SHIELD | Kirvano

Case Study

Kirvano faz parceria com SHIELD para eliminar fraude e impulsionar crescimento dos negócios de empreendedores digitais

"Com o Device Intelligence da SHIELD, conseguimos distinguir, de forma acurada, clientes genuínos de fraudadores. Nossa parceria com a SHIELD é fundamental para garantir segurança e impulsionar crescimento de negócio para os criadores de conteúdo digital que confiam na nossa plataforma."

Lorram Félix
CEO, Kirvano

Principais Resultados

99% de aumento em detecção de account takeover

Crescimento de receita para empreendedores digitais ao eliminar fraude

Detecção de tentativas de fraude de pagamento em tempo real, prevenindo prejuízos financeiros

Kirvano e sua jornada para garantir uma plataforma confiável aos usuários

A missão da Kirvano é capacitar criadores de conteúdo digital e empreendedores online, oferecendo uma plataforma segura e eficiente que facilite a criação, venda e promoção de seus produtos e serviços digitais.

Proporcionar uma boa experiência para os clientes que usam o ecossistema para vender e promover seus produtos é prioridade para a Kirvano. No entanto, eles estavam cientes de que a plataforma poderia ser alvo de fraudadores, que poderiam realizar fraudes de pagamento e ataques de account takeover. Tais ameaças colocariam em risco o crescimento dos negócios dos empreendedores digitais e a confiança na plataforma.

Para enfrentar esses desafios, a Kirvano escolheu fazer parceria com a SHIELD, plataforma de risco enriquecida por inteligência artificial.

Perfil do cliente
Fundada em 2022, a Kirvano é uma startup brasileira que oferece soluções de pagamento e gestão de vendas para criadores de conteúdo digital e empreendedores online. A plataforma se destaca pela facilidade de uso, tarifas competitivas e foco no cliente.

Indústria
Solução de pagamento para produtos e serviços digitais

Região
LATAM

A tecnologia da SHIELD detecta em tempo real e elimina todas as atividades fraudulentas, garantindo um ambiente confiável para os criadores de conteúdo digital. Essa parceria não só protege a plataforma, mas também impulsiona o crescimento dos negócios que dependem da Kirvano, reforçando sua missão de capacitar e apoiar o sucesso dos empreendedores digitais.

De ATO a fraudes de pagamento: as ameaças que afetam a Kirvano

Existem diferentes métodos que os fraudadores usam para atacar plataformas semelhantes à Kirvano.

Account takeovers (ATO) é uma tática comum que pode afetar tanto as contas dos criadores de conteúdo quanto as contas dos usuários (aqueles que compram os produtos/serviços oferecidos pelos empreendedores digitais). Utilizando técnicas como engenharia social e stuffing de credenciais, os fraudadores obtêm acesso a contas legítimas e podem:

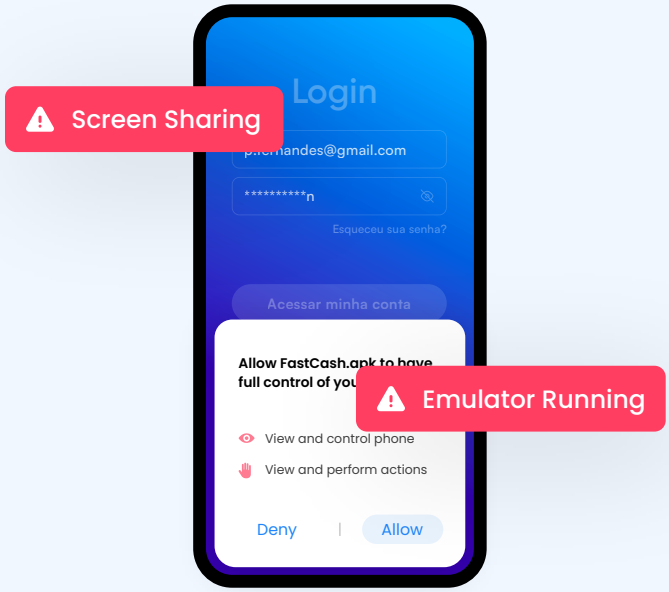
- **Contas de usuários:** Acessar informações de pagamento armazenadas na conta, como números de cartões de crédito, que podem ser usadas para atividades fraudulentas, como fraude de pagamento, ou até mesmo vendidas na dark web.
- **Contas de criadores de conteúdo:** Alterar informações pessoais e transferir o saldo disponível para sua própria conta bancária, levando a prejuízos financeiros.

Fraude de pagamento é outra ameaça significativa nessa indústria. Os fraudadores realizam transações não autorizadas usando contas falsas combinadas com informações sensíveis, como números de cartões de crédito, obtidas por meio de ataques de ATO, cartões de crédito roubados ou informações da dark web. Isso resulta não apenas em altas taxas de chargeback, mas também cria uma ilusão de um número maior de vendas, corroendo a confiança dos empreendedores digitais na plataforma.

Para impedir tentativas de ATO e fraudes de pagamento, a equipe da Kirvano conta com o **SHIELD Device ID**, que identifica persistentemente cada dispositivo físico que acessa a plataforma, eliminando a fraude em sua raiz. Ele detecta com precisão:

- **Múltiplas contas acessadas a partir de um único dispositivo:** Geralmente, as contas invadidas estão associadas a um único dispositivo operado pelo fraudador;
- **Dispositivos desconhecidos:** O surgimento repentino de dispositivos não reconhecidos logados na mesma conta ou múltiplos logins de diferentes locais;
- **Múltiplos endereços IP ou geolocalizações:** Se houveram múltiplas tentativas de login em uma única conta a partir de diferentes regiões geográficas.

Esses são sinais claros de tentativas de account takeover que a tecnologia da SHIELD pode detectar em tempo real para evitar esse tipo de fraude.



Além disso, o **Fraud Intelligence da SHIELD** monitora cada sessão de dispositivo, retornando sinais de risco em tempo real para fornecer uma visão completa da atividade do usuário na plataforma. Ela pode identificar o momento exato em que um usuário mostra sinais de comportamento fraudulento. Esse recurso permite a detecção de dispositivos que ativam ferramentas maliciosas, como emuladores e screen-sharings, frequentemente usadas em ataques de ATO e fraudes de pagamento.

Construindo uma plataforma confiável com a SHIELD

A Kirvano adotou uma postura proativa contra a constante evolução de fraudes ao fazer parceria com a SHIELD e implementar a solução de risco. Impulsionada por device fingerprinting e os mais recentes algoritmos de machine learning e IA, nossa solução fornece à Kirvano inteligência de dispositivos em tempo real. Isso capacita a equipe da Kirvano a detectar e mitigar ameaças rapidamente, protegendo os criadores de conteúdo digital.

"Com o Device Intelligence da SHIELD, conseguimos distinguir, de forma acurada, clientes genuínos de fraudadores. Nossa parceria com a SHIELD é fundamental para garantir segurança e impulsionar crescimento de negócio para os criadores de conteúdo digital que confiam na nossa plataforma", acrescentou Lorram Félix, CEO da Kirvano.