

# PDF-beveiliging bereikt een nieuw niveau met Adobe Reader® en Adobe Acrobat®

## Acrobat X-productreeks legt de lat hoger

### Inhoud

- 1 Verbeterde toepassingsbeveiliging
- 4 Nauwere integratie met de architectuur van het besturingssysteem
- 5 Totale eigendomskosten verlagen
- 5 Eenvoudiger implementeren en beheren
- 6 Beveiliging van inhoud
- 6 Conclusie

De nieuwe beveiligingsfuncties in Adobe Reader X en Adobe Acrobat X helpen risico's van PDF-gebaseerde malware te reduceren.

Adobe Reader X en Adobe Acrobat X tillen de beveiliging van PDF-documenten, en uw gegevens, naar een hoger niveau. Adobe Reader X en Adobe Acrobat X – beide ontworpen met bijzondere aandacht voor beveiliging – bieden betere toepassingsbeveiliging dankzij de geavanceerde 'sandboxing'-technologie, meer mogelijkheden voor granulaire controle en nauwere integratie met de architectuur van de Microsoft® Windows®- en Apple Mac OS X-besturingssystemen, gestroomlijnde patchfuncties en verbeterde gereedschappen voor implementatie en beheer. Dankzij de nieuwe functies in Adobe Reader X en Adobe Acrobat X profiteren gebruikers van lagere totale eigendomskosten in vergelijking met vorige versies van Adobe Reader X en Adobe Acrobat X.

Bovendien werken het Adobe Secure Software Engineering Team (ASSET) en het Adobe Product Security Incident Response Team (PSIRT) samen om ervoor te zorgen dat uw gegevens veilig zijn wanneer u Adobe-producten gebruikt. Aansluitend bij onze interne beveiligingsinspanningen is Adobe ook betrokken bij het Microsoft Active Protections Program (MAPP). Hierdoor kan op een geavanceerde manier informatie over kwetsbaarheden in producten worden gedeeld met leveranciers van beveiligingssoftware, zoals leveranciers van antivirussoftware en software voor inbraakdetectie en -preventie. Op die manier kan de sector samenwerken om de risico's op kwetsbaarheden in Adobe Acrobat X en Adobe Reader X te reduceren.

