Часто задаваемые вопросы о безопасности Adobe Creative Cloud для специалистов по ИТ

Политики безопасности, конфиденциальности и соответствия стандартам и нормативам — это область, в которой Adobe получает больше всего вопросов о Creative Cloud. Организации, использующие Creative Cloud, беспокоятся о безопасности своих данных и надежности доступа к ним. Этот документ ответит на многие вопросы на эту тему, задаваемые специалистами по безопасности информационных технологий, когда они рассматривают возможность использования Creative Cloud.

1. Где размещена служба Creative Cloud?

Служба Creative Cloud размещена в облачной системе Amazon Web Services (AWS), включая Amazon Elastic Compute Cloud (Amazon EC2) и Amazon Simple Storage Service (Amazon S3), в США, Европе и азиатско-тихоокеанском регионе. AWS обеспечивает надежную платформу для программных услуг, которыми пользуются тысячи организаций во всем мире. AWS предоставляет услуги в соответствии с новейшими методами обеспечения безопасности и проходит все сертификации и проверки, признанные в отрасли (aws.amazon.com/security/). Это означает, что пользователи Creative Cloud выигрывают от усилий, которые постоянно предпринимает компания Amazon для повышения безопасности хранимых активов.

2. Где хранятся клиентские данные?

Клиентские данные хранятся в службе Amazon S3, и Adobe указывает, в каком физическом регионе будут находиться данные и серверы клиентов. Репликация данных для объектов данных Amazon S3 производится внутри регионального кластера, где хранятся данные. В кластеры центров обработки данных, расположенные в других регионах, данные не реплицируются. Adobe управляет службой Creative Cloud из трех регионов: США, Европы и азиатско-тихоокеанского региона.

Например, по умолчанию все облачные данные клиентов Creative Cloud в Европе хранятся в центре обработки данных AWS в Европе и не передаются в центры обработки данных за пределами Европы.

3. Кто управляет центрами обработки данных Creative Cloud?

Для частей Creative Cloud, развернутых в AWS, физические компоненты находятся под управлением компании Amazon. Чтобы клиентам было легче понять, какие средства управления и контроля существуют в AWS и насколько эффективно они работают, AWS публикует отчет Service Organization Controls 1 (SOC 1), тип 2 (aws.amazon.com/security/), где определены средства управления и контроля для служб Amazon EC2, Amazon S3 и Virtual Private Cloud (VPC) и подробно описаны средства управления физической безопасностью и средой. Эти средства управления и контроля определены с высоким уровнем конкретности, который должен удовлетворить потребности большинства клиентов.

4. Разрешает ли Amazon посещать центры обработки данных AWS клиентам?

Нет. Так как в центрах обработки данных AWS хранятся данные многих пользователей, AWS не разрешает клиентам посещать эти центры, потому что в этом случае третьи лица получили бы возможность физического доступа к данным большого диапазона клиентов. Для удовлетворения этой потребности клиентов независимый и компетентный аудитор проверяет наличие и работу средств управления и контроля, как часть отчета SOC 1, тип 2. Такая широко принятая проверка третьими лицами обеспечивает клиентам независимую картину имеющихся средств управления и контроля. Компания Adobe подписала соглашение о неразглашении с AWS и может получить копию отчета SOC 1, тип 2 (aws.amazon.com/security/). Независимая проверка физической безопасности центров обработки данных также является частью проверки на соответствие стандарту ISO 27001 AWS, стандарту безопасности данных в области платежных карт (PCI) и международной торговли оружием (ITAR).

5. Могут ли третьи лица получить доступ в центры обработки данных AWS?

AWS строго контролирует доступ в центры обработки данных даже для собственных сотрудников. Третьи лица получают доступ в центры обработки данных AWS только в случае, если это разрешено соответствующим менеджером центра обработки данных AWS в соответствии с политикой контроля доступа AWS. См. отчет SOC 1, тип 2 (aws.amazon.com/security/) для получения информации о средствах контроля, связанных с физическим доступом, разрешением доступа в центры обработки данных и других.

6. Кто отвечает за исправления?

Adobe отвечает за внесение исправлений в наши гостевые операционные системы (ОС), программное обеспечение и приложения, работающие в AWS. AWS отвечает за внесение исправлений в системы, обеспечивающие предоставление услуг AWS, таких как услуги гипервизора и сетевые услуги. Это делается в соответствии с политикой AWS и требованиями стандартов ISO 27001, NIST и PCI.

7. Осуществляются ли мониторинг и контроль привилегированных действий?
Имеющиеся средства контроля ограничивают доступ к системам и данным, либо ограничиваются и отслеживаются данные. Кроме того, по умолчанию клиентские данные и экземпляры серверов логически изолированы от других клиентов. Контроль доступа привилегированных пользователей в инфраструктуре AWS проверяется независимым аудитором во время проверок AWS на соответствие стандартам SOC 1, ISO 27001, PCI, ITAR и FISMA.

8. Устраняет ли поставщик облачных услуг угрозу несанкционированного внутреннего доступа к клиентским данным и приложениям?
AWS обеспечивает специальный стандарт SOC 1, описанный в отчете SOC 1, тип 2 (aws.amazon.com/security/). Кроме того, Adobe проводит периодические оценки рисков, связанных с контролем и мониторингом внутреннего доступа.

9. Каким образом служба Creative Cloud изолирует клиентские данные?
Все данные, которые компания Adobe хранит для клиентов, защищены мощными средствами изоляции пользователей и контроля доступа. Creative Cloud Storage использует службу Amazon S3, которая обеспечивает современные средства контроля доступа.

