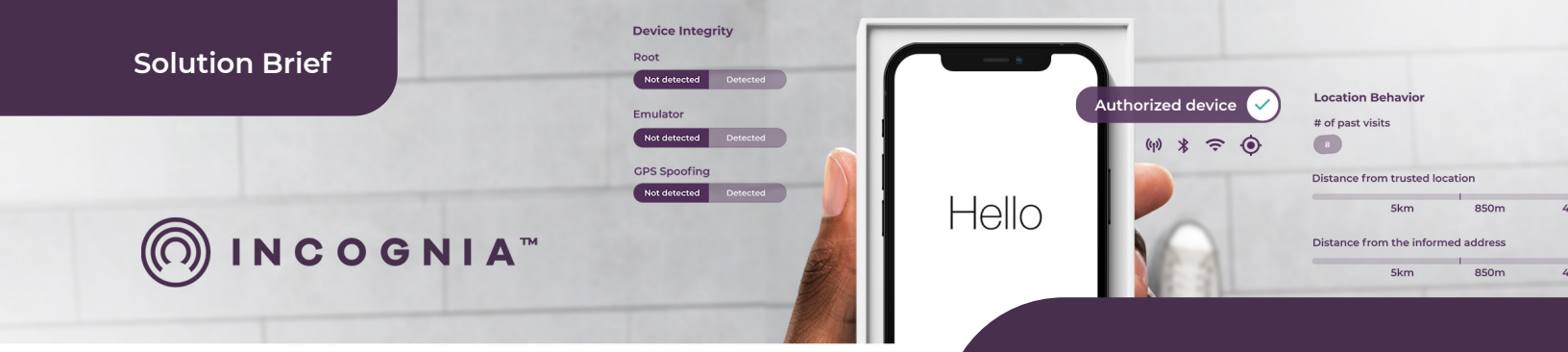
Solution Brief



Location-based Device Authorization

Establishing Trust in New Devices at Login and Onboarding

Challenges

New device authorization on mobile is one of the highest friction and highest risk points in the user journey. When new devices attempt a login, the challenge is determining whether this is the legitimate user, or a fraudster using stolen credentials. Traditional device fingerprinting solutions are useless in establishing trust in new devices since they have no knowledge of the device. As a result, most organizations have been forced to employ multi-factor authentication, increasing user friction and creating a poor user experience, which frequently results in the user requiring customer support.

One of the main contributors to friction and fraud for new device authorization is that the majority of mobile apps use one time password (OTP) over SMS, which has proven to be an insecure and unreliable channel. Many SMS messages are not received due to carrier and signal availability issues, leaving the user without access to their account. At the same time, fraudsters are capitalizing on SIM swap fraud, social engineering, and phishing to obtain OTP codes to access accounts from their phones and succeed at account takeovers.

As a result, in most mobile apps today, the device authorization process adds unwanted friction for legitimate users, and inadequate security to keep fraudsters out.

Solution

The Incognia **Location-based Device Authorization** solution is designed to address the challenges of establishing trust in new devices without adding user friction. Incognia is highly effective at protecting accounts from fraudulent device changes and SIM swap fraud, while recognizing those instances when legitimate users are accessing existing accounts from new devices.

Incognia provides a highly accurate risk signal using **anonymized location behavior and device intelligence** to detect high risk devices attempting to login before fraud happens. Each user has a unique location behavior pattern that comprises locations that they visit frequently and are considered the user's "trusted locations". Based on data from over 200 million devices using Incognia, 89% of legitimate device changes occur at trusted locations. When Incognia detects a user is in a trusted location, there is a higher probability of the transaction being legitimate and at lower risk for fraud, offering the opportunity of a frictionless authentication experience.

Solution

Going beyond traditional device fingerprinting solutions, **Incognia Location-based Device Authorization** analyzes both device integrity and device location behavior to deliver a highly accurate risk score.

Location Behavior

Incognia checks the consistency of the location behavior between the new device and former devices, and whether the login is occurring from a trusted location for that user.

Device Integrity

Incognia checks device characteristics including detection of the presence of emulators, rooted or jailbroken devices and use of location spoofing techniques.

Account Access

Incognia checks association between devices, re-installations and accounts, to assess if the same device is being used across multiple accounts, or an account is being accessed by multiple devices.

Watchlists

Incognia maintains Watchlists of devices and locations that have previously been associated with fraud, based on its network of over 200 million devices. All Incognia risk assessments cross reference these watchlists, enabling customers to block untrusted devices.

Key Benefits

Reduce Account takeovers due to fraudulent mobile device changes
Incognia Location-based Device Authorization goes beyond traditional device fingerprinting in assessing not only a device's integrity, but also its location behavior. Incognia establishes trust by understanding the relationship between the user's devices and location behavior. This enables apps to accurately assess risk whenever a new device attempts to login and access services.

Reduce friction when good users change their mobile device
Incognia Location-based Device Authorization solution provides a zero friction solution to detect a legitimate user whenever they decide to change their mobile phone. Incognia's solution is based on comparing the user location at the time of device change with the historical user location behavior.

Reduce friction at every login with zero-factor authentication
Incognia's advantages are not limited to the mobile device change use case. Incognia works silently in the background to enable zero friction, Zero Factor Authentication by leveraging location identity signals to deliver a highly accurate risk assessment at every login.

How it Works

Incognia's Location-based Device Authorization works silently in the background assessing risk when a user attempts to login with a new device.

At Onboarding:
Incognia delivers a risk assessment based on the device integrity check and also how far the current device location deviates from the onboarding address submitted by the user. If the device is at or near the address submitted by the user address, a low risk assessment is returned. If the device current location is not at or near the submitted address a high risk assessment is returned.

At Login
Incognia delivers a risk assessment based on the device integrity check and also how far the current device location deviates from the user's historical location pattern. If the device is at or near a trusted location for that user, a low risk assessment is returned. If the user's current location is not at or near a trusted location, a high risk assessment is returned. Trusted location parameters, including the number of visits required to establish a trusted location, as well as acceptable proximities or distances from trusted locations, are adjustable.

Key Features

Real-time validation of user trusted devices
- Supports iOS and Android mobile devices

Works in any geography
- Global location validation coverage

Highly accurate risk-assessments
- Location fingerprint and device integrity
- Behavior watchlist and network effect

Lightweight SDK
- 415 KB (Android)
- 1.5 MB (iOS)
- Battery usage: ~0.5% per day

Easy to integrate and use APIs & Webhook
- REST & JSON Response
- Average response time: 60 ms
- Low latency of the Incognia APIs

Advanced technical support
- Open documentation
- API reference
- How-To Guides
- Developer Portal

Privacy and Security
- GDPR, CCPA and SOC II Level 2 Compliant
- Use stand-alone or integrate to your risk-engine

About Incognia

Incognia is a privacy-first location identity company that provides frictionless mobile authentication to banks, fintech and mCommerce companies, for increased mobile revenue and lower fraud losses. Incognia's award-winning technology uses location signals and motion sensors to silently recognize trusted users based on their unique behavior patterns and is a key enabler for Zero-Factor Authentication. Deployed in over 200 million devices, Incognia delivers a highly precise risk signal with extremely low false positive rates.