## Verbeterde toepassingsbeveiliging

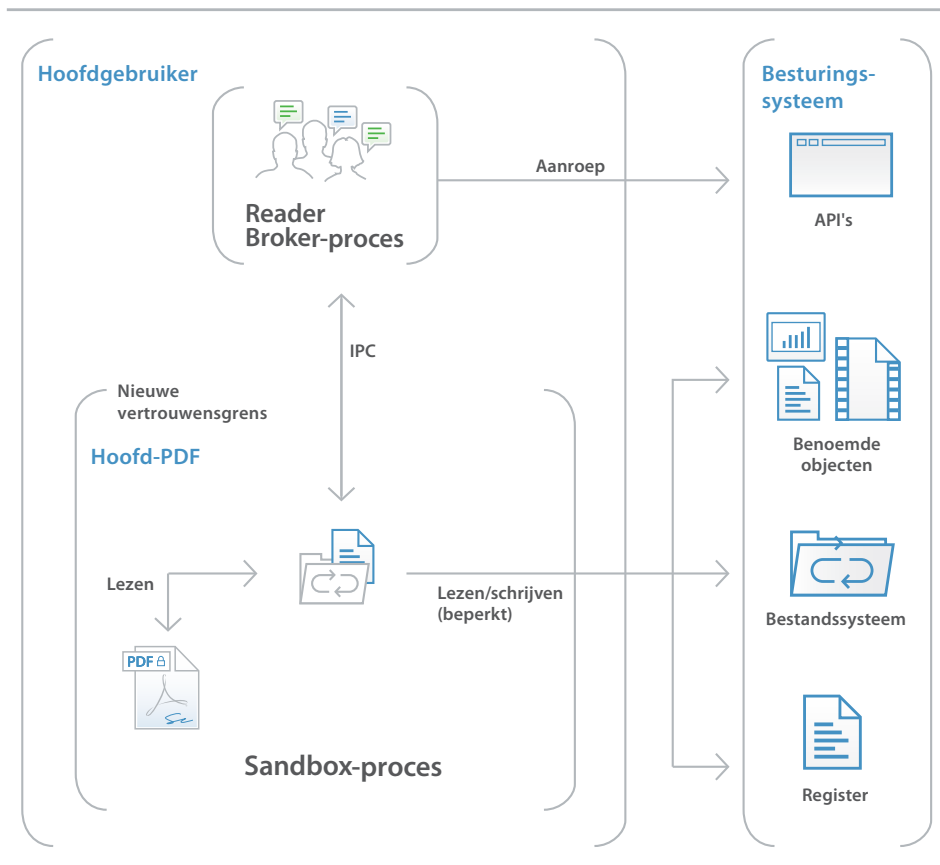
### Beveiligde modus in Adobe Reader X

Om u en uw organisatie te beschermen tegen schadelijke code die de PDF-bestandsindeling probeert te gebruiken om naar het bestandssysteem van een computer te schrijven, biedt Adobe u de Beveiligde modus, een implementatie van de 'sandboxing'-technologie.

De Beveiligde modus is standaard ingeschakeld wanneer u Adobe Reader X start en helpt zo te voorkomen dat aanvallers malware op het systeem van een gebruiker installeren, waardoor het risico op mogelijke bedreigingen wordt gereduceerd. De Beveiligde modus beperkt in feite het toegangsniveau dat aan het programma wordt toegekend, waardoor systemen waarop het Microsoft Windows-besturingssysteem wordt uitgevoerd, worden beschermd tegen schadelijke PDF-bestanden die mogelijk proberen naar het bestandssysteem te schrijven, bestanden te verwijderen of systeeminformatie op enige andere wijze aan te passen.

## Wat is 'sandboxing'?

Sandboxing – dat bijzonder wordt gewaardeerd door beveiligingsprofessionals – is een methode om een besloten uitvoeringsomgeving te creëren waarbinnen programma's met lage rechten of machtigingen worden uitgevoerd. Sandboxes beschermen systemen van gebruikers tegen beschadiging door niet-vertrouwde documenten die uitvoerbare code bevatten. In de context van Adobe Reader is de niet-vertrouwde inhoud een willekeurig PDF-bestand en de processen die het aanroept. Adobe Reader X beschouwt alle PDF-documenten als mogelijk schadelijk en beperkt alle bewerkingen die door het PDF-bestand worden aangeroepen tot de sandbox.



Als onderdeel van de voortdurende inspanningen van Adobe om beveiliging in elke fase van de levenscyclus van het product te integreren door middel van het Adobe Secure Product Lifecycle-proces (SPLC), voert Adobe regelmatig revisies van bestaande code uit en wordt deze zo nodig versterkt. Hierdoor wordt de toepassingsbeveiliging verbeterd en de veiligheid van uw gegevens verhoogd wanneer u Adobe-producten gebruikt.

## Beveiligde weergave in Adobe Acrobat X

De Beveiligde weergave, die vergelijkbaar is met de Beveiligde modus in Adobe Reader, is een implementatie van 'sandboxing'-technologie voor de rijke Adobe Acrobat-functionaliteit en is beschikbaar in Acrobat X versie 10.1. Net zoals de Beveiligde modus beperkt de Beveiligde weergave de uitvoering van niet-vertrouwde programma's (bijv. elk PDF-bestand en de processen die worden aangeroepen) tot een beperkte sandbox om te voorkomen dat kwaadaardige code via de PDF-bestandsindeling naar het bestandssysteem van uw computer wordt geschreven.

De Beveiligde weergave gaat ervan uit dat alle PDF-bestanden potentiaal kwaadaardig zijn en beperkt de verwerking tot de sandbox, tenzij u specifiek aangeeft dat u een bestand vertrouwt. Hoewel de Beveiligde weergave wordt ondersteund in beide scenario's waarin gebruikers PDF-documenten openen — in de autonome Adobe Acrobat X-software en in een browser — is de gebruikerservaring in elk van de scenario's enigszins verschillend.

In de autonome Adobe Acrobat X-software geeft Acrobat boven aan het weergavevenster een gele berichtenbalk (Yellow Message Bar, of YMB) weer wanneer u in de Beveiligde weergave een potentieel kwaadaardig bestand opent. Deze balk geeft aan dat het bestand niet-vertrouwd is en herinnert u eraan dat u zich in de Beveiligde weergave bevindt, en dat hierin vele Acrobat--mogelijkheden uitgeschakeld zijn en de interactie van de gebruiker met het bestand beperkt is. In wezen bevindt het bestand zich in alleen-lezenmodus en voorkomt de Beveiligde weergave dat enige ingesloten of meegebrachte kwaadaardige content met uw systeem knoeit. Als u het bestand wilt vertrouwen en alle Adobe Acrobat X-functies wilt inschakelen, kunt u op de gele berichtenbalk op de knop "Enable All Features" (Alle functies inschakelen) klikken. Adobe Acrobat zal dan de Beveiligde weergave afsluiten en het bestand permanent vertrouwen door het toe te voegen aan de lijst met gemachtigde locaties van Acrobat. Elke keer dat het vertrouwde PDF-bestand daarna wordt geopend, worden de beperkingen van de Beveiligde weergave uitgeschakeld.

