SOLUTION BRIEF

Arkose Labs

Unknown Sessions

Distinguish between benign anomalies and potential threats

You're tasked with driving outcomes that keep your business ahead of the curve, and that means ensuring your security stack is airtight. Solutions like WAFs and CDNs were developed to solve specific security issues, which they do very well. Similarly, customer identity and access management (CIAM) tools are designed to manage and protect customer identities, ensuring that legitimate users have secure access to your services. However, there's a critical gap between the network protection offered by WAFs/CDNs and the identity-based security of CIAM tools. As malicious bot threats become more sophisticated with the help of AI, they can slip past WAFs and CDNs, exposing your networks and systems to risk. This is especially true when it comes to empty sessions – traffic sessions that are "unknown," with no profile information to tell you if it's friend or foe.

Arkose Bot Manager provides that next layer of defense, working alongside your existing solutions to enhance your security posture. By eliminating the noise of unknown sessions, it improves data quality and strengthens the overall effectiveness of your tech stack. With Arkose Bot Manager, you're streamlining your entire security flow, cutting out the unnecessary and expensive analysis of irrelevant data, and staying focused on what truly matters – protecting your business.

Arkose Bot Manager for Unknown Sessions

Arkose Bot Manager sits between your CDN/WAF and your CIAM solution, collecting and analyzing real-time signals to accurately uncover the nature of your traffic so you can confidently determine the most appropriate response strategy.

Key features include real-time traffic analysis and device classification using self-learning models that identify anomalies and potential security risks. A proprietary IP scoring system, bolstered by third-party reputation lists, monitors unusual activities such as IP spoofing or the use of residential proxies, ensuring early threat detection.

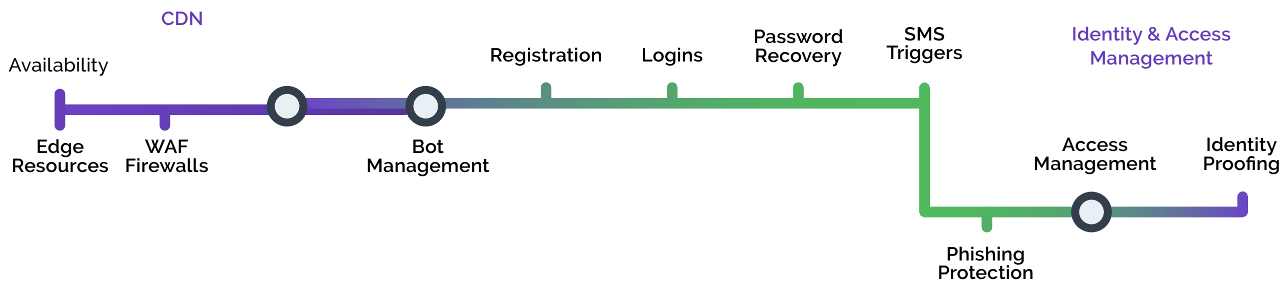
Enterprise Platform Highlights

→ Patented decisioning platform
→ Real-time feedback loop
→ Global intelligence network
→ Instant data visibility and integration
→ Enterprise-grade scalability
→ GDPR privacy compliance
→ WCAG 2.2 Level AA accessibility certification

The platform leverages collective intelligence from a global network, analyzing data from over 4.1 billion IP addresses to enhance threat detection and response. Flexible APIs allow seamless integration with proprietary and third-party risk engines, improving the accuracy of risk assessments and refining the challenge-response mechanism to maintain strong security while ensuring a seamless user experience.

At the core of Arkose Bot Manager is a decision engine utilizing hundreds of global rules that dynamically adapts to emerging threats through a feedback loop informed by real-time signals, historical data and shared customer insights. With features like open data sharing and dynamic attack response, the platform offers your business unparalleled security and peace of mind.

How Arkose Bot Manager Complements Your Tech Stack



Arkose Labs Proof of Value

The Arkose Labs proof of value (POV) process offers your business a hands-on opportunity to experience the platform's capabilities. During the POV, Arkose Labs provides expert guidance and consultation tailored to your specific needs, ensuring you can test the platform's effectiveness in real-world scenarios. This allows your business to define and track its own success metrics, such as fraud reduction, improved user experience or cost savings, giving you a clear view of the value Arkose Bot Manager can deliver.

The Arkose Labs Advantage

175+ risk signals and assements shared
Receive hundreds of session insights to enrich and tune your internal decisioning models.

Financial Warranties
Best efforts aren't good enough. We back our platform with million-dollar warranties and SLAs.

Arkose Global Intelligence Network
We see 99% of internet traffic every 20 minutes. Benefit from global risk signals and mitigation intel from our customer base.

Trusted by the most recognizable brands in the world
Built for enterprises, our technology, support, certifications and architecture meet your scalability requirements.

Global, proactive support
24/7/365 real-time SOC support with proactive incident response vs "on call".

Harnessing AI to stop evolving threat vectors
We're leveraging AI to defend against AI-driven bots.

ACTIR and the Arkose Labs SOC: Proactive Defense

Arkose Labs operates as an extension of your team, rapidly countering attacks and providing actionable insights without overburdening your internal resources. The Arkose Cyber Threat Intelligence Research (ACTIR) unit conducts proactive threat hunting, risk intelligence gathering and other counterintelligence methods to provide vital, fresh intelligence. Meanwhile, the 24/7/365 Security Operations Center (SOC) team focuses on identifying and stopping large-scale attacks immediately.

The SOC continuously monitors for new threats and collaborates with ACTIR. This feedback loop ensures a seamless collaboration between the SOC and ACTIR, enhancing the overall accuracy, timeliness and effectiveness of your cybersecurity defense.

Arkose Labs in Action

Large U.S. Bank Saves Six-Figure Sum Solving for Unknown Sessions

One of the largest and most established U.S. financial institutions was suffering from increasing unknown session rates. The costs associated with solution resources and FTEs were skyrocketing. Once Arkose Bot Manager was implemented between Akamai and ThreatMetrix, the bank saved hundreds of thousands of dollars on downstream costs, justifying the investment in Arkose Labs and proving the power of a defense-in-depth cybersecurity stack.

Results with Arkose Labs

- → Immediate reduction in the volume of unknown (empty) session traffic
- → Hundreds of thousands of dollars saved in downstream fraud detection costs
- → Online bank accounts compromised by automated attacks virtually eliminated

BOOK YOUR DEMO

Arkoselabs.com

The world's leading organizations, including two of the top three banks and largest tech enterprises, trust Arkose Labs to keep users safe. No one else is as proven at scale, provides more proactive support, or out-sabotages attackers' ROI. Based in San Mateo, CA, Arkose Labs operates worldwide with offices in Asia, Australia, Central America, EMEA and South America.