Adobe Creative Cloud Security FAQ for IT

Security, privacy and compliance policies are some of the most common areas for questions Adobe receives about Creative Cloud. Organizations using Creative Cloud are concerned about the safety of their data and that access to their data is reliable. This document aims to answer many of the frequently asked questions by IT security staff on these topics when they are considering Creative Cloud.

1 Where is Creative Cloud hosted?

Creative Cloud is hosted on Amazon Web Services (AWS), including Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3), in the United States, EU, and Asia Pacific. AWS offers a reliable platform for software services used by thousands of businesses worldwide. AWS provides services in accordance with security best practices and undergoes industry-recognized certifications and audits *(aws.amazon.com/security/)*. This means that Creative Cloud members benefit from Amazon's ongoing commitment to security practices for stored assets.

2 Where does customer data reside?

Customer data is stored in Amazon S3 and Adobe designates which physical region individual customers' data and servers will be located. Data replication for Amazon S3 data objects is done within the regional cluster where the data is stored and is not replicated to data center clusters in other regions. Adobe operates Creative Cloud out of three regions: United States, EU, and Asia Pacific.

Example: By default, all data from Creative Cloud customers in the EU will have their cloud data stored in the AWS data center in the EU and that data will not be transferred to data centers outside the EU.

3 Who controls the Creative Cloud data centers?

For the parts of Creative Cloud deployed in AWS, Amazon controls the physical components. To help customers better understand what controls AWS has in place and how effectively they are operating, AWS publishes a Service Organization Controls 1 (SOC 1), Type 2 report (*aws.amazon.com/security/*) with controls defined around Amazon EC2, Amazon S3, and Virtual Private Cloud (VPC), as well as detailed physical security and environmental controls. These controls are defined at a high level of specificity that should meet most customer needs.

4 Are AWS data center tours by customers allowed by Amazon?

No. Due to the fact that AWS datacenters host data for multiple customers, AWS does not allow datacenter tours by customers, as this exposes a wide range of customers to physical access by a third party. To meet this customer need, an independent and competent auditor validates the presence and operation of controls as part of a SOC 1, Type 2 report. This broadly accepted third-party validation provides customers with an independent perspective of the effectiveness of controls in place. Adobe has signed a non-disclosure agreement with AWS and can obtain a copy of the SOC 1 Type 2 report (*aws.amazon.com/security/*) . Independent reviews of data center physical security is also a part of the AWS ISO 27001 audit, the PCI assessment, and the ITAR audit process.

5 Are third parties allowed to access AWS data centers?

AWS strictly controls access to data centers, even for internal employees. Third parties are not provided access to AWS data centers except when explicitly approved by the appropriate AWS datacenter manager per AWS' access policy. See the SOC 1, Type 2 report (*aws.amazon.com/security/*) for specific controls related to physical access, datacenter access authorization, and other related controls.

6 Who is responsible for patching?

Adobe is responsible for patching our own guest operating systems (OS), software and applications running in AWS. AWS is responsible for patching systems supporting the delivery of AWS services, such as the hypervisor and networking services. This is done as required per AWS policy and in accordance with ISO 27001, NIST, and PCI requirements.

7 Are privileged actions monitored and controlled?
Controls in place limit access to systems and data or data is restricted and monitored. In addition, customer data and server instances are logically isolated from other customers by default. Privileged user access control for AWS infrastructure is reviewed by an independent auditor during the AWS SOC 1, ISO 27001, PCI, ITAR, and FISMA audits.

8 Does the cloud provider address the threat of inappropriate insider access to customer data and applications?
AWS provides specific SOC 1 covered in the SOC 1, Type 2 report *(aws.amazon.com/security/)*. In addition, Adobe conducts periodic risk assessments on how insider access is controlled and monitored.

9 How does Creative Cloud isolate customer data?
All data stored by Adobe on behalf of customers has strong tenant isolation security and control capabilities. Creative Cloud Storage utilizes Amazon S3 which provides advanced data access controls.

10 Is customer segregation implemented securely?
The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS 2.0 (*aws.amazon.com/security/pci-dss-level-1-compliance-faqs/*).

11 Has AWS addressed known hypervisor vulnerabilities?
Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. See the AWS security whitepaper (*media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf*) for more information on the Xen hypervisor and instance isolation.

12 Do the provided services support encryption?
Creative Cloud encrypts data in transit with SSL.

13 What are the cloud provider's rights over customer data?
Creative Cloud customers retain control and ownership of their data. Please review Adobe's Terms of Use (*www.adobe.com/go/gffooter_terms_of_use*) and Privacy Policy (*www.adobe.com/privacy/policy.html*) for more details.

14 Does AWS publish its physical and environmental controls?
Yes. Physical and environmental controls are specifically outlined in a SOC 1,Type 2 report *(aws.amazon.com/security/)*. Additionally, AWS supports ISO 27001 and FISMA certification, which require best practice physical and environmental controls.

15 Can customers secure and manage access to Creative Cloud from clients such as PCs and mobile devices?
Yes. Creative Cloud allows customers to manage client and mobile access to their own requirements.

16 Does AWS allow customers to secure their virtual servers?
Yes. Adobe has implemented its own security architecture on top of AWS based on industry best practices including SANS Top 20 Controls for Internet Security, Consensus Audit Guidelines, NIST guidelines, and Internet standards.

17 Does AWS include identity and access management (IAM) capabilities?
AWS has a suite of identity and access management offerings, allowing Adobe to manage user identities, assign security credentials, organize users in groups, and manage user permissions in a centralized way.

18 Will Adobe bring Creative Cloud systems down for maintenance?
Creative Cloud is implemented in such a way as to virtually eliminate downtime. The services should be accessible and reachable during new deployments due to the use of A/B environments and other mechanisms that allow for live-cutover with no externally visible downtime.

19 How does AWS protect against Distributed Denial Of Service (DDoS) attacks?
The AWS network provides significant protection against traditional network security. See the AWS Security Whitepaper (*media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf*) for more information on this topic, including a discussion of DDoS 1.20 Does Adobe have a business continuity plan for Creative Cloud?

20 Does Adobe have a business continuity plan for Creative Cloud?
AWS offers a business continuity program (*media.amazonwebservices.com/AWS_Disaster_Recovery.pdf*) and Creative Cloud is designed to run out of multiple regions and multiple availability zones, or data centers. Adobe designed, architected, and implemented Creative Cloud to utilize data redundancy replication, and multi-region/availability zone deployment architectures.

21 Does AWS specify data durability?
Creative Cloud stores data in Amazon S3, which provides a durable storage infrastructure. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 region. Once data is stored, Amazon S3 maintains the durability of objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data.

22 Does Adobe plan to obtain Federal Information Security Management Act (FISMA) Compliance?
Adobe has no immediate plans to obtain Federal Information Security Management Act (FISMA) compliance for Creative Cloud.

23 Is Creative Cloud HIPAA compliant?
Adobe does not intend to certify Creative Cloud as Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliant since Creative Cloud is not intended to process healthcare records.

References

Overview of AWS Security Practices Whitepaper, March 2013
(*media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf*)

AWS Risk and Compliance Whitepaper, January 2013
(*media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf*)

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