



Arkose Bot Manager


In the face of escalating cyber threats, the usual approach of reactive defense isn't enough. Cybercriminals are capitalizing on stolen data and sophisticated tools, launching bot attacks at scale in an endless game of keep-up that costs your business money, customer trust, brand reputation and more.

Arkose Bot Manager raises the bar for attackers by undermining their ROI. This proactive, long-term strategy not only disrupts their immediate efforts but also deters future attempts. By leveraging advanced risk-based detection and adaptive responses, Arkose Bot Manager ensures that both short-term attacks and sustained, sophisticated threats are met with formidable resistance.

Isn't it time the cybercriminals' resources were drained instead of yours?

Stop Attacks Before They Can Make a Downstream Impact


The Arkose Bot Manager platform cuts attacks off at the source. Unlike basic bot managers, it addresses the most sophisticated attacks. No other platform is more proven at scale, provides more proactive support for your security teams, or outperforms Arkose Labs in sabotaging attackers' ROI.



ACCOUNT REGISTRATION

New Account Fraud | Bonus Abuse | SMS Toll Fraud


- > Understand true intent of new users
- > Detect bulk fake account opening
- > Reduce downstream fraud and costs



ACCOUNT PROTECTION

Account Takeover | Credential Stuffing | Man-in-the-Middle Reverse Proxy Phishing | Loyalty Fraud | Payment Fraud

- > Protect accounts in real time
- > Eliminate large-scale attacks
- > Improve customer login experience



IN-PLATFORM AND BUSINESS MODEL ABUSE

Fake Listing & Reviews | API Abuse | Inventory Hoarding | GPT Prompt Compromise | LLM Platform Abuse

- > Protect the integrity of platforms
- > Eradicate malicious bot traffic
- > Safeguard customers from scams

Stop Bots, Not Good Users

Combining a dynamic risk engine with adaptive attack mitigation, the Arkose Bot Manager platform does the heavy lifting for you, distinguishing good vs. bad intent through multi-layered detection that aggregates real-time signals to spot hidden signs of bot and human-driven attacks. Legitimate customers seamlessly interact with digital properties – but when suspicious traffic is encountered, the platform expertly confronts it in real time via a state-of-the-art series of challenges with industry-leading security. The result is a secure and smooth digital experience for good users, while stamping out abuse in all its forms on your website and apps.

Defense-in-Depth Detection, Dynamic Response







Arkose Labs delivers long-term account protection and attack deterrence by combining sophisticated decisioning, threat intelligence and dedicated expertise to detect persistent bots and coordinated human attacks on the most targeted user touch points on websites and apps. Invisible risk assessments allow good users to pass through seamlessly. High-risk traffic is triaged for active attack response using innovative enforcement challenges that deter future attempts.

Proactive Defense	Adaptive Response	Actionable Data	Guaranteed Impact
Detect and mitigate attacks before they make impact	Dynamic interdiction traps bots without sacrificing CX	175+ signals drive precise, transparent decisioning	Industry-best service, warranty give confidence
<ul style="list-style-type: none"> Fingerprinting Detection Intelligence 	<ul style="list-style-type: none"> Multifaceted Challenges Dynamic Config 	<ul style="list-style-type: none"> Command Portal SEIM Flexible Integration 	<ul style="list-style-type: none"> 24 24/7 /365 SOC Custom Runbooks \$1M Warranty

Detection


Arkose Bot Manager collects and analyzes live intelligence signals to unearth suspicious patterns. The real-time risk assessment accurately uncovers the underlying nature of the traffic through ingestion signals including:

- Browser fingerprint
- Device profile and reputation
- Behavioral analytics
- Customer data exchange
- PII (phone, email, etc.) intelligence

 <p>Device Type Classification ></p> <p>Arkose Bot Manager categorizes types of devices by class to detect randomized attributes; self-learning models identify outlier signatures. It works for desktop, mobile, gaming consoles and smart TVs.</p>	 <p>Browser Fingerprinting ></p> <p>Arkose Bot Manager gathers detailed information about a user's browser and device configuration, such as browser type, operating system and plugins, to generate a unique fingerprint for each session.</p>	 <p>Behavioral Analytics ></p> <p>By monitoring interaction patterns like access time, time spent on site and other behavioral signals, the platform can then differentiate between legitimate humans and bots.</p>	 <p>Network Traffic Anomalies ></p> <p>A proprietary IP scoring system, combined with third-party reputation lists, monitors for abnormalities such as spoofing location or the use of IP addresses from data centers to residential proxies.</p>
 <p>Customer Network Intelligence</p> <p>Arkose Bot Manager aggregates and analyzes threat patterns across its global customer network, leveraging anonymized threat intelligence from over 4.1B IP addresses. Attacks on one customer can be defended across the entire customer base.</p>	 <p>Risk Data Integration</p> <p>Flexible APIs can ingest data from proprietary customer or third-party risk engines to improve risk assessment accuracy and inform the challenge-response mechanism.</p>		





Mitigation

Arkose Bot Manager utilizes a user-first approach to mitigation challenges to stop attacks before they cause damage. Good users sail through unchallenged, but the platform provides secondary screening and targeted attack response to stop bot and human-driven attacks. These adaptive and continuously learning challenges serve as effective mitigation while allowing edge-case genuine users to prove they are real and continue their experience.

