Защита от мошенничества для вас – быстрый и удобный сервис для ваших клиентов.

Kaspersky Fraud Prevention

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Подробнее о продукте на kfp.kaspersky.com

Предотвращение кросс-канальных атак в режиме реального времени

Обслуживание в офисе компании или отделении банка становится всё менее популярным. Для клиентов гораздо удобнее совершать операции, используя личный кабинет на сайте или в мобильном приложении, и бизнес стремится предоставить им эту возможность. С одной стороны – перенос сервиса в онлайн создает новые возможности, приводит новых клиентов и, конечно, увеличивает доход. С другой — он открывает двери для мошенников с их хитроумными схемами и кросс-канальными атаками как на устройство, так и на личный кабинет пользователя.

Kaspersky Fraud Prevention, работая в режиме реального времени, обрабатывает трафик по следующим параметрам:

Название метрики	Количество уникальных единиц в сутки
Устройство	~ 50 млн
Пользователь	~ 29 млн
Онлайн-сессия	~ 332 млн
Обработанное событие	~ 6 млрд

Анализ событий сессии с помощью технологий Kaspersky Fraud Prevention

Анализ устройства и окружения

Использует глобальное присутствие Лаборатории Касперского, чтобы идентифицировать «хорошие» устройства и использовать эти данные для аутентификации пользователя. На основании глобальной репутации устройств, IP-адресов, геолокационных показателей и других данных любой атрибут, некогда вовлечённый в мошеннические действия, проактивно обнаруживается и отображается как подозрительный или относящийся к фроду.

Поведенческий анализ

Исследует, что пользователь нажимает, как он ведет себя во время входа в личный кабинет и всей сессии. Также рассматриваются типичные элементы навигации, временные показатели и другие аспекты. Это позволяет сформировать профиль нормального, легитимного поведения и на ранней стадии выявлять любую аномальную или подозрительную активность даже на стадии логина.

Поведенческая биометрия

Анализирует различные виды взаимодействия пользователя с устройством, такие как движения мыши, нажатия, скроллы, прикосновения, движения по экрану устройства и т. д., чтобы определить, используется ли это устройство легитимным пользователем или злоумышленником, человеком или машиной. Эта технология позволяет выявлять ботов, средства удаленного администрирования, а также случаи кражи учётной записи.

Обнаружение вредоносных программ

Позволяет без установки дополнительных компонентов определить, заражена ли машина пользователя вредоносным ПО. Данные о возможном заражении используются для **Аутентификации на основе риска** (RBA), а также для определения легитимности транзакций.

Данные, обрабатываемые ключевыми технологиями, применяются в решениях линейки Kaspersky Fraud Prevention.

Результаты анализа событий сессии поступают во внутренние системы мониторинга, предоставляя детали для обнаружения автоматизированных средств, ботов, изменений показателей поведения, различных видов вредоносного ПО и других атак.

Готовые инциденты, генерируемые Kaspersky Fraud Prevention Cloud, позволяют детально изучить случаи кражи учётных записей, создания мошеннических учётных записей, а также отмывания средств.

Объединение ключевых технологий KFP в Kaspersky Fraud Prevention Cloud

Ключевые преимущества Kaspersky Fraud Prevention

- Постоянное проактивное обнаружение продвинутых схем мошенничества до кросс-канального обнаружения фрода
- Обнаружение схем отмывания денег и мошенников
- Улучшение удобства использования и уровня лояльности клиентов
- Предоставление подробных данных сессии для дальнейшего расследования инцидентов с поддержкой выделенной команды
- Дополнение к текущим решениям по мониторингу фрода
- Повышение продуктивности и сокращение издержек благодаря автоматизации и машинному обучению

Машинное обучение является ядром Kaspersky Fraud Prevention. Различные методы машинного обучения, такие как кластеризация, деревья решений и искусственные нейронные сети, применяются для повышения эффективности и точности технологий Kaspersky Fraud Prevention. Это позволяет вывести обнаружение фрода на новый уровень, а также мгновенно реагировать на случаи мошенничества уже во время сессии, до проведения операции. В то же время легитимные пользователи, благодаря **Аутентификации на основе рисков (RBA)**, минуют дополнительные шаги аутентификации и пользуются личным кабинетом без каких-либо неудобств.

