Arkose Labs | SOLUTION BRIEF

Credential Stuffing

Reduce account takeovers while improving customer satisfaction

Credential stuffing attacks have emerged as a formidable threat to global business security, with an astonishing 193 billion attacks recorded worldwide in a single year. This surge in malicious activity not only jeopardizes sensitive customer data but also poses severe risks to organizational integrity and consumer trust. As businesses continue to expand their digital footprints, the importance of implementing robust security measures to combat these attacks becomes increasingly critical.

The innovative Arkose Bot Manager, backed by a $1 million credential stuffing warranty, enables enterprises to wipe out credential stuffing by offering real-time intelligence and advanced analytics to detect and prevent fraudulent activities, all while enabling great experiences for legitimate users.

Arkose Bot Manager for Credential Stuffing

Arkose Bot Manager is the most advanced technology in the industry to proactively identify attackers and deliver adaptive responses against credential stuffing. Its engine gathers high-risk data from a global consortium and analyzes in-depth digital intelligence to understand underlying user intent and provide risk scores. Its sophisticated algorithm leverages 125+ real-time device, network and behavioral risk signals, with ML decisioning and adaptive, dynamic response.

Detection models enable genuine users to sail through unchallenged, for easy and secure digital experiences. But when malicious traffic is encountered, the platform expertly confronts it in real-time via Arkose MatchKey, a state-of-the-art series of challenges with industry-leading security.

- **AI-decisioning platform**
- **Real-time feedback loop**
- **Global intelligence network**
- **GDPR privacy compliance**
- **Enterprise-grade scalability**
- **Real-time data visibility and integration**
- **WCAG2 accessibility certification**

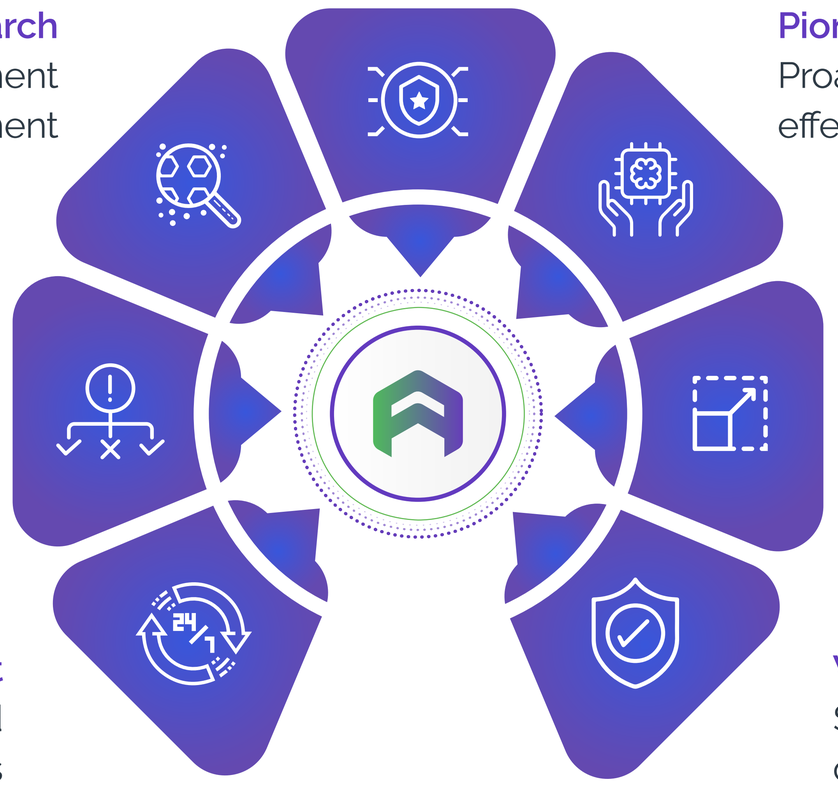
> "After implementing Arkose Labs, we saw an immediate ROI. The credential stuffing attacks stopped, and they have been a great partner with us in fighting fraud."
>
> – Engineering Manager, E-Signature Company

The Arkose Labs Advantage

Powerful collective impact
Global Intelligence Network data consortium for intelligence sharing

Unrivaled threat research
Dedicated threat-hunting, disarmament and enforcement

Pioneering technology
Proactively identifies attackers and effectively blocks attacks



Transparent risk signals
Real-time threat and response visibility for downstream decisioning

Proven at scale
Trusted by the world's largest B2C and global brands

Global, proactive support
24/7/365 SOC meets all cyber and privacy regulations

Warranties
$1M warranties per event for cyberattacks

ACTIR and the Arkose Labs SOC: Proactive Defense

Arkose Labs works as an extension of your team to thwart attacks fast and deliver actionable insights without putting a strain on your internal resources. The Arkose Cyber Threat Intelligence Research unit (ACTIR) safeguards against online attacks through threat hunting, risk intelligence, disarmament, and virtual enforcement, while the 24/7/365 Security Operations Center (SOC) team is dedicated to delivering rapid response against large-scale attacks.

ARKOSE LABS IN ACTION

Fast-Growing Neobank Faces off Against Credential Stuffing

Bots were relentlessly targeting a leading neobank's user accounts for credential stuffing, resulting in drained customer accounts and a deteriorating user experience. The financial services company implemented Arkose Bot Manager to protect its log-in forms and back-end APIs, leading to remarkable results.

Demonstrated Results

- 75% decrease in account takeover (ATO) attempts
- Slashed compromised account costs, which previously hit $100,000 per week
- Unleashed efficiencies through reduction in customer support demands

The world's leading organizations, including two of the top three banks and the largest tech enterprises, trust Arkose Labs to fight online fraud and keep users safe in digital transactions. Our patented, AI-powered platform detects, traps, and neutralizes bots and bad actors before they can make an impact, without sacrificing the experience of genuine users, and tracks and shares real time, global threat intelligence with our customers. No one else is more proven at scale, provides more proactive support for internal security teams, or outperforms Arkose Labs in sabotaging attackers' ROI. Our verified customer reviews on G2 reflect the value we add reducing the volume, internal cost, and impact of bot attacks and online fraud. Based in San Mateo, CA, Arkose Labs operates worldwide with offices in Asia, Australia, Central America, and South America.

Email:
demo@arkoselabs.com

Schedule Demo