AppsFlyer

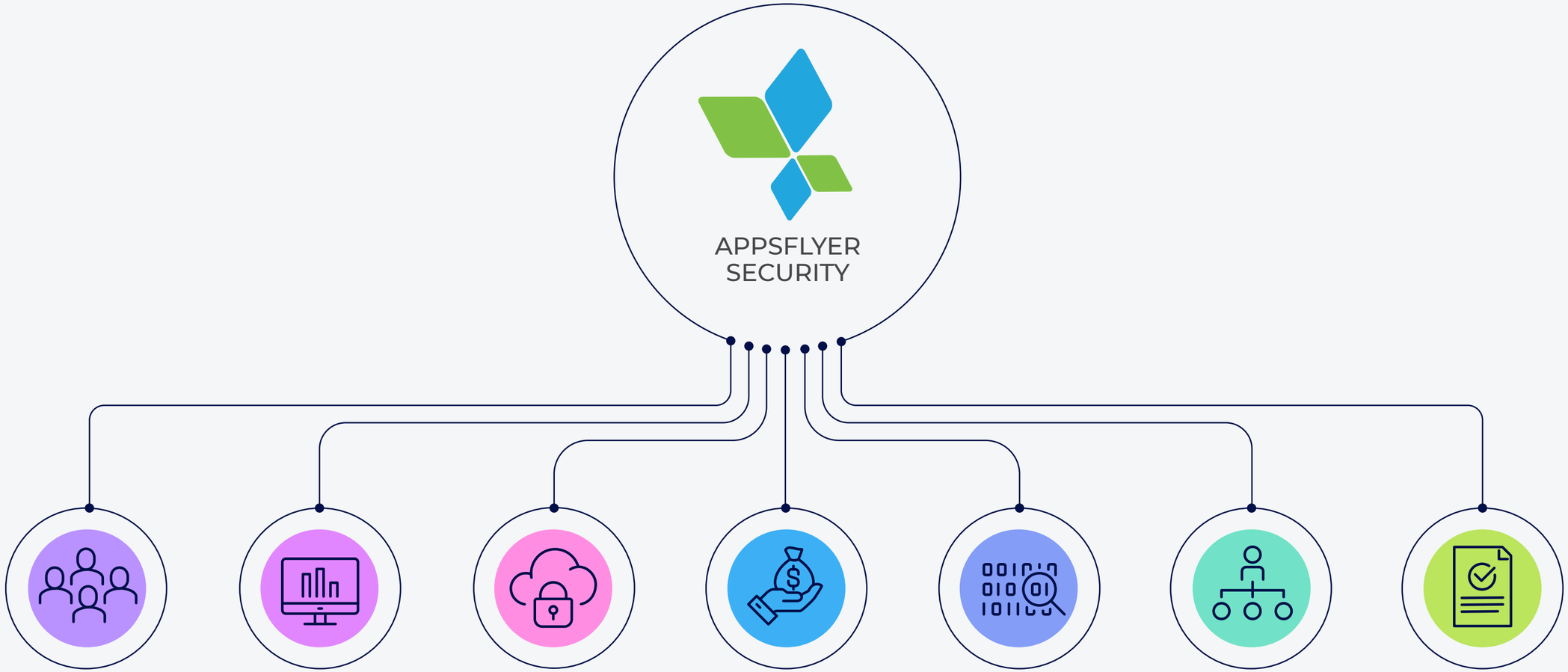
Политика и методы обеспечения безопасности

ВВЕДЕНИЕ

Безопасность данных, масштабируемость и эффективность — в основе всех продуктов AppsFlyer.
Наша ультрасовременная инфраструктура, передовые технологии безопасности и защиты данных, независимая сертификация и соответствие глобальным правовым нормам заслужили доверие ведущих мировых брендов.
Мы стремимся внедрить процессы и методы обеспечения безопасности самого высокого уровня во всех бизнес-подразделениях. В нашем штате есть директор по информационной безопасности (CISO) и специальный отдел по безопасности, который постоянно увеличивается.

