Arkose Labs

E-BOOK

THE BOT ECOSYSTEM: UNDERSTANDING AND MITIGATING AUTOMATED THREATS

Protecting digital experiences against bots and other advanced attacks

Automated online fraud is a huge problem, with bots launching thousands of attacks in the same time frame that a human could complete a mere handful. Despite myriad bot prevention solutions on the market, a massive 73% of all website and app traffic now comes from bots and other attack traffic, showing the scale of the challenge at hand. This escalation has led to a total increase of about 167% in all bot-related attacks.[1]

These days, anyone can launch automated attacks at scale with a small investment and minimal technical knowledge, due to the ubiquity of cybercrime-as-a-service (CaaS) platforms. The CaaS model allows threat actors to easily access pre-built, user-friendly tools and services designed for specific malicious activities. This increases the opportunity and reach for cybercrime and fraud, and can overwhelm even experienced internal security operation center (SOC) teams.

The driving force behind this shift is economic incentive – cybercriminals are constantly devising new methods to ensure their activities are profitable. They focus on maximizing their return on investment (ROI), often using advanced technologies that allow them to scale their operations rapidly and efficiently. These cyberattacks deplete revenue and cost businesses both time and money.

Winning the war against bad bots requires an approach that is optimized for detecting and mitigating advanced, automated attacks while ensuring that businesses are proactive instead of reactive in their efforts to secure their digital experiences.

A TIDAL WAVE OF ATTACKS

Cybercriminals use two primary bot attack vectors to carry out these attacks:

1. **Basic Bots.** Limited bots that perform simple, repetitive tasks. These tasks are usually rule-based, meaning the bots follow predefined scripts or commands. Their capabilities are limited to the scenarios they were explicitly programmed to handle, and they do not learn from interactions or improve over time.

2. **Intelligent Bots.** Intelligent bots are capable of complex, context-aware interactions, using a variety of methods to process and respond to information. They handle complex tasks within their programmed domain and often utilize machine learning techniques to improve their performance over time. The advent of generative AI means many intelligent bots now incorporate significantly enhanced computer vision technologies, which have made it trivial for them to solve traditional CAPTCHAs. These bots use advanced machine learning models, particularly deep learning and convolutional neural networks, which are highly effective at processing and interpreting visual data.

[1] *Breaking (Bad) Bots: Bot Abuse Analysis and Other Fraud Benchmarks*

Basic Bots

Limited bots that perform simple, repetitive tasks

Intelligent Bots

Bots capable of complex, context-aware interactions

Whatever the skill level, bots are used in the cybercrime ecosystem for a variety of reasons, including:

- Preparatory activity for downstream attacks, such as credential testing
- The primary avenue for an attack, e.g., account takeover, SMS toll fraud, new account fraud or GPT prompt compromise, where bots programmatically submit prompts and scrape the responses
- Evasion of known anti-bot defenses at scale

Different bot attack types have their own distinct paths to monetization. Much of the low-value, high-volume activity depends on being able to execute at scale. An example would include sending spam messages en masse, where only a few malicious links out of hundreds must be clicked for the attack to be profitable for the fraudster.

Bots are also used for indirect monetization – attacks that don't cause immediate financial losses but lay the groundwork for future monetization. Beyond the traditional attack points of new account creation, account login and payments, attackers target other customer touchpoints. Fraudsters can make money on these indirect touchpoints in many ways, including by creating fake reviews, upvoting or downvoting videos, or abusing in-platform economies in online gaming.

THE ONLINE FRAUD CHAIN

Objectives

- Identify target website with high account value
- Purchase list of stolen credentials on dark web

Reconnaissance

- Build or rent a botnet to automate validation
- Build or buy software tools to evade detection

Weaponization

- Validate list of stolen credentials against login page of target website
- Resell validated account credentials on dark web

Delivery

- Purchase compromised account for target site
- Use purchased account credentials to log in

Exploitation

- Perform fraudulent transactions using compromised account

Action

THE ROLE OF BOTS IN MONEY LAUNDERING SCHEMES

Money laundering often plays a critical role in the monetization strategies associated with different types of bot attacks, especially as they scale in complexity and aim. In the context of both direct and indirect monetization methods, illicit funds generated need to be integrated into the financial system without drawing regulatory attention. Bots facilitate this integration by automating processes like new account creation, login activities and transaction executions, which can be used to layer and obscure the origin of illicit earnings.

