Présentation de la sécurité d'Acrobat DC

La première solution PDF au monde pour créer, modifier et gérer des documents

Sommaire

Lorsque vous confiez vos données professionnelles à une application tierce, la sécurité est un élément crucial. Adobe possède plus de 20 ans d'expérience dans les documents digitaux sécurisés et a ouvert la voie aux normes PDF et de signature numérique. Si des centaines de milliers d'établissements dans le monde ont produit des milliards de PDF, c'est parce qu'ils misent sur le logiciel Adobe Acrobat et le format Adobe PDF pour préparer, protéger et partager quotidiennement leurs documents stratégiques.

Adobe Acrobat DC et les services Adobe Document Cloud constituent la solution PDF complète par excellence pour les utilisateurs mobiles et connectés. Outre la version Acrobat pour postes de travail et l'application mobile Adobe Acrobat Reader, il inclut des fonctionnalités mobiles avancées et les services Document Cloud pour permettre la création de workflows documentaires plus fluides et répondre à la demande de solutions mobiles, tout en garantissant la sécurité des documents sur l'ensemble des équipements. Avec Acrobat DC, vous avez systématiquement accès aux dernières fonctionnalités et mises à jour de sécurité (à déployer selon votre propre calendrier).

Ce document traite de l'approche globale de la sécurité adoptée par Adobe pour Acrobat DC — sécurité des documents, des applications et du cloud — afin de renforcer la protection de vos informations et de votre expérience.

Sécurité des documents

Les auteurs de documents peuvent utiliser Acrobat DC pour créer des documents PDF et appliquer toute une série de mesures de sécurité, comme le cryptage, le contrôle des accès, les signatures de certificat et la suppression définitive de texte et d'images à l'aide des outils de biffure. Grâce à la fonction Actions d'Acrobat DC qui permet de définir une série de tâches de sécurisation que tous les utilisateurs peuvent appliquer facilement sans formation ni outils spéciaux, les entreprises n'ont aucun mal à préserver la confidentialité de leurs informations.

Cryptage

Normes de sécurité prises en charge par Acrobat DC :

- Algorithme AES (Advanced Encryption Standard) 256 bits
- Normes prises en charge par l'ETSI (European Telecommunications Standards Institute)

Contrôle d'accès

Partagez des documents en toute confiance en appliquant facilement des mots de passe et des autorisations pour contrôler les accès aux documents PDF ou empêcher leur modification, mais aussi pour restreindre l'impression, la copie ou la modification des documents.

Signatures électroniques et numériques

Pour manipuler des signatures en toute sécurité, les utilisateurs d'Acrobat DC ont le choix entre les outils Envoyer pour signature et Certificats.

Le premier permet de gérer des processus de signature complets en conformité avec les lois *sur les signatures électroniques* applicables aux États-Unis, dans l'Union européenne et la plupart des pays industrialisés du monde. Les utilisateurs peuvent demander une signature, assurer le suivi du processus et archiver les documents signés et les pistes d'audit de manière automatique. Outre la gestion sécurisée du processus, les documents et pistes d'audit sont certifiés par Adobe à l'aide d'un sceau infalsifiable. L'outil Envoyer pour signature est intégré à *Adobe Sign*, une solution *Adobe Document Cloud* qui satisfait à des normes de sécurité très strictes, dont ISO 27001, SOC 2 Type 2, HIPAA et PCI DSS.

L'outil Certificats vous permet de signer des documents avec des identifiants numériques basés sur des certificats provenant de prestataires fiables figurant sur la liste AATL (Adobe Approved Trust List) ou EUTL (European Union Trusted Lists). L'utilisation d'un identifiant de certificat délivré par une autorité de certification tierce agréée est l'une des méthodes de signature électronique de documents les mieux sécurisées. L'identifiant est exclusivement lié au signataire et capable d'identifier ce dernier. Durant la phase de signature, le certificat du signataire est lié au document au moyen de la clé privée dont le signataire est le seul détenteur. Acrobat DC valide la signature de ce dernier — et l'authenticité du document qu'il a signé — en se connectant directement à l'autorité de certification pour procéder aux vérifications nécessaires. Ce type de signature est conforme aux normes sur la signature électronique des PDF, notamment la norme PAdES (PDF Advanced Electronic Signatures) parties 2, 3 et 4, ainsi qu'aux normes AES256/RSA4096/SHA512 dans le cadre de la certification JITC du ministère de la Défense des États-Unis pour l'utilisation de la cryptographie et des infrastructures à clé publique. Avec l'outil Certificats, vous pouvez aussi appliquer des horodatages sur les documents, et les certifier via un sceau infalsifiable.

