Adobe Creative Cloud для организаций. Вопросы безопасности.

Содержание

1. Краткий обзор

1. Creative Cloud для организаций

2. Системы идентификации

3. Архитектура

5. Amazon Web Services

7. Физические параметры и настройка среды AWS

8. Adobe Common Controls Framework

8. Структура безопасности в Adobe

9. Безопасность при разработке продуктов Adobe

10. Обучение по безопасности в Adobe

10. Управление рисками и уязвимостями в Adobe

11. Офисы Adobe

12. Сотрудники Adobe

12. Конфиденциальность данных клиентов

12. Соответствие нормам безопасности

13. Заключение

Краткий обзор

Adobe Creative Cloud для организаций обеспечивает крупным клиентам доступ к настольным и мобильным приложениям Adobe, облачным сервисам, средствам совместной работы и инструментам управления лицензиями. Поддерживаются гибкое развертывание и различные варианты управления идентификацией, в том числе Federated ID с профилем единого входа (SSO), ежегодная проверка лицензий и поддержка корпоративного уровня.

Мы серьезно подходим к защите ваших цифровых данных. Мы стремимся быть лучшими во всем — от тщательной интеграции средств безопасности в приложения до формирования групп реагирования на инциденты. Сотрудничество с партнерами помогает нам узнавать о новых видах угроз, осваивать передовые методы безопасности, а также внедрять технологии защиты.

Безопасность — один из важнейших элементов нашей архитектуры. Для управления доступом к Creative Cloud для организаций служит уникальный ID пользователя. Он формируется с помощью Admin Console и может быть привязан к корпоративной службе каталогов.
Данные шифруются при хранении и передаче; существует возможность дополнительной защиты выделенным ключом шифрования.

Сервисы Adobe, работающие с данными пользователей, либо имеют сертификаты SOC 2, ISO27001 или PCI, либо готовятся к их получению. Для защиты применяются самые современные решения и проверенные технологии безопасности.

Adobe использует хостинговую платформу Amazon Web Services в распределенной конфигурации, что обеспечивает лучшую сохранность данных.

В этой статье описывается архитектура безопасности, помогающая защитить ваши данные.

Creative Cloud для организаций

Creative Cloud для организаций — это решение корпоративного уровня. Оно состоит из четырех частей: 1) настольные приложения, 2) мобильные приложения, 3) Admin Console и 4) облачные сервисы.

Настольные приложения

Настольные приложения запускаются на рабочих станциях пользователей. Они могут либо разворачиваться стандартными методами (например, Microsoft SCCM/JAMF Casper Suite) из пакетов, либо скачиваться с ресурсов Adobe и устанавливаться индивидуально. Каждый пользователь получает лицензию через Admin Console после идентификации с помощью LDAP или Microsoft Active Directory ID. Кроме того, Admin Console регулирует доступ к конкретным приложениям и сервисам. При вызове приложения оно обращается к Admin Console для проверки, достаточно ли у пользователя прав. Информация передается в зашифрованном виде, а обработка данных ведется в соответствии со стандартами и безопасности.

Мобильные приложения

Мобильные приложения работают на мобильных устройствах пользователей. Управление ими может осуществляться с помощью MDM-решения — например, AirWatch. Данные, созданные в мобильных приложениях, хранятся как на самих устройствах, так и на облачных ресурсах с шифрованием (об этом пойдет речь ниже). Информация передается в зашифрованном виде, а доступ к сервисам предоставляется после идентификации согласно настройкам в Admin Console.

Admin Console

Инструмент Admin Console предназначен для конфигурирования выдачи лицензий и доступа к сервисам. Admin Console может работать в связке с корпоративной системой управления идентификацией, совместимой с SAML2.0, и имеет API для автоматизированной авторизации. Служба ИТ может сгруппировать лицензии так же, как в корпоративном каталоге, или назначить их конкретным рабочим группам. При работе с облачными сервисами Admin Console позволяет управлять выделенными ключами шифрования, а при необходимости отзывать разрешения на доступ к данным. Обмен данными с Admin Console ведется в режиме шифрования, а доступ к средствам администрирования ограничен кругом пользователей, назначенных при заключении договора.

Облачные сервисы

Облачные сервисы помогают специалистам работать эффективнее. С их помощью дизайнеры находят файлы, совместно работают над проектами, получают нужные им шрифты и стоковые фотографии. Доступ к облачным сервисам регулируется в Admin Console на основании уникальных ID пользователей. Облачные сервисы работают в мультиклиентской инфраструктуре на платформе Amazon AWS. Информация передается в зашифрованном виде; при хранении данные также шифруются и могут быть дополнительно защищены с помощью выделенного ключа шифрования.

Системы идентификации в Creative Cloud для организаций

Управление правами и идентификацией

ИТ-администраторы назначают пользователям права доступа к настольным приложениям Creative Cloud облачным сервисам, используя для этого лицензирование именованных пользователей в Adobe Admin Console.

