Sécurité d'Adobe Document Cloud

Partout dans le monde, Adobe Document Cloud aide les entreprises à transformer les processus documentaires et à proposer des expériences digitales attrayantes pour interagir avec les clients, gagner en productivité et se démarquer. Comprenant Adobe Sign, Acrobat DC, des applications web et mobiles, des API flexibles et des intégrations clé en main, les solutions Document Cloud s'intègrent parfaitement avec vos applications métier et systèmes d'entreprise. Document Cloud aide les différents services de l'entreprise à améliorer leur efficacité opérationnelle, à réduire les risques liés aux erreurs humaines et à créer des expériences digitales intuitives de bout en bout.

Les pratiques de sécurité sont profondément ancrées dans la culture d'Adobe, ainsi que dans ses processus de développement logiciel et d'opérations de service. Document Cloud applique des pratiques de sécurité standard — pour la gestion des identités, la confidentialité des données et l'intégrité des documents — afin d'assurer la protection de vos documents, données et informations personnelles. Les solutions Document Cloud s'appuient sur un réseau de partenariats technologiques, stratégiques et humains assurant la protection de vos données dans le respect des normes de sécurité de référence. Votre entreprise peut ainsi s'adapter à l'évolution des environnements et répondre aux impératifs du marché avec des workflows avancés, une gestion aisée des licences et une solide infrastructure cloud.

La sécurité, une priorité

Adobe attache une grande importance à la sécurité de vos expériences numériques. Nous surveillons et améliorons en permanence nos applications, systèmes et processus pour aider nos clients à relever les exigences et défis de plus en plus complexes de la protection des données. Les services Document Cloud, notamment *Adobe Sign* et les services PDF, s'appuient sur une approche rigoureuse pour garantir la confidentialité, l'intégrité et la disponibilité de vos documents. À l'heure actuelle, les centres de données Document Cloud sont gérés aux quatre coins du monde et exploités par notre partenaire de confiance AWS (Amazon Web Services). Chaque centre de données AWS intègre des contrôles physiques, environnementaux et d'accès pointus, qui sont décrits sur la page *https://aws.amazon.com/fr/security/*.

De plus, Adobe SPLC (Secure Product Lifecycle) — un ensemble d'activités de sécurité couvrant les pratiques, processus et outils de développement logiciel — est intégré à plusieurs étapes du cycle de vie du produit Document Cloud. Pour garantir une protection ascendante depuis la couche physique, Adobe met en œuvre tout un ensemble de processus et de contrôles de sécurité pour son infrastructure, ses applications et ses services. Pour en savoir plus sur les processus de sécurité d'Adobe, l'engagement communautaire et Adobe SPLC (Secure Product LifeCycle), consultez le site *www.adobe.com/fr/security*.

Reprise sur incident

Adobe peut se targuer d'un niveau d'excellence opérationnelle élevé et veille à ce que les incidents potentiels n'aient aucun impact sur ses clients. En cas d'incident, le personnel en charge des opérations de Document Cloud doit rétablir l'accès complet au service aussi vite que possible. Les centres de données sont conçus pour garantir un haut niveau de tolérance aux pannes système ou matérielles et limiter l'impact côté clients.

Contrôles environnementaux

Tous les centres de données Document Cloud sont capables de détecter les risques environnementaux et sont équipés de systèmes de climatisation pour maintenir une température de fonctionnement et un degré d'humidité constants conformément à la certification SOC 2 Type 2.

Cryptage et confidentialité des données

La confidentialité fait partie intégrante des produits et services Adobe, et notamment de 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*.

Détection des intrusions et surveillance des systèmes

Dans un environnement en pleine évolution où les menaces sont de plus en plus complexes, Document Cloud s'appuie sur divers systèmes pour détecter les anomalies de sécurité réseau, telles que les dénis de service, les usurpations d'adresses IP, les balayages de port et autres cyber-attaques sophistiquées. Les équipes de sécurité opérationnelles d'Adobe utilisent un ensemble de critères d'alerte de surveillance pour définir les normes de sécurité et de disponibilité critiques pour les environnements de production de nos services, ainsi que des outils de surveillance tiers pour détecter les pics d'activité dépassant les seuils prédéfinis. Ces équipes déploient également des capteurs de détection d'intrusion aux points critiques du réseau afin de détecter les tentatives d'accès non autorisées à Document Cloud et de déclencher alors des alertes. Les équipes opérationnelles de Document Cloud sont également chargées d'assurer une surveillance en continu des journaux sensibles et de réaliser des audits systèmes réguliers afin de prévenir tout accès non autorisé aux ressources stratégiques.

Dans la mesure du possible, Adobe automatise les processus et procédures pour générer des gains d'efficacité, préserver la cohérence et la reproductibilité, et réduire les risques d'erreur humaine. Document Cloud utilise l'automatisation dans des domaines tels que la gestion des configurations et des correctifs, la création et le renforcement des images de référence, et la surveillance des systèmes. Adobe applique un processus complet de gestion des changements pour s'assurer que les modifications apportées à l'environnement de production réseau ou Document Cloud ont été préalablement documentées, suivies, testées, autorisées et approuvées.

Pour les services cloud Adobe comme Document Cloud, nous centralisons les réponses aux incidents, leur suivi externe et les prises de décision au sein du Centre de coordination de la sécurité (SCC), ce qui garantit une cohérence transversale et une résolution rapide des problèmes.

Tests et évaluations en interne et par des tiers

Les nouvelles fonctionnalités des produits font l'objet de vérifications destinées à identifier d'éventuels défauts de conception pouvant nuire à la sécurité du client, et les tests de sécurité sont intégrés dans le cycle de développement applicatif. Des tests de vulnérabilité supplémentaires sont réalisés sous forme d'inspection du code source et d'analyses statiques et dynamiques. Chaque version majeure du service Document Cloud est soumise à des tests d'intrusion indépendants, et les bogues critiques sont résolus avant le lancement.

Conformité

Les services Document Cloud sont conformes à de nombreuses normes, certifications et réglementations sectorielles telles que la norme ISO 27001:2013 et les certifications PCI DSS* et SOC 2 Type 2. Par exemple, Adobe Sign est certifié SAFE-BioPharma® et est conforme aux normes HIPAA, FERPA, GLBA et 21 CFR Partie 11.

Pour plus d'informations

Sécurité Adobe :
www.adobe.com/fr/security

Politique de confidentialité d'Adobe :
www.adobe.com/fr/privacy

Contrôle d'accès

L'infrastructure de Document Cloud réside dans des centres de données haut de gamme gérés par notre fournisseur de services cloud de confiance AWS (Amazon Web Services). Adobe utilise des méthodes de contrôle d'accès basé sur les rôles restreignant l'accès privilégié aux informations sur la base du concept du privilège minimal. L'autorisation d'accès requiert l'approbation de la direction directement responsable de la confidentialité, de l'intégrité et de la disponibilité des ressources concernées. 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 aux sites sécurisés en Amérique du Nord, dans l'Union européenne, en Australie et au Japon.

* À l'exception du service Adobe Send & Track.

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

10/17