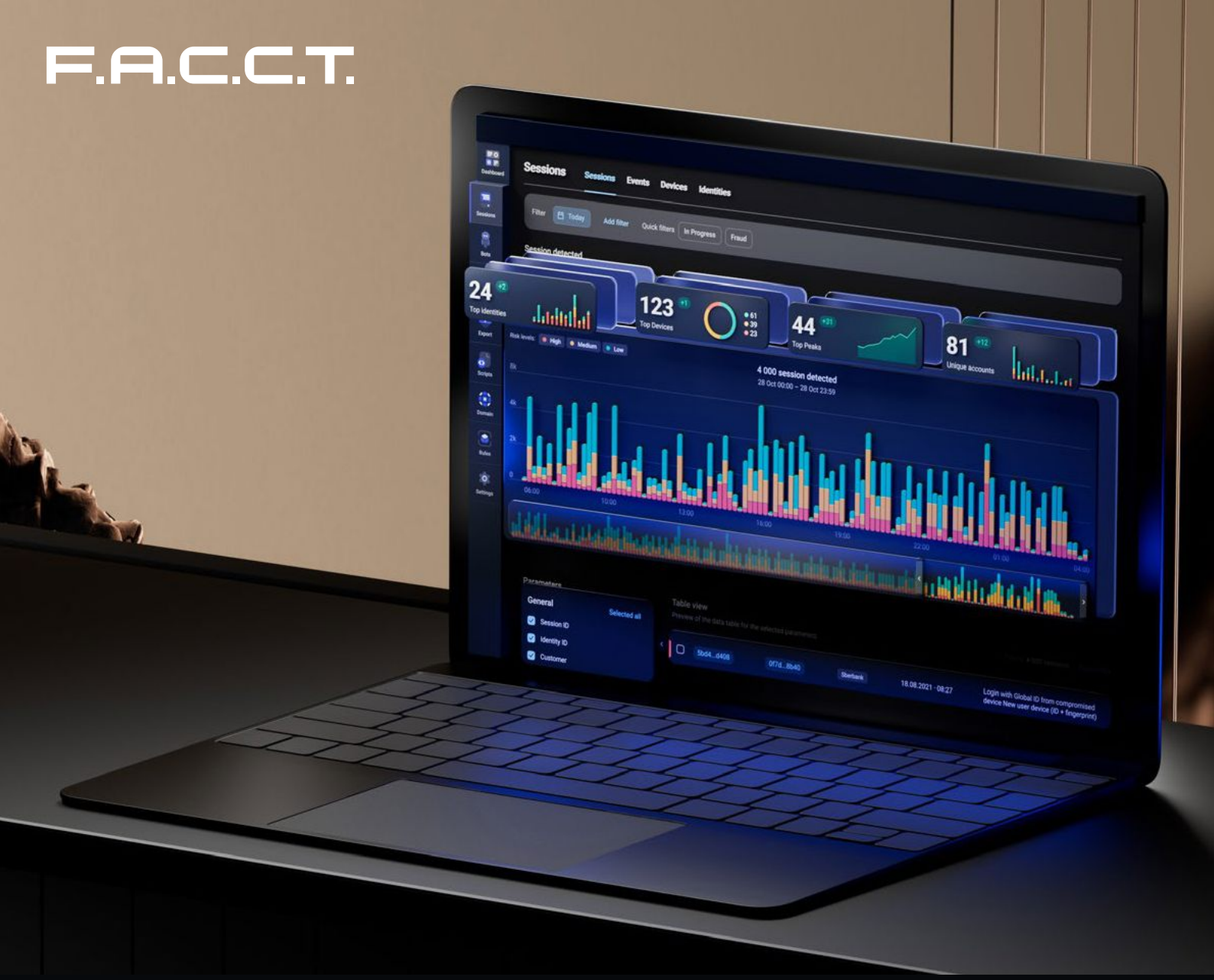
F.A.C.C.T.



ОБЗОР ПРОДУКТА

FRAUD PROTECTION

Предотвращение онлайн-мошенничества в реальном времени и во всех цифровых каналах

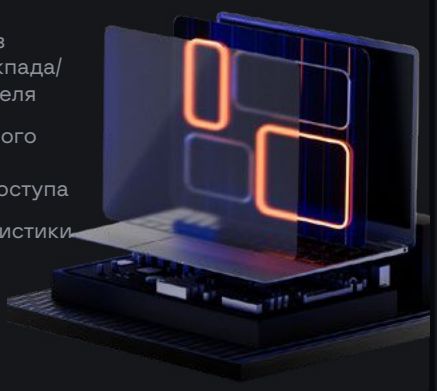
FACCT.RU

В борьбе с цифровым мошенничеством защищаем 300 миллионов пользователей веб и мобильных приложений

- Мошенничество с банковскими картами
- Атаки с использованием социальной инженерии
- Вредоносная бот-активность
- Мошенничество в онлайн-торговле
- Атаки на игорный и букмекерский сектора
- Мошенничество с использованием вредоносного ПО
- Отмывание доходов
- Платежное мошенничество

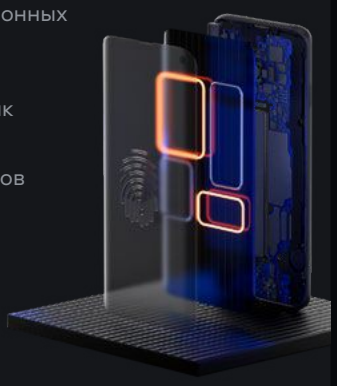
Защита веб-каналов

- Обезличенный поведенческий анализ активности мыши/трекпада/клавиатуры пользователя
- Выявление вредоносного ПО, бот-активности и троянов удаленного доступа
- Технические характеристики устройства
- Настройки дисплея
- Настройки браузера



