Vanlige spørsmål om sikkerhet for IT for Adobe Creative Cloud

Retningslinjer for sikkerhet, personvern og samsvar er noen av de vanligste emnene for spørsmål som Adobe mottar om Creative Cloud. Organisasjoner som bruker Creative Cloud, er opptatt av sikkerheten for dataene og at tilgangen til dataene er pålitelig. Formålet med dette dokumentet er å besvare mange av spørsmålene som ofte stilles av IT-sikkerhetsansatte om disse emnene, når de vurderer Creative Cloud.

1 Hvor driftes Creative Cloud fra?
Creative Cloud driftes på Amazon Web Services (AWS), inkludert Amazon Elastic Compute Cloud (Amazon EC2) og Amazon Simple Storage Service (Amazon S3), i USA, EU og Asia/Stillehavskysten. AWS tilbyr en pålitelig plattform for programvaretjenester som brukes av tusenvis av virksomheter over hele verden. AWS leverer tjenester i henhold til etablerte sikkerhetsprosedyrer og er underlagt sertifiseringer og kontroller som er anerkjent i bransjen (aws.amazon.com/security/). Dette betyr at Creative Cloud-medlemmer drar fordel av Amazons løpende forpliktelser om sikkerhetspraksis for lagrede aktiva.

2 Hvor er kundedataene plassert?
Kundedata lagres i Amazon S3, og Adobe tilordner den fysiske regionen som data for enkeltkunder og servere skal plasseres i. Datareplikering for Amazon S3-dataobjekter foretas innenfor den regionale klyngen som dataene lagres i, og replikeres ikke til datasenterklynger i andre regioner. Adobe drifter Creative Cloud ut fra tre regioner: USA, EU og Asia/Stillehavet.

Eksempel: Alle nettskydata fra Creative Cloud-kunder i EU, lagres som standard i AWS-datasenteret i EU, og disse dataene overføres ikke til datasentre utenfor EU.

3 Hvem kontrollerer Creative Cloud-datasentrene?
For delene av Creative Cloud som distribueres i AWS, kontrollerer Amazon de fysiske komponentene. For å gi kunder en bedre forståelse av hvilke kontroller AWS har iverksatt og hvor effektivt de opererer publiserer AWS en Service Organization Controls 1 (SOC 1), Type 2-rapport (aws.amazon.com/security/) med kontroller definert rundt Amazon EC2, Amazon S3 og Virtual Private Cloud (VPC), samt detaljert fysisk sikkerhet og miljøkontroller. Disse kontrollene defineres på et høyt spesifisert nivå som oppfyller de fleste behovene kundene har.

4 Tillater Amazon kunder å besøke AWS-datasentre?
Nei. På grunn av at AWS-datasentre er vert for data fra flere kunder, tillater ikke AWS datasenterbesøk fra kunder, ettersom dette innebærer fysisk tilgang til mange kunder for tredjeparter. For å innfri dette kundebehovet validerer en uavhengig og kompetent kontrollør eksistensen og gjennomføringen av kontroller som en del av en SOC 1, Type 2-rapport. Denne allment aksepterte tredjepartsvalideringen gir kunder et uavhengig perspektiv på effektiviteten av kontroller som finnes. Adobe har signert en avtale om taushetsplikt med AWS og kan skaffe en kopi av SOC 1 Type 2-rapporten (aws.amazon.com/security/). Uavhengige vurderinger av fysisk datasentersikkerhet er også en del av AWS ISO 27001-kontrollen, PCI-vurderingen og ITAR-kontrollprosessen.

5 Er det tillatt for tredjeparter å få tilgang til AWS-datasentre?
AWS fører streng kontroll på tilgang til datasentre, også for internt ansatte. Tredjeparter tillates ikke tilgang til AWS-datasentre unntatt når det er uttrykkelig godkjent av den aktuelle AWS-datasenterlederen i henhold til retningslinjene for tilgang til AWS. Se SOC 1, Type 2-rapporten (aws.amazon.com/security/) for bestemte kontroller relatert til fysisk tilgang, godkjenning for tilgang til datasenter og andre relaterte kontroller.

6 Hvem er ansvarlig for oppdatering?
Adobe er ansvarlig for oppdatering av våre egne gjesteoperativsystemer (OS), programvare og programmer som kjører i AWS. AWS er ansvarlig for oppdatering av systemer som støtter levering av AWS-tjenester, for eksempel hypervisor- og nettverkstjenestene. Dette gjøres slik det kreves i henhold til retningslinjene for AWS og i henhold til ISO 27001-, NIST- og PCI-krav.

7 Overvåkes og kontrolleres privilegerte handlinger?
Kontroller på stedet begrenser tilgang til systemer og data, eller data er begrenset og overvåket. I tillegg er kundedata og serverforekomster logisk isolert fra andre kunder som standard. Privilegert brukertilgangskontroll for AWS-infrastruktur vurderes av en uavhengig kontrollør under AWS SOC 1-, ISO 27001-, PCI-, ITAR- og FISMA-kontrollene.

8 Håndterer nettskyleverandøren trusselen om ugyldig innsidetilgang til kundedata og -programmer?
AWS gir spesifikk SOC 1 som dekkes i SOC 1, Type 2-rapporten (aws.amazon.com/security/). I tillegg utfører Adobe periodiske risikovurderinger av hvordan innsidetilgang kontrolleres og overvåkes.

9 Hvordan isolerer Creative Cloud kundedata?
Alle data som lagres av Adobe på vegne av kunder, har sterk isolasjonssikkerhet og kontrollfunksjoner for leiere. Creative Cloud Storage bruker Amazon S3, som gir avanserte datatilgangskontroller.

