SHIELD

SHIELD para Plataformas Bancárias

A plataforma de inteligência de fraude focada na identificação de dispositivos da SHIELD identifica a raiz da fraude por meio do **SHIELD Device ID** e do **Fraud Intelligence**, ajudando plataformas bancárias a se anteciparem a ameaças sofisticadas e complexas com algoritmos de alta performance.

Quem Confia em Nós

truemoney maya :ubank FE CREDIT WINK ZIGI ... and more

"O parceiro perfeito para nós precisa ser capaz de escalar junto com a TrueMoney, possuir forte expertise técnica em e-wallets e a agilidade para se manter à frente dos comportamentos em constante mudança tanto dos fraudadores quanto dos consumidores. A SHIELD preenche todos esses requisitos."

Monsinee Nakapanant
Co-Presidente, Ascend Money

Nossa solução

SHIELD Device ID
identifica de forma persistente a raiz da fraude & contas falsas >99.9% de precisão

SHIELD Fraud Intelligence
insights acionáveis em tempo real sobre atividades fraudulentas

Feature AI Engine
personaliza regras e políticas complexas para combater ataques avançados

Casos de Uso

Elimine Contas Falsas & Mulas de Dinheiro

O que são Contas Falsas e Mulas de Dinheiro?

Fraudadores usam ferramentas, como clonadores de aplicativos e emuladores, para criar contas falsas com alta velocidade e escala. Essas contas podem servir como veículos para lavagem de dinheiro, permitindo que "mulas" de dinheiro depositem e transfiram fundos ilegais. A facilidade e o baixo custo de criar contas falsas tornam um desafio para os bancos identificar todas e eliminá-las.

01

Elimine Contas Falsas e Mulas de Dinheiro pela Raiz

Elimine contas falsas com os device IDs persistentes da SHIELD, criados para identificar até mesmo reset de fábrica e adulterações avançadas.

02

Bloqueie Atividades Suspeitas em Tempo Real

Impeça a criação em massa de contas a partir do mesmo dispositivo. Detecte ferramentas e técnicas, como clonadores de apps, usados para conduzir atividades suspeitas.

03

Potencialize a Detecção de Contas "Mula"

Dobre a precisão da detecção de "mulas" e aperfeiçoe os modelos de dados existentes com a inteligência e os insights de risco acionáveis da SHIELD.

SHIELD Fraud Intelligence

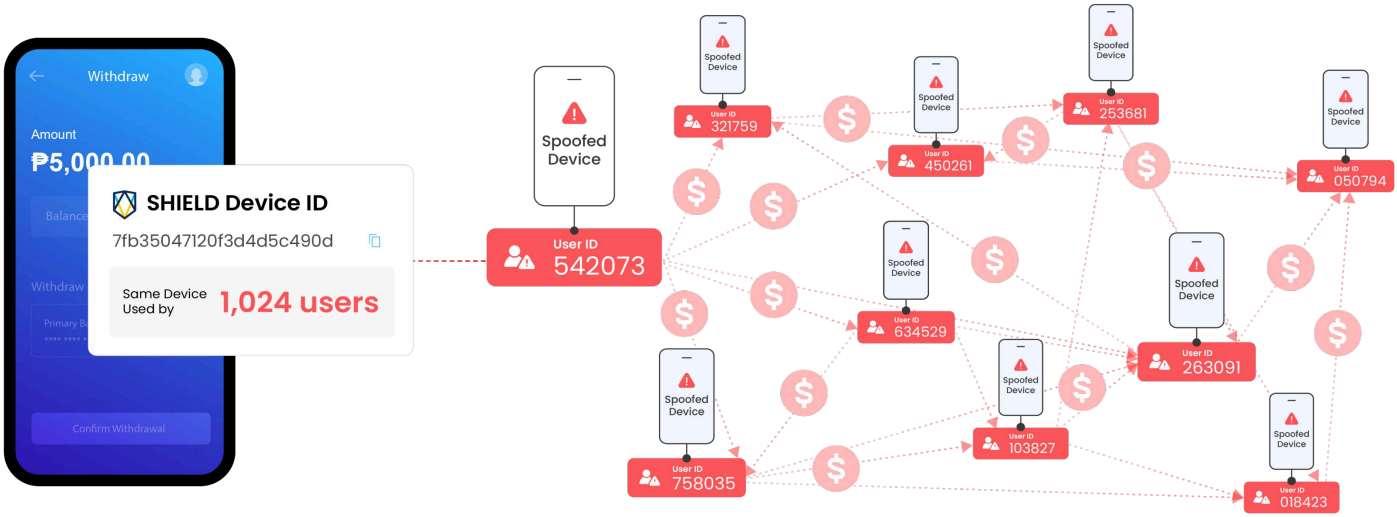
Uso de App Cloners
Uso de Emuladores
Uso de VPN
Reset de fábrica suspeito
Screen-sharing
Devices Jailbroken
Uso de App Tampering

Como funciona

Os fraudadores criam contas em larga escala usando identidades roubadas, clonadores de aplicativos e emuladores.
As contas falsas são utilizadas para que eles possam realizar:

- Transações repetidas de pequenas quantias em um curto período de tempo para contas "mula"
- Transações feitas pela mesma conta, controlada por diferentes dispositivos em várias localizações
- Saques em um curto período de tempo a partir de diferentes lugares
- Atividades de dispositivos em localizações sancionadas

A SHIELD identifica contas interconectadas controladas pelo mesmo dispositivo, revelando clusters complexos de fraude e interrompendo ataques sofisticados e coordenados.