For instance, through the automated creation of multiple accounts, fraudsters can disperse funds in smaller, less suspicious amounts across these accounts. The automated nature of bots allows this to happen at a scale and speed that would be unfeasible manually, thus efficiently laundering money through the digital ecosystem. These laundered funds can then be used to further finance the bot operations, creating a self-perpetuating cycle of fraud and monetization.

A notable example of this can be seen with Deutsche Bank, which faced fines for its role in a $10 billion Russian money-laundering scheme. This scheme involved cyber tactics such as the creation of fake accounts and other fraudulent activities to move money illicitly out of Russia. These activities often included sophisticated methods to hijack existing accounts or create new ones fraudulently, demonstrating how cyber-enabled financial crimes can leverage automated systems to facilitate large-scale money laundering.

Attackers do their homework; they know the processes and defenses that prevent fraud and how to overcome them. They will often test their attack types in one industry to perfect their methods, and then pivot to a higher-value industry like banking to exploit larger financial opportunities. When humans and bots work together to launch attacks, it can be very hard for businesses to find them, let alone stop them.

CASE STUDY: $3.7M SAVED ANNUALLY

SMS toll fraud – an attack carried out overwhelmingly by bots – was causing a rising star in global payments solutions to lose hundreds of thousands of dollars every month. With attacks quadrupling each year, the fintech company selected Arkose Labs to deploy stringent countermeasures. Arkose Bot Manager effectively detected, isolated and neutralized these threats, significantly cutting the costs associated with SMS toll fraud while maintaining a seamless experience for legitimate consumers.

- $3.7M estimated savings in SMS spend on an annualized basis
- 70.2% immediate reduction in overall SMS volume
- 99.9% success rate in stopping sophisticated SMS toll fraud attacks

THE EVER-CHANGING ATTACK SURFACE

Consumer transaction points across many devices — desktops, laptops, mobile devices and gaming consoles — provide many entry points for fraudsters to target. APIs provide yet another attack surface; they are directly targeted using bots that mimic traffic coming from a legitimate source. Your enterprise can reduce the impact and cost of online fraud for both your businesses and your users while improving your ROI by ensuring that all customer touch points are secure, reducing the risk of a successful cyberattack. Additionally, this helps protect and reinforce brand integrity so you maintain the trust of your consumers and safeguard your reputation.

ATTACK TOUCHPOINTS

Externally Facing Forms

- ATO/credential stuffing
- Man-in-the-middle advanced phishing
- New account fraud
- SMS toll fraud

In-app & Business Model Abuse

- Spam & malicious content
- Loyalty point theft
- Fake reviews
- Collusion and cheating
- Website scraping
- GPT prompt compromise
- LLM platform abuse

API Traffic

- Device emulation
- User impersonation

RIDESHARE LEADER SLAMS THE BRAKES ON BOTS

A prominent rideshare and delivery giant faced the challenge of protecting the superior customer experience on their platform while stopping bad actors from exploiting their services. Bad actors were using automated bots to create fake accounts at scale, causing skyrocketing SMS bills. The company used Arkose Bot Manager to detect, isolate and eradicate these attacks, resulting in a substantial reduction in SMS toll fraud costs and an enhanced, secure experience for genuine consumers.

- $2.5 million saved in annualized SMS toll fraud in select high-risk countries
- 94.4% of challenged sessions immediately gave up, indicating high bot detection accuracy
- 99.5% of low-risk traffic passed through unchallenged, indicating minimal customer friction