Pour en savoir plus sur les signatures électroniques et numériques, consultez l'article technique *Transformer les processus métier grâce aux solutions de signature électronique et numérique*.

Vraie biffure

Acrobat DC offre une palette d'outils de biffure qui vous aident à protéger les informations sensibles ou confidentielles. Vous pouvez définitivement supprimer le texte et les images d'un document avant de le distribuer. Vous pouvez même rechercher et biffer certaines informations sur la base de modèles, telles que des numéros de téléphone et de carte bancaire, des adresses e-mail, etc. Les informations sélectionnées sont entièrement supprimées du fichier, et pas simplement masquées, comme c'est le cas avec d'autres outils ou méthodes.

La fonction d'assainissement des documents sert à supprimer les informations cachées et les objets non graphiques, comme les métadonnées éventuellement présentes dans le document PDF.

Sécurité des applications

Les fonctions de sécurité renforcée d'Acrobat DC assurent une protection contre les attaques qui cherchent à exploiter le format de fichier PDF pour installer des programmes malveillants sur votre système et/ou extraire des données confidentielles de votre système.

Les pratiques de sécurité sont profondément ancrées dans la culture d'Adobe, ainsi que dans le développement logiciel et les processus d'ingénierie. Acrobat DC and Acrobat Reader ont été conçus conformément à des pratiques de sécurité standard — pour la gestion des accès, la confidentialité des données et l'intégrité des documents — afin d'optimiser la protection de vos documents, données et informations personnelles.

Ingénierie sécurisée

Les applications Adobe DC utilisent le processus SPLC (Adobe Secure Product Lifecycle), qui comprend plusieurs centaines d'activités de sécurité rigoureuses liées aux pratiques, processus et outils de développement logiciel. Le processus Adobe SPLC est intégré à plusieurs étapes du cycle de vie des produits Acrobat DC : conception et développement, assurance qualité, tests et déploiement. Pour en savoir plus sur les processus de sécurité d'Adobe, l'engagement communautaire et Adobe SPLC, consultez le site *www.adobe.com/fr/security*.

Mode protégé d'Adobe Acrobat Reader DC

Afin d'éviter toute utilisation du format PDF par du code malveillant pour réaliser des opérations en écriture ou en lecture dans le système de fichiers d'un ordinateur, Adobe propose un mode protégé qui implémente une technologie « sandbox » (bac à sable) de pointe et a été introduit pour la première fois dans Adobe Reader X.

Dans Acrobat Reader DC, le mode protégé offre une protection élargie contre les pirates qui tentent d'installer des programmes malveillants sur votre système informatique, mais aussi contre les utilisateurs malintentionnés en les empêchant d'accéder à vos données confidentielles et à votre propriété intellectuelle et de les extraire de votre ordinateur ou réseau d'entreprise.

Activé par défaut au lancement d'Acrobat Reader DC, le mode protégé restreint le niveau d'accès octroyé aux programmes, protégeant ainsi les postes sous Microsoft Windows® des fichiers PDF malveillants susceptibles d'essayer d'effectuer des opérations en écriture ou en lecture dans le système de fichiers de l'ordinateur, de supprimer des fichiers ou de modifier les informations système. Le mode protégé de Reader (sous Windows 8.1 et versions ultérieures) peut désormais s'exécuter dans un conteneur d'application. Pour en savoir plus sur le conteneur d'application, rendez-vous à l'adresse : *https://msdn.microsoft.com/en-us/library/windows/desktop/mt595898(v=vs.85).aspx*.

Par ailleurs, fidèle à une démarche visant à intégrer la sécurité à plusieurs stades du cycle de vie du produit via le processus SPLC, Adobe, qui procède régulièrement à des évaluations du code existant, fait appel à la programmation défensive. Les applications sont ainsi mieux sécurisées et vos données mieux protégées lorsque vous utilisez des produits Adobe.

