FAQ concernant la sécurité informatique d'Adobe Creative Cloud

Les politiques de sécurité, de confidentialité et de conformité sont au cœur de nombreuses questions posées à Adobe concernant Creative Cloud. Les organisations qui utilisent Creative Cloud sont préoccupées par la sécurité de leurs données et la fiabilité de l'accès à ces données. Ce document vise à répondre aux questions les plus fréquemment posées par les personnels de sécurité informatique concernant ces sujets dans le cadre de Creative Cloud.

1 Où est hébergé Creative Cloud ?
Creative Cloud est hébergé par Amazon Web Services (AWS), et notamment sur les services Amazon Elastic Compute Cloud (Amazon EC2) et Amazon Simple Storage Service (Amazon S3) pour les régions Etats-Unis, UE et Asie-Pacifique. AWS propose une plate-forme fiable pour les services logiciels, utilisée par des milliers d'entreprises du monde entier. Les services AWS sont conformes aux bonnes pratiques de sécurité et leur qualité est garantie par des certifications et audits reconnus par le secteur. (aws.amazon.com/security/). Les membres Creative Cloud bénéficient donc, pour leurs ressources stockées, de l'engagement permanent d'Amazon en matière de bonnes pratiques de sécurité.

2 Où se trouvent les données des clients ?
Les données des clients sont stockées dans Amazon S3, et Adobe choisit dans quelle région les serveurs et les données des clients individuels seront situés. La réplication des données pour les objets Amazon S3 est réalisée au sein du cluster régional où les données sont stockées. Aucune réplication n'est réalisée vers des clusters de centres de données situés dans d'autres régions. Adobe exploite Creative Cloud dans trois régions : Etats-Unis, UE et Asie-Pacifique.

Exemple : par défaut, toutes les données stockées en nuage pour les clients Creative Cloud résidant dans l'UE seront stockées dans le centre de données AWS situé dans l'UE. Ces données ne seront pas transférées vers des centres de données situés en dehors de l'UE.

3 Par qui les centres de données Creative Cloud sont-ils contrôlés ?
Amazon contrôle les composantes physiques pour les éléments de Creative Cloud déployés via les services AWS. Pour que les clients puissent se faire une idée plus précise de son degré de maîtrise et de l'efficacité de son fonctionnement, AWS publie un rapport SOC 1 (Service Organization Controls 1) de type 2 (aws.amazon.com/security/) présentant les procédures de contrôle définies pour Amazon EC2, Amazon S3 et Virtual Private Cloud (VPC), ainsi que les contrôles détaillés en termes de sécurité physique et d'environnement. Ces contrôles sont définis avec un niveau élevé de spécificité, afin de répondre à la plupart des besoins des clients.

4 Les clients sont-ils autorisés à visiter les centres de données AWS ?
Non. Dans la mesure où les centres de données AWS hébergent les données de plusieurs clients, AWS n'autorise pas les visites de ces centres, car cela exposerait de nombreux clients à un risque d'accès physique par un tiers. Pour répondre à ce besoin de la part des clients, un auditeur indépendant et compétent vérifie la présence et le fonctionnement de contrôles dans le cadre d'un rapport SOC 1 de type 2. Cette validation réalisée par un tiers permet aux clients de disposer d'un avis impartial sur l'efficacité des contrôles en place. Adobe a signé un accord de non-divulgation avec AWS et peut ainsi obtenir un exemplaire de ce rapport SOC 1 de type 2 (aws.amazon.com/security/). Des examens indépendants de la sécurité physique des centres de données font également partie intégrante du processus AWS pour les audits ISO 27001, les évaluations PCI et les audits ITAR.

