CASE STUDY - BRAZILIAN FINTECH

Asaas uses Darwinium to build end-to-end trust across the customer journey, reducing friction for good customers

↑ 97%

Darwinium Digital Signatures for devices and behavioral biometrics increased returning user recognition to 97% at login

94%

94% of returning users received a positive trust score using Darwinium models

↓ 46%

46% reduction in use of one-time passcodes (OTPs), with associated cost savings

49

Darwinium's entity linkage uncovered an account takeover network that executed 49 attempts in two days

Business Problem: Lack of customer trust creates high-friction user experience

Asaas, a Brazilian fintech specializing in business banking, was struggling to verify its online users' authenticity.

- The existing device fingerprinting solution had poor persistency, resulting in excess challenges at login via a one-time passcode (OTP).
- This increased friction for good customers, and required significant operational resource and budget.

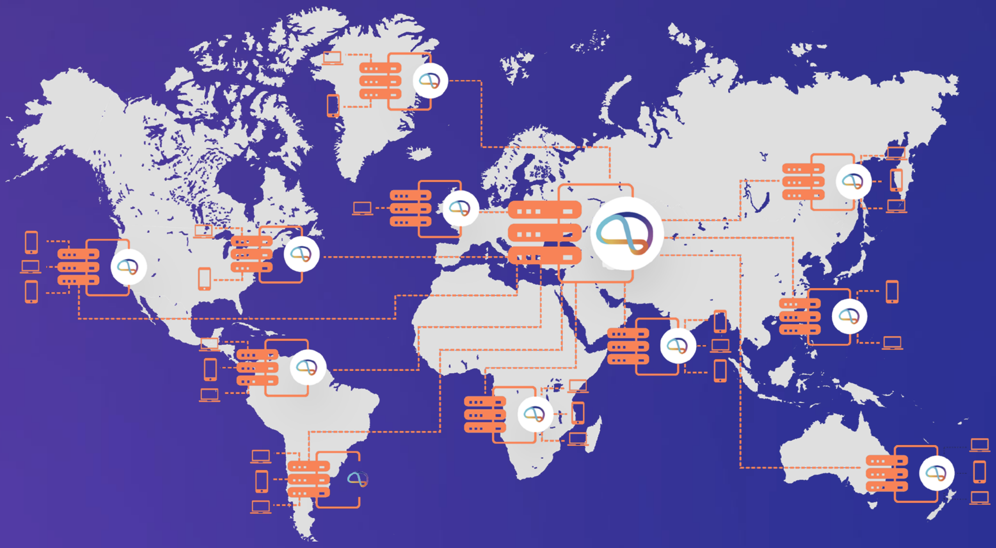
Asaas wanted a better way to improve UX while keeping accounts secure, reserving OTPs for genuinely high-risk interactions.

Several other fraud solutions had been discounted due to the high cost of covering multiple touchpoints in the customer journey.

The Darwinium Difference: Deploying at the edge provides full visibility of customer behavior

Asaas recognized the benefits Darwinium could deliver by deploying via a content delivery network (CDN), and decided to install AWS CloudFront. The Darwinium professional services team supported this implementation as part of the wider deployment.

Deploying at the edge allowed Asaas to collect hundreds of pieces of data relating to the user's network connection, device, location, transactions and journey analytics to establish a baseline of normal, trusted behavior. This benchmark was used to verify all future signup and login events, which established trusted versus riskier groups.



Darwinium

Business Benefits:

Complete customer journey visibility

Asaas could profile behaviors from the moment a customer registered for an account, through every interaction they made pre- and post-authentication, all via one simple integration.

Shorter time to value

Despite being new to CloudFront, deploying on the edge significantly reduced the time and effort associated with profiling the complete customer journey.

Superfast profiling

Distributing Darwinium decisioning via AWS CloudFront meant processing was reduced to microseconds, and served closer to end users' locations.

Cost efficiency

Operational costs fell as a result of deploying once, and then scaling simply across customer journeys from within the Darwinium portal.

Enhanced privacy

Asaas had the option of storing encrypted personally identifiable information (PII) in its own S3 bucket.

Key Product Capabilities:

Industry-leading device recognition and behavioral analytics using Darwinium Digital Signatures:

- Darwinium helped Asaas simplify customer recognition with proprietary Digital Signatures, allowing devices and behavioural biometrics to be compared just by similarity.
- These Digital Signatures provided the backbone for recognizing more users. Rather than a fixed identifier, the signatures can be compared in real time for percentage similarity. This gave Asaas the ability to test and choose their similarity threshold that optimized challenge rates with customer experience.
- This entity linking capability in the Darwinium portal detected an account takeover fraud ring that might otherwise have been missed.
- The similarity cluster view easily identified another IP within the same network that is performing the exact same credential stuffing / account takeover behavior.
- 49 account takeovers were confirmed within the overall network.

Key Product Capabilities (continued):

Continuous customer journey orchestration to reduce operational overheads:

- Darwinium's open, extensible platform allows the configuration of complete user journeys and data mapping within the product, rather than needing development resource to implement profiling and API calls on every web page.
- This removed the operational burden of relying on engineering or IT resource to make and maintain those points.
- Organizations can also conditionally enrich risk decisions with any third-party data, as well as via custom integrations in the app store.

Decision and action in real time with a flexible decision engine:

- Darwinium provides a powerful, real-time and extensible feature store. This means that Asaas was able to track statistical aggregates and risky behaviors over different lookback tmeframes.
- Asaas initially leveraged model templates for device recognition, and can now train, optimize and deploy both existing and new machine learning models.
- Darwinium removes the constraint of inflexible or obscure vendor scores, replacing these with models and scores that are open to trace, configure and update natively in the Darwinium portal.

About Darwinium

Darwinium unites digital security with fraud prevention across every customer journey, protecting your end users from fraud, scams and online abuse. With full visibility of trust and risk across your entire digital estate, businesses can accurately separate good and bad behavior, removing the reliance on 'point-in-time' API-based solutions that are vulnerable to exploitation. Combine continuous fraud analytics with customer journey orchestration to make better risk decisions, and take real-time action on evolving threats, via one simple integration.

For more information, email
contact@darwinium.com

darwinium.com

To see Darwinium in action
Take a Tour of the platform