## Adobe JavaScript-besturingselementen

Bovendien kunt u met de Adobe JavaScript-besturingselementen:

- De JavaScript-engine in- of uitschakelen
- Door JavaScript aangeroepen URL's in- of uitschakelen
- De uitvoering van bijzonder gemachtigd JavaScript beheren, onafhankelijk van overige machtigingen
- Bijzonder gemachtigd JavaScript in gecertificeerde documenten inschakelen

Adobe biedt u de flexibiliteit om deze beperkingen voor vertrouwde locaties, waaronder bestanden, mappen en hosts, desgewenst te omzeilen.

Wanneer u een PDF-bestand in een browser opent, biedt de Beveiligde weergave een gestroomlijnde ervaring waarbij geen gele berichtenbalk vereist is. In plaats daarvan zijn alle Adobe Reader-functies beschikbaar in de browseromgeving, alsook de functies die ingeschakeld werden indien de auteur van het document Acrobat heeft gebruikt om functies uit te breiden naar gebruikers van Adobe Reader — waaronder het ondertekenen van bestaande formulervelden, het toevoegen van nieuwe handtekeningvelden, het opslaan van formuliergegevens.

## JavaScript uitvoeren

De Adobe Acrobat X-productreeks biedt geavanceerde en granulaire besturingselementen om de uitvoering van JavaScript in Windows- en Mac OS X-omgevingen te beheren. Met het Adobe JavaScript Blacklist Framework kan JavaScript als onderdeel van bedrijfsworkflows worden gebruikt en worden gebruikers en systemen beschermd tegen aanvallen die op specifieke JavaScript API-aanroepen zijn gericht.

Door een specifieke JavaScript API-aanroep aan de blacklist toe te voegen, kunt u verhinderen dat deze wordt uitgevoerd zonder dat u JavaScript volledig hoeft uit te schakelen. U kunt ook voorkomen dat individuele gebruikers uw beslissing om een specifieke JavaScript API-aanroep te vergrendelen, overschrijven. Dit helpt uw hele onderneming te beschermen tegen schadelijke code. In Windows-omgevingen wordt de blacklist onderhouden in het Windows-register. In Mac OS X-omgevingen wordt deze in het FeatureLockdown-bestand van Mac OS X bewaard.

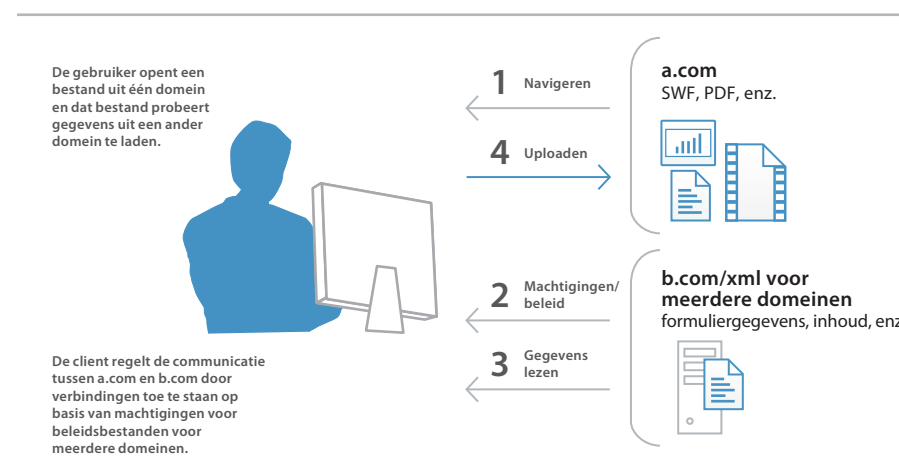
## Configuratie voor meerdere domeinen

De Adobe Acrobat X-producten schakelen onbeperkte toegang voor meerdere domeinen standaard uit voor Microsoft Windows- en Mac OS X-clients, waardoor wordt voorkomen dat aanvallers misbruik maken van rijke PDF-bestanden om toegang te krijgen tot een ander domein.