Automated Fraud Analytics

Реализация стратегии безопасности связана не только с передовыми технологиями. Речь также идёт о данных, которые поступают в ходе анализа пользовательской сессии, а также о способности использовать их наряду с технологиями.

Именно для этого существует Automated Fraud Analytics: бизнес должен знать о возможной мошеннической активности, когда она еще не началась, обладать данными, которые имеют решающее значение для принятия точных, своевременных решений и для выявления наиболее сложных случаев мошенничества.

Практическая применимость

Инциденты, сформированные Kaspersky Fraud Prevention

- Заражённое устройство **63%**
- Скомпрометированная учётная запись **34%**
- Отмывание денежных средств **3%**
- Средства автоматизации **0,39%**
- Мошенническая учётная запись **0,14%**

Кража учётной записи – Что если бы вы были уверены, что ваши цифровые каналы в данный момент используются легитимными юзерами? Что если бы вы знали, как пользователь ведёт себя в вашем приложении или на сайте? Это только часть того, что анализирует Kaspersky Fraud Prevention. Мы помогаем вам узнать больше о клиентах, предоставляя ценные данные и знания, чтобы увидеть аномалии и подозрительное поведение до того, как мошенничество было совершено, в то время как сами клиенты не теряют доступ к своей учётной записи.

Мошеннические учётные записи – для защиты бизнеса от такого рода атак применяются поведенческий анализ и биометрия, а также анализ устройства и окружения для построения моделей легитимного и мошеннического поведения. Такой подход позволяет выявить отклонения в пользовательском поведении, и распознать как реального пользователя, пытающегося воспользоваться услугой, так и мошенника, намеревающегося нанести вред бизнесу.

Отмывание денежных средств – построение связей между пользователями и устройствами, а также использование уникальных идентификаторов позволяет выявлять группы учётных записей, доступ к которым осуществляется с одного и того же устройства. Поведенческий анализ повышает эффективность обнаружения, отличая легитимных пользователей от мошенников. Благодаря глобальной репутации устройств Automated Fraud Analytics раскрывает связи между мошенническими аккаунтами и предотвращает сложные преступные схемы, реализуемые в разных организациях.

Аналитика мошенничества – на протяжении всей сессии, с самого ее начала, события, происходящие с пользователем, устройством, а также биометрические и поведенческие показатели тщательно анализируются. Объединение технологий и экспертизы аналитиков позволяет более точно указать виды подозрительной активности, которая выявляется в процессе, настраивать решение под запросы бизнеса, а также тщательно прорабатывать обнаруженные случаи мошенничества.

Угрозы

- **Мошенничество развивается** – растущие проблемы с клиентами
- **Более высокий уровень фрода** – штрафы со стороны регулятора
- **Угроза пропустить** стадию подготовки атаки
- **Растущая сложность атак** – привычные и устаревшие решения не справляются

Функциональные возможности

- **Построение и сопоставление связей** на глобальном уровне
- **Поведенческий анализ** на основе глубинного обучения
- **Гибкая настройка** правил

Advanced Authentication

Цифровая трансформация уже здесь. Компьютеры, планшеты и мобильные телефоны заменяют отделения и офисы, предоставляя доступ к сервисам, когда и где угодно. Ключевой задачей для бизнеса становится создание благоприятных условий для клиентов:

- **быстрый и беспрепятственный доступ в личный кабинет;**
- **удобные способы аутентификации;**
- **уверенность в безопасности используемых услуг.**

Advanced Authentication знает, кто использует сервисы в цифровых каналах: легитимный пользователь или мошенник, реальный человек или машина.

