Kaspersky Fraud Prevention

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.

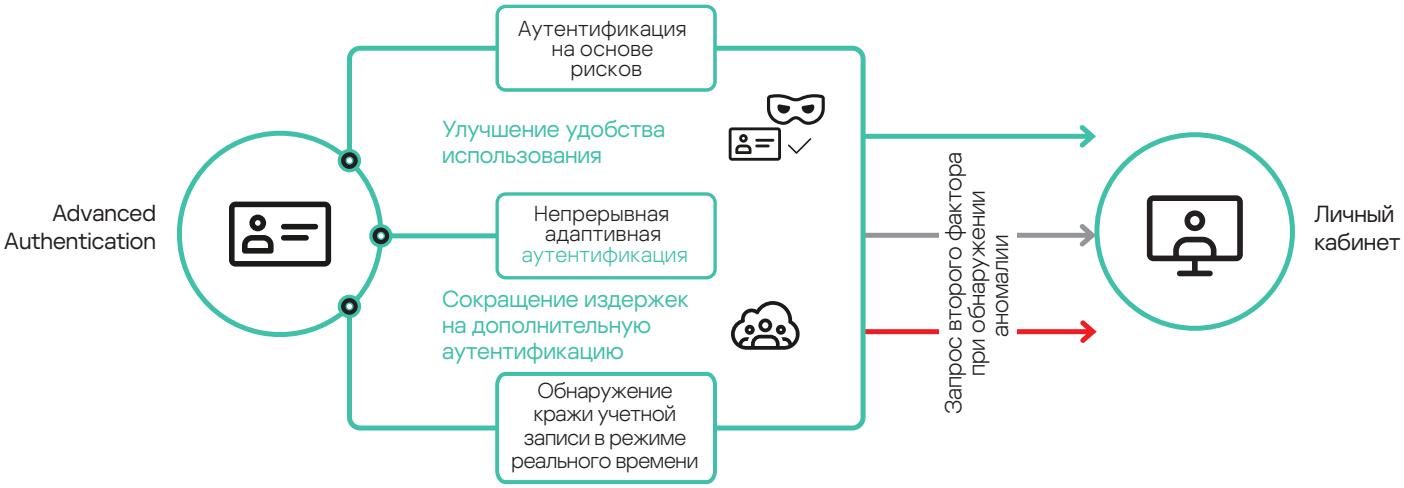
Advanced Authentication знает, кто использует сервисы в цифровых каналах: легитимный пользователь или мошенник, реальный человек или машина.
Анализ поведения пользователя, пассивных биометрических показателей, а также устройства и его окружения формируют объективную оценку риска сессии. Благодаря исследованию 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 – решение линейки Kaspersky Fraud Prevention, разработанное для улучшения удобства использования и сокращения издержек на дополнительные факторы аутентификации. Кроме того, обнаруживается и в последствии пресекается использование украденных учетных записей. Все это позволяет развивать бизнес без проблем с безопасностью, предоставляя клиентам комфортный доступ к сервисам.

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

Advanced Authentication продолжает обеспечивать высокий уровень безопасности на протяжении всей сессии за счет **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 учетной 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 ученых 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.

kfp@kaspersky.com
www.kaspersky.ru