Door gebruik te maken van ingebouwde ondersteuning voor servergebaseerde beleidsbestanden voor meerdere domeinen, kunt u Adobe Acrobat X en Adobe Reader X toestaan om gegevens in meerdere domeinen te verwerken. Dit beleidsbestand voor meerdere domeinen – in de vorm van een XML-document – wordt op het externe domein gehost. Het verleent toegang tot het brondomein en staat toe dat Adobe Acrobat X of Adobe Reader X doorgaat met de bewerking.

U wilt Adobe-ondersteuning voor meerdere domeinen in de volgende situaties uitschakelen:

- U hebt selectieve toegang voor meerdere domeinen nodig en wilt gebruikmaken van overige functies, zoals herkenning op basis van een digitaal certificaat.
- U wilt toegangsmachtigingen voor meerdere domeinen centraal beheren vanaf één servergebaseerde locatie.
- U wilt workflows implementeren die gegevensverzoeken van meerdere domeinen bevatten voor het verzenden van formuliergegevens, SOAP-verzoeken, verwijzingen naar streaming media en Net.HTTP-verzoeken.



## Gebruiksvriendelijke beveiligingswaarschuwingen

De Adobe Acrobat X-productreeks implementeert een gebruiksvriendelijke methode voor beveiligingswaarschuwingen door middel van een discrete gele berichtenbalk. De gele berichtenbalk vervangt de klassieke dialoogvensters die inhoud op de pagina verbergen, zodat waarschuwingen beter zichtbaar zijn en gebruikers er makkelijker op kunnen reageren.

In Adobe Acrobat X of de Adobe Reader X-client verschijnt de gele berichtenbalk boven aan het document met het waarschuwings- of foutbericht. De gebruiker kan ervoor kiezen om het document 'één keer' of 'altijd' te vertrouwen. Als hij 'altijd' kiest, wordt het document voor de toepassing toegevoegd aan de lijst met gemachtigde documenten.

Wanneer verhoogde beveiliging is ingeschakeld en het PDF-bestand nog niet als een gemachtigde (bijvoorbeeld, vertrouwde) locatie is ingesteld, verschijnt de gele berichtenbalk wanneer het PDF-bestand een mogelijk risicovolle actie probeert uit te voeren, zoals:

- Toegang voor meerdere domeinen aanroepen
- JavaScript uitvoeren
- Een door JavaScript aangeroepen URL aanroepen
- Een JavaScript API in de blacklist aanroepen
- Gegevens injecteren
- Scripts injecteren
- Ingesloten oudere multimedia afspelen

Met de knop 'Options' (Opties) kunnen gebruikers onmiddellijk hun vertrouwen instellen – eenmalig of voor altijd. U kunt binnen de hele onderneming het vertrouwen voor bestanden, mappen en hosts vooraf configureren zodat de gele berichtenbalk nooit verschijnt in een vertrouwde bedrijfsworkflow.

## Nauwere integratie met de architectuur van het besturingssysteem

### Beveiliging altijd ingeschakeld

De Adobe Acrobat X-productreeks biedt niet alleen een extra beschermingslaag tegen aanvallen waarbij wordt geprobeerd controle te krijgen over desktopsystemen of het geheugen te beschadigen, maar haalt ook voordeel uit ingebouwde, altijd ingeschakelde beveiligingsmechanismen in de Microsoft Windows- en Mac OS X-besturingssystemen.

- Data Execution Prevention (DEP) voorkomt de plaatsing van gegevens of gevaarlijke code op geheugenlocaties die zijn gedefinieerd als 'beschermd' door het Windows-besturingssysteem. Apple biedt een soortgelijke bescherming van uitvoerbare bestanden voor Mac OS X 10.6 in de 64-bits browser Safari.
- Address Space Layout Randomization (ASLR) verbergt geheugen- en paginabestandslocaties van systeemonderdelen, zodat het voor aanvallers moeilijker wordt om deze onderdelen te vinden en te benaderen. Zowel Windows als Mac OS X 10.6 gebruiken ASLR.

