kaspersky АКТИВИРУЙ БУДУЩЕЕ

Предотвращение кросс-канальных атак в режиме реального времени

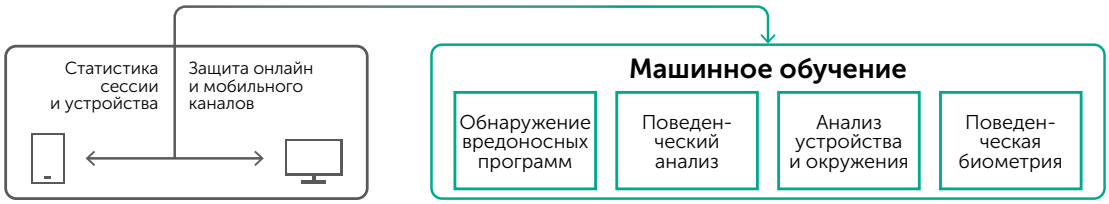
Kaspersky Fraud Prevention

Ready for GDPR

Обслуживание в офисе компании или отделении банка становится все 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.

Мошенничество с созданием новых учетных записей	Кража учетной записи	Автоматизированные инструменты
Отмывание денежных средств	Атаки с использованием средств удаленного доступа	Вмешательство в транзакции

Kaspersky Fraud Prevention использует сочетание передовых технологий с методами машинного обучения для проактивного обнаружения сложных мошеннических схем в онлайн- и мобильном каналах. Обнаружение происходит в режиме реального времени, еще до совершения транзакции.



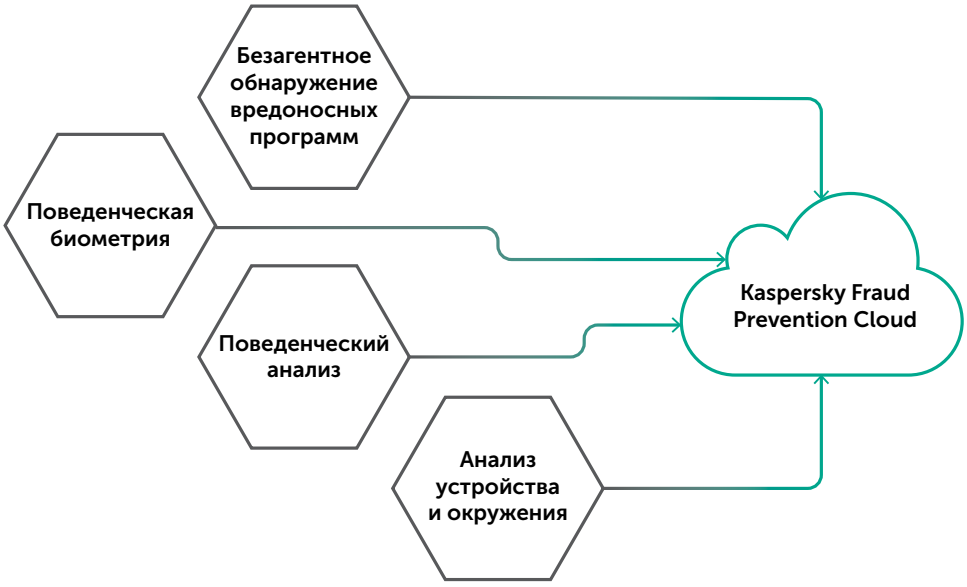
Анализ событий сессии посредством технологий Kaspersky Fraud Prevention

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 вовлеченный 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 учетной 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. .



Объединение ключевых технологий KFP в Kaspersky Fraud Prevention Cloud

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.

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 учетных записей, создания мошеннических учетных записей, а также отмывания средств.

Ключевые преимущества:

- Постоянное проактивное обнаружение продвинутых схем мошенничества до проведения транзакции в режиме реального времени
- Кросс-канальное обнаружение 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

Свяжитесь с нами, чтобы узнать больше: kfp@kaspersky.com

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Cybersecurity for SMB: kaspersky.com/business
Cybersecurity for Enterprise: kaspersky.com/enterprise

kfp@kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Known more at kaspersky.com/transparency

Proven.
Transparent.
Independent.