

# E-Signature Leader Stops Credential Stuffing Cold and Protects Millions of User Accounts

One of the world's leading e-signature and document workflow platforms, this organization serves hundreds of millions of users globally. The sensitive personal and financial data stored within its documents makes it a high-value target for account takeover attacks.



## The Challenges

**Credential Stuffing at Scale:** Attackers targeted the sign-in flow to compromise user accounts and access sensitive documents containing social security numbers, financial account details and other valuable personal information.

**Legacy Solution Failing:** The incumbent fraud prevention tool couldn't keep pace with modern bot capabilities. Off-the-shelf bot programs using advanced machine vision were routinely bypassing its detection engine.

**Gaps in Malicious IP Recognition:** The existing solution lacked the detection breadth to identify and challenge the full volume of malicious traffic reaching the platform, leaving significant exposure.



## The Arkose Titan Solution

**Incumbent Displaced via Parent Company Referral:** Arkose Titan was already in use by the company's parent organization, which recommended the platform based on its proven effectiveness protecting 700 million users against sustained fraud attacks.

**Login Flow Protection:** Arkose Titan was deployed on the login flow, detecting and stopping malicious traffic before it could reach the authentication point — with immediate results.

**Bot-Proof Enforcement:** Suspicious sessions were served real-time enforcement challenges purpose-built to defeat machine vision technology, causing all automated attacks to fail regardless of the tools attackers used.

**24/7 SOC Partnership:** The Arkose customer success team worked around the clock with the client to deliver actionable insights and tailored solutions calibrated to the specific threats the platform faced.



## Business Results

**Immediate Stop to Credential Stuffing:** Attacks dropped sharply upon deployment, delivering fast, measurable ROI from day one.

**Millions of User Accounts Protected:** Sensitive documents containing personal and financial data were secured across the platform's global user base.

**Zero Impact on Good Users:** Legitimate users experienced no added friction, maintaining the seamless digital experience the platform is known for.

"After implementing Arkose Labs, we saw an immediate ROI. The credential stuffing attacks stopped, and they have been a great partner with us in fighting fraud."

— Engineering Manager

**SCHEDULE CALL  
WITH AN EXPERT**

Arkose Labs is the leading global provider offering a proactive fraud deterrence platform purpose-built to neutralize modern attacks, including those powered by Agentic AI and large language models (LLMs). Its comprehensive solution combines proprietary device identification (device ID), behavioral analysis, phishing protection, email intelligence, scraping prevention, API defense and bot management. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America. © 2026 Arkose Labs. All rights reserved.