Casos de Uso

Elimine Fraudes de Account Takeover

Abuso de Serviços de Acessibilidade & Engenharia Social

O que é Fraude de Account Takeover?

A fraude de account takeover (ATO) ocorre quando um fraudador obtém acesso às credenciais de login da vítima para roubar fundos ou informações.

01

Abuso de Serviços de Acessibilidade

As vítimas, sem saber, baixam e concedem permissões de acessibilidade a aplicativos maliciosos. Isso permite que os fraudadores ganhem controle sobre o dispositivo, roubando dados, OTPs e mais.

02

Engenharia Social

Fraudadores se passam por ou fingem ser um executivo bancário para extrair credenciais e detalhes dos usuários, assumindo o controle das contas e roubando fundos. Isso leva a prejuízos financeiros e de reputação para os bancos.

SHIELD Device ID

Identifique novos dispositivos acessando contas com bom histórico de forma repentina, a partir de diferentes locais - um sinal de ATOs.

SHIELD Fraud Intelligence

Detecte comportamentos maliciosos, incluindo ferramentas de compartilhamento de tela e mascaramento de dispositivos - geralmente sinais de que o abuso de serviços de acessibilidade está ocorrendo.

Biometrias passivas

Conte com dados de sensores de dispositivos e interações dos usuários para identificar anomalias como usos incomuns do dispositivo, como deslizamentos rápidos e digitações não naturais.

Casos de Uso

Proteção contra Fraude de Pagamento

O que é Fraude de Pagamento?

Fraudadores podem realizar transações não autorizadas com detalhes de cartões e identidades roubados, o que pode resultar em altas taxas de chargeback, prejuízos financeiros e perda de confiança e credibilidade dos usuários.

Potencialize o Monitoramento de Transações com Feature AI Engine da SHIELD

Conjuntos de Recursos para Bancos

Conte com pacotes de recursos adaptados para combater fraudes bancárias. Simplifique a criação de recursos, economize tempo e esforço, e mantenha a conformidade com os requisitos regulatórios.

Personalização de Regras e Políticas de Risco

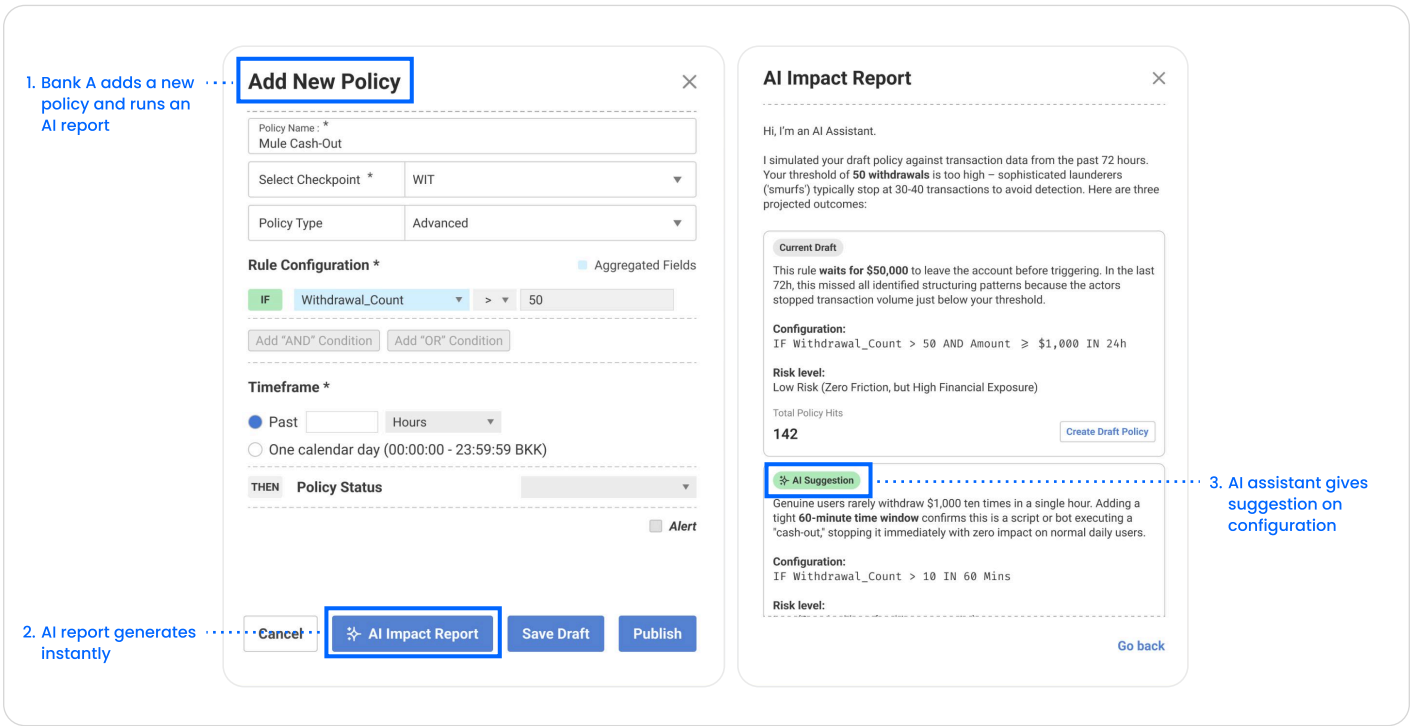
Recursos personalizados que se alinham precisamente com os requisitos do negócio. Integre a expertise interna no processo de criação de recursos para obter o máximo desempenho.

