Perguntas frequentes sobre a segurança da Adobe Creative Cloud para TI

As diretivas de segurança, privacidade e conformidade são algumas das perguntas mais comuns sobre a Creative Cloud feitas à Adobe. As organizações que usam a Creative Cloud estão preocupadas com a proteção do seus dados e a segurança no acesso a eles. Este documento visa responder a muitas perguntas frequentes feitas pela equipe de segurança de TI sobre esses tópicos quando a adoção da Creative Cloud está sendo considerada.

1 Onde a Creative Cloud está hospedada?
A Creative Cloud é hospedada na Amazon Web Services (AWS), incluindo o Amazon Elastic Compute Cloud (Amazon EC2) e o Amazon Simple Storage Service (Amazon S3), nos Estados Unidos, na União Europeia e na Ásia Ocidental. A AWS oferece uma plataforma confiável para serviços de software usados por milhares de empresas em todo o mundo. Ela fornece serviços em acordo com as melhores práticas de segurança e submete-se a certificações e auditorias reconhecidas pelo setor (http://aws.amazon.com/pt/security/). Isso significa que os membros da Creative Cloud beneficiam-se do compromisso contínuo da Amazon com as práticas de segurança para ativos armazenados.

2 Onde os dados dos clientes são armazenados?
Os dados dos clientes são armazenados no Amazon S3, e a Adobe especifica a região física onde os servidores e os dados dos clientes estarão localizados. A replicação de dados nos objetos de dados do Amazon S3 é realizada no cluster regional, onde os dados são armazenados e não são replicados para clusters de data centers em outras regiões. A Adobe mantém a Creative Cloud de três regiões: Estados Unidos, União Europeia e Ásia Ocidental.

Exemplo: por padrão, todos os dados dos clientes da Creative Cloud na União Europeia serão armazenados na nuvem do data center da AWS na UE, e esses dados não serão transferidos para data centers de fora da UE.

3 Quem controla os data centers da Creative Cloud?
A Amazon controla os componentes físicos dos ativos da Creative Cloud localizados na AWS. Para ajudar os clientes a entenderem melhor quais são os controles implantados na AWS e a eficiência operacional deles, a AWS publicou um relatório de controle organizacional de serviço 1 (SOC 1) de tipo 2 (http://aws.amazon.com/pt/security/), que apresenta controles definidos em relação ao Amazon EC2, ao Amazon S3 e ao Virtual Private Cloud (VPC), além de controles detalhados sobre a segurança física e ambiental. Esses controles são definidos com alto nível de especificidade que deve atender às necessidades da maioria dos clientes.

4 A Amazon permite que clientes visitem os data centers da AWS?
Não. Como os data centers da AWS hospedam dados para vários clientes, a AWS não permite que a visitação de clientes, pois isso exporia muitos dos nossos clientes ao acesso físico de terceiros. Para atender a essa necessidade de clientes, um auditor independente e qualificado valida a presença e a operação dos controles como parte de um relatório SOC 1 de tipo 2. Essa validação de terceiros amplamente aceita fornece aos clientes uma perspectiva independente da eficiência dos controles implementados. A Adobe assinou um contrato de confidencialidade com a AWS e pode obter uma cópia do relatório SOC 1 de tipo 2 (http://aws.amazon.com/pt/security/). Avaliações independentes da segurança física dos data centers também fazem parte da auditoria AWS ISO 27001, da avaliação PCI e do processo de auditoria ITAR.

5 O acesso aos data centers da AWS é permitido a terceiros?
A AWS limita o acesso aos data centers, até mesmo para funcionários internos. Os data centers da AWS não estão abertos a terceiros, exceto quando explicitamente aprovados pelo gerente do data center AWS específico, de acordo com a política de acesso da AWS. Consulte o relatório SOC 1 de tipo 2 (http://aws.amazon.com/pt/security/) para saber mais sobre os controles específicos ao acesso físico, a autorização de acesso ao data center e outros controles relacionados.

6 Quem é responsável por executar as atualizações de segurança?
A Adobe é responsável pelas atualizações de segurança dos nossos sistemas operacionais convidados, dos software e dos aplicativos em execução na AWS. A AWS é responsável pelas atualizações de segurança dos sistemas que dão suporte ao fornecimento de serviços da AWS, como os serviços de hipervisor e rede. Isso é feito de acordo com as exigências da política da AWS e atende aos requisitos ISO 27001, NIST e PCI.

7 Ações privilegiadas são monitoradas e controladas?
Os controles instalados limitam o acesso aos sistemas e aos dados, ou os dados são restritos e monitorados. Além disso, os dados dos clientes e as instâncias do servidor são isolados logicamente de outros clientes por padrão. O controle de acesso de usuário privilegiado na infraestrutura da AWS é revisado por um auditor independente durante as auditorias de AWS SOC 1, ISO 27001, PCI, ITAR e FISMA.

8 O provedor da nuvem tem alguma abordagem relacionada à ameaça de acesso interno indevido aos dados e aplicativos dos clientes?
A AWS fornece uma SOC 1 específica no relatório SOC 1 de tipo 2 (http://aws.amazon.com/pt/security/). Além disso, a Adobe conduz avaliações de risco periódicas sobre como o acesso interno é controlado e monitorado.

