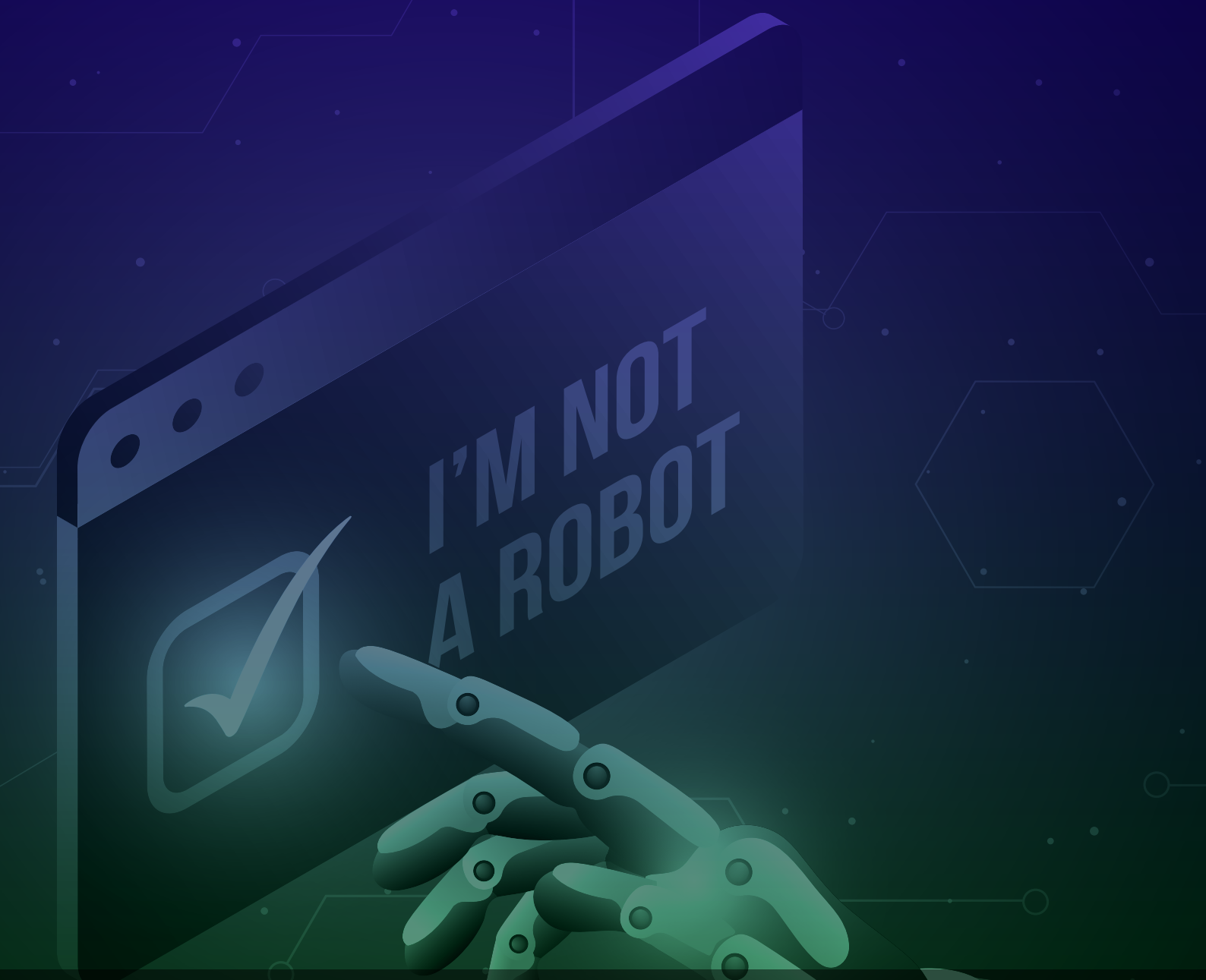
Arkose Labs

EBOOK



How Legacy CAPTCHAs are Being Conquered by Machines

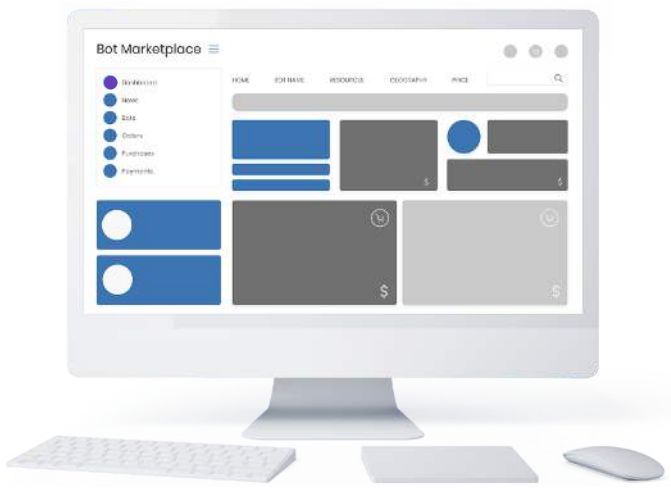
Are You Treating Your Customer like Robots?

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

Balancing fraud prevention with user experience is a fine line to walk for digital businesses. Offering a seamless customer experience is critical to acquiring customers and keeping them loyal, but with ever-increasing levels of online commerce, fraudsters are flocking like a moth to a flame. Businesses need to stop fraudsters from leveraging stolen credentials from compromised digital identities without being too heavy handed and leaving a bad taste in true consumers' mouths.

AN AUTOMATED ARMY OF FRAUD

Fraudsters deploy bots en masse so they can commit fraud at scale and make their enterprises profitable. Today, you don't even need to have any coding or programming skills to successfully use automation to attack