Frictionless Cybersecurity and Fraud Prevention for Global Fintech Company

Learn how Darwinium helped this global fintech company build end-to-end trust across the customer journey to reduce budget, operational resources, and good-customer friction.

Overview

A prominent global fintech company, specializing in business banking services, wanted to improve its user experience. However, the company struggled with excess challenges at login which increased friction for good customers while consuming operational resources and budget. The company turned to AWS Partner Darwinium, a next-generation cyberfraud and fraud platform. Soon after deployment, they increased returning user recognition to 97% while 94% of returning users received a positive trust score. This led to a reduction in one-time passcodes (OTPs). In addition, within a two-day period, Darwinium uncovered and blocked 49 attempted account network takeover attacks.

Frictionless UX vs. Total Security Across the Customer Journey

A leading global fintech company was grappling with what appeared to be two contradictory imperatives: provide a frictionless user experience while maintaining tight end-to-end security throughout the customer journey. In particular, the company struggled to verify its online users' authenticity because its existing device fingerprinting solution had poor persistency (ability to identify and track a user across multiple logins and devices over time) resulting in excess challenges at login via one-time passcodes (OTPs). This created burdensome friction for good customers while eating up significant operational resources and budget. They needed a solution that would significantly reduce friction across the customer journey while keeping accounts secure and reserve OTPs for genuinely high-risk interactions.

About Global Fintech Company

This global fintech company is a complete digital account services business. Beyond traditional banking and payment services, they help businesses automate and streamline financial processes and communication between a company and its customers to reduce manual work and administrative tasks, slash receivable default rates, increase profits and cash flow, and boost productivity while minimizing bureaucracy.

This dilemma is nothing new to AWS Partner Darwinium. The company's customers face increasingly complex challenges made worse by the ability of fraudsters to outpace legacy cybersecurity solutions. Further, Darwinium' s customers operate within the banking, financial, e-commerce, payments, and travel & hospitality industries where preserving a strong online reputation is just as critical as delivering an exceptional customer experience to maintain and grow loyalty and revenue. Darwinium customers often find that many fraud solutions are siloed and lack the agility to address threats proactively while also slowing fraud protection efforts and draining resources due to the engineering effort.

Aligning User Experience with Best-in-Class Security

After a period of due diligence, the company recognized that Darwinium offers the best of both: enhanced user experience with top-class security. In particular, the Darwinium cybersecurity and fraud prevention platform deployed on Amazon CloudFront is the only solution that unites security, fraud, and abuse with coverage across an organization's digital perimeter, including CDN, web, mobile, and APIs. Deploying Darwinium at the edge would allow the fintech to collect hundreds of pieces of data relating to a user's network connection, device, location, transactions, and journey analytics to establish a baseline of normal, trusted conduct. This benchmark is then used to verify all future signup and login events which establishes trusted versus riskier groups.

Key capabilities include Darwinium Digital Signatures which compare device, location, behavior and journey intelligence based on the context of the transaction. Businesses can look beyond fixed identifiers to identify similar patterns of behavior that can indicate either trust or risk. This provides a backbone for recognizing more users and empowers organizations to test and choose a similarity threshold that optimizes challenge rates with customer experience. Darwinium's Continuous Customer Journey Orchestration configures complete user journeys and data mapping within the product rather than devoting development resources to implement profiling and API calls on every web page. This removes the operational burden of relying on engineering or IT resources to make and maintain these points. The Darwinium's Flexible Decision Engine provides a powerful, real-time, and extensible feature store so that companies like this global fintech company can track statistical aggregates and risky behaviors over different lookback timeframes.

> **"AWS provides the core edge, networking, and storage infrastructure for our customers to implement and fight fraud at the Content Delivery Network (CDN) and across the customer journey in a privacy-first manner."**
>
> **Ben Davey**
> Global Head of Product, Darwinium

They can also move from inflexible or obscure vendor scores to models and scores that are open to trace, configure, and that update natively in the Darwinium portal. In addition, organizations can conditionally enrich risk decisions with any third-party data as well as via custom integrations.

A Secure and Enhanced User Experience

With Darwinium, the fintech company is able to proactively respond to new and evolving threats in real time rather than react to them after they have impacted customer accounts. The company is also able to provide a near-frictionless user experience with a solution that is simple to maintain and can adapt to new threats in real time.

Critical benefits include complete customer journey visibility: they can profile behaviors from the moment a customer registers for an account, through every pre- and post-authentication interaction, all in one simple integration. Shorter time to value: despite the company being new to Amazon CloudFront, deploying on the edge significantly reduces the time and effort associated with profiling the complete customer journey. Superfast profiling: by distributing Darwinium Decisioning via AWS CloudFront, processing is reduced to microseconds and served closer to the end users' locations. Cost and efficiency: deploying once and then scaling across customer journeys from within the Darwinium portal significantly reduced operational costs. **Enhanced privacy:** The company now has the option of storing encrypted personally identifiable information (PII) in its own Amazon Simple Storage (S3) bucket.

Better yet, the company achieved as close to a frictionless user experience as possible: 97% increase in returning user recognition, 94% of returning users receive a positive trust score, and a 46% reduction in the use of OTPs with associated cost savings. Simply stated: Darwinium bridged the divide between compete security across the user journey with a near frictionless user experience.

90%
increase

in returning user recognition using Darwinium device and behavioral fingerprinting at login

94%
receive a postive trust score

using Darwinium models

46%
reduction

in use of one-time passcodes (OTPs) with associated cost savings

49
account takeover attempts in 2 days

uncovered and blocked by Darwinium entity linkage

About Darwinium

San Francisco-based Darwinium is a next-generation cybersecurity and fraud prevention platform. The platform unifies intelligence across users' online journeys, orchestrates comprehensive data, and drives continuous analysis through an advanced decision engine. Darwinium protects against fraud, scams and online abuse, minimizes potential losses, and ensures a seamless secure experience for legitimate users across every digital interaction.

To learn more, visit www.darwinium.com