Présentation de la sécurité d'Adobe Acrobat DC avec services Document Cloud

Résumé

Adobe attache une très grande importance à la sécurité des expériences digitales. Les pratiques de sécurité sont profondément ancrées dans nos processus opérationnels et de développement logiciel, ainsi que dans nos outils, et sont scrupuleusement suivies par nos équipes transversales pour prévenir, détecter et résoudre rapidement les incidents. De plus, notre collaboration avec des partenaires, chercheurs de renom, instituts de recherche en sécurité et autres acteurs sectoriels nous permet de rester au fait des toutes dernières menaces et vulnérabilités. Nous incorporons régulièrement des techniques de sécurité avancées dans les produits et les services que nous proposons.

Les services Adobe liés aux contenus des clients ont également obtenu de nombreuses certifications sectorielles. Pour voir la liste détaillée de toutes les certifications et normes de conformité, ainsi que des règlementations actuellement prises en charge par les produits et solutions Adobe, consultez la liste actuelle des certifications, normes et règlementations. Pour obtenir des informations sur le Règlement général sur la protection des données (RGPD), consultez la page consacrée à la préparation au RGPD.

Cet article technique décrit l'approche de « défense en profondeur » et les procédures mises en œuvre par Adobe pour renforcer la sécurité des logiciels Adobe Acrobat DC et Acrobat Reader DC, de la solution et des services Document Cloud, ainsi que des données associées.

Sommaire

Bien qu'Adobe Sign fasse partie des services PDF de Document Cloud, ses fonctionnalités de sécurité sont indépendantes.

Présentation d'Acrobat DC avec services Document Cloud

En associant le dernier logiciel Acrobat pour ordinateur, les fonctionnalités avancées de l'application mobile Acrobat Reader et les services en ligne Adobe Document Cloud, Adobe Acrobat DC aide les entreprises à satisfaire les exigences des utilisateurs finaux qui veulent rester connectés et productifs sur l'ensemble des équipements, tout en garantissant leur sécurité. Avec Adobe Acrobat DC et les services Document Cloud, les clients peuvent convertir du contenu en un document électronique à partager, et générer, manipuler et transformer aisément des fichiers PDF à partir des services cloud, mais aussi des applications Adobe pour ordinateur et appareils mobiles.

Fonctionnalités de sécurité des documents Acrobat

Biffure

Adobe Acrobat DC inclut un ensemble d'outils de biffure permettant aux clients de protéger des informations sensibles ou confidentielles, et notamment de supprimer définitivement du texte et des images d'un document avant sa distribution. De plus, les utilisateurs peuvent rechercher et biffer différents contenus sur la base de modèles, tels que des adresses e-mail et des numéros de téléphone ou de carte bancaire. Les informations sélectionnées sont entièrement supprimées du fichier, et pas simplement masquées, comme c'est le cas avec d'autres outils ou méthodes. Grâce à la fonction d'assainissement des documents, les clients peuvent également supprimer les informations cachées et les objets non graphiques, comme les métadonnées éventuellement présentes dans le document PDF.

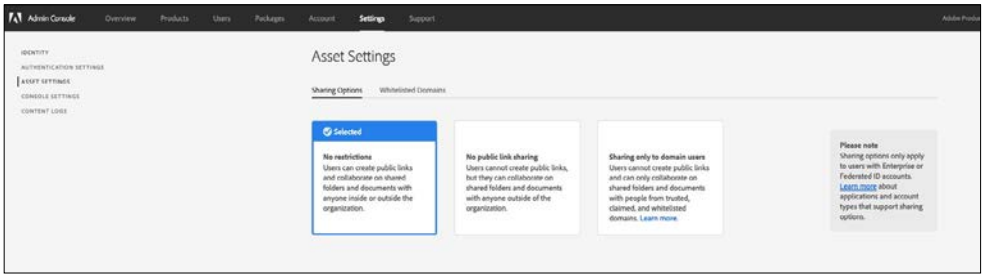
Partage de fichiers

Tous les fichiers Document Cloud stockés dans le cloud portent la mention « Privé », ce qui signifie que le contenu n'est visible que pour l'utilisateur qui l'a chargé. Ce dernier doit d'ailleurs prendre des mesures explicites pour partager ce contenu qui, à défaut, demeurera privé. Les fichiers Document Cloud peuvent être partagés en envoyant un lien par e-mail, par SMS ou via un logiciel de collaboration aux destinataires.

Les utilisateurs des services Document Cloud ont le choix entre deux options de partage : Afficher le fichier ou Réviser le fichier. Si l'utilisateur envoie le lien en activant l'option Afficher le fichier, le destinataire n'aura accès au contenu qu'en lecture seule. En revanche, s'il envoie le document pour révision, le destinataire pourra l'annoter, mais en aucun cas le modifier.

Paramètres des assets et restrictions de partage

Les paramètres des assets permettent de contrôler les modalités de partage des documents en dehors de l'entreprise. L'administrateur IT peut sélectionner un paramètre restrictif pour empêcher les employés d'utiliser certaines fonctions de partage au sein de Document Cloud. Il peut notamment limiter l'autorisation d'envoi d'invitations aux personnes faisant partie de domaines déposés, de confiance et en liste blanche. Lorsque cette règle est définie, les utilisateurs ne peuvent pas partager les assets détenus par l'entreprise avec des personnes qui ne figurent pas sur la liste des domaines autorisés.