Наши методы обеспечения безопасности основаны на ведущих отраслевых стандартах, таких как SSAE 16 SOC2, по которым мы ежегодно проходим аудит. Наша инфраструктура безопасности и конфиденциальности включает политики и процедуры управления ресурсами и доступом, обеспечения безопасности оборудования, сред, пользователей, продуктов, облачных и сетевых инфраструктур, сторонних лиц, управления уязвимостями, мониторинга безопасности и реагирования на инциденты.

Политики и стандарты информационной безопасности утверждаются руководством AppsFlyer и доступны для всех сотрудников AppsFlyer.


APPSFLYER
SECURITY
Сотрудники
СТРАНИЦА 4
Продукт
СТРАНИЦА 6
Облако
СТРАНИЦА 10
Непрерывность бизнеса
СТРАНИЦА 11
Данные
СТРАНИЦА 12
Третьи лица
СТРАНИЦА 14
Сертификация
СТРАНИЦА 15

Люди

Команды, стоящие за продуктами AppsFlyer, играют ключевую роль в защите наших сервисов на организационном уровне.

Команда по обеспечению безопасности

Команда бизнес-операций AppsFlyer — первоклассные эксперты в сфере безопасности и конфиденциальности, которые работают с информацией, приложениями и сетевой безопасностью. В задачи команды входит:

- Поддержка системы защиты компании
- Разработка процессов проверки безопасности
- Обеспечение безопасности инфраструктуры
- Применение политики безопасности AppsFlyer

Специальный отдел безопасности AppsFlyer внимательно следит за безопасностью с помощью коммерческих и индивидуально настраиваемых инструментов, тестирования на проникновение, мер по обеспечению качества (QA) и проверки безопасности программного обеспечения.

Сотрудники отдела информационной безопасности AppsFlyer регулярно проверяют планы обеспечения безопасности для всех сетей, систем и сервисов. Они консультируют продуктовые и инженерные команды AppsFlyer. Они отслеживают подозрительную активность в сетях AppsFlyer, устраняют угрозы информационной безопасности, выполняют дежурную оценку безопасности и аудиты, а также привлекают внешних экспертов для проведения регулярных проверок безопасности.

Люди

HR

Процесс отбора кандидатов в AppsFlyer основан на проверке благонадежности и личных интервью с менеджерами по подбору персонала и менеджерами по найму. При необходимости осуществляется дополнительная проверка в соответствии с местным законодательством.

Тренинги по информационной безопасности

Новые сотрудники проходят процесс адаптации, который включает правила безопасности, ожидания и кодекс поведения. Все сотрудники AppsFlyer ежегодно проходят тренинг на знание и понимание мер безопасности.

Постоянная коммуникация

Команда безопасности AppsFlyer находится в постоянном контакте со всеми сотрудниками и освещает такие темы, как новые угрозы, фишинг и другие вопросы, связанные с безопасностью.

Продукт

Безопасность приложения

Принятые в компании AppsFlyer стандарты безопасности жизненного цикла разработки (SDLC) обеспечивают высокий уровень защищенности платформы. Вот, что мы делаем для достижения этой цели:

Контроль за изменениями

AppsFlyer следует строгой процедуре контроля за изменениями. Мы отслеживаем, анализируем и утверждаем изменения рабочих процедур, чтобы они соответствовали бизнес-целям AppsFlyer и нормативным требованиям.

Предотвращение атак

AppsFlyer использует защиту от DDos-атак и различные инструменты для защиты WAF и API.

SDLC

Все продукты и функции проходят тщательную проверку безопасности и сканирование кода.

Тесты на проникновение

AppsFlyer проводит различные тесты на проникновение, привлекая внешних подрядчиков, а также проверки с использованием автоматических сканеров.