Vue protégée d'Acrobat DC

Semblable au mode protégé d'Acrobat Reader DC, la vue protégée est une mise en œuvre de la technologie « sandbox » pour les riches fonctionnalités d'Acrobat DC. Dans Acrobat DC, Adobe étend les fonctionnalités de la vue protégée en bloquant non seulement les attaques en écriture dans le système de votre ordinateur par du code malveillant utilisant le format PDF, mais aussi les attaques en lecture visant à dérober vos données confidentielles ou votre propriété intellectuelle via des fichiers PDF.

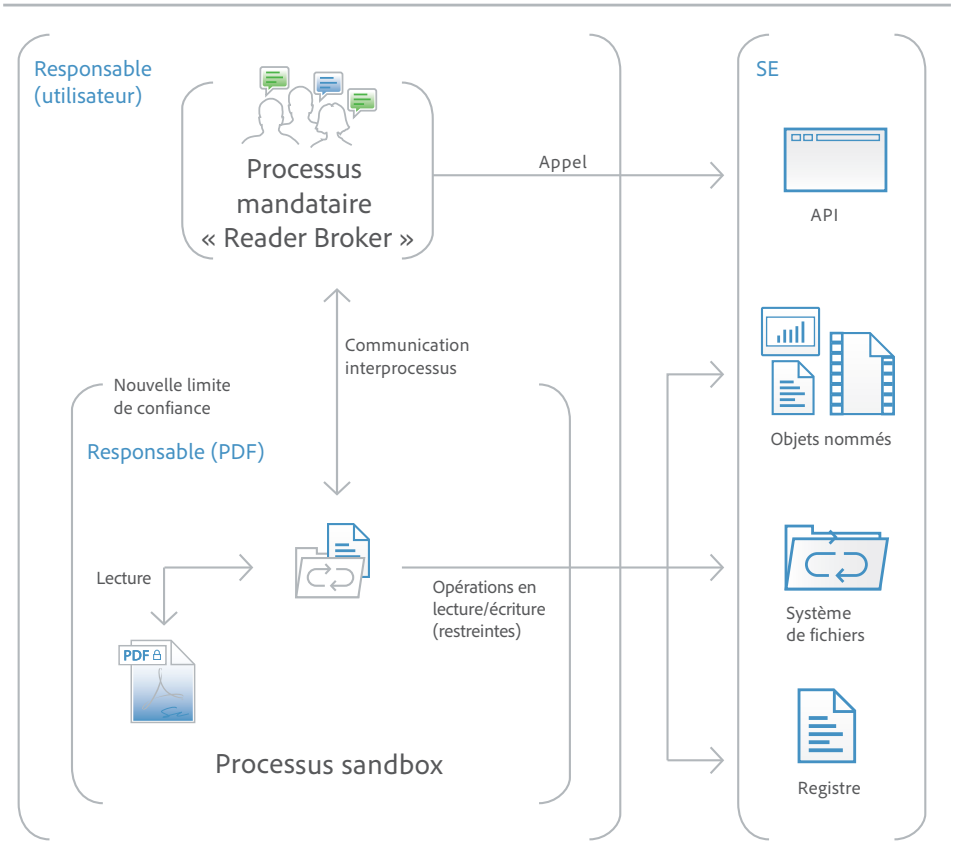
Présentation de la technologie « sandbox »

Très prisée des professionnels de la sécurité, la technologie « sandbox » consiste à créer un environnement confiné (bac à sable) pour l'exécution de programmes assortis de droits ou d'autorisations restreints. Ce bac à sable aide à protéger les systèmes des utilisateurs contre les dommages susceptibles d'être provoqués par des documents non fiables contenant du code exécutable. Dans le contexte d'Acrobat Reader DC, le contenu non fiable désigne tout fichier PDF et les processus qu'il met en œuvre. Reader DC traite tous les fichiers PDF comme s'ils étaient corrompus et isole les traitements invoqués dans le bac à sable.

À l'instar du mode protégé, la vue protégée confine l'exécution des programmes non fiables (par exemple, tout fichier PDF et les processus qu'il invoque) dans un bac à sable restreint afin d'empêcher les opérations en écriture ou en lecture dans le système de fichiers de votre ordinateur par du code malveillant utilisant le format PDF.