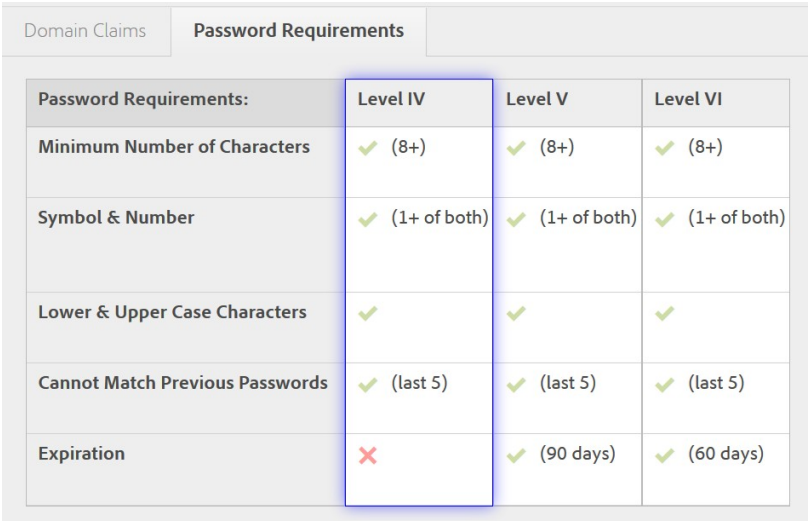
Существует три типа лицензирования именованных пользователей.

- Идентификатор **Adobe ID** создается, управляется конечным пользователем и принадлежит ему. Пользователи с Adobe ID имеют доступ к ресурсам Creative Cloud для организаций, только если им это разрешил ИТ-администратор.
- Идентификатор **Adobe Enterprise ID** создается и управляется ИТ-администратором организации. Учетные записи пользователей с таким идентификатором и все сопутствующие данные принадлежат организации.
- Идентификатор **Adobe Federated ID** применяется в организациях, где реализована система единого входа (SSO). Идентификационные профили и все сопутствующие данные создаются и управляются службой ИТ и принадлежат ей. Adobe работает с большинством поставщиков удостоверений стандарта SAML2.0.

Права доступа назначаются в Adobe Admin Console.

Политика в отношении паролей

Служба ИТ может применять три политики назначения паролей пользователям.



Password Requirements:	Level IV	Level V	Level VI
Minimum Number of Characters	✓ (8+)	✓ (8+)	✓ (8+)
Symbol & Number	✓ (1+ of both)	✓ (1+ of both)	✓ (1+ of both)
Lower & Upper Case Characters	✓	✓	✓
Cannot Match Previous Passwords	✓ (last 5)	✓ (last 5)	✓ (last 5)
Expiration	✗	✓ (90 days)	✓ (60 days)

Для Adobe ID и Enterprise ID используется алгоритм хэширования SHA-256 в сочетании с засаливанием паролей и множественными хэш-итерациями. Adobe ведет мониторинг учетных записей, выявляя факты необычного поведения и нейтрализуя угрозы. Для учетных записей Federated ID такой мониторинг отсутствует.

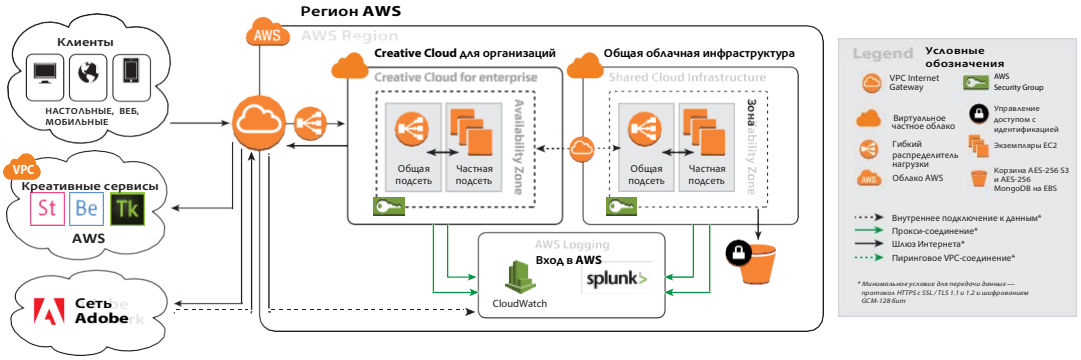
Управление учетными записями

Для управления учетными записями именованных пользователей служит Adobe Admin Console. Кроме того, через консоль осуществляется управление пользователями и правами для Adobe Document Cloud и Adobe Marketing Cloud. Через консоль также отправляются заявки на поддержку.

Служба ИТ может создавать и удалять учетные записи Enterprise ID и Federated ID. В облачном хранилище для каждой учетной записи выделяется индивидуальное пространство; это означает, что ИТ-специалисты не имеют прямого доступа к файлам пользователей. Тем не менее, сами учетные записи остаются во владении ИТ-специалистов, и у них есть право отзывать у пользователей разрешения. При удалении Enterprise ID или Federated ID, для которых активен сервис корпоративного хранения, данные становятся недоступны пользователям, а по истечении 90 дней удаляются из хранилища.

Через Adobe Admin Console служба ИТ может также выделять пространство в хранилище для учетных записей Adobe ID. Контролировать учетные записи Adobe ID ИТ-специалисты не могут, но у них есть возможность закрыть им доступ к хранилищу; данные при этом удаляются также через 90 дней.

Архитектура Creative Cloud для организаций



Adobe Creative Cloud для организаций — это сочетание настольных приложений, мобильных приложений и облачных сервисов. Именованные пользователи Creative Cloud для организаций, имеющие права доступа к облачным сервисам, могут обращаться к ним из следующих конечных точек:

- настольные приложения, такие как Adobe Photoshop и настольное приложение Creative Cloud;
- веб-браузер;
- мобильные приложения, такие как Adobe Capture CC, Adobe Photoshop Sketch и Adobe Lightroom Mobile.

Описание имеющихся в составе инструментов и сервисов приведено на странице http://www.adobe.com/ru/creativecloud/ business/enterprise.html.

В конечной точке пользователь Creative Cloud для организаций идентифицируется методами, о которых шла речь выше, и получает доступ к своему контенту.