Программа Bug Bounty

Компания AppsFlyer предлагает вознаграждение за обнаружение уязвимости в безопасности приложения.

Продукт

БЕЗОПАСНОСТЬ АККАУНТА

AppsFlyer предоставляет самые надежные меры безопасности аутентификации в индустрии мобильной атрибуции. В средствах аутентификации многие настройки полностью кастомизируются в соответствии с нуждами каждой организации.

Надежные пароли
Все пользователи должны создать пароли максимальной сложности: минимум 8 знаков, заглавные и строчные буквы, цифры и специальные символы.

SHA-2 + хеширование паролей с помощью соли
AppsFlyer не хранит пароли пользователей в текстовом виде на своих серверах. Для этих целей компания применяет стандарт хеширования SHA-2.

Неудачные попытки входа
Хотя рекомендуется блокировать пользователей после 10 неудачных попыток входа в систему, AppsFlyer производит блокировку после 5. Клиенты могут сами определить продолжительность блокировки.

Временные пароли
AppsFlyer требует от новых пользователей создать пароль вместо временного сразу же после регистрации.

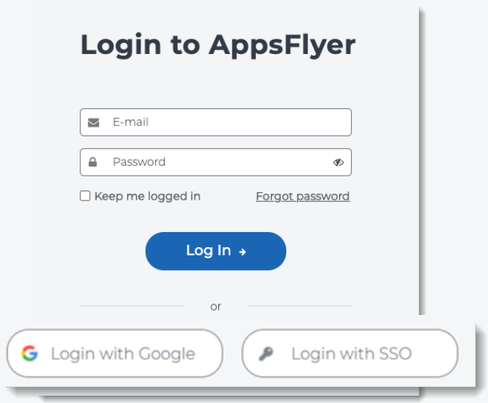
Продукт

БЕЗОПАСНОСТЬ АККАУНТА

Самообслуживание

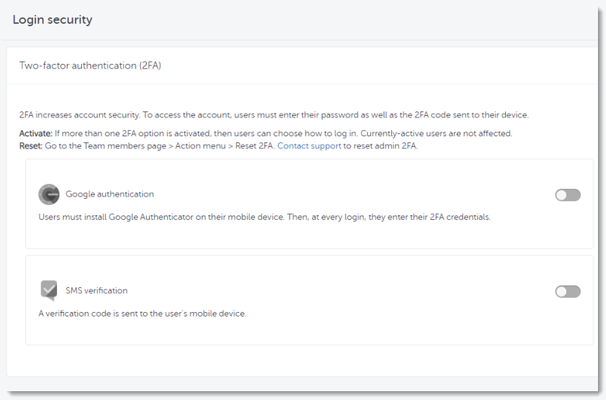
Двухфакторная аутентификация

Клиенты могут сделать обязательной двухфакторную аутентификацию при входе пользователя в аккаунт с нового устройства или после продолжительного бездействия.



Технология единого входа

Клиенты, чья организация использует решение IDP, могут подключить его к дэшборду AppsFlyer. AppsFlyer работает с протоколом единого входа SAML 2.0.

