# Domande frequenti su Adobe Creative Cloud per l'IT

Protezione, privacy e politiche sulla conformità sono alcune delle aree più comuni per le domande che Adobe riceve su Creative Cloud. Le organizzazioni che utilizzando Creative Cloud sono preoccupate per la sicurezza dei loro dati e che l'accesso ai loro dati sia affidabile. Lo scopo di questo documento è di rispondere alle diverse domande frequenti poste dal personale della protezione IT su questi argomenti quando prendono in considerazione Creative Cloud.

**1 Dove è ospitato Creative Cloud?**

Creative Cloud è ospitato in Amazon Web Services (AWS), compresi Amazon Elastic Compute Cloud (Amazon EC2) e Amazon Simple Storage Service (Amazon S3), negli Stati Uniti, nell'Unione Europea e nell'Asia Pacifica. AWS offre una piattaforma affidabile per i servizi software utilizzata da migliaia di aziende a livello mondiale. AWS offre servizi in conformità alle best practice sulla protezione ed è soggetto a certificazioni e controllo riconosciuti dal settore (aws.amazon.com/security/). Ciò significa che i membri di Creative Cloud beneficiano dall'impegno costante di Amazon rivolto verso le politiche di protezione per le risorse memorizzate.

**2 Dove risiedono i dati dei clienti?**

I dati dei clienti sono memorizzati in Amazon S3 e Adobe indica in quali area geografica fisica saranno localizzati i singoli dati e server dei clienti. La replicazione dei dati per gli oggetti dati di Amazon S3 viene effettuata entro il cluster regionale nel quale sono memorizzati i dati; i dati non sono replicati in cluster di datacenter in altre aree geografiche. Adobe gestiste Creative Cloud da tre aree geografiche: Stati Uniti, Unione Europea e Asia Pacifica.

Esempio: per impostazione predefinita, tutti i dati nel cloud dei clienti Creative Cloud nell'Unione Europea sono memorizzati nel datacenter AWS nell'Unione Europea e i dati non saranno trasferiti in datacenter al di fuori dell'Unione Europea.

**3 Chi controlla i datacenter Creative Cloud?**

Per i componenti di Creative Cloud distribuiti in AWS, Amazon controlla i componenti fisici. Per consentire ai clienti di comprendere meglio quali controlli sono predisposti in AWS e come funzionano effettivamente, AWS pubblica un rapporto Service Organization Controls 1 (SOC 1), Type 2 (aws.amazon.com/security/) con controlli definiti per Amazon EC2, Amazon S3 e Virtual Private Cloud (VPC), oltre a controlli per protezione e ambiente fisici dettagliati. Questi controlli sono definiti a un livello di specificità generale che dovrebbe soddisfare i requisiti dei clienti.

**4 I tour dei datacenter AWS da parte dei clienti sono consentiti da Amazon?**

No. Dato che i datacenter AWS ospitano dati di più clienti, AWS non consente ai clienti di visitare i datacenter, in quanto questo esporrebbe un'ampia gamma di clienti all'accesso fisico da una terza parte. Per soddisfare questo requisito dei clienti, un controllore indipendente e competente convalida la presenza e il funzionamento di controlli secondo il rapporto SOC 1, Type 2. Questa convalida da parte di una terza parte ampiamente accettata, fornisce ai clienti con una prospettiva indipendente sull'efficacia dei controlli utilizzati. Adobe ha firmato un accordo di non divulgazione con AWS e può ottenere una copia del rapporto SOC 1, Type 2 (aws.amazon.com/security/). Le verifiche indipendenti della protezione fisica dei datacenter fa anche parte dei controlli AWS ISO 27001, la valutazione PCI e il processo di verifica ITAR.

**5 L'accesso ai datacenter AWS è consentito a terze parti?**

AWS controlla rigorosamente l'accesso ai datacenter, anche per i dipendenti interni. L'accesso a terze parti non è consentito nei datacenter AWS eccetto se non esplicitamente approvato dal responsabile appropriato del datacenter AWS secondo le politiche di accesso di AWS. Consultate il rapporto SOC 1, Type 2 (aws.amazon.com/security/) per i controlli specifici correlati all'accesso fisico, all'autorizzazione per accedere al datacenter e altri controlli correlati.

**6 Chi è responsabile per l'applicazione di patch?**

Adobe è responsabile per l'applicazione di patch ai propri sistemi operativi guest, software e applicazioni in esecuzione in AWS. AWS è responsabile per l'applicazione di patch ai sistemi che supportano la fruizione dei servizi AWS quali hypervisor e servizi di rete. Questo viene effettuato come richiesto in base alle politiche AWS in conformità ai requisiti ISO 27001, NIST e PCI.

**7 Le azioni privilegiate sono monitorate e controllate?**
I controlli utilizzati limitano l'accesso a sistemi e dati o i dati sono vincolati e monitorati. Inoltre, per impostazione predefinita, i dati e le istanze dei server dei clienti sono isolati logicamente da altri clienti. Il controllo dell'accesso da parte di utenti privilegiati per l'infrastruttura AWS è esaminato da un revisore indipendente durante le verifiche AWS SOC 1, ISO 27001, PCI, ITAR e FISMA.

**8 Il provider del cloud gestisce la minaccia di accesso interno inappropriato ai dati e alle applicazioni dei clienti?**
AWS fornisce un SOC 1 specifico dettagliato nel rapporto SOC 1, Type 2 (aws.amazon.com/security/). Inoltre, Adobe conduce periodicamente valutazioni dei rischi su come l'accesso interno è controllato e monitorato.