Набор доступных сервисов определяется тем, из какой конечной точки происходит обращение к Adobe Creative Cloud. При работе на мобильных устройствах доступны такие возможности Creative Cloud, как подтверждение прав пользователей, синхронизация настроек и предоставление результатов работы в общий доступ. Настольное приложение Creative Cloud позволяет скачивать и обновлять креативные настольные приложения (Photoshop и др.), получать шрифты через Adobe Typekit, размещать файлы в хранилище Creative Cloud и загружать их оттуда в локальную систему.

Во всех конечных точках доступ к Creative Cloud осуществляется по протоколу HTTPS/SSL. При передаче контент шифруется с помощью симметричного блочного криптоалгоритма AES со 128-разрядным ключом GCM, а при хранении — с помощью симметричного криптоалгоритма AES с 256-разрядным ключом безопасности по стандарту FIPS 140-2, удовлетворяющему рекомендациям NIST 800-57. После того как Adobe Creative Cloud идентифицирует пользователя, ему предоставляется доступ к тем приложениям и сервисам, работать с которыми разрешил ИТ-администратор в Adobe Admin Console. Дальнейший круг разрешенных действий определяется тем, в какой конечной точке находится пользователь. Например, при работе в Photoshop пользователи имеют возможность взаимодействовать через Creative Cloud Libraries, а также делиться цветами, графикой и стилями внутри своей команды.

Хранение контента в Creative Cloud для организаций

В Creative Cloud для организаций используется мультиклиентский принцип хранения. Пользовательский контент обрабатывается экземпляром Amazon Elastic Compute Cloud (EC2) и помещается в группу корзин Amazon Simple Storage Services (S3), а также через экземпляр СУБД MongoDB — в Amazon Elastic Block Store (EBS).

Сам контент находится в корзинах S3, а его метаданные заносятся в EBS через MongoDB. Защита организуется путем назначения ролей в системе Identity and Access Management (IAM).

Контент и сопутствующая информация шифруются с помощью симметричного криптоалгоритма AES с 256-разрядным ключом безопасности. Ключи уникальны для каждого пользователя и каждого домена. Выделенными ключами управляет служба Amazon Key Management Service (KMS), которая обеспечивает дополнительные уровни контроля и безопасности. Adobe автоматически выполняет циклический сдвиг ключей на ежегодной основе. Если возникает потребность, ИТ-администраторы могут отзывать ключи через Admin Console, и тогда данные, которые зашифрованы с помощью этих ключей, становятся недоступны конечным пользователям. Подробнее см. раздел «Выделенный ключ шифрования» ниже.

Метаданные и сопутствующая информация в EBS шифруются с применением 256-разрядного алгоритма AES по криптографическому стандарту FIPS 140-2, удовлетворяющему рекомендациям Национального института стандартов и технологий США NIST 800-57.

Данные физически дублируются: их копии хранятся в нескольких центрах обработки данных (ЦОД), а внутри одного ЦОД — на нескольких устройствах. Весь сетевой трафик сопровождается верификацией данных и проверками контрольных сумм. Наконец, данные синхронно и автоматически реплицируются в другие ЦОД внутри регионального кластера, поэтому даже при утере данных в двух местоположениях нарушения их целостности не происходит.

Подробнее со службами Amazon можно ознакомиться по следующим адресам:

- MongoDB (на английском языке): http://www.mongodb.org
- Amazon S3: https://aws.amazon.com/ru/s3/faqs
- Amazon KMS: http://aws.amazon.com/ru/kms/faqs/
- Amazon EC2: http://aws.amazon.com/ru/ec2/

Выделенный ключ шифрования

Вы уже знаете, как шифруется контент, хранящийся в Creative Cloud для организаций. ИТ-администраторы могут добавлять дополнительные слои управления и безопасности, запросив у Adobe выделенный ключ шифрования для некоторых или даже всех доменов организации. Контент шифруется с применением этого ключа; если потребуется, в дальнейшем ключ шифрования может быть отозван из Admin Console. После отзыва весь контент, зашифрованный с выделенным ключом, становится недоступным конечному пользователю.

Подробнее об управлении шифрованием с помощью выделенных ключей можно узнать по следующим адресам:

- https://helpx.adobe.com/ru/enterprise/using/encryption.html
- https://helpx.adobe.com/ru/enterprise/using/encryption-faq.html

Типы сервисов Creative Cloud

В состав Creative Cloud входят облачные сервисы, способные хранить пользовательский контент. К ним могут обращаться другие сервисы Creative Cloud для организаций и конечные точки, если это разрешено администратором. Разрешения устанавливаются в Adobe Admin Console. Подробнее о сервисах Creative Cloud можно узнать здесь:

- Adobe Portfolio (на английском языке): https://www.myportfolio.com/
- Behance (на английском языке): https://www.behance.net/
- Creative Cloud Extract: http://www.adobe.com/ru/creativecloud/extract.html
- Lightroom: http://www.adobe.com/ru/products/photoshop-lightroom.html
- Phonegap Build (на английском языке): https://build.phonegap.com/
- Publish Online (InDesign): https://helpx.adobe.com/ru/indesign/using/publish-online.html
- Share Online (на английском языке): http://adobe.ly/2bYysLs
- Story Plus (на английском языке): https://creative.adobe.com/products/story-plus
- Typekit (на английском языке): https://typekit.com/

Amazon Web Services

Компоненты Creative Cloud для организаций размещены на серверах AWS, в том числе Amazon EC2 и Amazon S3, которые физически расположены в США, странах ЕС и в странах Азии. Amazon EC2 — это веб-сервис, предоставляющий автоматически масштабируемые вычислительные ресурсы в облаке. Amazon S3 — это надежная инфраструктура для хранения любых объемов данных.

