Często zadawane pytania dotyczące zabezpieczeń Adobe Creative Cloud dla specjalistów IT

Bezpieczeństwo, ochrona prywatności i zgodność z przepisami to obszary, których dotyczy najwięcej pytań zadawanych firmie Adobe w związku z usługą Creative Cloud. Firmy, które z niej korzystają, chcą mieć pewność, że ich dane są bezpieczne, a dostęp do nich — niezawodny. Ten dokument ma na celu odpowiedzieć na pytania najczęściej zadawane przez specjalistów IT zajmujących się zabezpieczeniami w związku z usługą Creative Cloud.

1. Gdzie jest hostowana usługa Creative Cloud?

Usługa Creative Cloud jest hostowana w ramach usług Amazon Web Services (AWS), obejmujących usługi Amazon Elastic Compute Cloud (Amazon EC2) oraz Amazon Simple Storage Service (Amazon S3), w Stanach Zjednoczonych, Unii Europejskiej i regionie Azji i Pacyfiku. AWS udostępnia niezawodną platformę do usług oprogramowania, wykorzystywaną przez tysiące firm na całym świecie, oraz świadczy usługi zgodnie z najlepszymi praktykami dotyczącymi zabezpieczeń. Usługa pomyślnie przeszła audyty i procesy certyfikacji rozpoznawalne w branży (aws.amazon.com/security/). Dbałość firmy Amazon o bezpieczeństwo przechowywanych zasobów przynosi korzyść również użytkownikom Creative Cloud.

2. Gdzie przechowywane są dane klientów?

Dane klientów przechowywane są na nośniku Amazon S3. Firma Adobe określa, w którym regionie świata znajdują się dane i serwery poszczególnych klientów. Replikacja danych dla obiektów danych Amazon S3 odbywa się w ramach lokalnego klastra, w którym dane są przechowywane. Dane nie są replikowane do klastrów centrów danych w innych regionach. Firma Adobe zarządza usługą Creative Cloud z trzech regionów: Stanów Zjednoczonych, Unii Europejskiej i regionu Azji i Pacyfiku.

Przykład: domyślnie wszystkie dane użytkowników Creative Cloud w Unii Europejskiej będą przechowywane w chmurze w centrum danych AWS w Unii Europejskiej, dane te nie będą przenoszone do centrów danych poza UE.

3. Kto sprawuje kontrolę nad centrami danych Creative Cloud?

W przypadku części usługi Creative Cloud znajdujących się w AWS składniki fizyczne kontroluje firma Amazon. Aby pomóc klientom w lepszym zrozumieniu, co kontroluje AWS i jak skutecznie to robi, opublikowany został raport Service Organization Controls 1 (SOC 1), Type 2 (aws.amazon.com/security/). Zawiera on sposób podziału kontroli pomiędzy Amazon EC2, Amazon S3 i Virtual Private Cloud (VPC), a także szczegółowy opis kontroli nad zabezpieczeniami fizycznymi i środowiskowymi. Opis jest bardzo szczegółowy, co powinno spełnić oczekiwania większości klientów.

4. Czy Amazon zezwala klientom na odwiedzanie centrów danych AWS?

Nie. Klienci nie mogą odwiedzać centrów danych AWS, ponieważ przechowywane są w nich dane wielu klientów, a odwiedziny umożliwiłyby fizyczny dostęp do nich osobom postronnym. Aby spełnić oczekiwania klientów, niezależny i kompetentny audytor sprawdza istnienie i skuteczność kontroli w ramach raportu SOC 1, Type 2. Ten ogólnie akceptowany proces zewnętrznej walidacji zapewnia klientom dostęp do niezależnej opinii dotyczącej kontroli w centrach danych. Firma Adobe podpisała niejawną umowę z AWS i może otrzymywać kopię raportu SOC 1, Type 2 (aws.amazon.com/security/). Niezależna ocena fizycznego bezpieczeństwa centrum danych jest również częścią audytu AWS ISO 27001, oceny PCI i audytu ITAR.