Microsoft Information Protection (MIP)

Les clients utilisant Acrobat DC ou Acrobat Reader DC pour ouvrir des fichiers protégés avec les solutions Microsoft Information Protection (MIP), dont Azure Information Protection (AIP) et Information Protection pour Microsoft 365, sont invités à consulter ce document.

Mode protégé d'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) et a été introduit pour la première fois dans Adobe Reader X.

La technologie « sandbox » permet de créer un environnement confiné pour l'exécution de programmes assortis de droits ou d'autorisations restreints. Cette solution 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 désignerait tout fichier PDF et les processus qu'il met en œuvre. Acrobat Reader DC traite tous les fichiers PDF comme s'ils étaient corrompus et isole les traitements invoqués dans la technologie « sandbox ».

Le mode protégé d'Acrobat Reader DC offre un rempart contre les pirates qui tentent d'installer des programmes malveillants sur un système IT, mais aussi contre les utilisateurs malintentionnés en les empêchant d'accéder aux données confidentielles et à la propriété intellectuelle de l'entreprise, et de les extraire de ses réseaux. Activé par défaut à chaque lancement d'Acrobat Reader DC, ce mode restreint le niveau d'accès octroyé aux programmes, protégeant ainsi les postes sous Microsoft Windows des fichiers PDF malveillants qui essaieraient 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.

Sous Windows 8 et versions ultérieures, le mode protégé peut également s'exécuter dans un conteneur d'application Windows, offrant ainsi un environnement encore plus solidement verrouillé aux clients qui activent ce mode.

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 » (bac à sable) pour les riches fonctionnalités d'Acrobat DC. Dans Acrobat DC, Adobe étend les fonctionnalités du mode protégé en bloquant non seulement les attaques en écriture dans le système de l'ordinateur par du code malveillant utilisant le format PDF, mais aussi les attaques en lecture visant à dérober les données confidentielles ou la propriété intellectuelle via des fichiers PDF.

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 une sandbox restreinte afin d'empêcher les opérations en écriture ou en lecture dans le système de fichiers de l'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 la sandbox, sauf si l'utilisateur déclare 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 et 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.

Lorsqu'un utilisateur ouvre un fichier non fiable dans la vue protégée, une barre de message s'affiche en haut de la fenêtre Acrobat DC. Elle indique que le fichier n'est pas fiable et rappelle à l'utilisateur qu'il se trouve dans la vue protégée, qui désactive plusieurs fonctionnalités d'Acrobat DC et limite les possibilités d'interaction avec le fichier. En fait, le fichier est en lecture seule et la vue protégée empêche tout contenu incorporé ou associé à une balise de modifier le système.

Pour faire confiance au fichier et activer toutes les fonctionnalités d'Acrobat DC, l'utilisateur peut cliquer sur le bouton « Activer toutes les fonctions » dans la barre de message. Ce faisant, il quitte 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.

Architecture des services Document Cloud

Les services Adobe Document Cloud sont les suivants :

- **Organiser un PDF** — Insérez, supprimez, réagencez et faites pivoter des pages dans un PDF.
- **Créer un fichier PDF** — Convertissez des documents Word, Excel et PowerPoint, ainsi que des images et des photos en fichiers PDF.
- **Exporter un fichier PDF** — Convertissez aisément des PDF en fichiers Microsoft Word, Excel, PowerPoint ou RTF modifiables.
- **Modifier un fichier PDF** — Modifiez aisément des PDF depuis votre appareil mobile ou ordinateur portable.
- **Combiner en PDF** — Regroupez plusieurs fichiers dans un seul et même PDF et assemblez des liasses de documents, où que vous soyez.
- **Envoyer et effectuer le suivi** — Envoyez des documents, assurez leur suivi et confirmez leur distribution.
- **Adobe Scan** — Capturez du contenu et convertissez-le en fichier PDF indexé de qualité.
- **Adobe Sign** — Préparez et envoyez des documents en vue d'y ajouter des signatures électroniques sécurisées, fiables et juridiquement recevables sur n'importe quel appareil.

Sécurité des services Document Cloud

Gestion des droits et des identités

Avec Adobe Admin Console, les administrateurs IT peuvent gérer les droits d'accès des utilisateurs aux services Adobe Document Cloud à l'aide de licences nominatives. Acrobat Document Cloud prend en charge trois (3) types de licence nominative :

- **Adobe ID** — Les comptes sont hébergés par Adobe et administrés par les utilisateurs qui les créent, les détiennent et les contrôlent. Pour les comptes associés à un Adobe ID, l'accès aux services Acrobat Document Cloud est soumis à l'autorisation d'un administrateur IT.
- **Enterprise ID** — Les comptes sont hébergés par Adobe et administrés par l'entreprise. Ils sont créés et contrôlés par les administrateurs IT de l'établissement client. L'entreprise détient et administre les comptes utilisateur et toutes les ressources associées.
- **Federated ID** — Les comptes sont administrés par l'entreprise. Tous les profils d'identité sont fournis par le système de gestion des identités SSO du client, et sont créés, détenus et contrôlés par le personnel IT. Adobe fournit une intégration avec la plupart des fournisseurs d'identité compatibles SAML 2.0.