Платформа AWS предоставляет услуги высочайшего качества и регулярно проходит сертификацию. Подробнее — на сайте «Безопасность облака AWS».

Области ответственности AWS и Adobe

AWS контролирует компоненты системы, начиная с верхнего гипервизорского уровня виртуализации и вплоть до физической безопасности инфраструктуры Adobe Creative Cloud для организаций. Adobe отвечает за обслуживание гостевой ОС (в т. ч. за установку обновлений и патчей) и прикладного ПО, а также за настройку межсетевого экрана AWS.

AWS также обеспечивает облачную инфраструктуру, предоставляя множество вычислительных ресурсов, среди которых — обработка и хранение данных. Инфраструктура AWS состоит из серверных помещений, сетей и оборудования, а также включает в себя программные системы (ОС сервера виртуальных машин, ПО для виртуализации и др.). Amazon строит AWS и управляет этой платформой согласно стандартам и нормативным требованиям.

Безопасное управление

Для подключения к инфраструктуре AWS и управления ею Adobe использует защищенные протоколы Secure Shell (SSH) и Secure Sockets Layer (SSL).

География размещения данных пользователей в сети AWS

Приведенная ниже информация взята из обзора процессов безопасности в AWS. С этим обзором (на английском языке) можно ознакомиться здесь.

Adobe хранит все данные пользователей Adobe Creative Cloud на серверах Amazon Web Services в восточном регионе США. Аналитические данные пользователей, которые находятся в США, размещаются в ЦОД в Сан-Хосе (шт. Калифорния) и в Далласе (шт. Техас). Аналитические данные пользователей, которые находятся за пределами США, размещаются в Лондоне (Великобритания).

Репликация объектов данных Amazon S3 осуществляется в пределах регионального кластера, где данные хранятся; в кластеры в других регионах они не отправляются.

Изолированное хранение данных / Обособление клиентов

В AWS реализованы мощные возможности обособления клиентов. Благодаря виртуализированной мультиклиентской среде AWS обеспечивает изолирование клиентов друг от друга. Для ограничения несанкционированного доступа к хранилищам и вычислительным ресурсам Adobe использует систему AWS Identity and Access Management (IAM).

Безопасная сетевая архитектура

AWS применяет специальное сетевое оборудование, в том числе межсетевые экраны и другие устройства, для контроля коммуникаций на внешнем периметре сети, а также на важных внутренних периметрах. В устройствах контроля задаются наборы правил, таблицы доступа (ACL) и конфигурации, направляющие поток информации в системные службы. ACL или политики потоков трафика существуют для всех управляемых интерфейсов. Служба Amazon Information Security утверждает политики ACL и автоматически передает их на исполнение в управляемые интерфейсы, используя AWS ACL- Manage. Это гарантирует, что в системе применяются новейшие ACL.

Сетевой мониторинг и защита

Для обеспечения надежности AWS использует различные системы автоматизированного мониторинга. Они помогают выявлять несанкционированные действия и состояния во входных и выходных коммуникационных точках. Сеть AWS обеспечивает высокий уровень защиты от проблем сетевой безопасности:

- DDoS-атаки;
- MITM-атаки;
- IP-спуфинг;
- сканирование портов;
- внедрение анализаторов трафика.

Подробнее о сетевом мониторинге и защите можно прочитать в обзоре процессов безопасности AWS на сайте Amazon.

Выявление вторжений

Adobe активно мониторит состояние Adobe Creative Cloud с помощью систем выявления вторжений (IDS) и систем предотвращения вторжений (IPS).

Работа с журналами

В Adobe организовано ведение журналов активности пользователей на стороне сервера. Это помогает диагностировать ошибки и перебои в обслуживании. В журналы записываются только Adobe ID клиентов, а не их имена и пароли. Доступ к файлам журналов для анализа проблем разрешен только авторизованному персоналу поддержки Adobe и авторизованным разработчикам ПО.

Мониторинг обслуживания

AWS ведет мониторинг электрического и механического оборудования, чтобы быстро выявлять проблемы с обслуживанием. Для того чтобы оборудование всегда оставалось работоспособным, AWS проводит регулярное техническое обслуживание.

Хранение и резервное копирование данных

Adobe хранит все данные Adobe Creative Cloud на надежных ресурсах Amazon S3. Используя операции PUT и COPY, Amazon S3 синхронно помещает пользовательские данные на разные сервера и создает их резервные копии в своем регионе. Кроме того, при сохранении и извлечении данных Amazon S3 проверяет контрольные суммы в сетевом трафике. Подробнее об обеспечении безопасности можно прочитать в обзоре процессов безопасности в AWS.

Управление изменениями

AWS утверждает, документирует и контролирует плановые и экстренные изменения в существующей инфраструктуре, руководствуясь действующими нормами. Amazon планирует обновления AWS так, чтобы это проходило незаметно для пользователей. Если выясняется, что без перебоев в обслуживании не обойтись, AWS оповещает клиентов по электронной почте или через AWS Service Health Console. За статусом служб можно также следить через Status Health Console for Adobe Creative Cloud.

Управление патчами

На AWS возлагается применение патчей к системам, задействованным для служб AWS. Задача Adobe — выполнение патчей для своих гостевых ОС и программных приложений, работающих на платформе AWS. Строго говоря, Adobe предоставляет не сам патч, а результат его применения к ОС или приложению.

Управление физической инфраструктурой AWS

Процессы управления физической инфраструктурой AWS детализированы в отчете SOC 1, Type 2. Ниже мы кратко опишем процедуры безопасности, принятые во всех ЦОД AWS. Подробнее об обеспечении безопасности можно прочитать в обзоре процессов безопасности AWS или на сайте Безопасность облака AWS.