Анализ поведения пользователя, пассивных биометрических показателей, а также устройства и его окружения формируют объективную оценку риска сессии. Благодаря исследованию сотен уникальных показателей во время сессии:

- легитимные пользователи попадают в личный кабинет без дополнительной верификации;
- пользователи, вызывающие сомнения, проходят дополнительную проверку;
- подозрительные действия являются поводом для тщательной идентификации и возможного ограничения доступа.

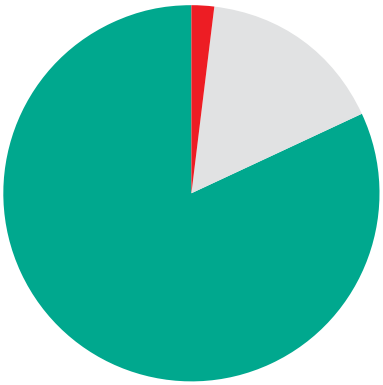
Advanced Authentication продолжает обеспечивать высокий уровень безопасности на протяжении всей сессии за счёт **Непрерывной аутентификации и анализа аномалий**. Решение оценивает данные о поведении пользователя, репутации устройства и другую уже накопленную информацию, поступающую в Kaspersky Fraud Prevention Cloud.

В случае обнаружения аномального поведения решение автоматически предоставляет данные об этом во внутренние системы мониторинга, а также задействует систему аутентификации для запроса второго фактора и определения легитимности транзакции и пользователя.

На основе обработки деперсонализированных данных и автоматического анализа информации Advanced Authentication выявляет случаи **Кражи учётной записи**. Решение умеет идентифицировать, а также выявлять новые, неиспользованные ранее устройства по уникальному отпечатку. Кроме того, анализ поведенческих и биометрических данных в режиме реального времени определяет отклонения от «типичного» пользовательского поведения.

Своевременное обнаружение скомпрометированных учётных записей позволяет как на этапе логина, так и во время сессии ограничить уровень доступа к личному кабинету и сократить потенциальные финансовые потери для бизнеса и для клиентов.

Вердикты Risk-Based Authentication



Красный (высокий риск мошенничества) **1,95%**

Серый (недостаточно информации, умеренный риск мошенничества) **16,21%**

Зелёный (легитимный пользователь) **82%**

Функциональные особенности

Аутентификация на основе рисков (RBA) ликвидирует дополнительные шаги аутентификации для легитимных пользователей, позволяя им войти в систему без излишних проверок. Благодаря постоянному анализу сотен различных показателей в режиме реального времени формируется динамическая оценка уровня риска. С высокой степенью уверенности она позволяет принять решение об уровне допуска в личный кабинет.

Кроме того, функциональность RBA дает возможность на раннем этапе обнаруживать подозрительную активность. Так, действия, которые отличаются от поведения легитимного пользователя, расцениваются как потенциально мошеннические и требующие дополнительного подтверждения.

Решение Advanced Authentication

- Повышает уровень удобства использования за счет снижения количества шагов аутентификации
- Снижает затраты на предоставление услуг второго фактора аутентификации
- Выявляет случаи кражи учетной записи, как на этапе логина, так и на протяжении всей сессии
- Помогает соответствовать законодательным требованиям, касающимся обеспечения безопасности платежей и противодействия мошенническим операциям

Что такое эффективная аутентификация?

Легитимный пользователь

Пользователя может раздражать необходимость получать SMS с кодом при каждой попытке получить доступ к своей учётной записи.

Двухфакторная аутентификация

- SMS
- E-mail
- Звонок

Учётная запись

Для бизнеса использование двухфакторной аутентификации приводит к дополнительным затратам и создает риск потери клиентов.

Второй Фактор Аутентификации

- Нарушает ход сессии
- Отнимает время
- Может быть украден

Для эффективной работы сервиса необходимо добиться оптимального баланса между безопасностью процесса аутентификации и удобством пользования.

Аутентификация на основе рисков

Дополнительная верификация нужна, только если уровень риска выше обычного. Таким образом, легитимные пользователи получают мгновенный доступ к своей учётной записи, а для мошенников доступ блокируется.