La plupart des entreprises utilisent des Enterprise ID ou Federated ID pour leurs employés, sous-traitants et indépendants, à condition que l'adresse e-mail fasse partie du domaine de la société, ce qui leur permet de gérer les droits ainsi que le contenu généré par l'utilisateur et stocké à l'aide de cet ID. Pour plus d'informations sur ces types d'identité, consultez le site du support technique d'Adobe.

Pour le stockage des mots de passe des Adobe ID et Enterprise ID, l'algorithme de hachage SHA-256 est associé à un salage des mots de passe et à un grand nombre d'itérations de hachage. Adobe surveille en permanence les comptes qu'il héberge pour identifier les activités inhabituelles ou anormales, et évalue ces informations afin de faire face rapidement aux menaces. En revanche, Adobe ne gère pas les mots de passe des comptes associés à un Federated ID. Pour en savoir plus, consultez la présentation de la sécurité des services de gestion des identités d'Adobe.

Signatures électroniques

Pour manipuler des signatures en toute sécurité, les utilisateurs des services Document Cloud ont le choix entre deux outils :

- **Remplir et signer** — Optimisé par Adobe Sign, cet outil 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 automatiquement les documents signés et les pistes d'audit. Outre l'application de mesures de sécurité tout au long du processus, les documents et pistes d'audit sont certifiés par Adobe à l'aide d'un sceau infalsifiable.

Le suivi n'est pas disponible sur les appareils mobiles.

Pour en savoir plus sur Adobe Sign et ses fonctionnalités de sécurité, consultez la présentation technique d'Adobe Sign.

- **Certificats** — Cet outil permet de signer des documents avec des signatures numériques basées sur des certificats provenant de prestataires fiables qui figurent sur la liste AATL (Adobe Approved Trust List) ou EUTL (European Union Trusted List). L'utilisation d'un identifiant de certificat délivré par une autorité de certification tierce agréée est, d'une manière générale, considérée comme une méthode de signature électronique sécurisée. 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 automatiquement 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 AES-256/RS-A4096/SHA-512 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 (PKI). Avec l'outil Certificats, les utilisateurs peuvent aussi appliquer des horodatages sur les documents et les certifier via un sceau infalsifiable.

Stockage de contenu via les services Document Cloud

Bien que les administrateurs soient habilités à allouer un espace de stockage dans le cloud aux comptes Enterprise ID et Federated ID via Adobe Admin Console, ils ne peuvent toutefois pas accéder directement aux fichiers Document Cloud de l'utilisateur. En configuration Services partagés, lorsqu'un Enterprise ID ou Federated ID avec espace de stockage est supprimé, les anciens utilisateurs de ces comptes n'ont plus accès aux données de l'espace de stockage qui sont supprimées au bout de 90 jours.

Les administrateurs peuvent également utiliser Admin Console pour allouer un espace de stockage aux comptes associés à un Adobe ID. S'ils ne peuvent pas supprimer ces comptes, ils ont néanmoins la possibilité de révoquer les droits d'accès aux services et applications et de supprimer l'espace de stockage octroyé à l'entreprise. Les données associées à ces comptes sont supprimées au bout de 90 jours.

Les services Adobe Document Cloud utilisent le stockage multilocataires. Les contenus des clients sont traités par une instance Amazon EC2 (Elastic Compute Cloud) et stocké dans une combinaison de conteneurs (« buckets ») Amazon S3 (Simple Storage Service) et via une instance MongoDB exécutée sur un Amazon EBS (Elastic Block Store). Le contenu proprement dit est stocké dans des conteneurs Amazon S3 et les métadonnées s'y rapportant dans un Amazon EBS via MongoDB. Le tout est protégé par un système IAM (Identity and Access Management) dans une région AWS (Amazon Web Services).

Le contenu stocké dans un Amazon EBS est protégé par un cryptage AES 256 bits basé sur des algorithmes de chiffrement validés par la norme FIPS (Federal Information Processing Standards) 140-2 et conformes aux directives 800-57 du NIST (National Institute of Standards and Technology).

Les données stockées font l'objet d'une redondance dans plusieurs centres de données et sur plusieurs équipements dans chaque centre. Tout le trafic réseau fait systématiquement l'objet d'une vérification des données et de calculs de contrôle pour prévenir toute corruption et garantir l'intégrité des données. Enfin, le contenu stocké est répliqué automatiquement de manière synchrone dans d'autres centres de données de la zone géographique du client afin de garantir l'intégrité des données même en cas de perte sur deux sites.

Pour plus d'informations sur les services Amazon sous-jacents, consultez les pages web suivantes :

- MongoDB
- Amazon S3
- Service de gestion de clés AWS KMS
- Service Amazon EC2

Clé de cryptage dédiée

Par défaut, le contenu et les ressources stockés dans des Amazon S3 sont cryptés à l'aide de clés de chiffrement symétriques AES 256 bits, propres à chaque client et à son domaine réservé. Si les administrateurs veulent ajouter des couches de contrôle et de sécurité supplémentaires pour tout ou partie des domaines de leur entreprise, ils peuvent utiliser une clé de cryptage dédiée, gérée par le service AWS KMS et faisant l'objet d'une rotation annuelle automatique.

Les administrateurs peuvent également révoquer cette clé dédiée via Admin Console, ce qui a pour effet de rendre les données cryptées avec cette clé inaccessibles aux utilisateurs finaux, et d'empêcher le transfert et le téléchargement de contenu jusqu'à réactivation de la clé.