5 Les tiers sont-ils autorisés à accéder aux centres de données AWS ?
AWS applique un contrôle d'accès strict pour ses centres de données, y compris concernant ses employés internes. Les tiers n'ont pas accès aux centres de données AWS, sauf en cas d'accord explicite du gestionnaire du centre de données AWS en question et selon la politique d'accès d'AWS. Consultez le rapport SOC 1 de type 2 (aws.amazon.com/security/) pour en savoir plus sur les contrôles spécifiques liés à l'accès physique, les autorisations d'accès aux centres de données et les autres contrôles liés.

6 Qui est en responsable de l'application des correctifs ?
Adobe prend en charge l'application de correctifs pour ses propres systèmes d'exploitation (OS) invités, logiciels et applications s'exécutant dans AWS. AWS est responsable des systèmes de mise à jour corrective permettant l'accès aux services AWS, comme l'hyperviseur et les services de mise en réseau. Ces opérations sont effectués selon la politique d'AWS et conformément aux exigences ISO 27001, NIST et PCI.

7 Les actions nécessitant des privilèges sont-elles surveillées et contrôlées ?
Les contrôles mis en place limitent l'accès aux systèmes et données, ou l'accès aux données est restreint et surveillé. De plus, les instances des serveurs et données des clients sont, par défaut, logiquement isolées de celles des autres clients. Le contrôle d'accès des utilisateurs disposant de privilèges concernant l'infrastructure AWS fait l'objet d'un examen par un auditeur indépendant lors des audits SOC 1, ISO 27001, PCI, ITAR et FISMA d'AWS.

8 Le fournisseur de services en nuage propose-t-il des solutions contre le risque d'accès interne inapproprié aux données et applications des clients ?
AWS propose des contrôles SOC 1 spécifiques, présentés dans le rapport SOC 1 de type 2 (aws.amazon.com/security/). Par ailleurs, Adobe procède régulièrement à des évaluations des risques portant sur le contrôle et la surveillance des accès internes.

9 Comment les données des clients sont-elles isolées dans Creative Cloud ?
Toutes les données stockées par Adobe pour le compte de ses clients sont protégées par de puissantes capacités de contrôle et de sécurité en termes d'isolation. Creative Cloud utilise le service de stockage Amazon S3, qui permet un contrôle avancé de l'accès aux données.

10 La répartition des clients est-elle mise en place de manière sécurisée ?
L'environnement AWS est virtualisé et multi-clients. AWS a mis en œuvre des processus de gestion de la sécurité, des contrôles PCI, ainsi que d'autres contrôles de sécurité destinés à isoler les clients les uns des autres. Les systèmes AWS sont conçus pour empêcher les clients d'accéder aux instances ou hôtes physiques qui ne leur ont pas été attribués, et ce via un filtrage par le logiciel de virtualisation. Cette architecture a été validée par un Qualified Security Assessor (QSA) PCI indépendant et s'est avérée conforme à toutes les exigences de la norme PCI DSS 2.0 (aws.amazon.com/security/pci-dss-level-1-compliance-faqs/).

11 Les vulnérabilités connues de l'hyperviseur ont-elles été corrigées par AWS ?
Amazon EC2 utilise actuellement une version hautement personnalisée de l'hyperviseur Xen. La sécurité de l'hyperviseur Xen d'AWS est régulièrement contrôlée par des auditeurs indépendants au cours d'évaluations et d'audits. Consultez le livre blanc d'AWS concernant la sécurité (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) pour en savoir plus sur l'hyperviseur Xen et l'isolation des instances.

12 Le service fourni prend-il en charge le chiffrement ?
Creative Cloud chiffre les données en transit avec SSL.

13 De quels droits le fournisseur de services en nuage dispose-t-il sur les données des clients ?
Les clients Creative Cloud conservent la maîtrise et la propriété de leurs données. Consultez les conditions d'utilisation d'Adobe (www.adobe.com/go/gffooter_terms_of_use) et la politique de confidentialité (www.adobe.com/privacy/policy.html) pour plus d'informations.