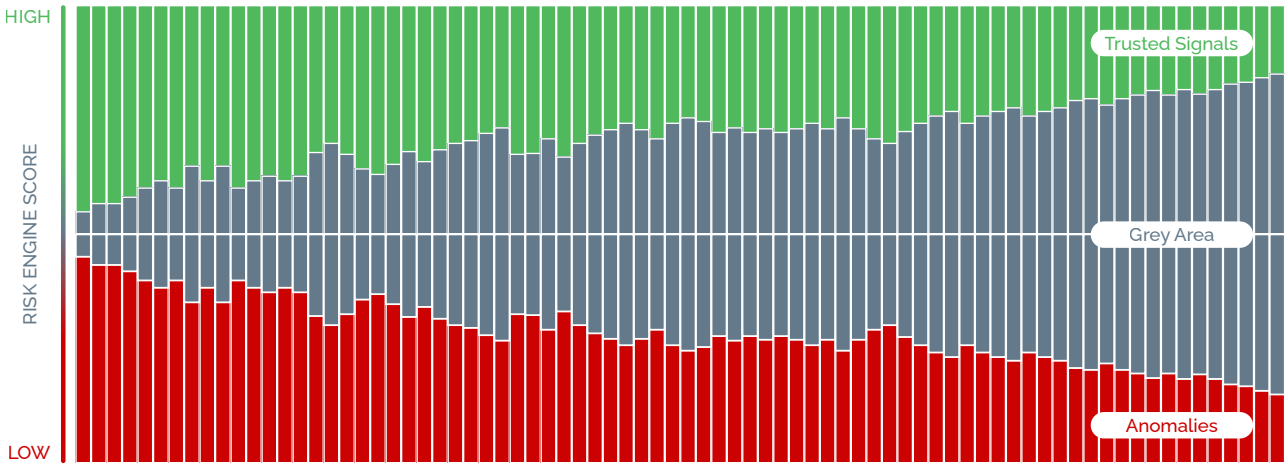
THE LIMITATIONS OF TRADITIONAL APPROACHES

Each of the three main historical approaches to bot detection and mitigation is flawed against modern, automated attacks

#1 BLOCKING TRAFFIC

Some solutions take the approach of blocking any traffic that appears to be suspicious. This means you must have a very high degree of confidence that you can accurately identify all bot attacks. But as we've seen with today's bot technology, which can mimic human behavior to a fine degree, this is nearly impossible. Blocking traffic generates a high number of false positives, creating a terrible experience for consumers. As a result, you risk turning off or turning away good consumers – and many bots still get through, regardless. In addition, this approach provides attackers with clear signals as to what isn't working, and allows them to adapt faster.

More and more traffic is falling into a "gray area," where only a small amount can appear as either explicitly good or bad.



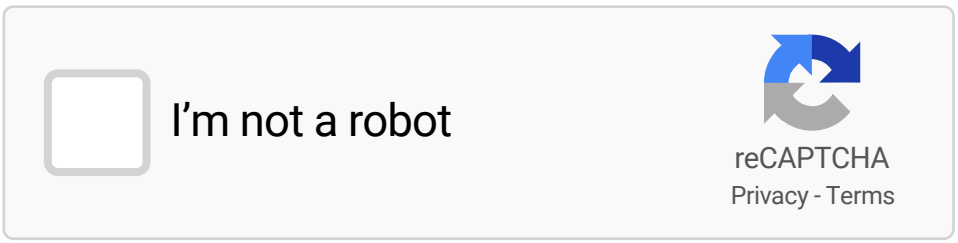
#2 TRADITIONAL RISK SCORING TRAFFIC

Traditional risk scoring is far less effective against today's attacks than it was even a few years ago. This method is manual, as humans must examine scores that aren't explicitly accepted or rejected for further review. Because of the lack of real-time decisioning, sophisticated bot attacks are frequently successful. Additionally, many organizations have complex tech stacks and receive many – often conflicting – scores from various sources.

#3 TRADITIONAL CAPTCHA

CAPTCHAs and similar tools have long been in place as a way to stop automated attacks. However, most CAPTCHAs struggle against modern bot technology. All it takes is a quick Google search for any fraudster to find and deploy automated scripts to bypass traditional CAPTCHAs. These attacks also provide undue friction to good customers, who are sick and tired of identifying crosswalks or buses each time they want to log in to an account.

"Has anyone had that moment recently where you have failed the I-am-not-a-robot test so many times that you have that moment where you stop and go…Maybe I am a robot?" comedian Jack Whitehall asked in a recent Netflix show. "I haven't been able to spot 10 lights in a row. I'm either a robot or a cyclist!"



SPOTLIGHT ON TRADITIONAL CAPTCHAs

Legacy CAPTCHA solutions are faulty in many ways. While the concept may be noble in execution, many of these solutions have faults.

Easily solved: Modern machine vision technology can easily bypass traditional solutions.

Too much friction: These authentication methods also have a low good-customer throughput rate.

Human-automation hybrid attacks: CAPTCHAs are powerless against coordinated attacks employing both bots and human power.

