Arkose Labs

THE ULTIMATE BOT PREVENTION PLAYBOOK

Secure your business with integrated detection and enforcement. Watch attacks disappear and ROI skyrocket.

ELIMINATING FRAUD AND AUTOMATED ABUSE ON WEB, MOBILE AND API TRAFFIC

Cyber criminals, like anyone else, get up each day to perform a job—as long as it's economically viable for them to do so. These bad actors need to ensure their return is greater than whatever time and money they put into carrying out attacks.

Automation plays a key role in this equation. Bots can launch a thousand attacks in the same time frame that a human could complete a mere handful. Also, bot programs can be bought easily and cheaply on the dark web. Some of them even have customer service functions built in. Now anyone can launch automated attacks at scale with a small investment and minimal technical knowledge.

Automated fraud is a huge problem, despite the myriad bot prevention solutions meant to tackle it. Cyberattacks deplete revenue and lead to a diminished ROI, costing businesses both time and money. The fact that bots are still such a prevalent issue in fraud and security shows that we are not yet winning the battle.

A TIDAL WAVE OF ATTACKS

Many bots are effective due to sheer volume. Only a fraction of them need to be successful for cyber criminals to make money. These types of attacks are carried out by generally unsophisticated, simple programs.

But there are also more advanced bots that are very good at imitating human behavior. Whatever the skill level, bots are used for three specific reasons in the cybercrime ecosystem:

- Preparatory activity for downstream attacks, such as credential testing
- The primary avenue for an attack—e.g. credential stuffing
- To evade known anti-fraud defenses at scale

Different bot attack types have their own distinct paths to monetization. Much of the low-value, high-volume activity has minimal success rates and 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 on in order for the attack to be profitable for the fraudster.

Bots are also used for indirect monetization—attacks that don't cause financial losses but actually 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.

Attackers do their homework; they know the processes and defenses that prevent fraud and how to overcome them. When humans and bots work together to launch attacks, it can be very hard for businesses to even find them, let alone stop them.

 **Basic Bots**	Unsophisticated bots are launched at scale, and are simple and inexpensive to deploy
 **Trained Bots**	Automated scripts can evade known defenses, such as those using machine vision technology
 **Evade Defenses**	Bots coded to escalate to human sweatshops when they meet challenges
 **Hybrid Attacks**	Low and slow attacks mimic human behavior, obfuscate or spoof identifying characters to evade detection

THE EVER-CHANGING ATTACK SURFACE

Consumers transact on many devices—desktops, laptops, mobile devices, and gaming consoles—which provides 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.

Not long after cyber criminals successfully perform ATO attacks or set up fake new accounts, they begin deploying automated abuse within applications or platforms when they are signed in. For instance, they use a cloud email account to send spam or run automated sessions in online games to collect in-game assets that they then sell on third-party platforms.

Businesses can lower costs and improve their ROI by ensuring that all customer touch points are secure, reducing the risk of data breaches. Additionally, data security can help businesses to gain the trust of their customers and improve their reputation, which brings increased ROI over time.

THE ATTACK SURFACE

		
Externally Facing Forms Unverified user	**In-Application Customer Actions** Logged in Users	**API Traffic**
• Credential Stuffing • Account enumeration • Content Scraping • Carding • Form Spam	• Spam and malicious content • Fake reviews Auction house abuse & fake bids • Collusion and cheating (gaming & gambling)	• Device emulation • Users impersonation

Microsoft

CASE STUDY

Spam & Phishing

Microsoft Outlook, one of the world's most popular cloud-based email applications, had a problem when automated bots created free new accounts at scale. The accounts were used to send messages containing malicious links (malware) to legitimate users. Cyber criminals would run phishing attacks with these accounts, attempting to extort users by claiming to have "incriminating information" that they would release unless given money.

To combat this, Outlook.com implemented 2FA authentication methods such as SMS messages. However, these not only failed to stop much of the fraudulent account creation but also alienated good users by providing too much friction when they tried to access their accounts.