La vue protégée part du principe que tous les fichiers PDF sont potentiellement malveillants et confine le traitement dans le bac à sable, sauf si vous déclarez qu'un fichier est fiable. La vue protégée est prise en charge par les deux scénarios d'ouverture de documents PDF — dans l'application Acrobat DC autonome ou dans un navigateur. La vue protégée sous Windows 8 et versions ultérieures s'exécute systématiquement dans un conteneur d'application. Résultat : un environnement encore plus solidement verrouillé pour les clients qui activent la vue protégée.

Lorsque vous ouvrez un fichier potentiellement malveillant dans la vue protégée, une barre de message jaune s'affiche en haut de la fenêtre Acrobat DC. Elle indique que le fichier n'est pas fiable et vous rappelle que vous vous trouvez dans la vue protégée, qui désactive plusieurs fonctionnalités d'Acrobat DC et limite l'interaction de l'utilisateur avec le fichier. En fait, le fichier est en lecture seule et la vue protégée empêche tout contenu malveillant incorporé ou associé à une balise de modifier votre système. Pour faire confiance au fichier et activer toutes les fonctionnalités d'Acrobat DC, vous pouvez cliquer sur le bouton « Activer toutes les fonctions » dans la barre de message jaune. Ce faisant, vous quittez la vue protégée. Le logiciel considère que le fichier est définitivement fiable en l'ajoutant à la liste des emplacements privilégiés d'Acrobat. Chaque ouverture suivante du fichier PDF fiable désactive les restrictions de la vue protégée.



Exécution de JavaScript

Acrobat DC offre des commandes sophistiquées et précises pour gérer l'exécution de JavaScript via des fonctions de liste blanche et de liste noire dans divers environnements comme Microsoft Windows et Macintosh. Le framework Adobe JavaScript Whitelist active JavaScript de manière sélective pour certains fichiers, sites, hôtes ou documents propres au format PDF dont la signature a été validée par un certificat approuvé. De plus, il permet d'utiliser JavaScript dans les workflows,

tout en protégeant les utilisateurs et systèmes contre les attaques ciblant des appels d'API JavaScript spécifiques. En ajoutant sur la liste noire un appel API JavaScript donné, vous empêchez son exécution sans désactiver totalement JavaScript. Les utilisateurs ne peuvent passer outre votre décision, et vous contribuez à protégez votre entreprise contre tout code malveillant.

Framework Whitelist

N'activez JavaScript que pour les workflows fiables en constituant des listes blanches de documents à l'aide des emplacements privilégiés. Ce faisant, vous accordez des autorisations aux zones sécurisées de Microsoft Windows, aux documents certifiés ou aux fichiers, dossiers ou hôtes qui y sont ajoutés.

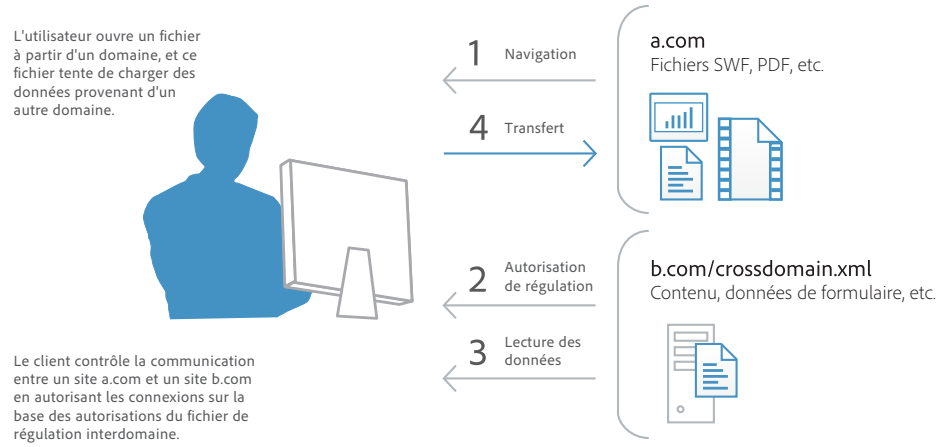
Configuration interdomaine

Par défaut, Acrobat DC désactive tout accès interdomaine interdit aussi bien sur des clients Windows que Mac OS X, empêchant ainsi les pirates d'exploiter des fichiers PDF riches pour accéder aux ressources d'un autre domaine.