Reforçado com Device Intelligence

Garanta detecção de esquemas de fraude sem interromper a experiência do usuário. Vincule usuários, dispositivos e atividades para identificar ataques coordenados pela raiz.

Customize Políticas & Regras de Risco

Defina políticas avançadas e personalizadas em múltiplos pontos de controle para atender a requisitos financeiros e regulatórios complexos. Execute simulações automatizadas para analisar como novas políticas impactariam seu ecossistema antes de entrarem em produção.



Casos de Uso

Previna Deepfakes & Bypass de E-KYC

Como acontece o bypass de E-KYC?

Fraudadores burlam processos de verificação de identidade injetando deepfakes gerados por IA por meio de técnicas de hooking, falsificando rostos, documentos e verificações de prova de vida (liveness). Esses ataques geralmente são realizados a partir do mesmo dispositivo, potencializados pelo uso de clonadores de aplicativos e emuladores. Em larga escala, fraudadores automatizam ataques para simular milhares de usuários reais.

Combata Deepfakes e Fraudes com IA

Impeça fraudadores de utilizarem vídeos e imagens gerados por IA para enganar mecanismos de detecção de prova de vida.

Bloqueie Hooking e Manipulação de Aplicativos

Detecte e bloqueie invasores que manipulam apps para desativar mecanismos de segurança e injetar dados falsos de identidade.

Previna Falsificação de Dispositivo

Impeça fraudadores de mascararem a identidade real do dispositivo por meio de emuladores, clonadores de app e outras técnicas de falsificação de dispositivos.

O Cenário de Fraude: Seguros e Crédito

Nos setores de seguros e crédito, fraudadores exploram falhas nos processos de onboarding, abusam de aprovações instantâneas e utilizam documentos gerados por IA para aplicar golpes em escala.

Fraude em Seguros

Identifique Sinistros Inflados

Sinistros fraudulentos ou inflados passam despercebidos, permitindo que fraudadores recebam pagamentos antes que a fraude seja detectada.

Monitore Agentes Maliciosos

Corretores e agentes mal-intencionados criam apólices fantasmas ou manipulam solicitações para atingir metas e aumentar comissões.

Bloqueie Fraudes no Onboarding

Detecte aplicações falsas, contas duplicadas e tentativas de bypass de eKYC antes que apólices fraudulentas sejam emitidas.

Fraude em Empréstimos

Proteja-se contra ATOs

Contas comprometidas (Account Takeovers) são usadas para acessar linhas de crédito e sacar recursos antes que os sistemas detectem a invasão.

Previna Loan Stacking

Fraudadores exploram aprovações instantâneas para contratar múltiplos empréstimos em diferentes plataformas, maximizando ganhos antes que sinais de risco sejam identificados.

Detecte Documentos Sintéticos

Documentos clonados ou gerados por IA são usados para burlar verificações, permitindo que fraudadores obtenham empréstimos utilizando identidades sintéticas ou roubadas.

Por que a SHIELD

As Limitações do App Hardening Estático

Por que o app hardening não é suficiente?

O app hardening protege o código da aplicação contra adulteração e engenharia reversa por meio de técnicas como ofuscação de código e verificações de integridade. No entanto, essas proteções são estáticas e deixam lacunas críticas de detecção durante sessões reais dos usuários.

À medida que as táticas de fraude se tornam mais sofisticadas e impulsionadas por IA — como deepfakes e ataques automatizados — a ausência de visibilidade em tempo de execução cria pontos cegos que ferramentas avançadas de fraude conseguem explorar.

Detecte Ferramentas de Fraude de Nova Geração

Frameworks modernos de fraude, incluindo ferramentas baseadas em IA, conseguem contornar proteções estáticas de hardening ao mascarar seus rastros.
A SHIELD atua como uma camada essencial de defesa, detectando essas táticas sofisticadas exatamente no momento em que são ativadas.

Proteção Durante Toda a Sessão do Usuário

A SHIELD oferece visibilidade contínua do comportamento do dispositivo em tempo de execução. Ao monitorar sinais em nível de dispositivo durante toda a sessão, bancos conseguem proteger toda a jornada do usuário — desde a abertura do aplicativo, passando pelo login, até a transação.