SHIELD | AQpago

Case Study

AQPago Combats Fake Accounts & ATOs with SHIELD's Device-First Fraud Intelligence

Valor de pagamento
R$ 1.000
taxa 4,18%
Crédito 1x
Bandeiras Visa | Master...
Vou receber R$ 958,20
Vou cobrar R$ 1.000
Parcela cliente

> "Since implementing SHIELD's Device Intelligence, we've seen a transformational shift in our ability to pinpoint suspicious devices and stop fraud attempts before they impact our users. SHIELD's high-accuracy malicious tool detection means that we're blocking fraudulent activities at an advanced level."

Luciano Fortuna
CEO, AQPago

Key Takeaways

Achieved **99% reduction** in account takeover attempts

100% accuracy in detecting malicious tools

Increased trust between users and the app

Strengthening AQPago's Platform Against Fraud

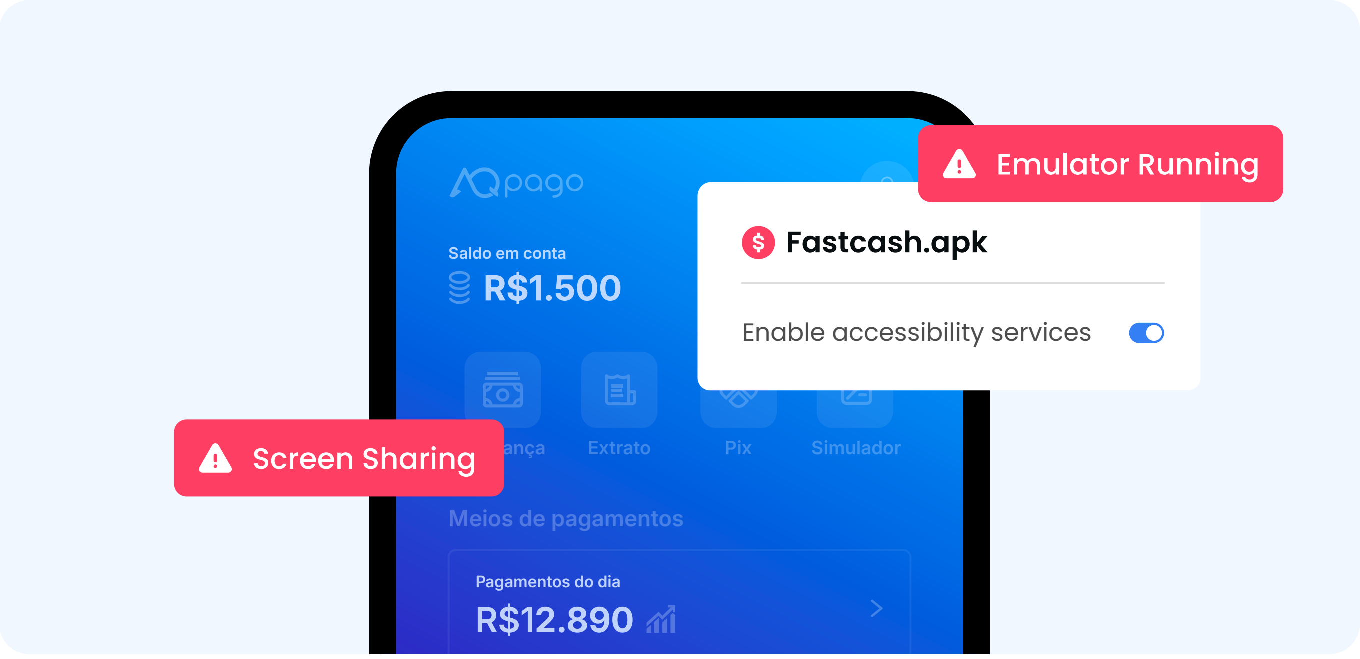
The financial sector has become a prime target for fraudsters, fueled by the surge in transaction volumes and the rapid shift toward digital banking. Fraudsters are leveraging increasingly sophisticated tactics, including AI-driven attacks, to exploit vulnerabilities in digital systems.

To combat this growing threat, AQPago took a proactive approach by partnering with SHIELD to protect its customers. Through **SHIELD's Device-First Fraud Intelligence** platform, AQPago fortified its defenses, enabling real-time detection and prevention of fraud before it could harm users. This partnership not only safeguards customers but also reinforces trust, ensuring a seamless and secure experience across digital transactions.

Customer Profile
AQPago is a fintech company that offers customized, end-to-end payment solutions for businesses. The platform provides robust tools for payments management, monitoring, control of the sales and digital accounts of accredited establishments in the network.

Industry
Financial Services

Region
LATAM



Defending Against Account Takeover

Account takeovers (ATO) cost financial institutions and their customers billions, representing a major fraud threat to the sector. Some of the methods fraudsters use to conduct ATO include:

- **Social Engineering Attacks:** In these attacks, fraudsters send messages or emails that appear to be from legitimate sources, such as banks. These messages often contain links to fake websites/apps designed to collect confidential information or trick the user into downloading and installing malware.
- **Accessibility Permission Abuse:** Scammers deceive users into installing malicious apps and granting accessibility permissions to these apps. Doing so paves the way for further fraudulent activities. Once installed, the app requests accessibility permissions, giving the fraudster control of the device to monitor activities and capture sensitive information, such as login credentials and credit card numbers.