Remarque : les clés de cryptage dédiées permettent de crypter les fichiers Adobe Document Cloud, mais pas les métadonnées correspondantes.

Pour en savoir plus sur la gestion du cryptage à l'aide d'une clé dédiée, consultez sur le site Adobe les pages d'aide suivantes :

- Gestion du cryptage
- Forum aux questions (FAQ) sur les clés de cryptage dédiées

Amazon Web Services

Comme mentionné précédemment, tous les composants des services Adobe Document Cloud sont hébergés sur AWS, et notamment Amazon EC2 et Amazon S3, aux États-Unis. Amazon EC2 est un service web qui fournit des fonctions de calcul automodulables dans le cloud. Amazon S3 est communément reconnu comme une infrastructure ultra-fiable qui permet de stocker et d'extraire des données, quel que soit leur volume.

La plateforme AWS propose des services conformes aux pratiques standard et passe régulièrement les certifications et audits reconnus sur le marché. Pour en savoir plus sur AWS et les contrôles de sécurité d'Amazon, consultez la page dédiée à la sécurité dans le cloud d'AWS.

Responsabilités opérationnelles d'AWS et d'Adobe

AWS exploite, gère et contrôle les composants des services Adobe Document Cloud depuis la couche de virtualisation (l'hyperviseur) jusqu'à la sécurité physique des sites où ils sont hébergés. Adobe est, pour sa part, responsable de la gestion du système d'exploitation invité (y compris des mises à jour et correctifs de sécurité) et des logiciels applicatifs, ainsi que de la configuration du pare-feu du groupe de sécurité fourni par AWS.

AWS gère également l'infrastructure cloud qu'utilise Adobe pour allouer des ressources IT élémentaires, notamment pour le traitement et le stockage des données. L'infrastructure AWS comprend des sites, des réseaux, des équipements, mais aussi des logiciels (systèmes d'exploitation hôtes, logiciels de virtualisation, etc.) prenant en charge l'allocation et l'utilisation de ces ressources. Amazon a conçu et gère AWS conformément aux pratiques standard et à de nombreuses normes de sécurité.

Gestion sécurisée

Adobe utilise les protocoles SSH (Secure Shell) et SSL (Secure Sockets Layer) pour gérer les connexions à l'infrastructure AWS.

Emplacement géographique des données clients sur le réseau AWS

L'ensemble du contenu généré par l'utilisateur, et transféré vers Document Cloud, est stocké dans des centres de données AWS en Virginie (côte Est des États-Unis). Il est sauvegardé dans chaque centre de données, ainsi que dans d'autres centres de la région, à des fins d'équilibrage de charge et de redondance.

Emplacement géographique des données d'identité sur le réseau AWS

Les données d'identité sont stockées dans des centres de données AWS situés en Virginie (côte Est des États-Unis), dans l'Oregon (côte Ouest des États-Unis), en Irlande (à l'ouest de l'UE) et à Singapour (partie sud-est de la région Asie Pacifique). Elles sont répliquées dans tous les centres de données. Adobe respecte les lois en vigueur relatives au transfert de données d'un pays à l'autre, comme l'explique en détail la page https://www.adobe.com/fr/privacy/eudatatransfers.html.

Isolement des données clients/séparation des clients

AWS utilise de puissantes fonctions de contrôle et d'isolement. En tant qu'environnement virtualisé multilocataire, AWS met en œuvre des processus de gestion de la sécurité et applique divers contrôles en vue d'isoler chaque client des clients AWS. Adobe utilise en outre le système IAM (Identity and Access Management) d'AWS pour restreindre l'accès aux instances de calcul et de stockage.

Architecture réseau sécurisée

AWS utilise des équipements réseau, notamment des pare-feu et autres systèmes de protection pour contrôler les communications qui transitent à l'intérieur et à l'extérieur du réseau. Ces équipements exploitent des jeux de règles, des listes de contrôle d'accès (ACL) et des configurations pour acheminer les informations vers certains systèmes IT. Des listes ACL ou règles de trafic sont présentes sur chaque interface gérée pour assurer et gérer le trafic.

L'équipe Amazon Information Security valide l'ensemble des règles ACL et les transfère automatiquement vers chaque interface gérée à l'aide de l'outil ACL-Manage d'AWS. Les listes ACL sont ainsi parfaitement à jour.

Contrôle et protection du réseau

AWS utilise divers systèmes de surveillance automatisés pour garantir un haut niveau de performance et de disponibilité. Les outils de contrôle servent à détecter les activités inhabituelles ou non autorisées aux points de communication (entrées et sorties). Le réseau AWS offre une solide protection contre les problèmes de sécurité réseau classiques :

- Attaques DDoS (Distributed Denial Of Service)
- Attaques MITM (Man in the Middle)
- Usurpation d'adresses IP
- Balayage de ports
- Reniflage de paquets par d'autres locataires

Pour en savoir plus sur le contrôle et la protection du réseau, consultez la page dédiée à la sécurité dans le cloud d'AWS.

Détection des intrusions

Adobe surveille activement les services Adobe Document Cloud au moyen de systèmes standard de détection et de prévention des intrusions.