5. Czy osoby postronne mają dostęp do centrów danych AWS?

AWS szczegółowo kontroluje dostęp do centrów danych, nawet wśród jej pracowników. Osoby postronne nie mają dostępu do centrów danych AWS z wyjątkiem sytuacji jednoznacznie zaakceptowanych przez odpowiedniego menedżera centrum danych AWS zgodnie z zasadami dostępu obowiązującymi w AWS. Szczegółowe informacje o kontroli dostępu fizycznego, autoryzacji dostępu do centrów danych i innych powiązanych kontrolach znajdują się w raporcie SOC 1, Type 2 (aws.amazon.com/security/).

6. Kto jest odpowiedzialny za wprowadzanie uaktualnień?

Firma Adobe jest odpowiedzialna za wprowadzanie uaktualnień w swoich gościnnych systemach operacyjnych, oprogramowaniu i aplikacjach wykorzystywanych przez AWS. AWS jest odpowiedzialna za wprowadzanie uaktualnień do systemu obsługującego usługi AWS, takie jak hipernadzorca i usługi sieciowe. Odbywa się to zgodnie z zasadami AWS i z wymaganiami certyfikatów ISO 27001, NIST i PCI.

7. Czy działania uprzywilejowane są monitorowane i kontrolowane?
Systemy kontroli w centrach danych ograniczają dostęp do systemów i danych, dane są też monitorowane. Ponadto dane poszczególnych klientów i instancje serwerów są od siebie domyślnie oddzielone w sposób logiczny. Kontrola dostępu uprzywilejowanych użytkowników do infrastruktury AWS jest oceniana przez niezależnego audytora podczas audytów AWS SOC 1, ISO 27001, PCI, ITAR i FISMA.

8. Czy dostawca usług w chmurze zajmuje się problemami związanymi z ryzykiem niewłaściwego dostępu pracowników wewnętrznych do danych klientów i aplikacji?
AWS udostępnia szczegółowy raport SOC 1 w ramach raportu SOC 1, Type 2 (aws.amazon.com/security/). Ponadto firma Adobe prowadzi okresową ocenę ryzyka dotyczącą kontroli i monitoringu dostępu pracowników wewnętrznych do danych.

9. W jaki sposób dane klientów są izolowane w usłudze Creative Cloud?
Wszystkie dane klientów przechowywane przez firmę Adobe poddane są izolacji związanej z zabezpieczeniami i kontrolą. W usłudze Creative Cloud Storage wykorzystywany jest nośnik Amazon S3, który zapewnia zaawansowane metody kontroli dostępu do danych.

10. Czy rozdzielanie klientów jest przeprowadzane w sposób bezpieczny?
Środowisko AWS jest wirtualizowane i wielodostępne. AWS wprowadziła procesy zarządzania zabezpieczeniami, kontrolę PCI i inne procesy kontroli zabezpieczeń, aby izolować od siebie klientów.
Systemy AWS uniemożliwiają klientom dostęp do fizycznych hostów lub instancji nieprzypisanych do nich dzięki filtrowaniu za pośrednictwem oprogramowania wirtualizacyjnego. Ta architektura została sprawdzona przez niezależnego rzeczoznawcę PCI Qualified Security Assessor (QSA), który uznał, że spełnia ona wszystkie wymagania standardu PCI DSS 2.0 (aws.amazon.com/security/pci-dss-level-1-compliance-faqs/).

11. Czy AWS zajmuje się znanymi słabymi punktami hipernadzorcy?
W serwisie Amazon EC2 wykorzystywana jest obecnie wersja hipernadzorcy Xen, którą można w znacznym stopniu dostosować. Zabezpieczenia hipernadzorcy Xen AWS są regularnie sprawdzane przez niezależnych audytorów podczas ocen i audytów. Więcej informacji o hipernadzorcy Xen i izolowaniu instancji znajduje się w dokumentacji zabezpieczeń AWS (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf).

12. Czy oferowane usługi obsługują szyfrowanie?
Usługa Creative Cloud szyfruje dane za pomocą protokołu SSL.

13. Jakie są prawa dostawcy usług w chmurze w stosunku do danych klientów?
Klienci usługi Creative Cloud zachowują kontrolę nad swoimi danymi i pozostają ich właścicielami. Szczegółowe informacje znajdują się w Warunkach użytkowania (www.adobe.com/go/gffooter_terms_of_use) i Zasadach prywatności (www.adobe.com/privacy/policy.html) określonych przez firmę Adobe.