In both cases, the fraudster can infiltrate the victim's bank account with the stolen data, facilitating fraudulent transactions and stealing funds.

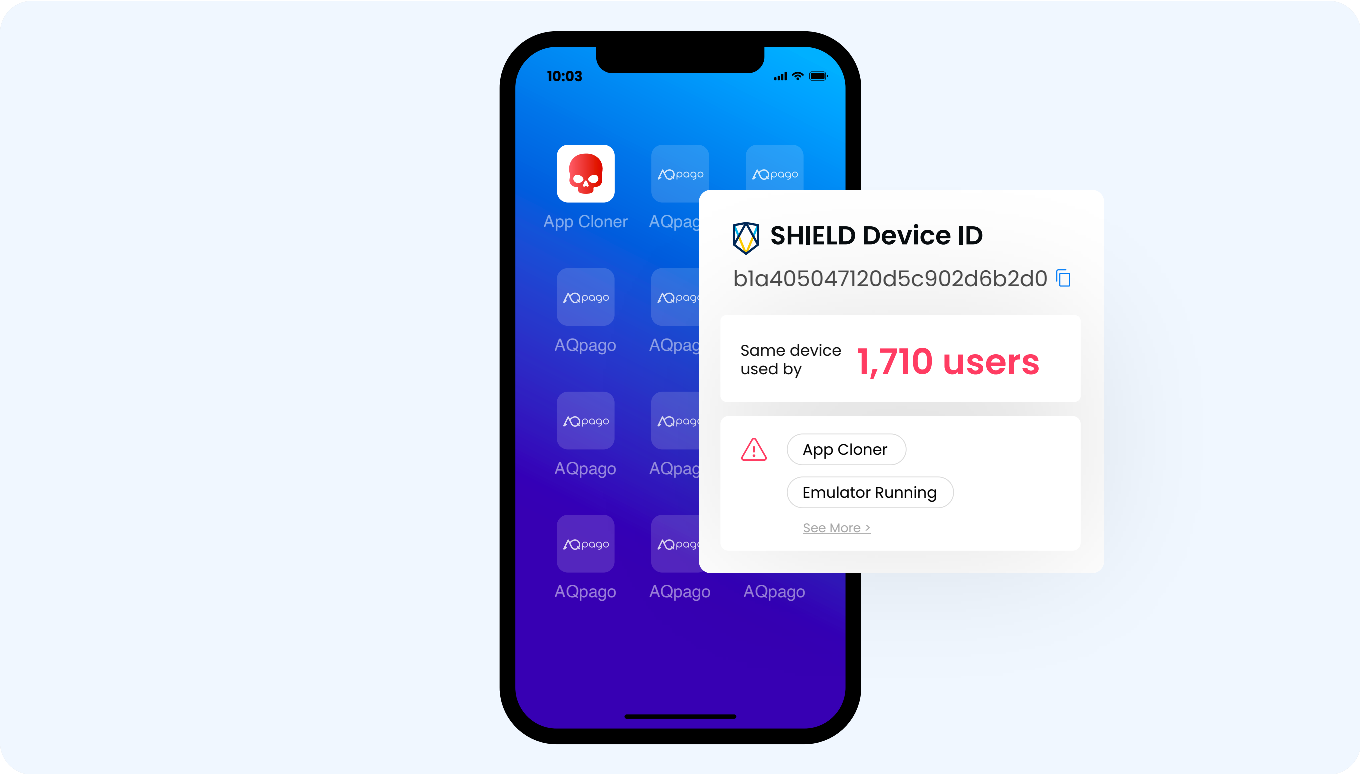
By leveraging SHIELD's Device Intelligence, AQ Pago is able to stop fraud at its root. SHIELD's detection capabilities, powered by the **SHIELD Device ID**, identify devices involved in suspicious activities and block access based on high-risk indicators such as unfamiliar devices, unusual locations, or unrecognized networks, preventing ATO attempts.

SHIELD also enables AQPago to detect tools like **emulators** and **screen-sharing** apps that are commonly used in ATO attacks, providing real-time fraud signals and continuously screening device sessions. This empowers AQPago to accurately pinpoint risky devices, without requiring any personally identifiable information.

Eliminating Fake Accounts for a More Trusted Platform

Fraudsters can create fake accounts using stolen or purchased data from the dark web, utilizing tools like **app cloners** and emulators to create them at scale.

These fraudulent accounts are used to transfer funds illicitly or apply for loans that will never be repaid. The widespread use of fake accounts undermines trust between financial institutions and their customers, resulting in significant financial losses, regulatory fines, and reputational damage.



SHIELD Device ID

b1a405047120d5c902d6b2d0

Same device used by 1,710 users

App Cloner

Emulator Running

See More ›

SHIELD's Device-First Fraud Intelligence platform empowers AQPago to proactively detect suspicious devices throughout the user's journey, identifying instances of multi-accounting coming from the same device.

"AQPago's security is our clients' security. That's why we rely on SHIELD's technology to prevent fraud, scams, and unauthorized financial activity on user accounts, boosting the reliability of transactions and app access", said Robson Marques, VP of Business and Compliance at AQPago.

"Since implementing SHIELD's Device Intelligence, we've seen a transformational shift in our ability to pinpoint suspicious devices and stop fraud attempts before they impact our users. SHIELD's high-accuracy malicious tool detection means that we're blocking fraudulent activities at an advanced level", added Luciano Fortuna, CEO at AQPago.