Consignation

Adobe effectue une journalisation côté serveur de l'activité des utilisateurs des services Adobe Document Cloud afin de diagnostiquer les interruptions de service, des problèmes spécifiques et autres bogues signalés. Pour faciliter l'analyse de ces incidents, les journaux stockent uniquement les identifiants Adobe et ne contiennent aucune combinaison nom d'utilisateur/mot de passe. L'équipe de support technique, les ingénieurs concernés et certains développeurs sont les seuls à avoir accès aux journaux pour diagnostiquer les problèmes spécifiques susceptibles de se produire.

Surveillance des services

AWS contrôle les systèmes et équipements électriques, mécaniques et de survie afin de repérer immédiatement les éventuels problèmes techniques. Une maintenance préventive est assurée en continu pour garantir le bon fonctionnement de ces équipements.

Stockage et sauvegarde des données

Adobe stocke la totalité des données des services Adobe Document Cloud dans Amazon S3, une infrastructure de stockage à haute durabilité. Pour préserver cette durabilité, les fonctions PUT et COPY d'Amazon S3 stockent en mode synchrone les données des clients sur plusieurs sites. Les objets sont, quant à eux, stockés de façon redondante sur plusieurs équipements dans divers centres d'une même région Amazon S3.

Amazon S3 détecte les corruptions de paquets de données lors des opérations de stockage et d'extraction par le biais de sommes de contrôle. Les objets de données Amazon S3 sont répliqués uniquement au sein du cluster régional où les données sont stockées.

Les métadonnées sont répliquées via la création d'instantanés des volumes Amazon EBS et stockées dans des conteneurs similaires à Amazon S3. Pour en savoir plus sur la sécurité d'AWS, consultez la page dédiée à la sécurité dans le cloud d'AWS.

Gestion des modifications

Les changements routiniers, en urgence et de configuration apportés à l'infrastructure AWS existante sont autorisés, consignés, testés, validés et documentés conformément aux normes sectorielles des systèmes similaires. Les mises à jour d'AWS sont programmées par Amazon de façon à limiter l'impact côté clients. Ces derniers sont informés par e-mail ou via l'AWS Service Health Dashboard des perturbations potentielles du service. Adobe gère également un système de suivi de l'état d'Adobe Document Cloud.

Gestion des correctifs

AWS est responsable des systèmes de correction permettant d'accéder à ses services, comme l'hyperviseur et la mise en réseau. Adobe prend en charge l'application de correctifs pour ses systèmes d'exploitation (OS) invités, logiciels et applications exécutés dans AWS. Lorsque des correctifs sont nécessaires, Adobe propose une nouvelle instance à sécurité renforcée du système d'exploitation et de l'application plutôt qu'un correctif à proprement parler.

Contrôles physiques et environnementaux AWS

Les contrôles physiques et environnementaux AWS sont décrits dans les rapports SOC Type 1 et SOC Type 2. La section ci-dessous présente une partie des mesures et contrôles de sécurité mis en place dans les centres de données AWS du monde entier. Pour en savoir plus sur la sécurité d'AWS, consultez la page dédiée à la sécurité dans le cloud d'AWS.

Sécurité des sites physiques

Les centres de données AWS reposent sur des techniques standard en matière d'architecture et d'ingénierie. Ils sont hébergés sur des sites banalisés. L'accès physique est contrôlé à la fois dans l'enceinte et aux points d'accès du bâtiment par des professionnels de la sécurité, des systèmes de vidéo-surveillance et de détection d'intrusion, et d'autres moyens électroniques. Le personnel autorisé doit procéder à deux reprises au moins à une authentification à deux facteurs pour pouvoir accéder aux étages des centres de données. Tous les visiteurs et sous-traitants sont tenus de présenter une pièce d'identité. Ils sont enregistrés à leur arrivée, puis accompagnés en permanence par des personnes habilitées.

AWS n'autorise l'accès aux centres de données et la diffusion d'informations qu'aux personnes qui en ont besoin à des fins professionnelles. Lorsqu'un employé n'a plus besoin de tels privilèges, son accès est immédiatement révoqué, même s'il fait toujours partie d'Amazon ou d'AWS. L'accès physique aux centres de données par le personnel d'AWS est systématiquement consigné et audité.

Systèmes anti-incendie

Un équipement de détection et d'extinction automatique des incendies est installé dans chaque centre de données AWS. Des détecteurs de fumée sont présents dans tous les centres de données, les sites abritant l'infrastructure mécanique et électrique, les salles de refroidissement et les pièces contenant les générateurs. Ces zones sont protégées soit par des installations d'extinction automatique à eau et à préaction à double verrouillage, soit par des extincteurs automatiques à gaz.

Environnement contrôlé

AWS utilise un système de climatisation pour maintenir une température de fonctionnement constante pour les serveurs et autres équipements, ce qui empêche les surchauffes et réduit les risques d'interruption de service. Les centres de données AWS garantissent le maintien de conditions ambiantes optimales. La température et l'humidité sont surveillées et régulées par le personnel AWS et différents systèmes.

Alimentation de secours

Les systèmes d'alimentation électrique des centres de données AWS offrent une totale redondance et fonctionnent 24 heures sur 24, 7 jours sur 7, y compris lors des opérations de maintenance. Des systèmes d'alimentation sans interruption (UPS) fournissent une alimentation de secours en cas de panne électrique au niveau des charges critiques essentielles des installations. Les centres de données utilisent des générateurs pour alimenter l'ensemble des installations en cas de panne.