Безопасность физических объектов

ЦОД AWS построены с учетом стандартных для отрасли архитектурно-инженерных принципов. Физический доступ по периметру ЦОД и на входах в здания контролируется профессиональными охранными службами, а также с помощью электронных средств, таких как видеонаблюдение и охранная сигнализация. Чтобы попасть в ЦОД, авторизованные сотрудники должны не менее двух раз пройти двухфакторную идентификацию. Посетителям и сторонним специалистам необходимо предъявить удостоверение личности; они регистрируются в журнале, а на территории ЦОД их постоянно сопровождают сотрудники объекта.

AWS разрешает находиться в ЦОД и получать информацию только тем лицам, которым это требуется для решения профессиональных задач. Когда такая потребность исчезает, разрешение на доступ незамедлительно отзывается, даже если сотрудник продолжает работать в Amazon или Amazon Web Services. Физический доступ сотрудников AWS в ЦОД регистрируется и отслеживается.

Пожарная безопасность

Во всех ЦОД AWS установлены автоматические системы пожаротушения. Датчики дыма расположены в рабочих залах, а также в помещениях механической и электрической инфраструктуры, местах нахождения кондиционеров и генераторов. Применяются либо водяные, либо газовые спринклерные установки.

Управление климатом

Системы управления климатом поддерживают постоянную рабочую температуру в серверных и других помещениях AWS, предотвращая перегрев и ограничивая вероятность перебоев в обслуживании. Обеспечиваются оптимальные климатические условия. Персонал AWS и автоматические системы контролируют как температуру, так и влажность.

Резервное электропитание

Системы электропитания в ЦОД AWS спроектированы с резервированием, чтобы при техническом обслуживании работа ни на секунду не прерывалась. Критически важные нагрузки подключены к источникам бесперебойного питания (ИБП). Кроме того, в ЦОД установлены генераторы, обеспечивающие резервное электропитание для всего объекта.

Видеонаблюдение

Профессиональные охранные агентства тщательно контролируют физический доступ по периметру ЦОД и на входах в здания, используя такие электронные средства, как видеонаблюдение и охранная сигнализация.

Восстановление после аварий

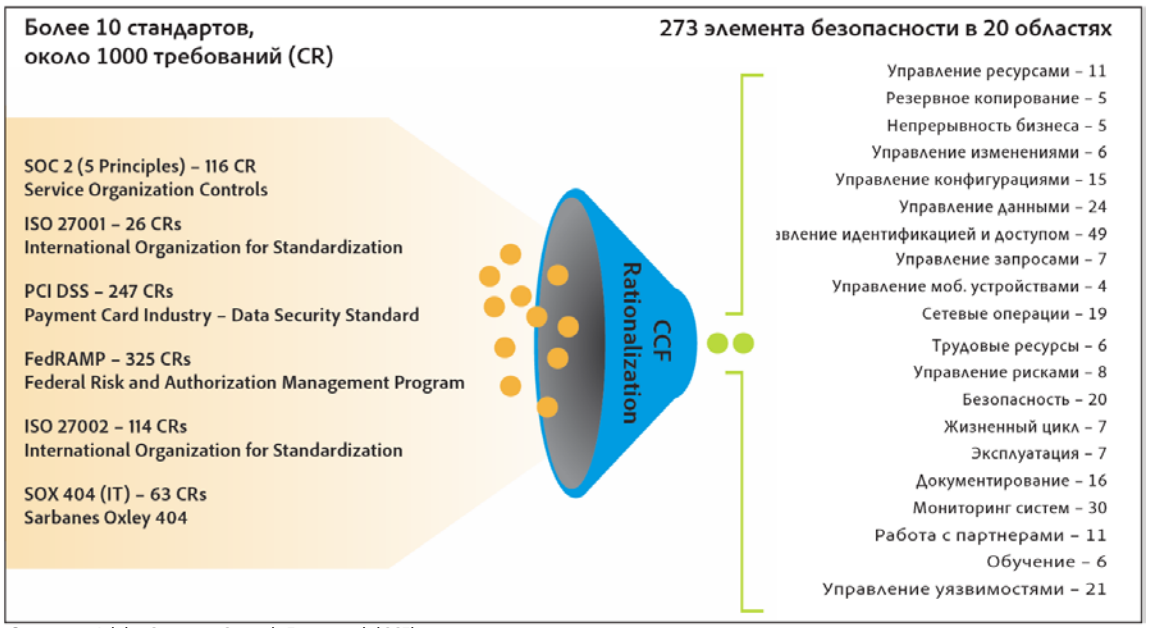
ЦОД AWS обладают высокой степенью устойчивости к системным сбоям и поломкам оборудования. ЦОД объединены в региональные кластеры и обслуживают клиентов непрерывно. В случае аварий автоматизированные процедуры перенаправляют трафик данных.

Базовые системы резервируются по схеме N+1, и при выходе одного ЦОД из строя потоки информации балансируются на других исправных ЦОД. Более подробная информация о протоколах восстановления AWS после аварий приведена на сайте Безопасность облака AWS.

Adobe Common Controls Framework

Для защиты на программном уровне и ниже Adobe использует комплекс Secure Product Lifecycle. Для защиты на физическом уровне и выше Adobe внедрила фундаментальную среду процессов и элементов управления, которая обеспечивает безопасность инфраструктуры, приложений и служб на высочайшем уровне.