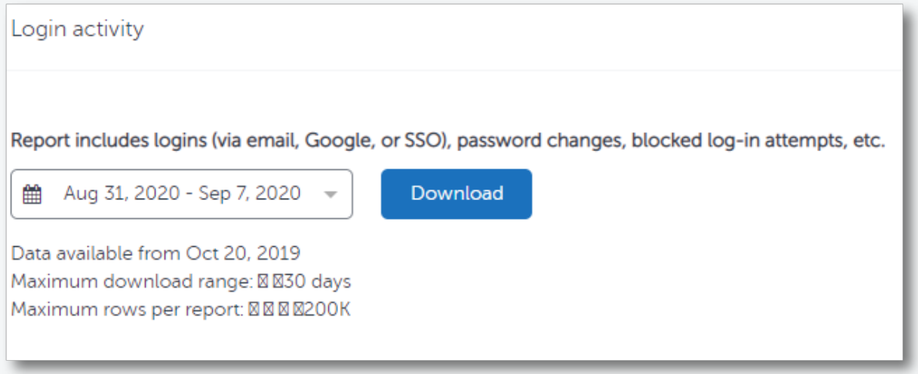


Продукт

МОНИТОРИНГ И ПРОЗРАЧНОСТЬ

Наша команда по обеспечению безопасности непрерывно контролирует и оценивает соответствие, нормы и риски. Тесты на уязвимость позволяют нам отслеживать уязвимости, сортировать их по приоритету и своевременно реагировать на них. Чтобы обеспечить безопасность платформы, компания AppsFlyer постоянно совершенствует и расширяет свои возможности в области обеспечения безопасности: непрерывный круглосуточный мониторинг и применение целого ряда инструментов и компонентов для выявления и предотвращения любых угроз, инцидентов и уязвимостей.

Мы хотим, чтобы клиенты имели полное представление о том, что происходит в их учетной записи, и даем им возможность отслеживать активность собственного аккаунта. Для этого мы предоставляем полный журнал действий аккаунта, включая неудачные попытки входа, внесенные изменения и экспорт данных.



Регистрация событий
У клиентов компании есть вся информация об активности аккаунта: неудачные и успешные попытки входа, вносимые изменения и экспорт данных.

Круглосуточный мониторинг
Команда AppsFlyer по обеспечению безопасности осуществляет круглосуточный мониторинг инфраструктуры и приложения. Любое оповещение об угрозе запускает процесс минимизации риска.

Облачная инфраструктура

Безопасность нашей инфраструктуры и сетей имеет решающее значение. Главная цель нашей облачной безопасности – защита платформы для приложения AppsFlyer и инноваций наших клиентов.

НОРМАТИВНОЕ СООТВЕТСТВИЕ ИНФРАСТРУКТУРЫ

Мы используем многоуровневые элементы управления, чтобы защитить нашу инфраструктуру, постоянно отслеживая и улучшая наши приложения, системы и процессы, чтобы соответствовать растущим требованиям и задачам безопасности. Кроме того, мы используем AWS и GCP – строго регламентированные и соответствующие требованиям центры обработки данных, отвечающие региональным и международным требованиям сертификации.

ЗАЩИТА ОТ DDoS-АТАК

В рамках подхода многоуровневой защиты была создана специальная экосистема защиты от DDoS-атак. AppsFlyer использует защиту от DDos-атак и различные инструменты для защиты WAF и API.

УПРАВЛЕНИЕ РЕСУРСАМИ И ОТВЕТСТВЕННОСТЬ

Каждому ресурсу назначается владелец, который за него отвечает. Доступ к производственной инфраструктуре ограничен минимальным числом лиц и основан не на привилегиях, а на непосредственной необходимости работы с данным ресурсом.

ПОЛНОЕ РЕЗЕРВИРОВАНИЕ

Специалисты AppsFlyer применяют ряд инструментов мониторинга среды ЦОД на уровне серверов и приложений. Параметры собираются и агрегируются в центральном хранилище, где с помощью резервных копий анализируются с целью выявления аномалий, трендов, пороговых значений и т.д.

Непрерывность бизнеса

Хотя мы не можем предсказать будущее, мы можем быть уверены, что полностью к нему готовы. Это подразумевает контроль над возможными перебоями в обслуживании и минимизацию времени восстановления.

ПЛАН НЕПРЕРЫВНОСТИ БИЗНЕСА (BCP)

BCP AppsFlyer гарантирует, что у клиентов всегда будет доступ к экстренной службе во время любых аварии и перебоев в работе, от временных отключений электричества до катастроф глобального масштаба.

АВАРИЙНОЕ ВОССТАНОВЛЕНИЕ

Сервисы AppsFlyer размещаются на AWS и GCP, что позволяет нам непрерывно работать во всем мире, даже в случае сбоя в одной локации. AWS и GCP охватывают несколько географических зон и предоставляют множество резервных копий, что гарантирует отказоустойчивость серверов AppsFlyer в аварийных ситуациях.

РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ

AppsFlyer регулярно выполняет резервное копирование данных клиентов, используя облачное хранилище Amazon S3. Все резервные копии надежно шифруются при передаче и хранении.

ДАННЫЕ

ПЕРЕДАЧА ДАННЫХ

Когда данные передаются через интернет или внутри сетей, они подвергаются угрозе несанкционированного доступа. Поэтому для AppsFlyer обеспечение защиты передаваемых данных является приоритетной задачей. Наши веб-серверы поддерживают эффективные протоколы шифрования, служащие для защиты подключений, на одной стороне которых находятся клиентские устройства, а на другой — веб-серверы и API-интерфейсы AppsFlyer. Любой трафик, поступающий в AppsFlyer, шифруется по протоколу https с помощью TLS1.2.

ХРАНЕНИЕ ДАННЫХ

По умолчанию для хранения информации мы используем шифрование данных AES256.

ДАННЫЕ

МАСКИРОВКА

Наши клиенты могут по желанию применить еще более серьезные методы обеспечения безопасности, например, дополнительные уровни защиты аккаунта. Чтобы убедиться в соблюдении всех требований к безопасности, в частности, таких как маскировка IP-адресов, клиенты всегда могут обратиться к своим менеджерам в AppsFlyer.

ИЗОЛЯЦИЯ АККАУНТА И ДОСТУП

Чтобы обеспечить конфиденциальность и безопасность данных, AppsFlyer логически изолирует данные учетной записи каждого клиента от других клиентов и пользователей, даже если они хранятся на одном физическом сервере.
Права и уровни доступа сотрудников AppsFlyer основаны на должностных функциях и ролях по принципу предоставления минимальных прав. По умолчанию доступ сотрудников к ресурсам компании ограничен. Дополнительные разрешения могут быть утверждены менеджером в соответствии с политиками безопасности AppsFlyer. Настройки авторизации сотрудника используются для управления доступом ко всем ресурсам, включая данные и системы.

ТРЕТЬИ ЛИЦА

Каждая компания полагается на другие организации, будь то провайдер сервиса электронной почты, серверная ферма или кафе, из которого по пятницам доставляют обеды. Проверкой подрядчиков нужно заниматься так же, как любым другим элементом корпоративной безопасности. Инвестировать во внутреннюю безопасность, но игнорировать возможные риски извне — это как повесить замок на входную дверь и настежь открыть окно. Уязвимость есть уязвимость, и третьи лица могут стать источником угрозы безопасности.

AppsFlyer в свою очередь также является сторонней организацией для некоторых глобальных компаний. Кроме того, в продукты AppsFlyer интегрированы сторонние решения, и помимо этого, мы нанимаем подрядчиков для оказания внутренних услуг в разных департаментах. Поэтому мы относимся к уровню безопасности третьих лиц так же серьезно, как к мерам внутренней безопасности:

ПРОЦЕДУРА ПРОВЕРКИ

Сторонние поставщики AppsFlyer проходят предварительную проверку на соответствие стандартам безопасности AppsFlyer. Третьи лица и субподрядчики не имеют доступ к данным клиентов.

НЕПРЕРЫВНЫЙ МОНИТОРИНГ

Команда по обеспечению безопасности AppsFlyer каждый год проверяет контрагентов. Такие оценки могут проводиться либо по процедуре команды AppsFlyer, либо посредством проверки на соответствие сторонним нормам и стандартам (например, SSAE 16 SOC2, ISO27001). Процедура учитывает такие параметры как тип доступа к данным, уровень секретности данных, к которым предоставлен доступ (если предоставлен), а также меры защиты данных, законодательные и нормативные требования.