businesses; bot scripts can be easily and cheaply purchased on the Dark Web, and video tutorials abound showing the aspiring fraudster a step-by-step lesson on how to deploy them.



Bots come in many different forms. Simple programs can be used to perform brute force attacks, where the individual success rate might be low but the attacks are carried out at such scale that enough are successful. There are also sophisticated, cutting-edge bots that can mimic real human behavior with a frightening degree of accuracy. Unlike humans, bots never need to eat, sleep or go out for walks, meaning they can run attacks continually 24/7.

HERE ARE JUST SOME OF THE COMMON TYPES OF ATTACKS CARRIED OUT BY BOTS:

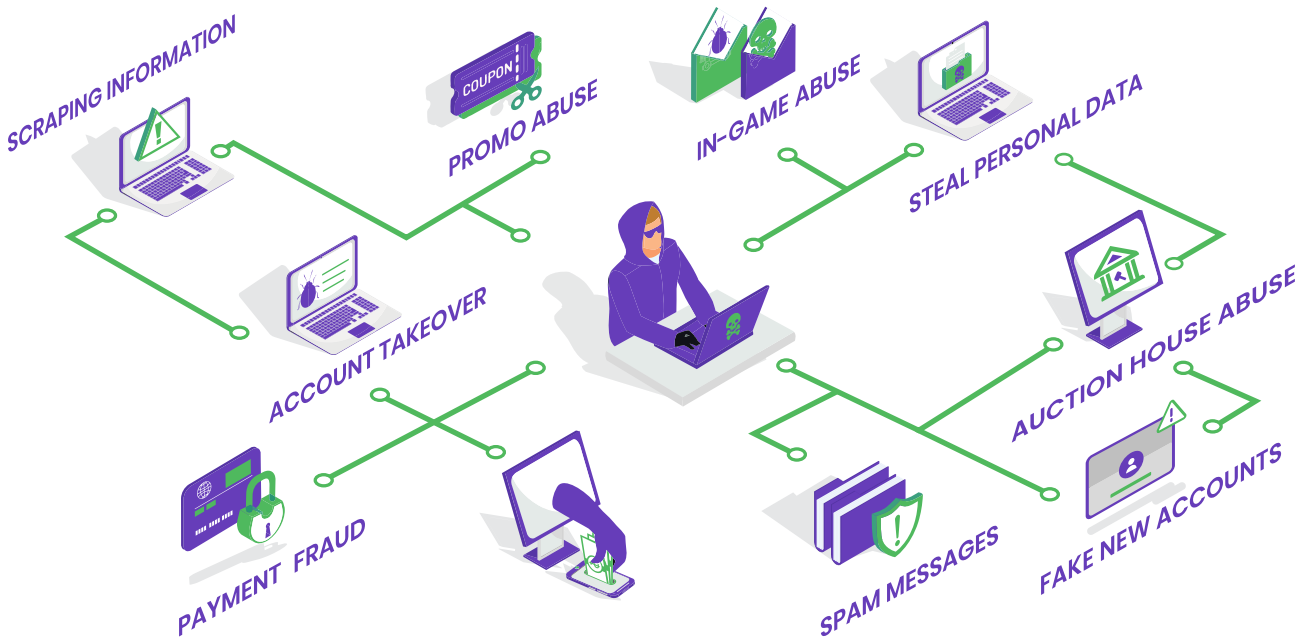
Identity Testing : Whereby bots are used to attempt to verify whether a certain user account exists or not. Once these accounts are known as valid, social engineering or even purchasing login credentials directly can then be used to gain access.