Lack of insights: Many of these solutions are inexpensive or free with no managed services. They can't give businesses insight into attack patterns, nor can they evolve.

A CAT AND MOUSE GAME WITH FRAUDSTERS

Traditional bot mitigation tools that rely solely on risk scoring and parsing the veracity of digital identities are flawed in today's fraud landscape. Fraudsters know the parameters that companies use when taking a risk-based authentication approach, and are able to circumvent traditional CAPTCHAs and other solutions at scale. This leads many businesses to play a game of "whack-a-mole:" stopping one attack while several others pop up at the same time.

Businesses need to proactively identify attackers and deliver adaptive responses that stop attackers before they can make an impact – all while improving customer satisfaction through easy and secure digital experiences.

CASE STUDY

The growing popularity of the Roblox gaming platform began attracting cybercriminals who executed automatic scripts to create new accounts and monetize the games' virtual currency. They used bots to create numerous poorly crafted games that ranked ahead of the superior user-created games. This adversely affected the game ranking data, disrupted the user experience, and diluted player engagement.

- After implementing the Arkose Labs solution, Roblox realized:
- 96x reduction in abuse
- 10% uplift in good player throughput vs. reCAPTCHA
- 15% uplift in revenue generation

A LAYERED APPROACH TO BOT DETECTION

Many bot detection solutions only focus on one aspect of bot detection and remediation. But a multilayered approach is needed to combat advanced threats, without sacrificing the experience of good consumers, while finding long-term savings. An optimal bot mitigation solution should include dynamic evaluation of traffic in real-time, traffic segmentation based on suspicion level, and then the delivery of an appropriate response. It should include all of the following:

01 **Continuously evolving detection methods** that collect and analyze real-time intelligence signals to unearth suspicious patterns

02 **Fully transparent decisioning** that gives clear insights into how decisions are made regarding security measures, risk assessments and the identification of potentially fraudulent activities

03 **A dynamic response strategy** that presents challenges matched to the type of threat detected with appropriate sophistication

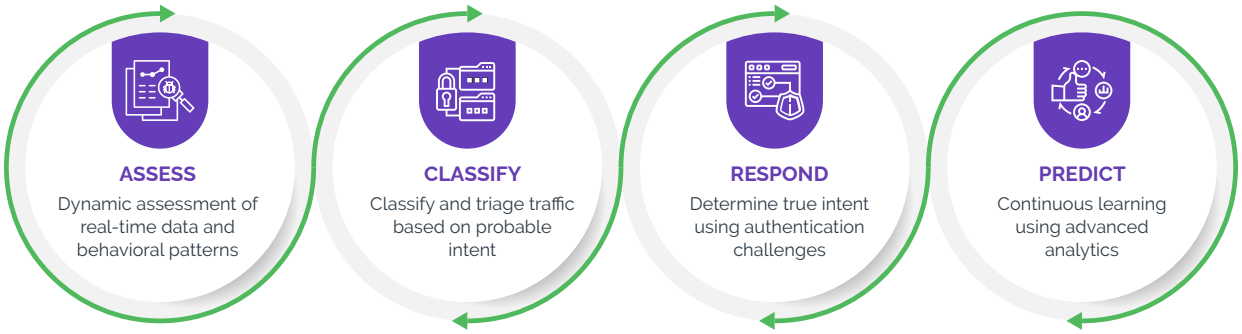
04 **A global data consortium** to share large-scale risk signals and mitigations, along with insights regarding good user throughput

05 **Actionable insights and remediation reporting** to enable analysis and visibility on bot vs. human traffic

06 **Detailed configurations**, such as the ability to tune the detection engine and refine the response strategy

07 **Feedback loops**, where the system is not just reactive but is continuously evolving based on new threats and data, enabling rapid adaptation to evolving attacks

08 **Proactive SOC and threat intelligence teams** to help detect and stop attacks before they can make an impact



ASSESS: To stop bots, you need a dynamic evaluation of traffic in real time. Instead of certain signature-based approaches, real-time data analysis—based on known rule-based signals of fraud and parsing hundreds of different data points—is needed.

CLASSIFY: The business must go beyond the risk score. Traffic must be prioritized to allow good users to pass with ease, whereas high-risk activity is further assessed to deterministically classify true intent.