Grâce à la prise en charge intégrée des fichiers de régulation interdomaines au niveau du serveur, vous permettez à Acrobat DC et Acrobat Reader DC de gérer des données entre plusieurs domaines. Le fichier de régulation interdomaine — un document XML — est hébergé sur le domaine distant. Il donne accès au domaine source et permet à Acrobat DC ou Acrobat Reader DC de poursuivre la transaction.

L'activation interdomaine Adobe s'avère utile dans les cas de figure suivants :

- Vous avez besoin d'un accès interdomaine sélectif et souhaitez bénéficier d'autres fonctionnalités, telles que l'identification basée sur un certificat numérique.
- Vous voulez centraliser la gestion des autorisations d'accès interdomaine à partir d'un serveur unique.
- Vous implémentez des workflows avec requêtes auprès de plusieurs domaines pour le renvoi de données de formulaire, requêtes SOAP, références à des contenus diffusés en continu et requêtes Net HTTP.



Alertes de sécurité conviviales

En dehors des processus de résolution des incidents et des alertes de sécurité d'Adobe, Acrobat DC met en œuvre une méthode conviviale pour l'affichage des alertes de sécurité, qui apparaissent dans une barre de message jaune. Lorsque la sécurité renforcée est activée et que le fichier PDF n'est pas associé à un emplacement privilégié (répertoriant le contenu fiable), la barre jaune apparaît si le fichier PDF tente d'exécuter les types d'action risqués suivants :

- Accès interdomaine
- Exécution de code JavaScript privilégié
- Lancement d'une URL appelée par JavaScript
- Appel d'une API JavaScript sur liste noire
- Injection de données
- Injection de scripts
- Lecture de contenu multimédia propriétaire incorporé

Dans Acrobat DC et Reader DC, la barre de message jaune qui apparaît en haut du document comporte l'avertissement ou le message d'erreur. L'utilisateur peut approuver ce document une seule fois ou toujours. S'il opte pour « toujours », ce document est ajouté à la liste des documents privilégiés de l'application.

Le bouton « Options » permet aux utilisateurs de configurer la fiabilité à la volée, « une seule fois » ou « toujours ». À l'échelle de l'entreprise, vous pouvez également préconfigurer la fiabilité de fichiers, dossiers et domaines hôtes de sorte que la barre de message jaune n'apparaisse jamais dans le cadre d'un processus fiable.

Sécurité du cloud

Nous surveillons et améliorons en permanence nos services cloud, systèmes et processus pour aider nos clients à faire face aux exigences et défis de plus en plus complexes de la protection des données. Les services Document Cloud, notamment Adobe Sign et les services PDF utilisés par Acrobat DC, sont conçus pour garantir la confidentialité, l'intégrité et la disponibilité de vos documents. Les services Document Cloud sont conformes à de nombreuses normes, certifications et réglementations sectorielles telles que la norme ISO 27001 et les certifications PCI DSS et SOC 2 Type 2. Pour en savoir plus sur notre approche de la sécurité du cloud, consultez notre *Présentation de la sécurité Adobe Document Cloud*.

Sécurité du centre de données

Aujourd'hui, le centre de données de Document Cloud qui héberge les services PDF et le stockage des fichiers réside dans un centre de données ANSI (American National Standards Institute) de niveau 4, géré par notre fournisseur de services cloud de confiance, AWS (Amazon Web Services). AWS contrôle de façon très stricte l'accès aux centres de données, la tolérance aux pannes, les paramètres environnementaux et la sécurité. Seuls les employés approuvés et habilités d'Adobe, les employés des fournisseurs de services cloud et les sous-traitants exerçant une activité légitime et documentée sont autorisés à accéder au site sécurisé en Virginie (États-Unis). Pour en savoir plus sur la sécurité du centre de données AWS, consultez le site *https://aws.amazon.com/fr/security/*.

Cryptage et confidentialité des données

La confidentialité fait partie intégrante des produits et services Adobe, et notamment des services Document Cloud. Document Cloud sécurise les documents et ressources stockés à l'aide d'un cryptage AES 256 bits (conforme aux directives du National Institute of Standards and Technology) et protège les données transmises à l'aide du protocole HTTPS et d'une connexion cryptée TLS.