Credential Stuffing : Bots can be used by an attacker that has purchased a list of credentials on the dark web to use them against a targeted website in an attempt to take over an account. Accounts that are taken over are then used to commit fraud or sold on the dark web for someone else to carry out the fraud.

Fake Reviews : Bots are used to leave fake reviews, upvote or downvote videos, create fraudulent ratings for other users on a platform, and similar manipulation. This is done for a variety of reasons, for example an eBay seller using automation to leave negative feedback for other sellers in order to gain a competitive edge. This type of abuse erodes trust in ecommerce and P2P platforms, which ultimately undermines the credibility of the entire ecosystem.

Online Gaming Attacks : Bots have infested gaming platforms to perform fraud such as auction house abuse or manipulating in-game economies. They are also deployed to open new accounts at scale to take advantage of promotional or bonus offers meant to entice new customers to sign up for the service.

Phishing : Bots have also been deployed to send spam and phishing messages in platforms where users frequently message one another. One example of this is dating apps, where fraudulent, bot-powered accounts send messages en masse to good users seeking to get them to download a malicious link that could install malware on their device.



LEGACY SOLUTIONS HAVE SEVERE LIMITATIONS

Automated attacks in the digital realm are nothing new -- fraudsters have been using bots for almost as long as the internet has been around. The difference is that bot-mitigation solutions have not evolved along with the attacks themselves. Most are playing catch-up to the advanced automation available today, which ends up as a constant cat and mouse game between businesses and attacker; one where good users end up being the victim.

Bot prevention solutions range greatly in how they operate and how effective they are. They can range from simple signature-based one-off solutions, to those focused on stopping one specific use case (such as scraping) and those that employ risk-based metrics.