При создании среды Adobe Common Controls Framework (CCF) специалисты Adobe проанализировали критерии различных сертификаций по безопасности и обнаружили, что в ряде областей они перекрываются. Анализ более 1000 требований к стандартам безопасности позволил рационализировать структуру и выделить около 200 специфичных для Adobe элементов. На схеме приведена структура действующей CCF.

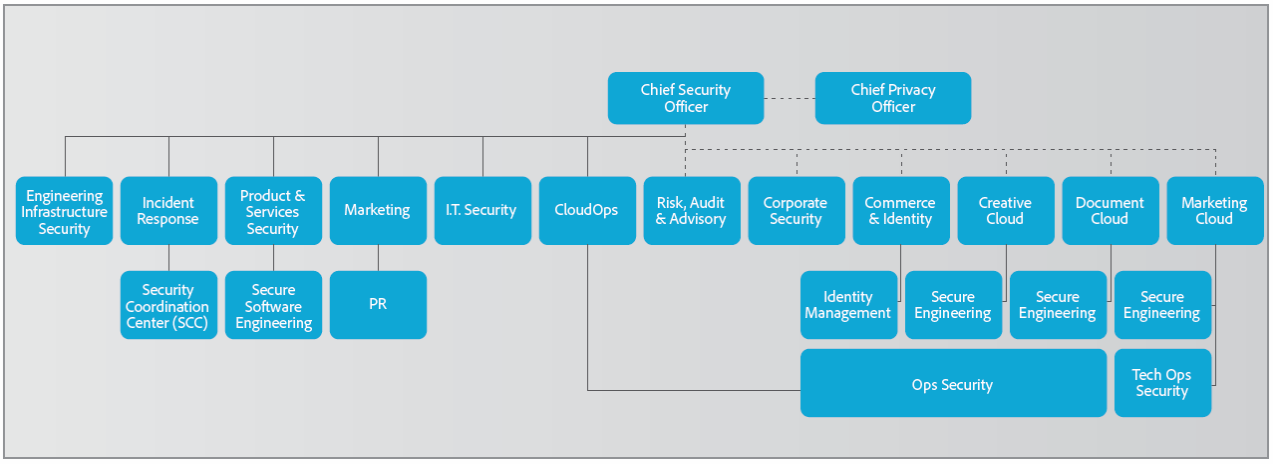


Структура Adobe Common Controls Framework (CCF)

Структура безопасности в Adobe

Вся деятельность по обеспечению безопасности продуктов и услуг координируется директором Adobe по безопасности (CSO). Его круг задач — согласование инициатив и практическая реализация комплекса мер Adobe Secure Product Lifecycle (SPLC).

CSO также руководит группой Adobe Secure Software Engineering Team (ASSET), составленной из экспертов по безопасности, которые консультируют специалистов по разработке ПО, в том числе участников группы разработчиков Creative Cloud. Представители ASSET помогают обеспечить должный уровень безопасности в продуктах и службах — в первую очередь для процессов разработки, развертывания, эксплуатации и реагирования на инциденты.



Безопасность при разработке продуктов Adobe

Как и для других продуктов и служб Adobe, при разработке Creative Cloud задействован процесс SPLC. Это строгий комплекс мер безопасности (всего их несколько сотен), охватывающих практику, процессы и инструменты разработки ПО. Adobe SPLC интегрирован во множество стадий жизненного цикла продуктов: от выработки архитектуры и инженерной разработки до контроля качества, тестирования и развертывания. Специалисты ASSET дают рекомендации по каждому ключевому продукту и каждой службе, основанные на оценке потенциальных нарушений безопасности. Adobe SPLC постоянно дорабатывается с учетом новых технологий, методик безопасности и масштабов угроз, а также мнений сообщества.

Adobe Secure Product Lifecycle

Комплекс мер Adobe SPLC охватывает некоторые или все (в зависимости от конкретной службы) рекомендованные методики, процессы и инструменты:

- Обучение разработчиков продуктов методам безопасности; сертификация
- Анализ устойчивости продуктов, рисков и ситуации с угрозами
- Рекомендации и правила написания безопасного кода
- Планы разработки служб, инструменты безопасности и методы тестирования, помогающие разработчикам Creative Cloud бороться с 10 главными проблемами безопасности веб-приложений по классификации OWASP и избегать 25 самых опасных программных ошибок по классификации CWE/SANS
- Проверка архитектуры безопасности и тестирование на проникновение
- Анализ исходного кода на потенциальную уязвимость
- Проверка пользовательского контента
- Анализ статического и динамического кода
- Сканирование приложений и сетей
- Контроль готовности, планы реагирования, выпуск учебных материалов для разработчиков