Les employés Document Cloud et fournisseurs de confiance ont accès aux données client uniquement dans le cadre de certaines activités commerciales et de support, ou pour se conformer aux obligations légales. Adobe ne fournit aux administrations aucun accès direct ou systématique aux données clients stockées dans ses centres de données. Pour en savoir plus sur les politiques de confidentialité d'Adobe, consultez le site *www.adobe.com/fr/privacy*.

Intégration avec les architectures des systèmes d'exploitation

Sécurité permanente

En exploitant les mécanismes de sécurité intégrés et permanents de Windows et Mac OS X, Acrobat DC offre un niveau de protection supplémentaire contre les tentatives de corruption de mémoire ou de prise de contrôle des postes de travail.

La prévention de l'exécution des données (DEP) limite l'injection de données ou de code dangereux dans les emplacements mémoire protégés par le système d'exploitation Windows. Apple offre une protection similaire sous Mac OS X Lion, notamment aux niveaux « stack » et « heap », et l'étend aux applications 32 bits et 64 bits, rendant la totalité des applications plus résistantes aux attaques.

La technologie de randomisation de l'espace d'adressage (ASLR) masque les emplacements des composants système dans la mémoire et les fichiers d'échange afin de compliquer la tâche des pirates. Elle est utilisée à la fois sous Windows et Mac OS X Lion. Sous Mac OS X Lion, cette technologie ASLR est étendue aux applications 32 bits et 64 bits.

Configuration au niveau du registre et des listes de propriétés

Acrobat DC vous procure une multitude d'outils pour gérer les paramètres de sécurité, y compris les préférences de niveau registre (Windows) et liste de propriétés (Mac OS). Ces paramètres permettent de configurer les clients avant et après le déploiement de manière à :

- activer ou désactiver la sécurité renforcée ;
- activer ou désactiver les emplacements privilégiés ;
- spécifier des emplacements privilégiés prédéfinis ;
- verrouiller certaines fonctionnalités et désactiver l'interface de l'application afin que les utilisateurs finaux ne modifient pas les paramètres ;
- désactiver, activer ou configurer la quasi-totalité des autres fonctions de sécurité.

Déploiement et administration facilités

Renforcement de la sécurité logicielle

Les renforcements de la sécurité, comme la vue protégée, sont le fruit des investissements massifs réalisés par Adobe dans l'ingénierie pour protéger Acrobat DC contre les menaces. En renforçant la protection des logiciels contre les attaques, Adobe peut réduire, voire éliminer le recours aux mises à niveau de sécurité hors bande et diminuer l'urgence des mises à niveau régulières programmées. Tout cela contribue à améliorer la flexibilité opérationnelle et à réduire le coût total de possession, notamment dans les grands environnements qui exigent une sécurité maximale.

Prise en charge de Citrix et de la virtualisation d'applications

Grâce à la prise en charge des licences nominatives pour Citrix XenApp, Citrix XenDesktop, VMware Horizon et Microsoft App-V, vous pouvez offrir à vos utilisateurs un accès distant et sécurisé aux fonctionnalités d'Acrobat dont ils ont besoin.

Prise en charge des solutions de gestion de la mobilité

Adobe s'engage à aider les entreprises à répondre à la demande de solutions de productivité mobiles tout en préservant la sécurité et la conformité de l'entreprise. Les applications mobiles Acrobat Reader et Adobe Sign prennent toutes deux en charge la plate-forme de gestion de la mobilité, Android for Work, et Adobe Acrobat Reader pour Microsoft Intune est disponible pour les appareils iOS and Android. Acrobat Reader prend également en charge la plate-forme AppConfig. Pour en savoir plus sur les *ressources informatiques*.

Prise en charge de Windows Server Group Policy Objects et Microsoft Active Directory

Windows Server Group Policy Objects (GPO) et Microsoft Active Directory vous permettent d'automatiser l'administration de systèmes informatiques sur le mode 1 à n. En prenant désormais en charge les modèles d'administration Microsoft ADM (Active Directory Administrative) certifiés pour la stratégie de groupe dans Acrobat DC, Adobe autorise l'installation de logiciels à la demande et la réparation automatique des applications. Si vous avez besoin de procéder à une configuration complémentaire des applications après leur déploiement, utilisez les modèles ADM pour propager l'application des paramètres requis à l'échelle de votre établissement.