Reprise sur incident

Les centres de données AWS offrent un haut niveau de disponibilité et de tolérance aux pannes système ou matérielles. Clusterisés dans différentes zones géographiques, ils restent en ligne 24 heures sur 24, 7 jours sur 7, 365 jours par an. Aucun d'entre eux n'est « inactif ». En cas de panne, le trafic des données clients est automatiquement détourné de la zone impactée.

Les applications stratégiques étant déployées selon une configuration N+1, en cas de panne, la capacité reste suffisante pour permettre un équilibrage de la charge du trafic vers les autres sites. Pour en savoir plus sur les protocoles de reprise sur incident d'AWS, consultez la page dédiée à la sécurité dans le cloud d'AWS.

Gestion des risques et des vulnérabilités par Adobe

Adobe met un point d'honneur à garantir la souplesse et la précision du processus de gestion des risques et des vulnérabilités, de résolution des incidents et de limitation des menaces. Nous surveillons en permanence les menaces, partageons nos informations avec les experts de la sécurité dans le monde entier, résolvons rapidement les incidents et transmettons ces informations à nos équipes de développement afin d'atteindre un niveau de sécurité maximal pour tous les produits et services Adobe.

Tests d'intrusion

Adobe valide des entreprises de sécurité tierces de premier plan et travaille avec elles pour réaliser des tests d'intrusion capables de détecter des vulnérabilités potentielles et d'améliorer la sécurité globale de ses produits et services. Après réception du rapport établi par le tiers, Adobe documente ces vulnérabilités, évalue les niveaux de gravité et de priorité, puis définit une stratégie de limitation des risques ou un plan de réparation. Adobe effectue un test d'intrusion complet chaque année et procède à une analyse des vulnérabilités tous les mois.

En interne, chaque trimestre et avant chaque lancement, l'équipe en charge de la sécurité d'Adobe Document Cloud soumet l'ensemble des composants et services à une évaluation des risques. Elle collabore avec les responsables du développement et des opérations techniques pour neutraliser toutes les vulnérabilités à haut risque avant le lancement de chaque version. Pour en savoir plus sur les procédures de test d'intrusion d'Adobe, consultez la présentation de l'ingénierie sécurisée d'Adobe.

Résolution et notification des incidents

Adobe met tout en œuvre pour limiter les vulnérabilités et menaces qui apparaissent chaque jour. La société est d'ailleurs abonnée aux listes d'annonce des vulnérabilités du secteur, notamment US-CERT (Computer Emergency Readiness Team), Bugtraq et SANS, ainsi qu'aux listes des dernières alertes publiées par les principaux éditeurs de logiciels de sécurité.

Pour en savoir plus sur le processus de résolution et de notification des incidents mis en œuvre par Adobe, consultez la présentation de la résolution des incidents.

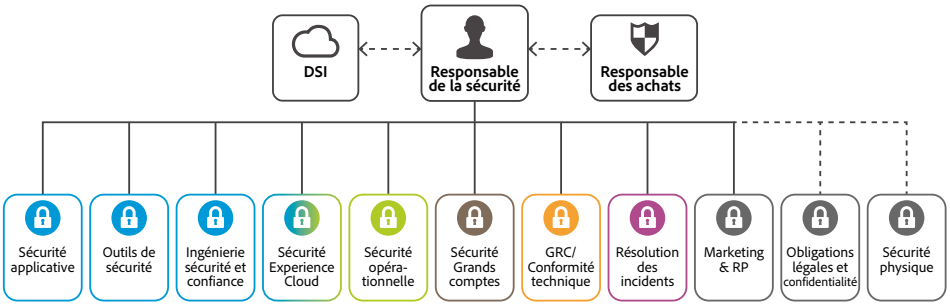
Analyse scientifique

Pour ses investigations sur les incidents, l'équipe Document Cloud applique un processus d'analyse scientifique, avec capture d'images complète ou vidage de la mémoire des machines concernées, conservation sécurisée des preuves et enregistrement de la chaîne de traçabilité.

Pôle de sécurité Adobe

Tous les efforts de sécurité déployés par Adobe sont placés sous l'autorité du responsable en chef de la sécurité (CSO). Le bureau du CSO coordonne l'ensemble des initiatives de sécurité concernant les produits et services, ainsi que la mise en œuvre du processus Adobe SPLC (Secure Product Lifecycle).

Le CSO dirige également l'ASSET (Adobe Secure Software Engineering Team), une équipe centrale dédiée, composée d'experts en sécurité qui conseillent les équipes en charge des opérations et produits Adobe, y compris l'équipe Adobe Document Cloud. Les chercheurs ASSET collaborent avec chacune de ces équipes pour assurer un niveau de sécurité adapté aux différents produits et services, et leur recommandent les pratiques de sécurité qui leur permettront de mettre en place des processus clairs et reproductibles en matière de développement, de déploiement, d'opérations et de résolution des incidents.



