smartid

Intelligent fraud prevention

Zero friction

AI Platform for digital banking
+125 billion transactions · +12 billion protected sessions

Financial Fraud in LATAM

Causes millions in losses across LATAM.

Traditional solutions are no longer enough.

Our Suite has achieved zero fraud in electronic channels for our clients.

SmartID is a cloud-based security service powered by Artificial Intelligence that identifies users, devices, and transactions, enabling real-time prevention of cyber fraud

smartid

Digital fraud in LATAM
IS GROWING EXPONENTIALLY

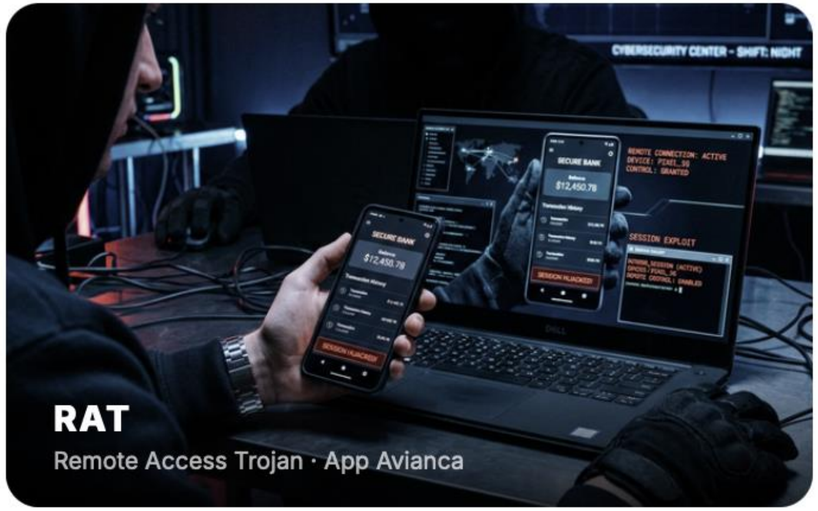
Alarming Increase
83% increase in fraud reports by financial organizations in LATAM — Kaspersky 2025

4X Mobile Malware
Banking trojans on smartphones quadrupled in 2025 vs 2024. — Kaspersky 2025

3x Device Theft
Fraud cases from stolen or compromised devices tripled in the region. — BioCatch 2025