Сертификация

AppsFlyer стремится снизить риски и обеспечить соответствие сервисов AppsFlyer нормам безопасности. Компания соответствует требованиям законодательства, отраслевым нормам, а также применяет передовые технологии индустрии и накопленный опыт.

В отличие от других разработчиков инструментов атрибуции, регулярно сталкивающимися с атаками, утечками данных и нарушениями требований, компания AppsFlyer разработала и продолжает совершенствовать беспрецедентную международную программу обеспечения соответствия требованиям и сертификации, которой неукоснительно следует. Программа соответствия AppsFlyer не имеет себе равных в отрасли.

Compliance	AppsFlyer	Branch	Adjust	Kochava	Singular
SSAE16 SOC2	✓	✗	✗	✗	✗
TRUSTe	✓	✗	✗	✗	✗
ePrivacy	✓	✗	✓	✗	✓
ISO27001	✓	✗	✓	✗	✗
ISO27017	✓	✗	✗	✗	✗
ISO27018	✓	✗	✗	✗	✗
ISO27032	✓	✗	✗	✗	✗
ISO27701	✓	✗	✗	✗	✗
CSA STAR	✓	✓	✗	✗	✓

SSAE16 SOC2

AppsFlyer прошел сертификацию SOC2, что является подтверждением контроля безопасности и дает клиентам уверенность в нашей программе безопасности. Критерии доверия, на которых основан SOC2, смоделированы вокруг четырех широких областей: регламентирования, коммуникации, процедур и мониторинга. Каждый из критериев имеет соответствующие точки фокусировки, которые должны быть выполнены для демонстрации соответствия общим критериям.

TRUSTe

AppsFlyer соответствует всем требованиям конфиденциальности, установленными TRUSTe и/или применяемыми регулирующими органами. Наш регулярно продлеваемый сертификат TRUSTe демонстрирует прозрачность AppsFlyer. TRUSTe проверяет наш веб-сайт и его поддомены, пакет для разработки программного обеспечения ("SDK") и API.

ISO 27001, 27017, 27018, 27032, 27701

Семейство стандартов ISO/IEC 27000 помогает организациям обеспечивать и управлять безопасностью информационных ресурсов. AppsFlyer соответствует ISO 27001, 27017, 27018 и 27032, которые подтверждают, что AppsFlyer продемонстрировал (и даже превысил) необходимые меры для управления безопасностью организации, информационной безопасности, безопасности в облаке PII и конфиденциальности.

CSA STAR

Обязательство AppsFlyer обеспечивать безопасность данных распространяется и на облачные сервисы, используемые компанией. CSA STAR Certification — это строгая независимая оценка безопасности поставщика облачных услуг. Сертификация STAR основана на соответствии стандарту ISO/IEC 27001 и набору критериев, изложенных в матрице управления облаком.

ePrivacyseal

ePrivacy GmbH присуждает знак качества защиты данных после тщательного аудита онлайн- и мобильных продуктов компании. Сертификация охватывает требования GDPR для цифровых продуктов. После тщательной оценки AppsFlyer был награжден ePrivacyseal за соответствие всем критериям, установленным ePrivacyseal.

РЕЗЮМЕ

Как ведущий поставщик с большим опытом работы в отрасли мы понимаем, что работа в многопользовательской облачной среде может вызывать опасения, связанные с конфиденциальностью и защитой конфиденциальных данных. Механизмы AppsFlyer для защиты физических и сетевых компонентов и приложений платформы, а также прозрачность наших политик и процессов безопасности позволяют брендам доверять нам свои самые конфиденциальные данные. Это доверие помогает нашим клиентам пользоваться бизнес-преимуществами нашего многопользовательского решения SaaS.

Если у вас есть вопросы или вам нужны более подробные объяснения по темам, затронутым в этом техническом документе, не стесняйтесь обращаться к нашей команде безопасности через службу поддержки или к вашему менеджеру по работе с клиентами.

Подробную информацию см. на сайте www.appsflyer.com/ru