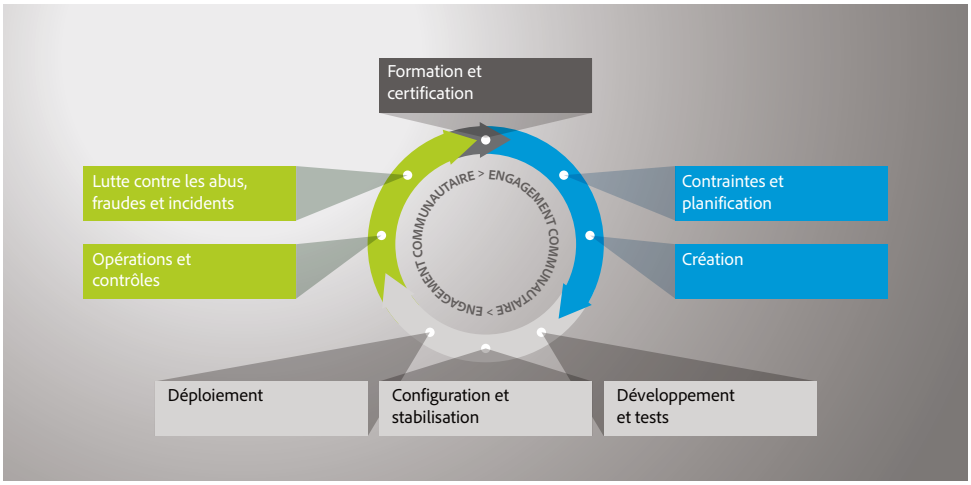
Développement sécurisé des produits Adobe

Au même titre que les autres grands pôles dédiés aux produits et services Adobe, le pôle Adobe Document Cloud applique le processus Adobe SPLC. Adobe SPLC, qui regroupe plusieurs centaines d'activités de sécurité liées aux pratiques, processus et outils de développement logiciel, est intégré à plusieurs étapes du cycle de vie du produit, de la création au déploiement, en passant par le développement, les tests et l'assurance qualité. Les chercheurs ASSET fournissent des conseils sur l'utilisation du processus SPLC pour chaque produit et service en se basant sur une évaluation des risques potentiels de sécurité. Bénéficiant, en outre, du soutien permanent de la communauté, Adobe SPLC évolue au rythme des dernières tendances en matière de technologies, de pratiques de sécurité et de menaces.

Processus Adobe SPLC

Les activités Adobe SPLC varient en fonction du composant Adobe Document Cloud. Elles peuvent inclure tout ou partie des bonnes pratiques, processus et outils suivants :

- Formation et certification de sécurité pour les équipes produit
- Analyse de l'intégrité, des risques et des menaces associés aux produits
- Modalités, règles et analyses de programmation sécurisées
- Roadmaps des services, outils de sécurité et méthodes de test pour aider l'équipe en charge de la sécurité d'Adobe Document Cloud à appréhender les dix principaux risques de sécurité des applications web recensés par l'OWASP (Open Web Application Security Project) et les 25 erreurs de programmation les plus dangereuses, répertoriées dans le rapport CWE/SANS
- Analyses de l'architecture de sécurité et tests d'intrusion
- Analyses du code source pour favoriser l'élimination des failles connues pouvant provoquer des vulnérabilités
- Validation du contenu généré par l'utilisateur
- Analyse des applications et du réseau
- Analyses d'aptitude, plans de réponse et publication de supports de formation pour les développeurs



Programme de certification ASSET

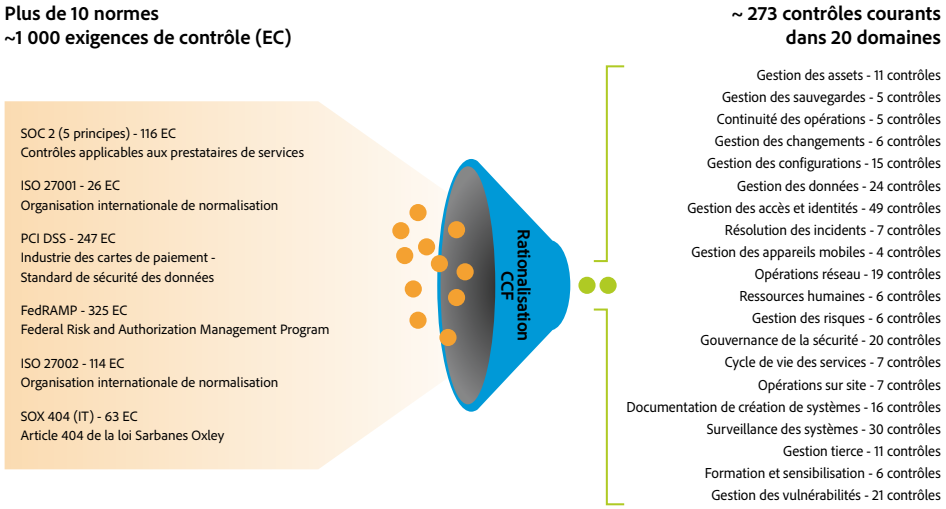
Dans le cadre du processus SPLC, Adobe dispense des formations continues aux équipes de développement afin de mieux les sensibiliser aux questions de sécurité et de renforcer la sécurité globale des produits et services. Les employés participant à ce programme de certification atteignent différents niveaux de certification en réalisant des projets de sécurité. Pour en savoir plus sur les pratiques de sécurité appliquées à nos produits, consultez la présentation de l'ingénierie sécurisée d'Adobe.