### Register- and plist-configuratie

De Adobe Acrobat X-productreeks biedt u tal van gereedschappen om beveiligingsinstellingen te beheren, waaronder ook register- (Windows) en plist-voorkeuren (Macintosh). Met deze instellingen kunt u clients configureren, zowel vóór als na de implementatie, om een van de volgende acties uit te voeren:

- Verhoogde beveiliging in- of uitschakelen
- Gemachtigde locaties in- of uitschakelen
- Vooraf gedefinieerde gemachtigde locaties opgeven
- Bepaalde functies vergrendelen en de gebruikersinterface voor de toepassing uitschakelen zodat eindgebruikers de instellingen niet kunnen wijzigen
- Vrijwel alle andere beveiligingsgerelateerde functies uitschakelen, inschakelen en anderszins configureren

## Totale eigendomskosten verlagen

### Versterking van softwarebeveiliging

Beveiligingsverbeteringen zoals de Beveiligde modus van Adobe Reader en de Beveiligde weergave van Adobe Acrobat zijn slechts twee voorbeelden van de uitgebreide engineeringinvesteringen die Adobe heeft gedaan om Acrobat-producten nog sterker te beveiligen tegen actuele en opkomende bedreigingen. Door de software robuuster te maken tegen aanvalspogingen, kan Adobe de behoefte aan out-of-band beveiligingsupdates reduceren of zelfs elimineren en de urgentie van regelmatig geplande updates verlagen. Al deze maatregelen verhogen de operationele flexibiliteit en verlagen de totale eigendomskosten, met name in grote omgevingen met hoge vereisten op het gebied van beveiliging en zekerheid.

### Ondersteuning voor Microsoft SCCM en SCUP

Met de Adobe Acrobat X-producten kunt u updates op efficiënte wijze importeren en publiceren via Microsoft System Center Configuration Manager (SCCM) om ervoor te zorgen dat uw beheerde Windows-desktops altijd zijn bijgewerkt met de recentste beveiligingspatches en -updates.

Dankzij de nieuwe ondersteuning voor Microsoft System Center Updates Publisher-catalogi (SCUP) kunt u updates voor uw Adobe Acrobat X- en Adobe Reader X-software voor uw hele organisatie automatiseren, alsook de oorspronkelijke software-implementaties stroomlijnen. SCUP kan updates die door Adobe worden uitgebracht, automatisch importeren zodra ze beschikbaar zijn, waardoor u uw Adobe Acrobat X- en Adobe Reader X-implementaties makkelijker en efficiënter kunt bijwerken. De nieuwe integratie met SCCM/SCUP helpt de totale eigendomskosten van uw Adobe-software te reduceren, omdat patches eenvoudiger en sneller over de hele organisatie kunnen worden geïmplementeerd.

### Ondersteuning voor Apple Package Installer en Apple Remote Desktop

In de Adobe Acrobat X-producten heeft Adobe de standaard Apple Package Installer van Mac OS X geïmplementeerd in plaats van het eigen Adobe-installatieprogramma. Hierdoor wordt het gemakkelijker om Adobe Acrobat- en Adobe Reader-software te implementeren op Macintosh-desktops in de onderneming, omdat u nu de Apple Remote Desktop-beheerssoftware kunt gebruiken om uw initiële software-implementatie en alle volgende upgrades en patches te beheren vanaf een centrale locatie.

## Eenvoudiger implementeren en beheren

### Cumulatieve, regelmatig geplande updates en patches

Om u te helpen uw software up-to-date te houden, brengt Adobe proactief regelmatig geplande updates uit die zowel upgrades van functies als oplossingen voor beveiligingsproblemen bevatten. Om snel te kunnen reageren op aanvallen via eerder onbekende kwetsbaarheden, biedt Adobe u zo nodig patches buiten de normale cyclus. Adobe maakt ook zo veel mogelijk gebruik van cumulatieve patching om de inspanningen en kosten te reduceren die vereist zijn om systemen up-to-date te houden. Daarnaast test Adobe beveiligingspatches ook intensief alvorens ze vrij te geven, om compatibiliteit met bestaande installaties en workflows te helpen garanderen.

Adobe biedt tevens de volgende beveiligingswebsites en kennisgevingsservices:

Voor de recentste beveiligingsbulletins en -adviezen over Adobe-producten bezoekt u [www.adobe.com/nl/support/security](http://www.adobe.com/nl/support/security).

De recentste meldingen van beveiligingsincidenten en oplossingen voor kwetsbaarheidsproblemen kunt u bekijken op de Adobe PSIRT-blog op [blogs.adobe.com/psirt](http://blogs.adobe.com/psirt).

Voor gedetailleerde informatie over Adobe-producten en -beveiligingsfuncties bezoekt u de Adobe-beveiligingsbibliotheek op [www.adobe.com/go/learn\\_acr\\_appsecurity\\_en](http://www.adobe.com/go/learn_acr_appsecurity_en).

