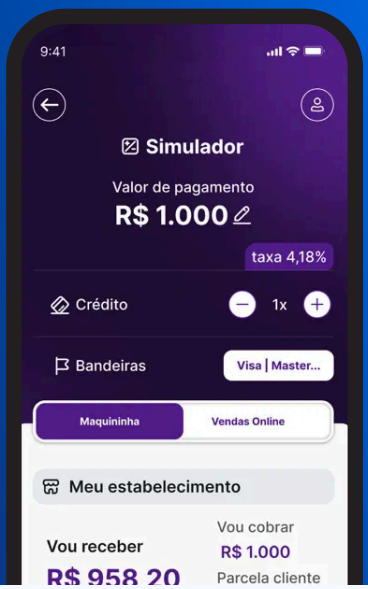
SHIELD | AQpago

Case Study

AQPago combate contas falsas e ATO com plataforma de inteligência de fraude da SHIELD



"Desde que implementamos o Device Intelligence da SHIELD, vimos uma mudança significativa na nossa capacidade de identificar dispositivos suspeitos e interromper tentativas de fraudes antes que afetem nossos usuários. A detecção de ferramentas maliciosas de alta precisão da SHIELD garante o bloqueio de atividades fraudulentas em um nível superior."

Luciano Fortuna
CEO, AQPago

Principais Resultados

99% de redução em tentativas de account takeover

100% de acurácia em detecção de ferramentas maliciosas

Aumento de confiança entre usuários e o app

Fortalecendo a Plataforma AQPago Contra Fraude

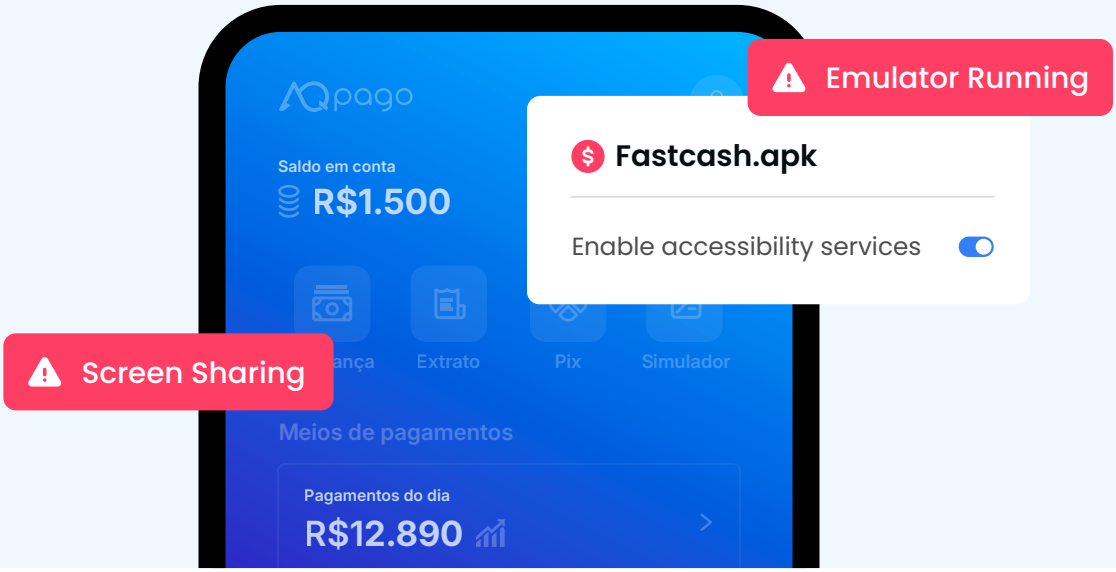
O setor financeiro se tornou principal alvo para fraudadores, impulsionado pelo alto volume de transações e pela rápida adoção de canais digitais. Fraudadores estão utilizando táticas cada vez mais sofisticadas para explorar vulnerabilidades nos sistemas digitais.

Com o crescimento de ataques de fraude cada vez mais sofisticados e enriquecidos por IA, a AQPago firmou uma parceria com a SHIELD para proteger seus clientes contra ameaças de forma proativa.
Ao implementar a **plataforma de Inteligência de Fraude** focada na identificação de dispositivos da SHIELD, a AQPago passou a detectar e prevenir fraudes antes que afetem os usuários.

Perfil do cliente
AQPago é uma fintech que fornece soluções de meio de pagamento para empresas de forma customizada e completa. A plataforma fornece gestão, acompanhamento e controle de vendas, soluções como: POS, TEF, Boleto, Split de Pagamentos, PIX,recorrência e, além disso, conta digital dos estabelecimentos credenciados.

