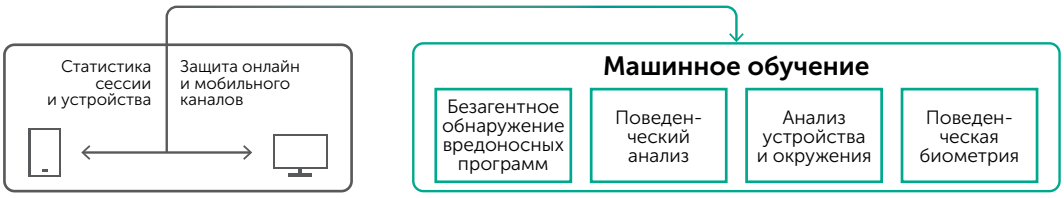
Kaspersky®
Fraud Prevention

Предотвращение кросс-канальных атак в режиме реального времени

Обслуживание в офисе компании или отделении банка становится все менее популярным. Для клиентов гораздо удобнее совершать операции, используя личный кабинет на сайте банка 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 (NAF)	Захват учетной записи (ATO)	Автоматизированные инструменты
Вмешательство в транзакции	Атаки с использованием средств удаленного доступа	Вредоносное ПО и фишинг (т. е. с маленькой буквы)

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.



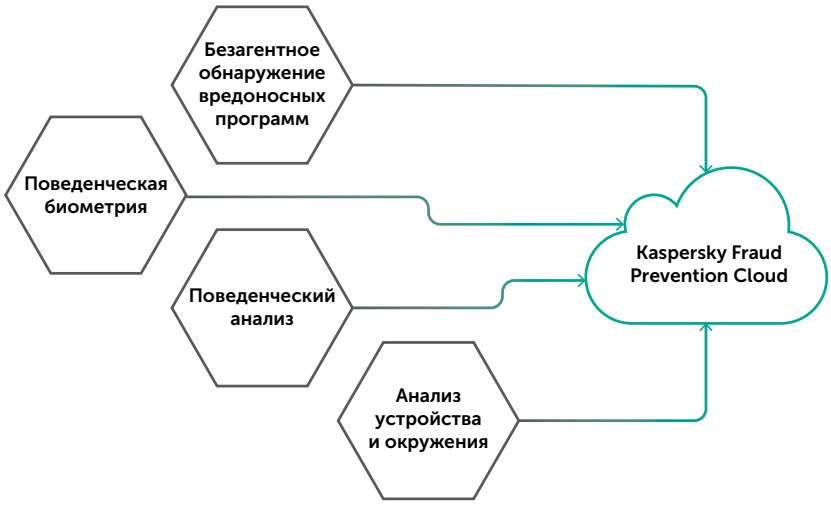
Обработка статистики технологиями Kaspersky Fraud Prevention

Безагентное обнаружение вредоносных программ. Позволяет определить, заражена ли машина пользователя вредоносным ПО. Пользователю при этом не нужно устанавливать дополнительных программ. Эти данные используются для Аутентификации на основе риска (RBA), поведенческого моделирования при помощи машинного обучения, а также для определения легитимности транзакций.

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.

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 реальным пользователем. Эта технология позволяет выявлять ботов и средства удаленного администрирования.

Анализ устройства и окружения использует данные репутационной облачной сети безопасности Kaspersky Security Network, 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.



Объединение ключевых технологий KFP в Kaspersky Fraud Prevention Cloud

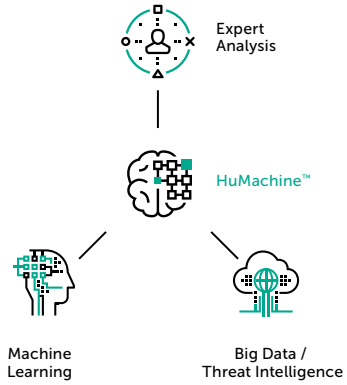
Машинное обучение является ядром платформы Kaspersky Fraud Prevention. Различные методы машинного обучения, такие как кластеризация, деревья решений и искусственные нейронные сети, применяются для повышения эффективности и точности технологий Kaspersky Fraud Prevention. Это позволяет вывести обнаружение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

Обезличенные данные, обрабатываемые четырьмя ключевыми технологиями, трансформируются в вердикты в режиме реального времени внутри Kaspersky Fraud Prevention Cloud. На основе постоянного проактивного анализа репутации устройства и сессии в онлайн и мобильном каналах, поведенческих и биометрических показателей и других аспектов, облачное решение снабжает ваши внутренние системы мониторинга данными, особо необходимыми для своевременного обнаружения фрода. Это позволяет вашим текущим системам использовать дополнительный контекст для более быстрого и точного принятия решений, а также для интеллектуального и адаптивного использования поэтапной аутентификации.

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА:

- Постоянное проактивное обнаружение продвинутых схем мошенничества до проведения транзакции в режиме реального времени
- Кросс-канальное обнаружение фрода
- Обнаружение схем отмывания денег и дропперов
- Улучшение удобства использования за счет RBA, что привлекает новых и помогает удержать существующих 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



www.kaspersky.ru

#ИстиннаяБезопасность