Защита мобильных каналов

- Мониторинг настроек операционных систем Android и iOS
- Мониторинг сенсоров на устройствах и характеристик оператора мобильной связи
- Выявление ВПО, ботов и троянов удаленного доступа
- Обезличенный мониторинг поведения пользователей
- Мониторинг технических характеристик устройств



Команда экспертов

Доверьте свой кейс команде F.A.C.C.T. по расследованиям высокотехнологичных преступлений

- Проприетарные технологии выявления киберпреступлений
- Сотрудничество с международными правоохранительными организациями
- Всестороннее знание мошеннических схем
- Индивидуальный подход к клиентам и привлечение специализированных проектных команд

Проактивный анализ угроз

Интеграция с F.A.C.C.T. Threat Intelligence позволяет получить следующие данные:

- Данные кибер разведки по IP-адресам: TOR, прокси-сервера, хостинг-сервисы
- Фишинговые и вредоносные домены
- Типичное поведение и сигнатуры вредоносного ПО
- Скомпрометированные пользовательские аккаунты
- Скомпрометированные банковские карты

Блокирование «плохих» ботов

Preventive Proxy защищает мобильные и веб-приложения от разных видов бот-активности, включая:

- Атаки на мобильный API
- Нелегитимное использование API
- Системы автоматизации
- Использование украденных данных
- DDoS-атаки на уровне приложений
- Кража cookie-файлов
- Скрапинг
- Брутфорс

Ключевые технологии

Перекрестный анализ клиентов

Точная идентификация поведения пользователей и устройств по всему миру для всех каналов

Графовый анализ связей

Комплексный графовый анализ связей между пользователями и устройствами

Защита от ботов с Preventive Proxy

Проактивное выявление и блокирование ботов и их вредоносной активности

Машинное обучение

Непревзойденное сочетание контролируемого, неконтролируемого и глубокого машинного обучения для восстановления полного контекста пользовательской сессии

Поведенческий анализ

Выявление нетипичного поведения пользователей и устройств, предотвращение фрода,снижение издержек на доп. этапы аутентификации

Выявление мошеннических звонков

Выявление мошеннических звонков на мобильных устройствах и предотвращение мошеннических транзакций

Выгода для бизнеса

Увеличение количества предотвращенных угроз

Мошенничество с банковскими картами

Снижение операционных затрат

Снижение количества ложноположительных срабатываний на 20% по сравнению с конкурирующими решениями*

Оптимизация опыта пользователей

В ходе двухфакторной аутентификации на 30% реже возникает необходимость вводить одноразовый пароль*

Высокий показатель ROI и быстрый возврат инвестиций

За полгода ROI составил 130% по сравнению с уровнем лидера рынка*

Качественные результаты

Долгосрочная лояльность клиентов

Для бизнеса борьба с мошенничеством – это путь к установлению длительных доверительных отношений с клиентами

Удобство в использовании

Обеспечение беспрепятственного пользовательского опыта во всех каналах за счет упрощения процесса проверки безопасности

* Данные из отчета Total Economic Impact™: сокращение издержек бизнеса на защиту от рисков при переходе от старого антифрод-решения к F.A.C.C.T. Digital Fraud Protection

Отчет Forrester Solution Cost Savings And Business Benefits («Экономия затрат и преимущества для бизнеса, получаемые за счет внедрения решения»)

Описание компании

F.A.C.C.T. — один из ведущих мировых разработчиков решений для обнаружения и предотвращения кибератак, выявления мошенничества и защиты интеллектуальной собственности в сети.

1 300+
успешных исследований по всему миру

550+
enterprise-клиентов

120+
патентов и заявок

№1
первый поставщик услуги Incident Response в России

20 млрд +
сохраняют наши технологии в бюджете клиентов ежегодно

20 лет
практики и уникальной экспертизы на рынке РФ

Технологии и инновации

Кибербезопасность

- Threat Intelligence
- Управление поверхностью атаки
- Защита электронной почты
- Анализ сетевого трафика
- Детонация ВПО
- Защита конечных станций (EDR)
- XDR

Противодействие мошенничеству

- Противодействие мошенничеству client-side
- Адаптивная аутентификация
- Защита от ботов
- Выявление платежного мошенничества
- Поведенческий анализ

Защита бренда

- Антифишинг
- Антипиратство
- Антимошенничество
- Антиконтрафакт
- Выявление утечек данных
- Защита VIP-персон

Портфолио услуг

Аудит и консалтинг	• Анализ защищенности • Тестирование на проникновение • Red Teaming • Оценка соответствия и консалтинг	• Выявление следов компрометации • Проверка готовности к реагированию на инциденты
Обучающие программы	• Для технических специалистов • Для широкой аудитории	• Мастер-классы для детей
Реагирование на инциденты и цифровая криминалистика	• Реагирование на инциденты • Реагирование на инциденты по подписке	• Цифровая криминалистика • eDiscovery
Managed Services	• Managed Detection • Managed Threat Hunting	• Managed Response
Исследование высокотехнологичных преступлений	• Исследование киберпреступлений	

Предотвращаем и исследуем киберпреступления с 2003 года