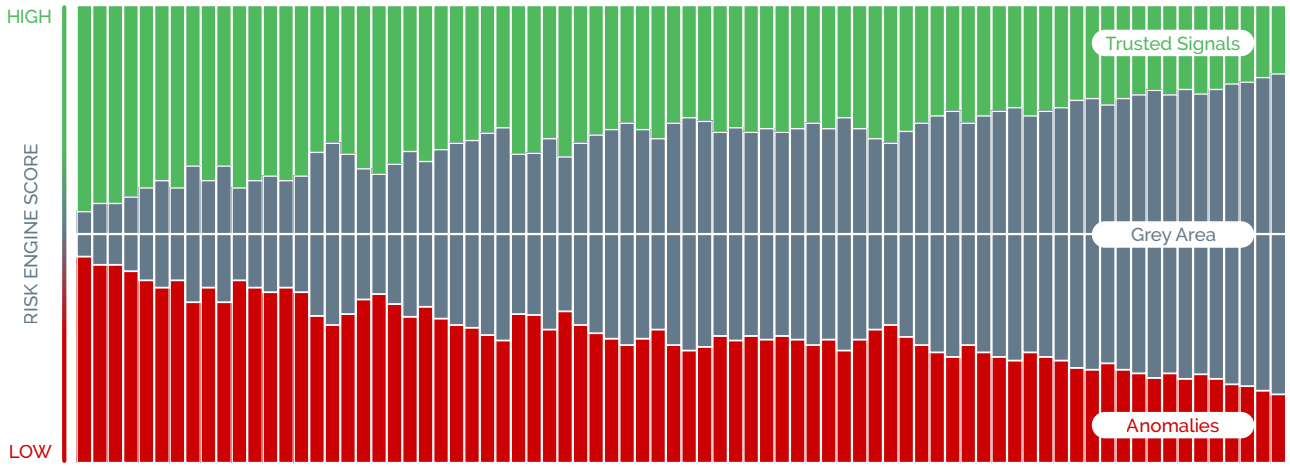
By implementing the Arkose Labs state-of-the-art bot detection platform, however, nearly all of these attacks were stopped and the user experience improved.

THE LIMITATIONS OF TRADITIONAL APPROACHES

There are three main approaches to bot detection and prevention. That said, they are flawed against modern, sophisticated automated attacks.

01 , Blocking Traffic

Some solutions take the approach of blocking any traffic that appears to be suspicious. However, you must have a very high degree of confidence that you can accurately identify all bot attacks. As we've seen, with today's bot technology that can mimic human behavior to a fine degree, this is nearly impossible. That means you risk turning away some good customers, which in turn hurts the bottom line, erodes customer loyalty, and diminishes cost savings. Many bots still get through, regardless. More and more traffic is falling into a so-called "gray area," where only a small amount can appear as either explicitly good or bad.



02 , Risk Scoring Traffic

Traditional risk scoring is far less effective against today's attacks. 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 different

03 , 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.

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 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 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 take a zero-trust approach to the data and device characteristics they see coming into their website, as fraudsters can easily change their source IP addresses, spoof legitimate customers' devices, hide their true location, and so on. Implementing secondary screening for high-risk traffic is essential, not only to eliminate automated attacks without impacting legitimate user traffic, but also to save costs and ensure a better ROIa

CASE STUDY

The growing popularity of the Roblox gaming platform began attracting cyber criminals 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 user experience, and diluted player engagement.

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

A TRUST AND SAFETY MINDSET

Customers want a seamless experience, and they want to know that their information is safe. They don't want to actively think about fraud—they want to know that safety is ensured. That's why successful organizations are investing in creating an ecosystem that fosters trust for customers.