10. Используются ли надежные средства разделения пользователей?
Среда AWS — это виртуализованная, многопользовательская среда. AWS использует процессы управления безопасностью и средства контроля (PCI и другие) для изоляции клиентов друг от друга. Системы AWS спроектированы таким образом, чтобы клиенты не имели доступа к физическим узлам или экземплярам, что достигается с помощью фильтров в программном обеспечении виртуализации. Эта архитектура была проверена независимым аудитором со статусом PCI Qualified Security Assessor (QSA) и показала полное соответствие всем требованиям стандарта PCI DSS 2.0 (aws.amazon.com/security/pci-dss-level-1-compliance-faqs/).

11. Устранила ли система AWS проблему известных уязвимостей гипервизора?
Сейчас служба Amazon EC2 использует чрезвычайно адаптируемую версию гипервизора Xen. Безопасность гипервизора Xen в системе AWS регулярно оценивается независимыми аудиторами во время различных оценок и проверок. См. официальный документ по безопасности AWS (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) для получения дополнительной информации о гипервизоре Xen и изоляции экземпляров.

12. Поддерживают ли предоставляемые услуги шифрование?
Creative Cloud шифрует данные по протоколу SSL.

13. Какие права на клиентские данные имеет поставщик облака?
Клиенты Creative Cloud сохраняют контроль над своими данными и остаются владельцами этих данных. См. Условия использования Adobe (www.adobe.com/go/gffooter_terms_of_use) и Политику конфиденциальности (www.adobe.com/privacy/policy.html) для получения дополнительных сведений.

14. Публикует ли AWS информацию об используемых средствах физического контроля и контроля среды?
Да. Средства физического контроля и контроля окружающей среды отдельно описаны в отчете SOC 1, тип 2 (aws.amazon.com/security/). Кроме того, AWS поддерживает сертификацию по стандартам ISO 27001 и FISMA, что требует использования современных методов физического контроля и контроля среды.

15. Могут ли клиенты получить доступ и управлять доступом к Creative Cloud с клиентских устройств, таких как ПК и мобильные устройства?
Да. Creative Cloud позволяет клиентам управлять доступом с клиентских и мобильных устройств в соответствии с их требованиями.

16 Позволяет ли AWS клиентам иметь собственные виртуальные серверы?
Да. Компания Adobe внедрила собственную архитектуру безопасности поверх AWS на основе современных отраслевых методов, включая 20 лучших средств контроля SANS для безопасности а Интернете (SANS Top 20 Controls for Internet Security), рекомендации CAG (Consensus Audit Guidelines), рекомендации NIST и стандарты Интернета.

17. Включает ли AWS средства управления идентификацией и доступом (Identity and Access Management, IAM)?
AWS имеет набор продуктов для управления идентификацией и доступом, которые дают возможность компании Adobe централизованно управлять идентификацией пользователей, назначать учетные данные безопасности, группировать пользователей и управлять правами пользователей.

18. Будет ли Adobe останавливать системы Creative Cloud для обслуживания?
Система Creative Cloud построена таким способом, что простои практически исключены. Во время новых развертываний службы должны быть доступны и открыты для обращения благодаря использованию A/B-сред и других механизмов, позволяющих отключать систему без видимого простоя для внешних пользователей.

19. Как AWS защищает от распределенных атак типа «отказ в обслуживании» (DDoS)?
Сеть AWS обеспечивает значительную защиту от традиционных угроз безопасности сети. См. официальный документе по безопасности AWS (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) для получения дополнительных сведений на эту тему, включая атаки DDoS.

20. Есть ли у компании Adobe план бесперебойности работы для Creative Cloud?
AWS предлагает программу бесперебойности работы (media.amazonwebservices.com/AWS_Disaster_Recovery.pdf), а служба Creative Cloud рассчитана на работу во многих регионах и зонах доступности или центрах обработки данных. Компания Adobe проектировала, конструировала и внедряла службу Creative Cloud таким образом, чтобы она использовала репликацию данных для избыточности и архитектуры развертывания для доступности в разных регионах и зонах доступности.

21. Указывает ли AWS средства сохранения целостности данных?
Creative Cloud хранит данные в службе Amazon S3, обеспечивающей архитектуру длительного хранения данных без угрозы потери. Объекты хранятся с избыточностью на нескольких устройствах в нескольких центрах в регионе Amazon S3. Когда данные заносятся в хранилище, Amazon S3 защищает объекты от возможной потери, быстро обнаруживая и устраняя случаи потери избыточности. Кроме того, Amazon S3 регулярно проверяет целостность хранимых данных с помощью контрольных сумм. Если обнаруживается повреждение, оно устраняется с помощью избыточных данных.

22 Планирует ли Adobe получить сертификат соответствия Закону США по управлению информационной безопасностью (Federal Information Security Management Act, FISMA)?
В настоящее время Adobe не планирует получение сертификата FISMA для Creative Cloud.

23. Соответствует ли Creative Cloud стандарту HIPAA?
Компания Adobe не намерена получать сертификат на соответствие требованиям Закона США о преемственности страхования и отчетности в области здравоохранения (Health Insurance Portability and Accountability Act, HIPAA) 1996 г., так как служба Creative Cloud не предназначена для обработки данных в области здравоохранения.

Ссылки

AWS Security Practices (официальный документ по методам обеспечения безопасности AWS), март 2013 г. (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

AWS Risk and Compliance (официальный документ AWS о рисках и соответствии стандартам), январь 2013 г. (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

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.