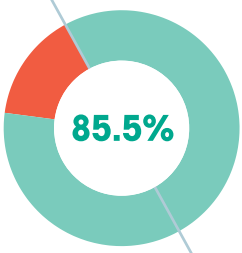
Преимущества для пользователя

— Более удобная работа с сервисом
— Более быстрые транзакции и покупки
— Высокий уровень защиты данных

Преимущества для бизнеса

— Технологии машинного обучения
— Возможности цифровой криминалистики
— Сокращение операционных расходов

Согласно статистике **Kaspersky Fraud Prevention**, **85.5%** пользователей получают доступ к своей учётной записи без дополнительной верификации.



RBA оценивает в режиме реального времени многочисленные уникальные параметры, такие как:

- Поведение пользователя
- Геолокация
- Время авторизации
- Биометрия
- Обычно используемое устройство
- Более 40 других уникальных параметров

Что общего у Fraud Prevention и Managed Security?

Компании считают, что сервисы MSSP (Managed Security Service Provider – от англ. поставщик услуг управляемой безопасности) могут помочь им сократить расходы на безопасность. Они стремятся перевести всю IT-инфраструктуру на аутсорсинг, включая безопасность, так как не обладают достаточными внутренними ресурсами и необходимой экспертизой.*

* Источник: Global IT Security Risk Survey 2017

Более широкий спектр услуг, предоставляемых вместе с Kaspersky Fraud Prevention

Увеличение доходов

- Более широкий клиентский охват благодаря улучшенной аутентификации, обнаружению мошенничества и расследованию инцидентов.
- Гибкая и масштабируемая бизнес модель позволяет оперативно приспосабливаться к требованиям клиентов.
- Интеграция cloud, private cloud или on premise в зависимости от предпочтений покупателя.

Поддержка продаж

- Маркетинговые материалы.
- Возврат части вложенных средств (Rebate).
- Совместные программы продаж.
- Возможность тренингов технических специалистов и специалистов отдела продаж.

Дополнительный уровень защиты

- Advanced Authentication в рамках расширенного пакета для онлайн канала компаний.
- Мониторинг и анализ сессии клиентов в онлайн каналах обслуживания.
- Возможности машинного обучения.

Клиентский пакет, включающий исследования и анализ в области кибермошенничества

- Обнаружения и мониторинга часто недостаточно, чтобы предотвратить будущие атаки. Анализ является обязательной функцией предотвращения атак мошенников до того, как будет нанесен какой-либо ущерб.
- Исследовательско-аналитическая группа «Лаборатории Касперского» опирается на более чем 22-летний опыт работы в области кибербезопасности и всегда готова провести глубокое расследование выявленных случаев мошенничества и аномалий.

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Развивайте бизнес безопасно

Kaspersky Fraud Prevention

Уверенно планируйте финансовые вложения в бизнес и создавайте удобный и быстрый в использовании сервис для клиентов

Преимущества для бизнеса

Снижение операционных издержек

Разоблачение сложных схем отмывания денег

Улучшенный уровень обслуживания клиентов

Автоматизированный подробный анализ подозрительных действий

kfp.kaspersky.com
@KasperskyFP

IT Security News:
www.kaspersky.com/blog
Cyber Threats News:
www.securelist.com

www.kaspersky.com

TOP 100 **Kaspersky Fraud Prevention** включен в 100 лучших изобретений 2017 года по версии Роспатента: https://kas.pr/100best

Kaspersky Fraud Prevention Automated Fraud Analytics [156555] включена в Реестр по Приказу Минкомсвязи РФ от 19.11.2019 №742, Приложение 1, № пп. 72, реестровый № 5954

Kaspersky Fraud Prevention Advanced Authentication [156556] включена в Реестр по Приказу Минкомсвязи РФ от 19.11.2019 №742, Приложение 1, № пп. 73, реестровый № 5955

WORLD BRANDING AWARDS BRAND OF THE YEAR