14. Czy AWS publikuje wyniki kontroli bezpieczeństwa fizycznego i środowiskowego?
Tak. Wyniki kontroli bezpieczeństwa fizycznego i środowiskowego znajdują się w raporcie SOC 1, Type 2 (aws.amazon.com/security/). Ponadto AWS posiada certyfikaty ISO 27001 i FISMA, które wymagają postępowania zgodnie z najlepszymi praktykami w zakresie kontroli fizycznej i środowiskowej.

15. Czy klienci mogą zarządzać dostępem do usługi Creative Cloud z takich urządzeń jak komputery i telefony komórkowe?
Tak. Klienci mogą zarządzać dostępem do usługi Creative Cloud i urządzeniami umożliwiającymi taki dostęp zgodnie z własnymi wymaganiami.

16. Czy AWS umożliwia klientom zabezpieczanie serwerów wirtualnych?
Tak. Firma Adobe wprowadziła własną architekturę zabezpieczeń jako dodatek do usługi AWS w oparciu o najlepsze praktyki, takie jak SANS Top 20 Controls for Internet Security, Consensus Audit Guidelines, wytyczne NIST oraz standardy internetowe.

17. Czy AWS umożliwia zarządzanie tożsamością i dostępem (IAM)?
AWS udostępnia zestaw usług do zarządzania tożsamością i dostępem, umożliwiając firmie Adobe zarządzanie tożsamościami użytkowników, przydzielanie uwierzytelnień, łączenie użytkowników w grupy i zarządzanie poziomem dostępu użytkowników w sposób scentralizowany.

18. Czy firma Adobe wstrzymuje działanie usługi Creative Cloud na czas konserwacji?
Usługa Creative Cloud została stworzona w taki sposób, aby wykluczać przerwy w działaniu. Usługi powinny być dostępne podczas nowych wdrożeń dzięki wykorzystaniu środowisk A/B i innych mechanizmów umożliwiających modernizację bez zauważalnych przerw w pracy.

19. W jaki sposób AWS chroni się przed atakami DDos (Distributed Denial Of Service)?
Sieć AWS zawiera rozbudowane systemy chroniące ją przed typowymi zagrożeniami sieciowymi. Więcej informacji na ten temat, w tym dyskusja o DDoS, znajduje się w dokumentacji zabezpieczeń AWS (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf).

20. Czy firma Adobe planuje ciągłość działania usługi Creative Cloud?
AWS oferuje program ciągłości działania (media.amazonwebservices.com/AWS_Disaster_Recovery.pdf), a usługa Creative Cloud działa w oparciu o kilka centrów danych, czyli o lokalizacje w kilku regionach i kilku strefach dostępności. Usługa Creative Cloud wykorzystuje replikację nadmiarowości danych i architektury rozmieszczania w wielu regionach i strefach dostępności.

21. Czy AWS określa trwałość danych?
W usłudze Creative Cloud dane przechowywane są na nośniku Amazon S3, który zapewnia trwałą infrastrukturę magazynu. Dane przechowywane są w sposób redundantny na wielu urządzeniach i w wielu lokalizacjach należących do Amazon S3. Po ich zapisaniu Amazon S3 dba o trwałość danych przez szybką reakcję na ewentualną utratę redundancji danych. Amazon S3 regularnie sprawdza spójność danych za pomocą sum kontrolnych. Ewentualne wykryte nieprawidłowości są naprawiane za pomocą zachowanych kopii danych.

22. Czy firma Adobe planuje uzyskać zgodność z normą Federal Information Security Management Act (FISMA)?
W najbliższym czasie firma Adobe nie planuje uzyskać zgodności usługi Creative Cloud z normą Federal Information Security Management Act (FISMA).

23. Czy usługa Creative Cloud jest zgodna z normą HIPAA?
Firma Adobe nie zamierza zdobywać certyfikatu HIPAA (Health Insurance Portability and Accountability Act of 1996) dla usługi Creative Cloud, ponieważ nie jest ona przeznaczona do przechowywania danych służby zdrowia.

Materiały referencyjne

Omówienie dokumentacji dotyczącej zabezpieczeń w AWS, marzec 2013
(media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

Dokumentacja dotycząca ryzyka i zgodności z przepisami w AWS, styczeń 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