 <p>Response Orchestration</p> <p>Combining real-time insights with the risk profile of the user, our defense determines the appropriate mitigation response. Behind the scenes, the SOC team constantly monitors traffic flow and attack patterns to adjust signals and enforce pressure and challenges accordingly.</p>	 <p>Dynamic Defense</p> <p>Bots are presented with a deep bench of dynamic challenges that machines are unable to solve. This forces attackers to retrain models and invest more time and money in an attempt to circumnavigate challenges.</p>	 <p>AI Resistance</p> <p>AI-resistant challenges confuse and disrupt machine-based solvers. By subtly altering images in ways that only affect AI interpretation, these challenges remain fully accessible to legitimate users but create significant hurdles for bots.</p>
---	---	---

Data Sharing & Feedback Loop

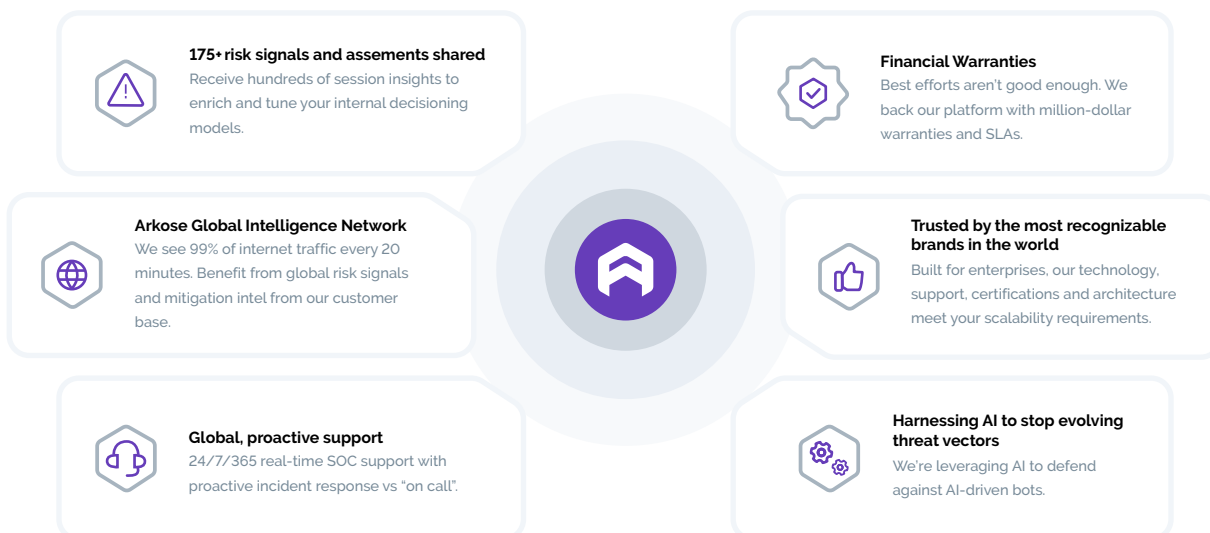
With 175+ global rules out of the box, the platform detects signs of fraud on day one that others miss. Detection and mitigation strategies are backed by deep sharing and feedback loops to make threat intelligence more actionable.

 <p>Open Data Sharing</p>	 <p>Arkose Command Center</p>	 <p>Dynamic Feedback Loop</p>	 <p>Attack Pattern Correlation</p>
<p>Arkose Bot Manager provides hundreds of risk signals for better visibility behind each risk score. All risk signals collected by Arkose Bot Manager can be ingested into existing models to improve decision accuracy early in the user journey, while providing better insight downstream.</p>	<p>Beyond direct API connections, customers have access to our central hub for data insights and self-service functions for monitoring and managing applications protected by Arkose Bot Manager. It consists of configurable dashboards that empower security analysts and business users to better understand and mitigate attacks. Other overall functionalities are user management, data filtering for dashboards and reporting.</p>	<p>Feedback loops create a dynamic and proactive environment where both our detection models and mitigation challenges are not just reactive but are also continuously evolving based on new threats and data, enabling rapid adaptation to evolving attacks.</p>	<p>Arkose Bot Manager leverages collective insights across the global customer network, enhancing defenses by sharing detected attack strategies network-wide.</p>

Attack SLA & Warranties

We stand by our customers with a contractually guaranteed attack SLA and industry-first warranties that cover up to \$1M in the event of credential stuffing, card testing and SMS toll fraud attacks.

The Arkose Labs Advantage



Arkose Bot Manager in Action



Fintech Beats ATOs

One of the world's most prominent fintech firms was targeted by bots executing credential stuffing attacks at scale. Successful attacks led to the draining of customer funds and poor user experience.



Attack Impact

- ATO costs of \$100K per week
- Damaged relationships and lack of customer trust



Results with Arkose Labs:

- 75% reduction in ATO attempts
- Slashed compromised account costs
- Minimal credential resetting led to significant resource savings



Global Payments Co. Stomps Out SMS Fraud

The fintech company selected Arkose Labs to ring up SMS toll fraud savings, significantly cutting costs while maintaining a seamless customer experience.



Attack Impact

- Millions of dollars in annual losses
- Legitimate customer experience harmed



Results with Arkose Labs:

- \$3.7M projected annual savings
- 99.9% success rate in stopping sophisticated SMS fraud attacks



Arkose Labs Takes On EvilProxy

EvilProxy is a sophisticated and widely used MITM phishing-as-a-service kit that allows attackers to bypass MFA protections. Arkose Labs conducted an analysis of requests on three login endpoints of 250 suspicious domains.



Traditional Detection

- Only 10/250 - or 4% - of total suspicious domains detected



Results with Arkose Labs:

- Detected 49 domains less than 30 days old (indicating they were likely created for attack)
- Detected 191 short-lived URLs (indicating they served their attack purpose and soon disappeared)

[BOOK YOUR DEMO](#)

[Arkoselabs.com](https://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. © 2024 Arkose Labs. All rights reserved.