Pour en savoir plus sur le programme de certification ASSET, consultez notre article technique sur le développement d'une culture de la sécurité.

Conformité des services Document Cloud

Adobe CCF (Common Controls Framework) désigne un ensemble d'activités de sécurité et de contrôles de conformité mis en œuvre par nos équipes en charge des opérations produits et, à divers niveaux, par nos équipes responsables de l'infrastructure et des applications.

En créant CCF, Adobe a analysé les critères des principales certifications de sécurité pour les activités cloud et défini des contrôles Adobe pour plus de 1 000 exigences, correspondant à une dizaine de normes.



Pour en savoir plus sur les certifications de conformité et le cadre règlementaire respecté par Adobe Acrobat DC avec services Document Cloud, consultez le Centre de données Adobe.

Pour en savoir plus sur l'état actuel de la conformité d'Adobe Sign, consultez la présentation de la sécurité d'Adobe Sign.

Enfin, il appartient aux clients de se conformer à leurs obligations légales, c'est-à-dire de s'assurer que nos solutions répondent à leurs impératifs de conformité et sont correctement sécurisées.

Employés Adobe

Adobe possède des équipes et des bureaux dans le monde entier, et met en œuvre les procédures et processus ci-après pour contrer les menaces de sécurité.

Accès des employés aux données clients

Pour Adobe Document Cloud, Adobe segmente les environnements de développement et de production, et applique des contrôles techniques pour limiter l'accès aux systèmes de production en direct à partir du réseau et des applications. Les employés disposent d'autorisations spécifiques pour accéder aux systèmes de développement et de production, dont l'accès est interdit à ceux ne pouvant justifier d'un motif professionnel valable.

Vérification des antécédents

Adobe réunit des rapports de vérification des antécédents pour ses futurs employés. La société s'intéresse tout particulièrement à leur parcours universitaire et professionnel, à leur casier judiciaire (notamment les condamnations pénales) et aux références fournies par leurs contacts professionnels et personnels, conformément à la loi en vigueur. Aux États-Unis, cette vérification des antécédents concerne les nouvelles recrues, notamment les personnes qui seront chargées d'administrer les systèmes ou qui auront accès aux données des clients. Les nouveaux employés intérimaires sont soumis à ces vérifications par le biais de l'agence de travail temporaire contactée, conformément aux directives d'Adobe. En dehors des États-Unis, Adobe vérifie les antécédents de certaines nouvelles recrues, conformément à sa stratégie de vérification des antécédents et aux législations locales en vigueur.

Départ des employés

En cas de départ d'un employé Adobe, son responsable soumet un formulaire de sortie. Une fois ce dernier approuvé, le service des ressources humaines d'Adobe adresse un e-mail aux personnes compétentes pour les informer des mesures à prendre avant le dernier jour de travail de l'employé. En cas de licenciement d'un employé, le service des ressources humaines d'Adobe envoie un courrier similaire aux personnes compétentes, leur indiquant la date et l'heure de fin du contrat de travail.

Le service de sécurité d'Adobe programme alors les actions suivantes, de sorte que l'employé ne puisse plus avoir accès aux fichiers confidentiels ni aux bureaux d'Adobe une fois son contrat terminé :

- Suppression de l'accès à la messagerie électronique
- Suppression de l'accès VPN à distance
- Désactivation du badge d'accès aux bureaux et aux centres de données
- Suppression de l'accès réseau

Les responsables peuvent éventuellement demander au personnel de sécurité du bâtiment de raccompagner l'employé jusqu'à la sortie des bureaux ou du bâtiment Adobe.

Sécurité des installations

Chaque bureau Adobe emploie des gardiens sur site pour protéger les installations 24 heures sur 24, 7 jours sur 7. Les employés disposent d'un badge à leur nom pour accéder au bâtiment. Les visiteurs empruntent l'entrée principale, signent un registre à l'entrée et à la sortie, portent un badge visiteur temporaire et sont accompagnés d'un employé. Les équipements serveur, machines de développement, systèmes téléphoniques, serveurs de fichiers et de messagerie et autres systèmes sensibles sont systématiquement enfermés dans des salles serveur à environnement contrôlé dont l'accès est réservé au personnel qualifié autorisé.

Protection contre les virus

Adobe analyse tous les e-mails entrants et sortants afin de détecter les programmes malveillants connus.

Confidentialité des données clients

Adobe traite toujours les données des clients comme des données confidentielles. Les informations collectées pour le compte d'un client ne sont jamais utilisées ni divulguées, sauf disposition contraire figurant dans le contrat conclu avec ce client et prévue par les Conditions générales d'utilisation et la Politique de confidentialité d'Adobe.

Conclusion

L'approche proactive d'Adobe en matière de sécurité et les procédures rigoureuses décrites dans ce document contribuent à préserver la sécurité des logiciels Adobe Acrobat DC et Acrobat Reader DC, des services Document Cloud et de vos données confidentielles. Adobe attache une très grande importance à la sécurité des expériences digitales. Nous surveillons en permanence un environnement où les menaces évoluent constamment, afin de conserver une longueur d'avance sur les activités malveillantes et de garantir la sécurité des données de nos clients.

Pour en savoir plus, consultez le Centre de données Adobe.

Adobe Inc.
345 Park Avenue
San Jose, CA 95110-2704
États-Unis
www.adobe.com/fr/trust.html