### Adobe Customization Wizard en AIM

Voor meer controle over uw implementaties binnen de hele onderneming biedt Adobe deze gereedschappen:

- Adobe Customization Wizard — Een gratis, downloadbaar hulpprogramma waarmee u het Acrobat-installatieprogramma kunt aanpassen en toepassingsfuncties vóór de implementatie kunt configureren.
- Administrator Information Manager (AIM) — Een aanpasbare Adobe AIR®-toepassing die automatisch wordt bijgewerkt en voorkeursreferenties bevat. AIM bevat tevens een groeiende lijst met overige bronnen die van belang zijn voor beheerders in ondernemingen.

## Beveiliging van inhoud

Adobe biedt niet alleen toepassingsbeveiliging, maar ondersteunt ook een groot aantal industriestandaard mechanismen om de informatie die in uw PDF-documenten wordt opgeslagen, te helpen beveiligen en verifiëren, zoals digitale handtekeningen, rechtenbeheer en beste praktijken voor documenten.

### Digitale handtekeningen

Met digitale handtekeningen bespaart u tijd en geld in vergelijking met handgeschreven handtekeningen. Bovendien helpen ze de integriteit en authenticiteit van de inhoud van een document te verzekeren voor de auteurs en ontvangers van documenten. Met Adobe Reader X en Adobe Acrobat X kunt u eenvoudig een op standaarden gebaseerde digitale handtekening aan een document toevoegen, die handtekening valideren en machtigingen en beperkingen toevoegen om de workflow van de handtekening te regelen.

### Rechtenbeheer

De Acrobat X-producten werken met Adobe LiveCycle® Rights Management ES2-software om mogelijkheden voor rechtenbeheer aan te bieden waarmee u vertrouwelijke gegevens of andere gevoelige informatie kunt beschermen tegen openbaarmaking buiten uw organisatie of misbruik door onbevoegden. Hiermee kunt u zowel de toegang als het afdrukken, kopiëren en bewerken beheren op document-, gebruikers- of groepsniveau en kunt u deze beleidsregels dynamisch aanpassen gedurende de levenscyclus van het document. Omdat iedereen met Adobe Reader veilig toegang krijgt tot deze inhoud, kunnen beveiligde documenten bovendien eenvoudig worden weergegeven en hoeft de ontvanger geen extra producten of plug-ins aan te schaffen of te downloaden.

### Consistente beste praktijken

Met de nieuwe handelingenwizard in Adobe Acrobat X kunt u eenvoudig scripts maken voor documentprocessen en ze vervolgens in de hele organisatie implementeren, zodat u weet dat alle gebruikers beste praktijken volgen wanneer uitgaande documenten worden voorbereid en beveiligd.

### Gevoelige informatie beheren

Gebruikers kunnen gevoelige informatie consistent en snel met slechts één muisklik uit bestanden verwijderen met opschonings- en uitgebreide redactiegereedschappen. Krachtige, op standaarden gebaseerde coderingstechnologieën stellen eindgebruikers in staat om wachtwoorden en machtigingen in te stellen en zo de toegang te controleren of wijzigingen in PDF-documenten te vermijden.

## Conclusie

Met de Adobe Acrobat X-productreeks brengt Adobe de beveiliging van PDF-documenten en uw gegevens op een hoger niveau. Van verbeterde toepassingsbeveiliging en meer granulaire controles tot nauwere integratie met besturingssystemen, Acrobat X en Reader X zijn ontworpen met bijzondere aandacht voor beveiliging. Gebruikers van Adobe Reader X en Adobe Acrobat X profiteren van sterk verlaagde totale eigendomskosten in vergelijking met vorige versies van Adobe Reader en Adobe Acrobat dankzij de betere toepassingsbeveiliging, nauwere integratie in besturingssystemen, gestroomlijnde patchfuncties en verbeterde gereedschappen voor implementatie en beheer.

Bovendien worden Adobe Acrobat X en Adobe Reader X ondersteund door het Adobe-team van product-beveiligingsexperts: het Adobe Secure Software Engineering Team (ASSET). ASSET werkt samen met het Product Security Incident Response Team (PSIRT) van Adobe om te helpen ervoor te zorgen dat uw gegevens veilig en beschermd zijn wanneer u Adobe-producten gebruikt.

## Meer informatie

Details over de oplossing: [www.adobe.com/nl/security](http://www.adobe.com/nl/security)