Indústria
Serviços financeiros

Região
LATAM



Protegendo Contra Account Takeover

As invasões de conta (ou account takeovers, também conhecidos como ATO) custam bilhões às instituições financeiras e seus clientes, representando uma grande ameaça de fraude para o setor. Alguns dos métodos que os fraudadores usam para conduzir ATO incluem:

- **Ataques de Engenharia Social:** Nesses ataques, os criminosos enviam mensagens ou e-mails que parecem ser de fontes legítimas, como bancos. Essas mensagens geralmente contêm links para sites/apps falsos criados para coletar informações confidenciais ou enganar o usuário a instalar malware.
- **Abuso de Permissões de Acessibilidade:** Golpistas enganam usuários para instalar aplicativos maliciosos e conceder permissões de acessibilidade a esses apps. Ao fazer isso, o caminho é aberto para atividades fraudulentas, já que, através das permissões de acessibilidade, o fraudador tem controle do dispositivo para monitorar atividades e capturar informações sensíveis, como credenciais de login e números de cartão de crédito.

Em ambos os casos, o fraudador pode se infiltrar na conta bancária da vítima com os dados roubados, facilitando transações fraudulentas e o roubo de fundos.

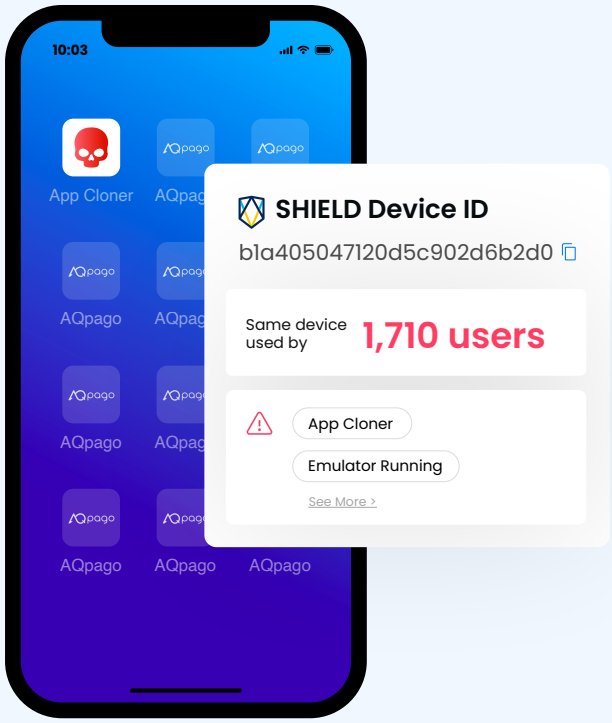
Com o uso do Device Intelligence da SHIELD, a AQPago consegue interromper a fraude antes que ela aconteça. As capacidades avançadas de detecção da SHIELD, impulsionadas pelo **SHIELD Device ID**, identificam dispositivos envolvidos em atividades suspeitas e bloqueiam o acesso com base em indicadores de alto risco, como dispositivos desconhecidos, localizações incomuns ou redes não reconhecidas, prevenindo tentativas de ATO.

A SHIELD também permite que a AQPago detecte ferramentas como **emuladores** e aplicativos de **compartilhamento de tela**, que são usados em ataques de ATO, fornecendo sinais de fraude em tempo real e monitorando continuamente as sessões dos dispositivos. Isso capacita a AQPago a identificar dispositivos de risco com precisão, sem a necessidade de coletar informações pessoais identificáveis.

Eliminando Contas Falsas Para uma Plataforma Mais Confiável

Fraudadores conseguem criar contas falsas usando dados roubados ou comprados na dark web e utilizam ferramentas como **clonadores de aplicativos** e emuladores para criá-las em escala.

Essas contas fraudulentas são usadas para transferir fundos de forma ilícita ou solicitar empréstimos que nunca serão pagos. A proliferação de contas falsas abala a confiança entre instituições financeiras e seus clientes, levando a prejuízos financeiros, multas regulatórias e danos à reputação da instituição financeira.



A plataforma de Inteligência de Fraude focada na identificação de dispositivos da SHIELD permite que a AQPago detecte de forma proativa dispositivos suspeitos durante toda a jornada do usuário, identificando casos de multi-contas associadas a um mesmo dispositivo.

"A segurança da AQPago é a segurança do nosso cliente, por isso, acreditamos no poder da tecnologia da SHIELD para evitar fraudes, golpes e movimentações financeiras indevidas nas contas dos nossos usuários, aumentando a confiabilidade das transações e acessos realizados em nosso app", comenta Robson Marques, VP de Negócios e Compliance na AQPago.

"Desde que implementamos o Device Intelligence da SHIELD, vimos uma mudança significativa na nossa capacidade de identificar dispositivos suspeitos e interromper tentativas de fraudes antes que afetem nossos usuários. A detecção de ferramentas maliciosas de alta precisão da SHIELD garante o bloqueio de atividades fraudulentas em um nível superior", finaliza Luciano Fortuna, CEO na AQPago.