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 while finding long-term savings. An optimal bot mitigation solution should include all of the following:

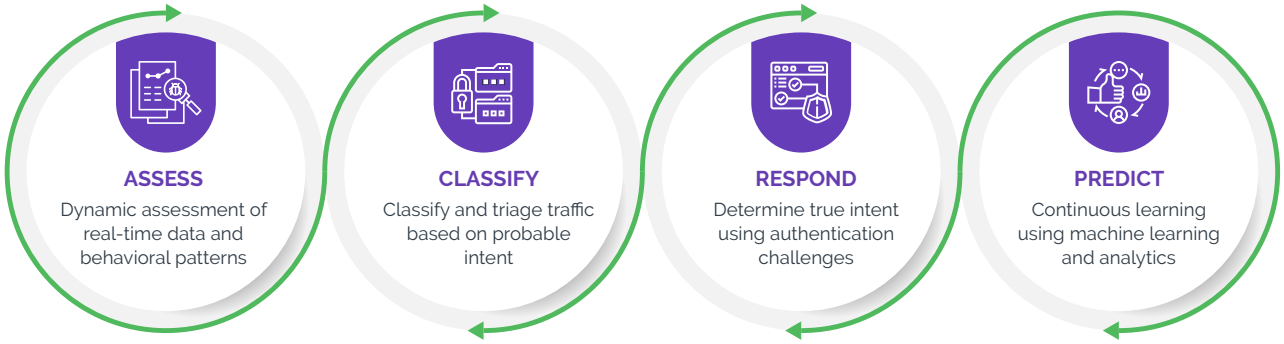
01 **Continuously evolving detection methods** using probabilistic, statistical, and machine learning-based models to detect patterns

02 **Configuration and Customization,** such as the ability to tune the detection engine and refine the response strategy

03 **Adaptive response strategy** that presents challenges with increasing difficulty based on the proper risk score

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

Businesses need to take a multilayered approach to identifying and rooting out automated attacks. This should include a dynamic evaluation of traffic in real-time, segmenting traffic based on suspicion level, and then delivering an appropriate response. The following is a four-step approach to successfully identifying and stopping bot traffic.



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 telltale signals of fraud and parsing hundreds of different data points—is needed.

CLASSIFY: 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 machine learning and advanced analytics, that ensures that bot detection capabilities are constantly evolving and challenge rates are decreasing.

A New Approach of Trust and User Experience

There needs to be a new approach to eliminating automated fraud and bot-driven attacks. Traditional mitigation-focused strategies sacrifice eliminating bot activity for user experience—or vice versa. A robust solution, however, eradicates bot activity while also improving customer throughput rates.

By deploying enforcement challenges that cannot be solved by even the advanced machine vision technology, the user experience is not adversely impacted, and businesses realize higher ROI

How it Works

The Arkose Labs platform combines real-time intelligence, rich analytics, and sophisticated step-up challenges. When cyber criminals are forced to spend more time and money to attack a site, they will abandon their efforts. The Arkose Labs platform constantly adapts to evolving attack patterns and can be tailored to business needs:

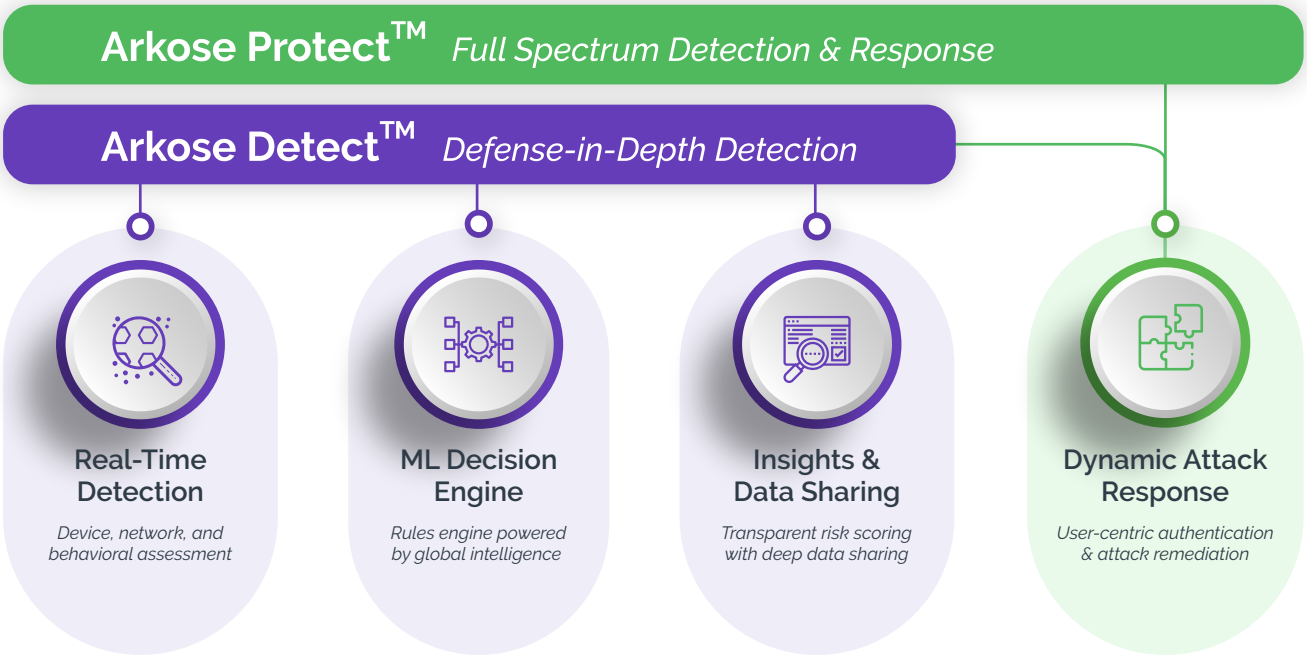
Arkose Detect:

Arkose Detect looks at real-time global data from user sessions and how they interact with technology to find "telltale signs" of automated attacks. Combining this data with behavioral patterns, Arkose Detect accurately triages traffic based on the risk profile, and bots are delivered an enforcement challenge that cannot be scripted around using automation.

Arkose Protect:

The Arkose Protect unified detection and response solution provides real-time 3D visual adaptive enforcement challenges that can't be solved by bots. Arkose Protect also protects against API abuse; bots that target API keys are met with interactive puzzles they cannot solve. Through seamless integration with Arkose Detect, it preserves challenges for risky traffic only.

Arkose Labs Fraud and Abuse Prevention Platform



CONCLUSION

While businesses must stop automated attacks and maintain a good customer experience, they should also look for cost savings and better ROI.

That's why Arkose Labs uses the dual approach of intricate analysis of traffic and the appropriate and targeted use of friction. With data analytics and analysis of heuristics, the platform can determine the intent of each user, and then serve the appropriate step-up challenge to stop bots in their tracks.

Arkose Labs

Arkose Labs' mission is to create an online environment where all consumers are protected from malicious activity. Recognized by Gartner as a "Cool Vendor in Fraud and Authentication," the company offers the world's first $1 million credential stuffing warranty. Its AI-powered platform combines powerful risk assessments with a dynamic attack response that undermines the ROI behind attacks while improving good-user throughput and saving businesses money. Headquartered in San Mateo CA, the company debuted as the 83rd fastest-growing company in North America on the 2021 Deloitte Fast 500 ranking

Sales:

(800) 604-3319

Mail:

support@arkoselabs.com

Address:

USA • 2 W 5th Ave, Fl 3, San Mateo, CA. 94402
Australia • 315 Brunswick St, Fl 2, Brisbane, QLD. 4006
UK • 167-169 Great Portland Street, 5th Floor, London, W1W 5PF
Costa Rica • San José, Escazú, San Rafael, Escazú, Village Torre II

Schedule Demo