RESPOND: Secondary screening to establish whether traffic is malicious or genuine. Use interactive challenges that have been designed and tested to be resistant to bot activity. Good users who are in the "gray area" can easily pass these challenges.

PREDICT: Leverage the combined learnings from risk assessments and authentication challenge results. Establish a continuous learning protocol, powered by advanced analytics, that ensures that bot detection capabilities are constantly evolving and challenge rates are decreasing.

A MODERN APPROACH OF TRUST AND USER EXPERIENCE

Traditional mitigation strategies sacrifice eliminating bot activity for user experience – or vice versa. A robust solution, however, eradicates bot activity while also improving consumer throughput rates.

By precisely pinpointing and then targeting only suspicious traffic with enforcement challenges that cannot be solved by even advanced machine vision technology, businesses realize higher ROI without adversely impacting the user experience. This approach forces attackers to invest time and money to solve the challenges. And while no challenges are 100% foolproof, a modern solution continuously presents new challenges, ensuring that attackers must expend additional resources to overcome them.

HOW IT WORKS

Arkose Labs offers technology, services and intelligence that protect critical, value-generating experiences, like websites and apps, against bots and other advanced attacks.

The Arkose Bot Manager platform constantly adapts to evolving attack patterns and can be tailored to business needs. Arkose Bot Manager combines real-time intelligence, rich analytics and sophisticated, adaptive challenges.

It looks at more than 125 real-time global data signals from user sessions to find telltale signs of automated attacks. Combining this data with behavioral patterns, it accurately triages traffic based on the risk profile. Bots are delivered enforcement challenges that cannot be scripted around using automation.

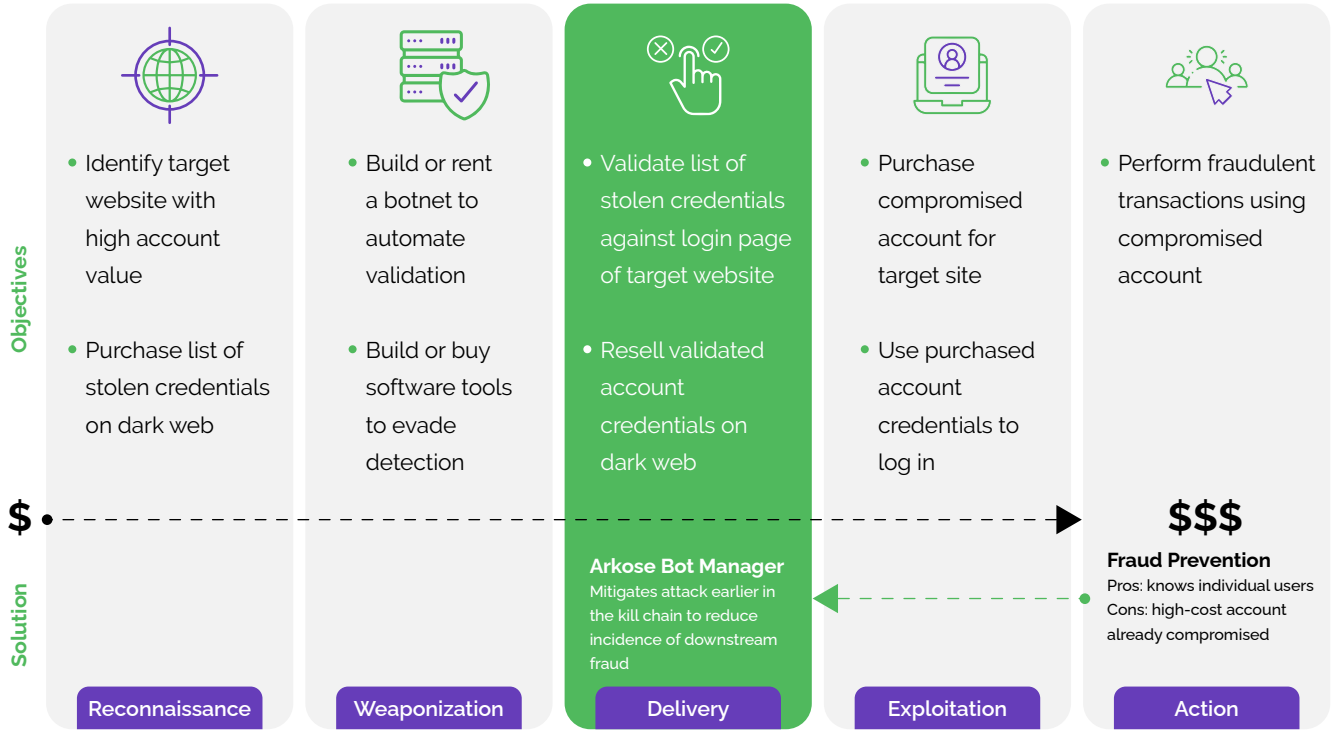
Arkose Bot Manager includes a challenge-response mechanism that serves up real-time 3D visual adaptive, enhanced audio, and other fully WCAG 2.2 Level AA-compliant enforcement challenges that can't be solved by bots. This suite of AI-resistant challenges is designed to confuse AI-based solvers by introducing variations in images that are imperceptible to humans but disrupt machine interpretation.