THE ARKOSE HIERARCHY OF BOT DETECTION SOLUTIONS

NO SUCH THING AS A FREE LUNCH

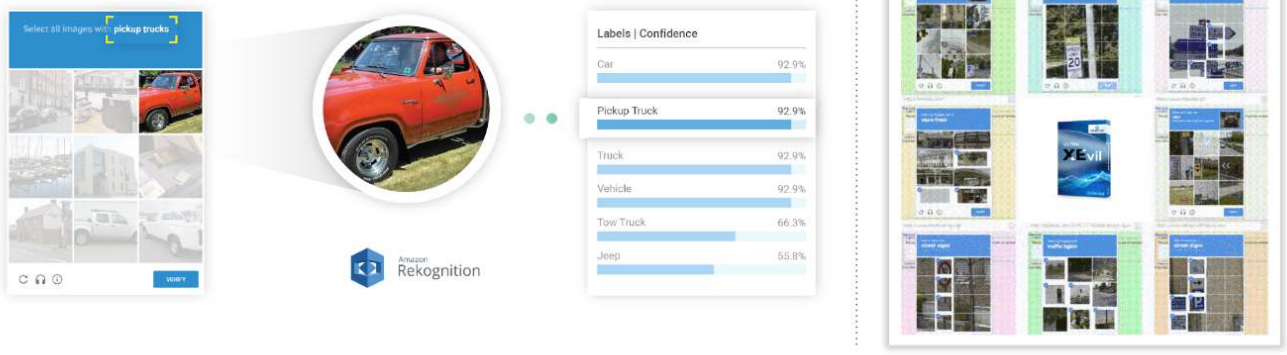
Unfortunately, many companies utilize free -- or nearly free -- bot defense solutions with the notion that they can then defend against this masse of automated attacks without a large investment. However, though their cost may be little, businesses are actually paying a heavy price by using these tools in two key ways:

Effectiveness : Legacy CAPTHCAS are routinely bypassed by even the most basic automated scripts. Even doing just a simple web search reveals dozens of marketplaces offering to sell bots that bypass CAPTCHAs for as little as twenty dollars per year. It's safe to say that even the most novice fraudster can initiate attacks that can easily bypass these.

Furthermore, legacy solutions can be a black box approach that offer no insight or analysis to the companies that use them, making decisions without giving the context. It can tell you the amount of instances where bots or malicious humans broke through, but not why, or how to remediate the problem in the future and prevent it from happening again.

User Experience : There's a common saying: if you aren't paying for the product, you are the product. That's certainly true for free solutions and unfortunately, your customers are the ones paying. These solutions are, ironically, easy for bots to pass through but frustrating for humans. User complaints about having to continually click on crosswalks or images of buses have become commonplace in today's internet. Also, some free solutions collect vast amounts of user data, which leads to privacy concerns among consumers, and a distrust towards businesses that force them to jump through these hoops.

These free solutions don't effectively stop bots, and annoy your genuine customers. You get what you pay for, and the ultimate cost far exceeds the initial investment.



Typical reCAPTCHA
Standard puzzle

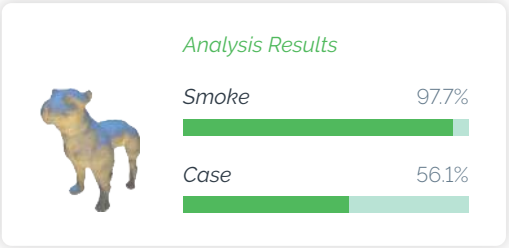
Image Recognition API
Processes each image in grid

95% Automated Solve Rate
Using AWS Rekognition

xEvil.net Weaponized
$400, 100% solve rate

A BETTER PATH FORWARD

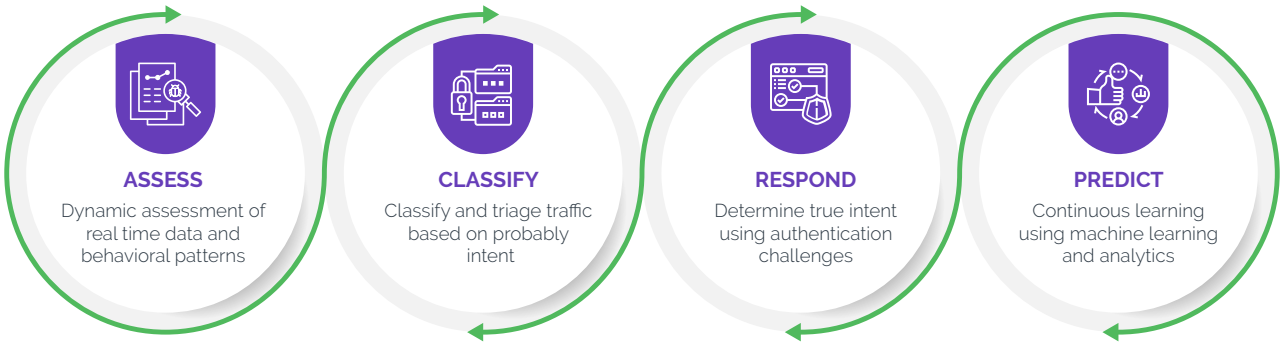
Companies need solutions that are designed against the latest innovations in machine learning, and constantly evolve to adapt to the latest threats in bot technology. It's also imperative to go beyond mitigation-focused strategies such as threat scores and behavioral analysis to overcome fraud and