14 Les contrôles physiques et environnementaux d'AWS sont-ils rendus publics ?
Oui. Les contrôles physiques et environnementaux sont spécifiquement mentionnés dans le rapport SOC 1 de type 2 (aws.amazon.com/security/). De plus, AWS dispose des certifications ISO 27001 et FISMA, qui exigent des contrôles physiques et environnementaux conformes aux bonnes pratiques.

15 Les clients peuvent-ils sécuriser et gérer l'accès à Creative Cloud à partir d'appareils client comme les mobiles et les PC ?
Oui. Les membres Creative Cloud peuvent gérer l'accès client et mobile en fonction de leurs besoins.

16 AWS permet-il aux clients de sécuriser leurs serveurs virtuels ?
Oui. Adobe a mis en place sa propre architecture de sécurité, qui vient s'ajouter aux bonnes pratiques AWS qui comprend notamment les 20 principaux contrôles en matière de sécurité Internet de l'institut SANS, les Consensus Audit Guidelines (bonnes pratiques en matière de sécurité informatique), les recommandations NIST et les normes Internet.

17 Les services AWS incluent-ils des possibilités de gestion des accès et des identités (Identity and access management, IAM) ?
AWS propose plusieurs fonctionnalités de gestion des accès et des identités, ce qui permet à Adobe de gérer les identités d'utilisateurs, d'attribuer des identifiants de sécurité, d'organiser les utilisateurs en groupes et de gérer les autorisations de manière centralisée.

18 Les systèmes Creative Cloud seront-ils interrompus en cas de maintenance ?
Creative Cloud est déployé de façon à ne connaître pratiquement aucune période d'interruption. Les services devraient être accessibles pendant les nouveaux déploiements grâce à l'utilisation d'environnements A/B et d'autres mécanismes permettant un basculement en direct sans interruption perceptible en externe.

19 Comment la protection contre les attaques par déni de service (DDoS) est-elle assurée par AWS ?
Le réseau AWS offre une bonne protection en matière de sécurité des réseaux classique. Consultez le livre blanc d'AWS concernant la sécurité (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) pour en savoir plus sur ce sujet, notamment sur les DDoS.

20 Existe-t-il un plan de continuité des activités pour Creative Cloud ?
AWS propose un programme de continuité des activités (media.amazonwebservices.com/AWS_Disaster_Recovery.pdf) et Creative Cloud est conçu pour s'exécuter depuis plusieurs régions et zones de disponibilité ou centres de données. Adobe a conçu, développé et mis en service Creative Cloud afin d'exploiter la réplication des données redondantes et les architectures de déploiement sur plusieurs régions/zones de disponibilité.

21 La durabilité des données est-elle indiquée par AWS ?
Creative Cloud stocke les données dans Amazon S3, qui offre une infrastructure de stockage durable. Les objets sont stockés de manière redondante sur plusieurs appareils dans différentes installations d'une même région Amazon S3. Une fois les données stockées, Amazon S3 garantit la durabilité des objets en détectant et réparant rapidement toute perte de redondance. Amazon S3 procède également à des vérifications régulières de l'intégrité des données stockées par le biais de sommes de contrôle. Toute corruption détectée est réparée à l'aide de données redondantes.

22 Est-il prévu qu'Adobe valide sa conformité à la loi américaine FISMA (Federal Information Security Management Act) ?
Dans l'immédiat, Adobe ne compte pas démontrer la conformité de Creative Cloud à la loi FISMA (Federal Information Security Management Act).

23 Le service Creative Cloud est-il conforme à la loi HIPAA ?
Adobe n'a pas l'intention d'obtenir une certification relative à la conformité de Creative Cloud à la loi HIPAA (Health Insurance Portability and Accountability Act) de 1996, car Creative Cloud n'est pas conçu pour traiter des enregistrements du domaine médical.

Références

Présentation générale du livre blanc d'AWS concernant les pratiques de sécurité, mars 2013 (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

Livre blanc d'AWS sur les risques et la conformité, janvier 2013 (media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf)

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com