Real fraud cases in LATAM

LAST 3 MONTHS

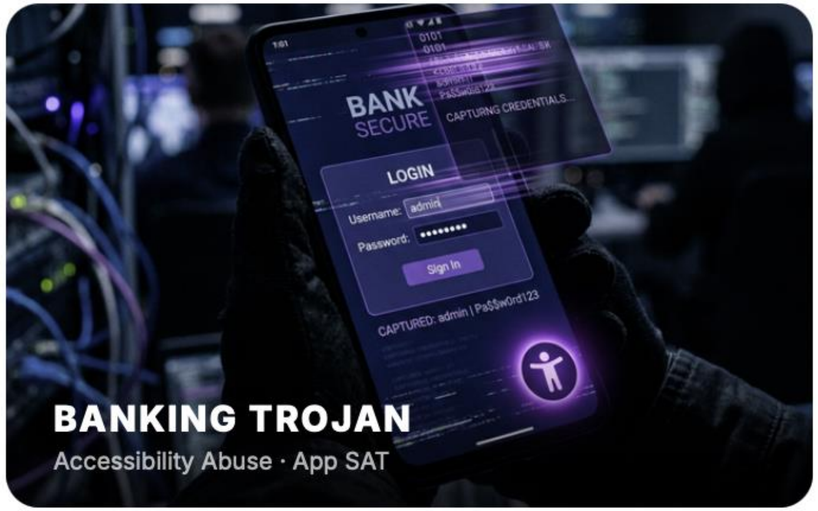


RAT

Remote Access Trojan · App Avianca

SPYWARE

Info-Stealer



BANKING TROJAN

Accessibility Abuse · App SAT

INJECTION ATTACK

Bypass biométrico · Deepfake / Video

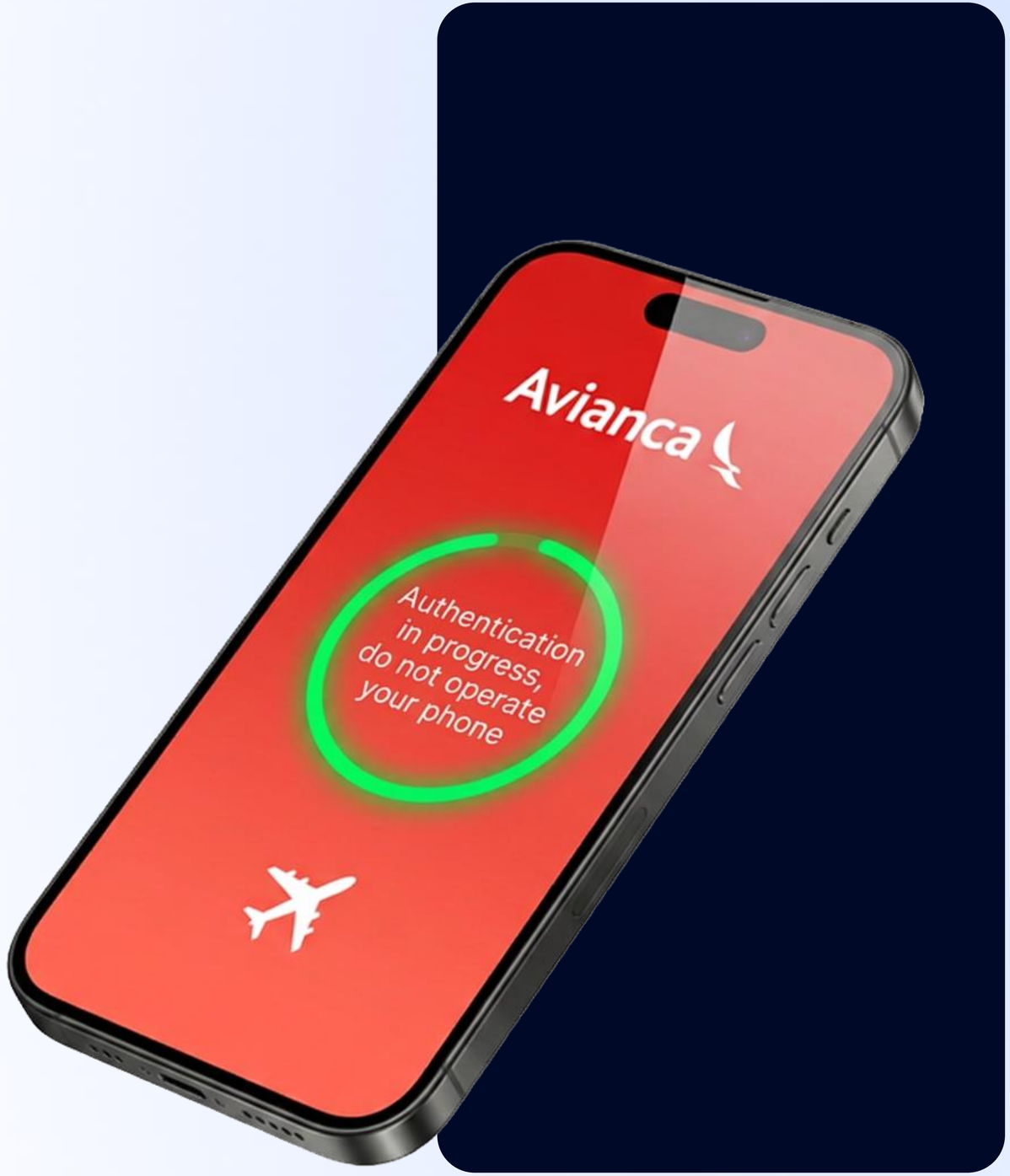
smartid

RAT – December 2025

APP AVIANCA

The user downloads a fake Avianca app containing a RAT (Remote Access Trojan). Once installed, the attacker takes **remote control of the device in real time**: enables screen sharing and displays a fake screen (overlay) covering the banking app. While the user thinks they see their normal banking, the attacker operates the account behind the scenes — transferring funds, changing passwords, or registering new beneficiaries.

- **Remote access tool identification.**
- **Detection of device screen being streamed to a third party.**



smartid

SPYWARE – December 2025

APP REWARDS

The user receives a link to a fake app that simulates a bank rewards program. **This malware operates completely silently in the background**.

Silently read SMS to intercept 2FA codes
Record camera and microphone capturing conversations and faces
Extract the contact list to spread the attack to more victims

- **We verify device integrity at the Google level**
- **Device binding**
- **Velocity Checks + Geo-Anomaly Detection**

BANKING TROJAN – January 2026

APP SAT

The user downloads a fake SAT app that requests enabling the **Accessibility Service** on Android. Once active, the trojan monitors the screen in real time, detects when the banking app is opened, automatically captures credentials, and executes transfers without human intervention. This is the same vector used by Grandoreiro and BrasDex — the most dangerous banking malware families in Latin America.

- **Detection of unauthorized applications with accessibility services**

smartid

INJECTION ATTACK – Feb 2026

VIRTUAL CAMERA

The attacker uses a virtual camera to feed a deepfake or pre-recorded video directly into the bank's biometric verification process. The system believes the person is physically present when in reality it receives a synthetic identity generated by AI. It does not require malware or device access — it is a direct attack against the liveness check.

- **Virtual camera detection**
- **Injected stream.**
- **Active/passive liveness check**
- **Deepfake Score**

smartid

Comprehensive solution

DEVICE RECOGNITION

IDENTITY VERIFICATION

OPERATIONS AND TRANSACTIONS MONITORING

AI & MACHINE LEARNING

MULTIFACTOR AUTHENTICATION

smartid

How does it work?

Integrated cybersecurity strategy and regulatory compliance

BEFORE LOGIN

Spoofing Prevention

We evaluate the device before permitting access: root, jailbreak, emulators, VPN, malicious apps, virtual cameras, liveness and deepfake detection.

52+ signals in <100ms

DURING THE SESSION

Session Intelligence

We profile each user's behavior. We detect anomalies: impossible location, new device, unusual interaction rhythm, rhythm, remote access.

Continuous 24/7 monitoring

AT EACH TRANSACTION

Transaction Risk Scoring

A risk score of 0-100 per operation, combining device signals, user history and context. Automatic and intelligent decisions.

Configurable rules engine

smartid

Proven results
in the region

+95%
Fraud detection accuracy

+125B
Protected transactions

+12B
Protected sessions

Zero friction – the legitimate user does not notice the protection

Does not replace – adds to your current security stack

360° Console – Full visibility of devices, sessions, and transactions

Lightweight SDK – Integration in days, < 200kb

Experience with banks in the region

ISO27001 Certification in information security

smartid

30-day pilot

no integration cost

In 30 days you will see exactly how many attacks you are not detecting today and how many false positives you can eliminate.

https://smartidsuite.ai sales@smartidsuite.ai ISO 270001 Certified