9 Como a Creative Cloud isola os dados dos clientes?
Todos os dados de clientes armazenados pela Adobe são protegidos por recursos de controle e segurança para isolamento dos locatários. O armazenamento da Creative Cloud usa o Amazon S3, que fornece controles avançados de acesso a dados.

10 A segregação de clientes é implementada de forma segura?
O ambiente da AWS é virtualizado e com multilocatários. A AWS implementou processos de gerenciamento de segurança, controles PCI e outros controles de segurança criados para isolar os clientes. Os sistemas da AWS foram criados para impedir o acesso dos clientes aos hosts físicos ou às instâncias não atribuídas a eles por meio de filtragem do software de virtualização. Essa arquitetura foi aprovada pelo Consultor de segurança qualificado (QSA) do PCI e está em conformidade com todas as exigências do PCI DSS 2.0 (http://aws.amazon.com/pt/security/pci-dss-level-1-compliance-faqs/).

11 A AWS corrigiu vulnerabilidades conhecidas do hipervisor?
Atualmente, o Amazon EC2 usa uma versão altamente personalizada do hipervisor Xen.
A segurança do hipervisor Xen da AWS é frequentemente avaliada por auditores independentes durante as avaliações e auditorias. Consulte o white paper de segurança da AWS (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) para obter mais informações sobre o hipervisor Xen e o isolamento de instâncias.

12 Os serviços fornecidos podem ser criptografados?
A Creative Cloud criptografa dados que estão sendo transferidos para/do SSL.

13 Quais são os direitos do fornecedor da nuvem sobre os dados dos clientes?
Os clientes da Creative Cloud têm o controle e a propriedade de seus dados. Consulte os Termos de uso (www.adobe.com/br/misc/terms.html) e a Política de privacidade (www.adobe.com/br/privacy/policy.html) da Adobe para obter mais informações.

14 A AWS publica seus controles físicos e ambientais?
Sim. Os controles físicos e ambientais estão especificamente descritos no relatório SOC 1 de tipo 2 (http://aws.amazon.com/pt/security/). Além disso, a AWS tem as certificações ISO 27001 e FISMA, que requerem melhores práticas de controle físico e ambiental.

15 Os clientes podem proteger e gerenciar o acesso à Creative Cloud de clientes, como PCs ou dispositivos móveis?
Sim. A Creative Cloud permite que os clientes gerenciem o acesso de clientes e dispositivos móveis da forma que desejarem.

16 A AWS permite que clientes protejam seus servidores virtuais?
Sim. A Adobe implementou sua própria arquitetura de segurança em cima da AWS baseada nas melhores práticas do setor, inclusive nos Top 20 Controls for Internet Security (20 principais controles de segurança de Internet) e Consensus Audit Guidelines (diretrizes de auditoria de consenso) da SANS, diretrizes NIST e padrões da Internet.

17 A AWS contém recursos de gerenciamento de identidade e acesso (IAM)?
A AWS tem uma suíte de ofertas de gerenciamento de identidade e acesso, o que permite que a Adobe gerencie suas IDs de usuários, atribua credenciais de segurança, organize os usuários em grupos e gerencie as permissões de usuários de forma centralizada.

18 A Adobe derrubará os sistemas da Creative Cloud para manutenção?
A implementação da Creative Cloud é feita para praticamente eliminar os tempos de inatividade. Os serviços ficam acessíveis e em operação durante as novas implantações, pois o uso de ambientes A/B e outros mecanismos de possibilitam a substituição em tempo real sem que haja tempo de inatividade para os usuários.

19 Como a AWS protege o sistema contra ataques de negação de serviço distribuído (DDoS)?
A rede da AWS fornece grande proteção para a segurança tradicional de rede. Consulte o white paper de segurança da AWS (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) para obter mais informações sobre esse assunto, além de uma discussão sobre o DDoS.

20 A Adobe tem um plano de continuidade dos negócios para a Creative Cloud?
A AWS oferece um programa de continuidade dos negócios (media.amazonwebservices.com/AWS_Disaster_Recovery.pdf), e a Creative Cloud foi criada para ser instalada em diversas regiões e zonas de disponibilidades ou data centers. A Adobe criou, estruturou e implementou a Creative Cloud para usar replicação de redundância de dados e arquiteturas de implantação em diversas regiões/zonas de disponibilidade.

21 A AWS especifica a durabilidade dos dados?
A Creative Cloud armazena dados no Amazon S3, que fornece uma infraestrutura de armazenamento durável. Os objetos são armazenados de forma redundante em diversos dispositivos em várias instalações de uma região do Amazon S3. Quando os dados são armazenados, o Amazon S3 mantém a durabilidade dos objetos ao detectar e reparar redundâncias perdidas. O Amazon S3 também verifica com regularidade a integridade dos dados usando as somas de verificação. Se alguma corrupção for detectada, ela será reparada usando os dados redundantes.

22 A Adobe planeja obter a conformidade com o Federal Information Security Management Act (FISMA)?
A Adobe não tem nenhum plano imediato para obter a conformidade com o Federal Information Security Management Act (FISMA) para a Creative Cloud.

23 A Creative Cloud está em conformidade com o HIPAA?
A Adobe não pretende obter a conformidade com o Health Insurance Portability and Accountability Act of 1996 (HIPAA), pois a Creative Cloud não pretende processar registros relacionados à saúde.

Referências

Visão geral do white paper de práticas de segurança da AWS, março de 2013 (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

White paper sobre conformidade e riscos da AWS, janeiro de 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