von PDF-Dokumenten und die Ihrer Daten oberste Priorität. Acrobat X und Reader X sind mit dem Hauptaugenmerk auf dem Aspekt Sicherheit konzipiert: von verbesserter Anwendungssicherheit und erweiterten Steuerungsmöglichkeiten bis zu engerer Integration in das Betriebssystem, optimierten Patch-Funktionen und verbesserten Bereitstellungs- und Verwaltungswerkzeugen. Anwender von Reader X und Acrobat X profitieren von erheblich geringeren Gesamtbetriebskosten gegenüber den früheren Versionen der beiden Produkte.

An der Entwicklung von Acrobat X und Reader X sowie an eventuell nötigen Nachbesserungen sind auch die Adobe-Experten für Produktsicherheit beteiligt: das Adobe Secure Software Engineering Team (ASSET). Gemeinsam mit dem Adobe Product Security Incident Response Team (PSIRT) stellt ASSET sicher, dass Ihre Daten gesichert sind und bleiben, wann immer Sie Adobe-Produkte verwenden.

Weitere Informationen
www.adobe.com/de/security



Adobe

Adobe Systems GmbH
Georg-Brauchle-Ring 58 • D-80992 München
Adobe Systems (Schweiz) GmbH
World Trade Center • Leutschenbachstrasse 95
CH-8050 Zürich
www.adobe.de
www.adobe.at
www.adobe.ch
www.adobe.com

Adobe, the Adobe logo, Acrobat, Adobe AIR, AIR, LiveCycle, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Apple, Mac OS, and Macintosh are trademarks of Apple Inc., registered in the U.S. and other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2011 Adobe Systems Incorporated. Alle Rechte vorbehalten. Printed in Germany.