10 Implementeres kundesegregering på en sikker måte?
AWS-miljøet er et virtualisert miljø for flere leiere. AWS har implementert sikkerhetsadministrasjonsprosesser, PCI-kontroller og andre sikkerhetskontroller som er utformet for å isolere hver kunde fra andre kunder. AWS-systemer er utformet for å forhindre at kunder får tilgang til fysiske verter eller forekomster som ikke er tilordnet til dem, ved å filtrere gjennom virtualiseringsprogramvaren. Denne arkitekturen er validert av en uavhengig PCI Qualified Security Assessor (QSA) og funnet å være i samsvar med alle krav i PCI DSS 2.0 (aws.amazon.com/security/pci-dss-level-1-compliance-faqs/).

11 Har AWS håndtert kjente hypervisor-sårbarheter?
Amazon EC2 bruker for øyeblikket en kraftig tilpasset versjon av Xen-hypervisoren. AWS Xen-hypervisor-sikkerheten evalueres regelmessig av uavhengige kontrollører under vurderinger og kontroller. Se hviteboken for AWS-sikkerhet (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) for mer informasjon om Xen-hypervisoren og forekomstisolasjon.

12 Støtter de leverte tjenestene kryptering?
Creative Cloud krypterer data i transitt med SSL.

13 Hvilke rettigheter har nettskyleverandøren over kundedata?
Creative Cloud-kunder beholder kontroll og eierskap over dataene. Se Adobes vilkår for bruk (www.adobe.com/go/gffooter_terms_of_use) og retningslinjer om personvern (www.adobe.com/privacy/policy.html) for mer informasjon.

14 Publiserer AWS fysiske og miljømessige kontroller?
Ja. Fysiske og miljømessige kontroller beskrives spesifikt i en SOC 1, Type 2-rapport (aws.amazon.com/security/). I tillegg støtter AWS ISO 27001- og FISMA-sertifisering, som krever etablerte prosedyrer for fysiske og miljømessige kontroller.

15 Kan kunder sikre og administrere tilgang til Creative Cloud fra klienter som PC-er og mobile enheter?
Ja. Creative Cloud tillater kunder å administrere klient- og mobiltilgang etter egne behov.

16 Tillater AWS kunder å sikre virtuelle servere?
Ja. Adobe har implementert sin egen sikkerhetsarkitektur på toppen av AWS, basert på etablerte retningslinjer for bransjen, inkludert SANS Topp 20-kontroller for Internett-sikkerhet, Consensus Audit-retningslinjer, NIST-retningslinjer og Internett-standarder.

17 Inkluderer AWS funksjoner for identitets- og tilgangsadministrasjon (IAM)?
AWS har en programserie med identitets- og tilgangsadministrasjonstilbud, som gjør det mulig for Adobe å administrere brukeridentiteter, tilordne sikkerhetsinformasjon, organisere brukere i grupper og administrere brukertillatelser på en sentralisert måte.

18 Vil Adobe stenge Creative Cloud-systemer for vedlikehold?
Creative Cloud er implementert på en måte som praktisk talt eliminerer nedetid. Tjenestene skal være tilgjengelige og kan nås under nye distribusjoner takket være bruken av A/B-miljøer og andre mekanismer som muliggjør direkte overgang uten eksternt synlig nedetid.

19 Hvordan beskytter AWS mot distribuerte tjenestenektangrep (DDoS)?

AWS-nettverket gir betydelig beskyttelse mot tradisjonelle trusler mot nettverkssikkerheten. Se hviteboken for AWS-sikkerhet (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) for mer informasjon om dette emnet, inkludert en beskrivelse av DDoS.

20 Har Adobe en kontinuitetsplan for Creative Cloud?

AWS tilbyr et kontinuitetsprogram (media.amazonwebservices.com/AWS_Disaster_Recovery.pdf), og Creative Cloud er utformet for å kjøre fra flere regioner og flere tilgjengelighetssoner eller datasentre. Adobe har utformet og implementert Creative Cloud med en arkitektur for å bruke redundansreplikering for data og distribusjonsarkitekturer for flere regioner/tilgjengelighetssoner.

21 Spesifiserer AWS holdbarhet for data?

Creative Cloud lagrer data i Amazon S3, som gir en varig lagringsinfrastruktur. Objekter lagres redundant på flere enheter på tvers av flere fasiliteter i en Amazon S3-region. Når data lagres, opprettholder Amazon S3 holdbarheten for objekter ved raskt å oppdage og reparere eventuell tapt redundans. Amazon S3 verifiserer også regelmessig integriteten for data som lagres, ved hjelp av kontrollsummer. Hvis skade oppdages, repareres den ved hjelp av redundansdata.

22 Planlegger Adobe å anskaffe Federal Information Security Management Act (FISMA)-samsvar?

Adobe har ingen umiddelbare planer om å anskaffe Federal Information Security Management Act (FISMA)-samsvar for Creative Cloud.

23 Er Creative Cloud HIPAA-kompatibelt?

Adobe har ikke planer om å sertifisere Creative Cloud som kompatibelt i henhold til Health Insurance Portability and Accountability Act av 1996 (HIPAA) ettersom Creative Cloud ikke er ment for å behandle informasjon om helsetjenester.

Referanser

Hvitebok for AWS-sikkerhetsprosedyrer, mars 2013
(media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

Hvitebok for AWS-risiko og -samsvar, januar 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/no

Adobe, the Adobe logo, Lightroom, and Photoshop are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Mac and Mac OS are trademarks of Apple, Inc., registered in the United States and other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2013 Adobe Systems Incorporated. All rights reserved. Printed in the USA.