automated abuse. This has the ancillary effect of improving the customer experience, reducing false positives and ensuring the least amount of good users see any friction at all.

The Arkose Labs approach is different from others on the market today. The platform utilizes deep data analytics and analysis of heuristics to determine the intent of each user, examining more than 300 data points in real-time to create digital "telltales." It then serves the appropriate step-up challenge to bots or malicious human traffic. It's important to note these challenges are specifically designed against even the most bleeding-edge innovations in bot technology. Arkose Labs looks at intent, rather than identity, and captures no user PII except for IP addresses.

Additionally, Arkose Labs offers ongoing managed services and actionable insights to help businesses continually better identify and stop fraud. The platform utilized machine learning to constantly evolve and combat every form of fraud attack.



ARKOSE LABS HELPS MICROSOFT OUTLOOK.COM ELIMINATE BOT-POWERED ATTACKS

Business Problem

- Large-scale fake account registrations
- Email accounts used for malicious and fraudulent purposes
- Fraud mitigation disrupted good user experience

Outlook.com needed a new way to stop fraudulent new account creations, reduce abuse, while improving customer experience - all in a cost-effective manner. This was important not only to protect their own users but to create a safer environment for the wider ecosystem.

Solution

- Unified authentication for new users
- Innovative challenges stop bots and fraudsters
- Malicious emails detected and challenged downstream

Results

- 33% improvement in good customer throughput
- 98% reduction in fraud and abuse
- Stopped customer complaints about SMS verification

CAFFEINE.TV KICKS FRAUDSTERS OUT OF DIGITAL STREAMING WITH ARKOSE LABS

Business Problem

- Bot attacks emanating from bogus accounts
- Potential disruption to users watching and streaming events
- Fake accounts hindered customer experience

Caffeine.tv, an up-and-coming social broadcasting platform popular with a younger demographic, saw a spike in bot-powered new accounts that would attempt to disrupt the platform. As an innovative live streaming service which is experiencing rapid growth in popularity, Caffeine.tv knew it had to protect itself from these fraud attacks and maintain the top-notch digital experience its customers have come to expect.

Solution

- Arkose Labs detected anomalous traffic that indicated bot activity
- Automated attacks were then subsequently stopped
- Arkose Labs showed significant improvement over previous solution (reCaptcha)

Results

- All bot attacks attempting to disrupt the site were stopped
- Spam against good users was eliminated
- Overall better customer experience was created

CONCLUSION

Legacy CAPTHCAS are an antiquated tool from another age. Using them would be like going into modern warfare with a broadsword and knight's armor. Bots -- and the sophistication of fraud attacks in general -- have evolved to the point where these solutions are no longer viable. In today's fast-moving digital environment, companies need a fraud prevention platform that can accurately determine the intent of each user, and then serve the appropriate step-up challenge to stop bots in their tracks. With a constantly evolving platform, you can be assured that your businesses will be p;rotected from fraud both now and in the future.

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.

Sales:

(800) 604-3319

Mail:

support@arkoselabs.com

Address:

USA • 250 Montgomery St, Fl 10, San Francisco, CA. 94104

Australia • 315 Brunswick St, Fl 2, Brisbane, QLD. 4006

Schedule Demo