Prise en charge de Microsoft SCCM/SCUP

Avec Acrobat DC, vous pouvez dorénavant importer et publier efficacement les mises à jour via Microsoft System Center Configuration Manager (SCCM) pour que les postes de travail Windows gérés disposent toujours des derniers correctifs et mises à jour en date.

Avec la prise en charge des catalogues Microsoft SCUP (System Center Updates Publisher), vous automatisez les mises à jour d'Acrobat DC et simplifiez les déploiements logiciels. SCUP, qui assure l'importation automatique des mises à jour publiées par Adobe dès qu'elles sont disponibles, facilite et rationalise vos déploiements Acrobat DC. L'intégration avec SCCM et SCUP contribue à réduire le coût total de possession de vos logiciels Adobe, car vous pouvez gagner en simplicité et en rapidité en appliquant les correctifs à l'échelle de l'entreprise.

Prise en charge d'Apple Package Installer et d'Apple Remote Desktop

Dans Acrobat DC, Adobe a implémenté le programme Apple Package Installer standard fourni avec Mac OS X au lieu du programme d'installation Adobe propriétaire. Ce choix facilite le déploiement des logiciels Acrobat sur les postes de travail Macintosh dans l'entreprise, car vous pouvez à présent utiliser le logiciel d'administration Apple Remote Desktop pour gérer leur déploiement initial, puis les mises à jour et correctifs ultérieurs depuis un point central.

Mises à jour et correctifs cumulatifs régulièrement programmés

Pour vous aider à maintenir vos logiciels à jour, Adobe fournit régulièrement des mises à niveau qui contiennent des mises à jour de fonctionnalités et des correctifs de sécurité. Pour répondre rapidement aux attaques ponctuelles, Adobe fournit également des correctifs d'urgence. Adobe utilise le plus souvent possible des correctifs cumulatifs pour réduire les efforts et les coûts nécessaires pour maintenir les systèmes à jour. Adobe teste également ses correctifs de sécurité de manière intensive préalablement à leur publication en vue de garantir leur compatibilité avec les installations et processus existants.

La date de chaque mise à jour planifiée est annoncée en avant-première sur le blog Adobe PSIRT (Product Security Incident Response Team) à l'adresse *blogs.adobe.com/psirt*.

Pour accéder aux derniers bulletins et avis de sécurité sur les produits Adobe, consultez le site *www.adobe.com/fr/support/security*. Pour plus d'informations sur les produits et fonctionnalités de sécurité Adobe, consultez l'Adobe Security Library à l'adresse *www.adobe.com/go/learn_acr_appsecurity_en*.

Adobe Customization Wizard et Enterprise Toolkit

Pour mieux maîtriser les déploiements dans l'entreprise, Adobe propose les outils suivants :

- **Adobe Customization Wizard** — Utilitaire téléchargeable gratuitement qui vous permet de personnaliser le programme d'installation d'Acrobat et de configurer les fonctionnalités de l'application avant le déploiement.
- **Adobe Enterprise Toolkit (ETK) pour Acrobat et Windows** — Application personnalisable avec mises à jour automatiques, qui contient le guide de référence sur les préférences. Adobe ETK inclut également de nombreuses ressources pertinentes pour les administrateurs.

Pour en savoir plus sur ces outils, consultez la page *ressources informatiques*.

Conclusion

Avec Acrobat DC, Adobe renforce la sécurité des documents PDF et de vos données. Sécurité applicative renforcée conçue pour vous aider à vous prémunir contre le vol de données confidentielles et de propriété intellectuelle, blocage de l'installation de programmes malveillants dangereux sur vos systèmes informatiques, intégration avec d'autres outils simplifiant considérablement l'administration des déploiements dans toute l'entreprise : Acrobat DC offre des niveaux de sécurité accrus pour un coût d'exploitation modique, jamais égalé par les précédentes versions d'Acrobat.

Pour plus d'informations
Informations détaillées
sur la solution :
www.adobe.com/fr/security

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
États-Unis
www.adobe.com, www.adobe.com/fr

7/17