



SOLUÇÕES ANTIFRAUDE

Device Risk

Riscos de Dispositivos

VISÃO GERAL

No cenário digital em rápida evolução de hoje, a fraude tornou-se cada vez mais sofisticada e disseminada, representando desafios significativos para as organizações. Desde ataques de invasão de contas e fraude de identidade sintética, até manipulação de dispositivos, essas ameaças digitais são numerosas e estão em constante evolução, frequentemente resultando em danos financeiros e reputacionais para as organizações.

Truvalidate™ Device Risk ajuda a prevenir fraudes digitais em tempo real.

O **Truvalidate Device Risk** foi projetado para abordar esses desafios de forma proativa, fornecendo capacidades avançadas de detecção e prevenção para proteger sua organização. Ao aplicar análises de ponta e aprendizado de máquina (*Machine Learning*) combinados com detecção avançada de evasão e anomalias, o TruValidate Device Risk capacita as organizações a se manterem à frente dos fraudadores - sem impactar as experiências dos bons clientes.

TRUVALIDATE DEVICE RISK PERMITE QUE AS ORGANIZAÇÕES:

Combatam fraudes sem impactar bons clientes

Distinguir fraudadores de clientes reais usando reconhecimento avançado de dispositivos, análise contextual e insights comportamentais. Garantir que usuários legítimos desfrutem de uma experiência perfeita enquanto mantêm os fraudadores afastados.

Construir conexões confiáveis

Aproveitar o histórico extenso de dispositivos associados que se beneficia de insights de risco de mais de 111 bilhões de verificações de reputação de dispositivos e mais de 185 milhões de relatórios detalhados de fraude para fortalecer suas medidas de segurança.

Personalizar a solução de acordo com seu apetite a risco

Aplicar inteligência de dispositivos para abordar seus desafios específicos de fraude com regras de negócios personalizadas e configuráveis. Adaptar a solução para atender às suas necessidades específicas, ajudando à garantir máxima roteção, captura de fraudes e eficiência.

Aumentar a eficiência operacional

Racionalize seus processos de detecção de fraudes com avaliações de risco automatizadas e alertas em tempo real. Reduza a intervenção manual e concentre seus recursos em iniciativas estratégicas.

Melhorar a conversão de clientes

Avalie o risco de transações digitais com impacto mínimo na experiência do consumidor, identificando sinais de risco antecipadamente na jornada do cliente, a fim de elevar taxas de aprovação para usuários legítimos.

Obter insights acionáveis

Utilize análises detalhadas e relatórios da maior e mais antiga rede global de risco de dispositivos para obter insights sobre tendências e padrões de fraude em evolução. Tome decisões baseadas em dados para melhorar suas estratégias de prevenção de fraudes.

COMO FUNCIONA?

O TruValidate Device Risk rastreia relações entre dispositivos e contas aproveitando o histórico de dispositivos e relatórios de fraude confirmados em tempo real de nossa extensa rede global de insights sobre padrões de fraudes. Ele pode ser facilmente integrado em qualquer aplicativo nativo ou aplicação web.

Agora você pode proteger sua organização em toda a jornada do cliente. Aplique nossa solução em qualquer ponto de contato com o cliente onde o risco de fraude seja uma preocupação, como criação de conta, onboarding, login, alteração de detalhes, pagamento e checkout.

Tecnologia inovadora, capacidades diversas

Ao reconhecer dispositivos conectados à internet sem exigir informações pessoais identificáveis (PII), o Device Risk adiciona uma camada independente de identidade digital separada dos dados pessoais que podem ter sido comprometidos.

Reconheça com precisão todos os tipos de dispositivos

O Device Risk analisa milhares de atributos para identificar um dispositivo com precisão, minimizando falsos positivos.

Rastreie e descubra padrões ocultos de fraude

Análises avançadas combinadas com modelos de aprendizado de máquina podem identificar transações suspeitas e padrões de dispositivos – que podem ser rapidamente rastreados usando nosso editor flexível de regras de negócios.

Atenda às necessidades únicas da sua organização

Apresenta conjunto de regras personalizadas que podem ser adaptadas à estratégia única de fraude da sua organização. Capacidades de rastreamento, pesquisa e relatórios impulsionadas por aprendizado de máquina sinalizam transações suspeitas e padrões de dispositivos.

Descubra ligações arriscadas entre dispositivos e contas

Descubra conexões ocultas entre dispositivos e contas para ajudar a descobrir anéis de fraude e dispositivos “culpados por associação”.

Aproveite as capacidades avançadas de detecção de evasão

Previna melhor os fraudadores que se escondem atrás de servidores proxy, redes TOR, VPNs e outras tecnologias de anonimização enquanto detecta atividades de risco, como discrepâncias de fuso horário, idioma, resolução de tela e anomalias de dados de endereço IP.