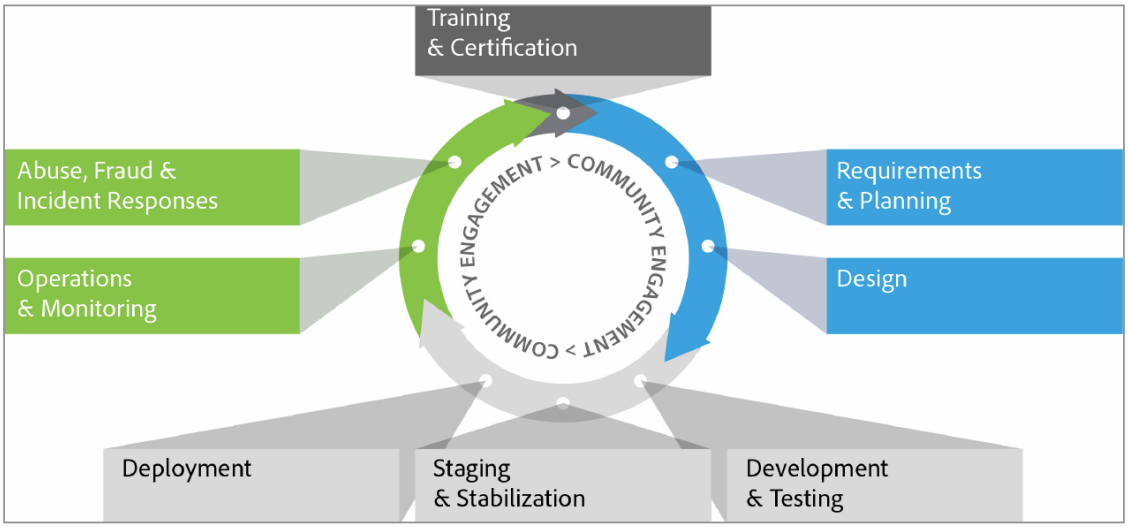


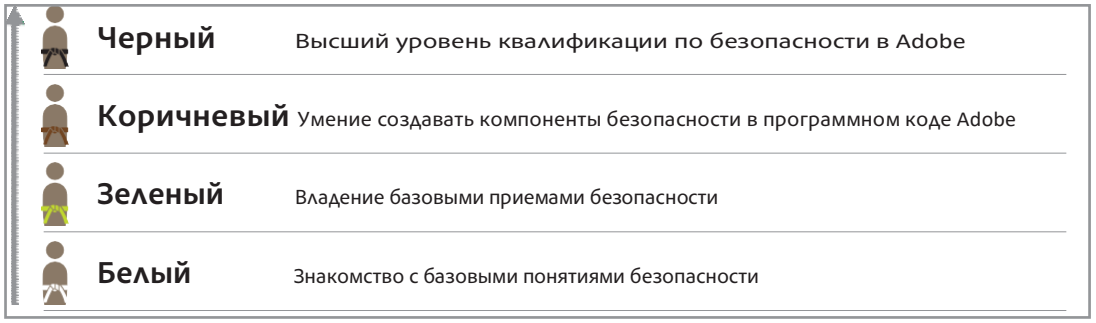
Схема Adobe Secure Product Lifecycle (SPLC)

Обучение по безопасности в Adobe

Программа Adobe Software Security Certification

В рамках процесса SPLC Adobe проводит непрерывное обучение разработчиков методам безопасности, чтобы повысить квалификацию специалистов в этой области и сделать более защищенными наши продукты и сервисы. Сотрудники, участвующие в программе Adobe Software Security Certification, выполняют проекты, посвященные вопросам безопасности, и получают сертификаты.

Программа разделена на 4 уровня, которым соответствуют цветные «пояса»: белый, зеленый, коричневый и черный. Получить белый и зеленый пояса можно, пройдя электронные курсы. Для того чтобы претендовать на коричневый и черный пояса, необходимо выполнить практические проекты в области безопасности. Такие сотрудники получают звание экспертов. Adobe регулярно обновляет учебную программу, отражая новые угрозы и методы борьбы с ними, а также новые элементы управления и языки программирования.



Уровни сертификации Adobe Secure Software Engineering

Для разработчиков Creative Cloud организуются дополнительные курсы, цель которых — дать им больше знаний о значении безопасности для конкретных ролей и компании в целом.

Безопасное управление

Для подключения к инфраструктуре AWS и управления ею Adobe использует защищенные протоколы Secure Shell (SSH) и Secure Sockets Layer (SSL).

Управление рисками и уязвимостями в Adobe

Тестирование на проникновение

В сотрудничестве с ведущими компаниями Adobe проводит тестирование на проникновение в систему, чтобы выявить потенциальные уязвимости и сделать свои продукты и сервисы более защищенными. Получив информацию, Adobe документирует уязвимости, оценивает критичность и приоритетность, а затем формирует стратегию противодействия и план устранения последствий.

В рамках внутренних процессов группа, отвечающая за безопасность Adobe Creative Cloud, проводит оценку рисков для Creative Cloud перед выпуском каждой новой версии. Эту задачу выполняют высококвалифицированные специалисты. При проверке происходит поиск потенциально опасных сетевых настроек в межсетевых экранах, распределителях нагрузки, серверном оборудовании. Проверяются также уязвимости на уровне приложений. В контактных точках имитируются угрозы и сканирование на уязвимость, статический и динамический анализ приложения. Группа безопасности Creative Cloud перед выпуском каждой новой версии совместно с разработчиками убеждается, что все уязвимости нейтрализованы.

Тесты на проникновение выполняются по меньшей мере ежегодно — или после выпуска новой основной версии. Сканирование на уязвимость производится ежемесячно, а сканирование веб-контента и баз данных — ежеквартально.

Реагирование на инциденты

Новые угрозы возникают ежедневно, и Adobe делает все возможное, чтобы нейтрализовать их. Мы подписаны на рассылки по вопросам уязвимостей US-CERT, Bugtraq и SANS, а также на новости от ведущих экспертов по безопасности.

Если уязвимость представляет риск для Creative Cloud, группа реагирования Adobe PSIRT передает информацию разработчикам Creative Cloud и координирует меры по противодействию.

Для облачных сервисов, таких как Creative Cloud, Adobe аккумулирует информацию о реагировании на инциденты, принятых решениях и внешнем мониторинге в Координационном Центре SCC, благодаря чему обеспечиваются межфункциональная согласованность и ускоренное разрешение проблем.

Если с продуктами или сервисами Adobe возникают инциденты, SCC вступает в контакт с группами разработчиков и совместно с ними выявляет источники проблем и находит пути борьбы с ними, используя следующий типовой процесс:

- оценка статуса уязвимости;
- минимизация риска для производства;
- перевод в карантин, анализ и удаление подвергшихся атаке узлов (только для облачных служб);
- выработка противодействия уязвимости;
- развертывание противодействия;
- мониторинг активности и подверждение решения проблемы.