**9 In che modo Creative Cloud isola i dati dei clienti?**
Tutti i dati memorizzati da Adobe per conto dei clienti dispongono di funzionalità avanzate di protezione e controllo dell'isolamento dei tenant. La memorizzazione di Creative Cloud utilizza Amazon S3 che fornisce controlli di accesso ai dati avanzati.

**10 La segregazione dei clienti è implementata in modo sicuro?**
L'ambiente AWS è un ambiente virtualizzato a più tenant. AWS ha implementato processi di gestione della protezione, controlli PCI e altri controlli di protezione progettati per isolare ciascun cliente dagli altri. I sistemi AWS sono progettati per prevenire l'acceso da parte dei clienti agli host fisici o alle istanze non assegnate a loro filtrando tramite il software di virtualizzazione. Questa architettura è stata convalidata da un QSA (Qualified Security Assessor) PCI indipendente ed è stata certificata in conformità a tutti i requisiti PCI DSS 2.0 (aws.amazon.com/security/pci-dss-level-1-compliance-faqs/).

**11 AWS ha gestito le vulnerabilità note di hypervisor?**
Amazon EC2 utilizza una versione altamente personalizzata dell'hypervisor Xen. La protezione dell'hypervisor Xen di AWS è valutata regolarmente da revisori indipendenti durante le valutazioni e i controlli. Consultate il whitepaper sulla protezione di AWS (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) per ulteriori informazioni sull'hypervisor Xen e l'isolamento delle istanze.

**12 I servizi forniti supportano la crittografia?**
Creative Cloud cifra i dati in transito con SSL.

**13 Quali sono i diritti del provider del cloud sui dati dei clienti?**
I clienti di Creative Cloud mantengono il controllo e la proprietà dei loro dati. Esaminate le Condizioni d'uso (www.adobe.com/go/gffooter_terms_of_use) e l'Informativa sulla privacy di Adobe (www.adobe.com/privacy/policy.html) per maggiori dettagli.

**14 AWS pubblica i suoi controlli fisici e ambientali?**
Sì. I controlli fisici e ambientali sono delineati nello specifico nel rapporto SOC 1, Type 2 (aws.amazon.com/security/). Inoltre, AWS supporta la certificazione ISO 27001 e FISMA, che richiedono controlli fisici e ambientali secondo best practice.

**15 I clienti possono proteggere e gestire l'accesso a Creative Cloud da client quali PC e dispositivi mobile?**
Sì. Creative Cloud consente ai clienti di gestire l'accesso client e mobile a seconda dei propri requisiti.

**16 AWS consente ai clienti di proteggere i loro server virtuali?**
Sì. Adobe ha implementato la propria architettura di protezione su quella di AWS basata su best practice del settore compresi i 20 controlli principali SANS per la protezione Internet, le linee guida di controllo Consensus, le linee guida NIST e gli standard Internet.

**17 AWS comprende funzionalità di gestione dell'identità e dell'accesso (IAM)?**
AWS dispone di un insieme di prodotti per la gestione dell'identità e dell'accesso che consentono ad Adobe di gestire le identità utente, assegnare credenziali di protezione, organizzare gli utenti in gruppi e gestire le autorizzazioni degli utenti in modo centralizzato.

**18 Adobe prevede di arrestare i sistemi Creative Cloud per la manutenzione?**
Creative Cloud è implementato in modo tale da eliminare virtualmente i periodi di inattività. I servizi dovrebbero essere accessibili e raggiungibili durante nuove distribuzioni grazie all'utilizzo di ambienti A/B e altri meccanismi che consentono operazioni di conversione live senza tempi di inattività percettibili.

**19 In che modo AWS protegge contro gli attacchi DDoS (Distributed Denial Of Service)?**
La rete AWS fornisce un'ampia protezione controllo la protezione di rete tradizionale. Consultate il whitepaper sulla protezione di AWS (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) per maggiori informazioni su questo argomento, compresa una discussione sui DDoS.

**20 Adobe ha un piano di continuità aziendale per Creative Cloud?**
AWS offre un piano di continuità aziendale (media.amazonwebservices.com/AWS_Disaster_Recovery.pdf) e Creative Cloud è progettato per funzionare da più aree geografiche e più zone o datacenter disponibili. Adobe ha progettato, architettato e implementato Creative Cloud per utilizzare la replicazione di ridondanza dei dati e le architetture di distribuzione di zona a più aree geografiche/disponibilità.

**21 AWS specifica la durata dei dati?**
Creative Cloud memorizza i dati in Amazon S3 che offre un'infrastruttura di memorizzazione duratura. Gli oggetti sono memorizzati in modo ridondante su più dispositivi tra più strutture all'interno di un'area geografica S3. Quando i dati sono memorizzati, Amazon S3 mantiene la durabilità degli oggetti rilevando e riparando rapidamente qualsiasi perdita di ridondanza. Amazon S3 verifica inoltre regolarmente l'integrità dei dati memorizzati utilizzando i checksum. Se si rileva un danno, questo viene riparato utilizzando i dati ridondanti.

**22 Adobe prevede di ottenere la conformità al Federal Information Security Management Act (FISMA)?**
Adobe non prevede di ottenere immediatamente la conformità al Federal Information Security Management Act (FISMA) per Creative Cloud.

**23 Creative Cloud è conforme a HIPAA?**
Adobe non prevede di ottenere la conformità alla certificazione HIPAA (Health Insurance Portability and Accountability Act) del 1996 per Creative Cloud, in quanto Creative Cloud non è inteso per l'elaborazione di documenti sanitari.

**Riferimenti**

Whitepaper sulla panoramica delle politiche di protezione di AWS, marzo 2013 (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

Whitepaper su rischi e conformità di AWS, gennaio 2013 (media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf)

Adobe

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