Detecte ambientes virtuais e bots

Identifique ambientes virtuais por meio da análise de dados do navegador, sinais de reputação de IP e técnicas avançadas de detecção de anomalias e evasão. A maioria dos ataques automatizados se origina de dispositivos virtuais, permitindo que os fraudadores realizem atividades maliciosas em escala e apaguem rastros.

Aumente a precisão na captura de fraudes

Beneficie-se de análises extensas de padrões e tendências históricas e maior granularidade de dados para melhorar a precisão e a identificação de esquemas de fraude sofisticados que evoluem ao longo do tempo. Fique à frente das ameaças emergentes com capacidades avançadas de detecção.

Análise padrões complexos com modelos de aprendizado de máquina preditivos e proativos

Use modelos de aprendizado de máquina preditivos e dinâmicos com regras personalizadas e sinais robustos de dispositivos para analisar padrões complexos e detectar atividades fraudulentas com mais precisão.

CASOS DE USO COMUNS PARA O DEVICE RISK

Prevenção de tomadas de conta (ATO)

Desafio: Plataformas de banco online enfrentam riscos significativos de tomadas de conta, onde fraudadores usam credenciais roubadas para obter acesso não autorizado a contas de usuários.

Solução: O Device Risk pode detectar comportamentos incomuns de dispositivos e sinalizar possíveis tentativas de ATO, ajudando a prevenir acessos não autorizados e protegendo as contas dos clientes.

Detecção de fraude de identidade sintética

Desafio: Instituições financeiras enfrentam dificuldades com fraudes de identidade sintética, onde fraudadores criam identidades falsas usando uma mistura de informações reais e fabricadas.

Solução: Ao analisar padrões e comportamentos de dispositivos, o Device Risk pode identificar inconsistências que podem indicar identidades sintéticas potenciais, permitindo que as instituições tomem medidas antes que a fraude ocorra.

CASOS DE USO ESPECÍFICOS POR INDÚSTRIA

Prevenção de fraudes no e-commerce

Desafio: Varejistas online enfrentam altos volumes de transações fraudulentas, levando a perdas financeiras e estornos.

Solução: O Device Risk pode identificar comportamentos suspeitos de dispositivos e sinalizar transações de alto risco, reduzindo fraudes e minimizando estornos.

Mitigação de fraudes em pagamentos

Desafio: Empresas de e-commerce enfrentam altos volumes de transações fraudulentas, levando a perdas financeiras e estornos.

Solução: O Device Risk pode identificar comportamentos suspeitos de dispositivos e sinalizar transações de alto risco, reduzindo fraudes e minimizando estornos.

Prevenção de abuso de promoções

Desafio: Varejistas online e provedores de serviços frequentemente lidam com abuso de promoções, onde fraudadores exploram ofertas promocionais e descontos.

Solução: O Device Risk pode monitorar o comportamento dos dispositivos e detectar padrões indicativos de abuso de promoções, ajudando a garantir que as ofertas promocionais sejam usadas por clientes genuínos.

Serviços bancários e financeiros

Desafio: Instituições financeiras enfrentam dificuldades com fraudes de identidade sintética, onde fraudadores criam identidades falsas usando uma mistura de informações reais e fabricadas.

Solução: Ao analisar padrões e comportamentos de dispositivos, o Device Risk pode detectar e prevenir melhor o acesso não autorizado, ajudando a garantir a segurança das contas dos clientes.

Detecção de fraudes em seguros

Desafio: As seguradoras precisam identificar reivindicações fraudulentas para prevenir abusos de políticas.

Solução: O Device Risk pode descobrir conexões ocultas entre dispositivos e contas, ajudando a detectar e prevenir reivindicações fraudulentas.

Saúde

Desafio: Provedores de saúde precisam proteger os dados dos pacientes e prevenir o acesso não autorizado a registros médicos.

Solução: O Device Risk pode monitorar o comportamento dos dispositivos e detectar anomalias, garantindo que apenas dispositivos autorizados acessem informações sensíveis.

Viagens e hospitalidade

Desafio: Empresas de viagens e hospitalidade precisam se proteger contra fraudes de reservas e acesso não autorizado a dados de clientes.

Solução: O Device Risk pode analisar o comportamento dos dispositivos durante os processos de reserva, sinalizando atividades suspeitas e prevenindo fraudes.



Telecomunicações

Desafio: Provedores de telecomunicações enfrentam riscos de aberturas fraudulentas de contas e roubo de dispositivos.

Solução: O Device Risk pode verificar a autenticidade dos dispositivos e detectar atividades suspeitas, ajudando a prevenir fraudes e reduzir perdas.

Jogos e serviços online

Desafio: Plataformas de jogos e serviços online enfrentam riscos de tomadas de conta e atividades fraudulentas, incluindo abuso de promoções.

Solução: Ao aproveitar a inteligência dos dispositivos, o Device Risk pode identificar e bloquear atividades fraudulentas, promovendo um ambiente de jogo mais seguro e justo.