Экспертный анализ

Для экспертного анализа инцидентов группа Creative Cloud использует дампы памяти подвергшихся атакам компьютеров, резервные безопасные данные и документацию о размещении ПО на серверах.

Офисы Adobe

Офисы Adobe расположены во множестве стран мира. Ниже описывается общекорпоративная политика компании по предотвращению угроз безопасности.

Физическая безопасность

Все офисы Adobe круглосуточно охраняются. Для входа в здания сотрудники Adobe используют электронные карты. Посетители офисов проходят через главный вход, регистрируются в журнале и получают гостевую карту. В офисах их постоянно сопровождают сотрудники Adobe. Все серверное оборудование Adobe, применяемые для сборки компьютеры, АТС, файловые серверы, почтовые серверы и другие критически важные системы находятся в помещениях с ограниченным доступом и надлежащим кондиционированием.

Защита от вирусов

Adobe проверяет всю входящую и исходящую почту на наличие вредоносного кода.

Антивирусные механизмы внедрены во все корпоративные системы и оборудование сотрудников (ноутбуки и др.). Для защиты от вредоносного ПО применяется следующий сценарий:

- ежедневное обновление сигнатур для сканирования;
- обновление механизма сканирования для синхронизации с новыми версиями ПО;
- еженедельное полное сканирование системы;
- составление журнала событий и оповещений;
- передача информации о выявленных проблемах соответствующим сторонам;
- включение сканирования в реальном времени;
- невозможность отключения антивирусных механизмов.

Сотрудники Adobe

Доступ сотрудников к пользовательским данным

В Adobe организована сегментированная среда разработки и сборки Creative Cloud. Доступ к системам сборки извне ограничивается с помощью технических средств. На работу с ними сотрудникам требуется отдельная авторизация. Права доступа персонала ежеквартально пересматриваются.

Проверка анкетных данных

Adobe проверяет анкетные данные поступающих на работу сотрудников. Особое внимание компания обращает на образование, трудовой стаж, случаи привлечения к ответственности (в том числе к уголовной), а также на частные и корпоративные рекомендации, насколько это допускается законом. Проверка проводится в отношении всех новых сотрудников, в первую очередь тех, кому будет поручено администрирование систем и предоставлен доступ к пользовательским данным. Сотрудники, принимаемые в сотрудничающие с Adobe агентства, проходят анкетный контроль в этих агентствах на основании инструкций Adobe. Проверка анкетных данных за пределами США осуществляется в строгом соответствии с законодательством соответствующих государств.

Увольнение сотрудников

Когда сотрудник покидает Adobe, отдел кадров оповещает по электронной почте все заинтересованные стороны о том, что по истечении последнего дня его работы необходимы соответствующие действия. Для того чтобы сотрудник далее не имел доступа к файлам и не мог входить в офисы Adobe, служба Adobe Corporate Security предпринимает следующие меры:

- отключение корпоративной электронной почты;
- отключение удаленного доступа по VPN;
- деактивация электронных карт доступа в офисы и ЦОД;
- закрытие доступа к корпоративной сети.

Если увольнение сотрудника происходит по инициативе Adobe, для его сопровождения к выходу может быть привлечена служба безопасности.

Конфиденциальность данных клиентов

Adobe всегда считает данные клиентов конфиденциальными. Adobe никогда не использует в собственных целях и не разглашает полученные от клиентов данные, кроме случаев, установленных в Общих условиях пользования услугами Adobe и в Политике конфиденциальности Adobe. С подробностями можно ознакомиться в Центре обработки конфиденциальной информации Adobe.

Соответствие нормам безопасности

Соблюдение норм безопасности в AWS основано на положениях ISO 27001, SOC 1, SOC 2, PCI DSS и других стандартов.

Во всех подразделениях Adobe применяются документированные процессы безопасности; они регулярно подвергаются проверкам в этом отношении. Adobe постоянно проверяет свои подразделения согласно стандарту ISO 27001 и сертифицирует инфраструктуру служб по SOC 2 - Security.

Разработка, реализация и совершенствование процессов и элементов безопасности в Adobe Creative Cloud полностью согласуются с принципами SOC 2 Trust Services и стандартом ISO 27001. Adobe Creative Cloud для организаций имеет статус «FERPA-ready», что означает возможность действовать в качестве официального лица при обработке данных учащихся образовательных учреждений.

На странице http://www.adobe.com/security/resources.html опубликованы статьи по вопросам безопасности — в частности, обзор безопасности облачных служб Adobe. Из них вы можете узнать больше о стратегии безопасности Adobe и стремлении компании к соблюдению всех нормативных требований.

Заключение

Мы серьезно подходим к защите ваших цифровых данных. Наш упреждающий подход к безопасности, описанный в этой статье, помогает защитить ваши данные в Creative Cloud. Если у вас еще остались вопросы о безопасности, свяжитесь с нашим представителем или посетите страницу http://www.adobe.com/security.

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

Adobe, логотип Adobe, Behance, Creative Cloud, логотип Creative Cloud, Illustrator, Photoshop, Lightroom и Typekit являются либо зарегистрированными товарными знаками, либо товарными знаками компании Adobe Systems Incorporated в США и/или других странах. Все остальные товарные знаки принадлежат соответствующим владельцам.

© 2018 Adobe Systems Incorporated. Все права защищены. Переведено по заказу МОНТ, авторизованного дистрибьютора Adobe в России.

2018