Major U.S. Bank Eliminates Unknown Sessions and Saves Six Figures

One of the largest and most established U.S. financial institutions faced dual bot-related threats: significant account takeover attacks compromising consumer accounts and increasing volumes of unknown sessions driving costly downstream fraud analysis.

The Challenges

Persistent Account Takeover Attacks: Massive bot-based ATO attacks compromised consumer accounts despite layered security with Akamai and LexisNexis ThreatMetrix, eroding customer trust.

Unknown Session Crisis: Increasing volumes of unknown sessions (blank session IDs with no profile information) created material risk and prevented accurate traffic assessment, while operational costs skyrocketed.

Downstream Data Pollution: Junk data from unknown sessions flooded existing security tools, reducing effectiveness of the security stack.

The Arkose Titan Solution

Strategic Stack Positioning: Deployed Arkose Titan platform between Akamai and ThreatMetrix at top-of-funnel stages (sign-in, sign-up), bridging gaps in existing security infrastructure and reducing costly risk analysis on irrelevant data.

Comprehensive Risk Monitoring: Leveraged 225+ risk signals using progressive device and behavioral fingerprinting to detect account takeover, credential stuffing, fake account creation and phishing threats before impact.

Adaptive Challenge-Response: Deployed intelligent challenge suite to determine user authenticity, classifying and triaging traffic based on risk profile.

Business Results

Immediate Unknown Session Reduction: Steep drop-off in unknown session volumes, eliminating confusing empty traffic that previous solutions couldn't profile.

Six-Figure Cost Savings: Saved hundreds of thousands of dollars in downstream fraud detection costs by stopping junk data before it reached expensive analysis tools.

Virtually Eliminated Bot-Based ATO: Detected and stopped automated account takeover attacks, restoring consumer confidence in digital banking security.

Proven Defense-in-Depth Value: Demonstrated that Arkose Titan platform working alongside Akamai and ThreatMetrix delivers superior results through strategic "better together" approach.

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.