This innovative approach effectively thwarts malicious bots, enhancing security for business operations and improving the user experience for legitimate consumers. Additionally, the challenge-response mechanism also protects against API abuse; bots that target API keys are met with interactive challenges they cannot solve.

In addition, Arkose Bot Manager's email intelligence component stops bots from utilizing fake, throw-away or other high-risk email addresses in attacks on online services and applications. This is designed to tackle abuse at the point of maximum impact: the top of your application's user flow.

Lastly, its phishing protection component detects, alerts and stops dangerous man-in-the-middle (MITM) and reverse-proxy advanced phishing attack campaigns. It includes real-time detection using client- and server-side signatures, managed phishing detection rulesets, hostname allow and deny lists, immediate end-user warning messages, support for both active interception and monitor-only modes, and in-depth visibility and reporting.

UNDERSTANDING THE ONLINE FRAUD KILL CHAIN



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 solution also includes proactive defense in the forms of:

- **The Arkose Labs SOC:** The 24/7/365 Security Operations Center (SOC) team is dedicated to delivering rapid response against large-scale attacks. This setup ensures that threats are managed efficiently without overwhelming internal resources. The SOC engages in analyzing emerging attack patterns, employs supervised machine learning models, and offers collaborative, ongoing tuning of security measures.

- **ACTIR:** The Arkose Cyber Threat Intelligence Research (ACTIR) unit is a dedicated and specialized counterintelligence team embedded in Arkose Labs. Comprising full-time experts in cyber threat analysis, digital forensics and cybersecurity operations, ACTIR's primary mission is to detect, assess and neutralize sophisticated cyber threats. By leveraging cutting-edge technologies and methodologies, ACTIR provides actionable intelligence and orchestrates coordinated responses to mitigate threats posed by nefarious entities. Recently it partnered with Microsoft DCU and law enforcement to disrupt alleged Vietnamese threat actor group Storm-1152. Through collaboration with our award-winning SOC, ACTIR plays a pivotal role in enhancing an enterprise's cybersecurity posture.

- **The Arkose Global Intelligence Network:** This robust consortium, composed of major corporations and category leaders across the globe, provides a critical mass of data that Arkose Labs uses to derive insights and understand the evolving threat landscape. It allows us to assess billions of sessions and interactions so we can detect, analyze and respond to an array of cyber threats.

THE ARKOSE LABS ADVANTAGE

Powerful collective impact
Global Intelligence Network data consortium forintelligence sharing

Unrivaled threat research
Dedicated threat-hunting, Disarmament and enforcement

Pioneering technology
Proactively identifies attackers and effectively stops 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 SOC meets all cyber and privacy regulations

Warranties
$1M warrranties per cent event for cyberattacks

CONCLUSION

This ebook underscores the critical need for innovative and adaptive strategies to mitigate the pervasive threat that automated bots pose to today's enterprises. By leveraging advanced technologies and a collaborative intelligence network, your business can not only counteract these threats but also enhance the digital experience for legitimate users, thereby safeguarding their assets and boosting overall ROI.

With a strong emphasis on a trust and safety mindset, your organization will be better positioned to adapt to the changing cybercrime landscape, ensuring robust security measures are in place to protect against the ever-growing wave of automated bot attacks.

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, Arkose Bot Manager 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, EMEA and South America.

Schedule Demo

demo@arkoselabs.com
(800) 604-3319
arkoselabs.com