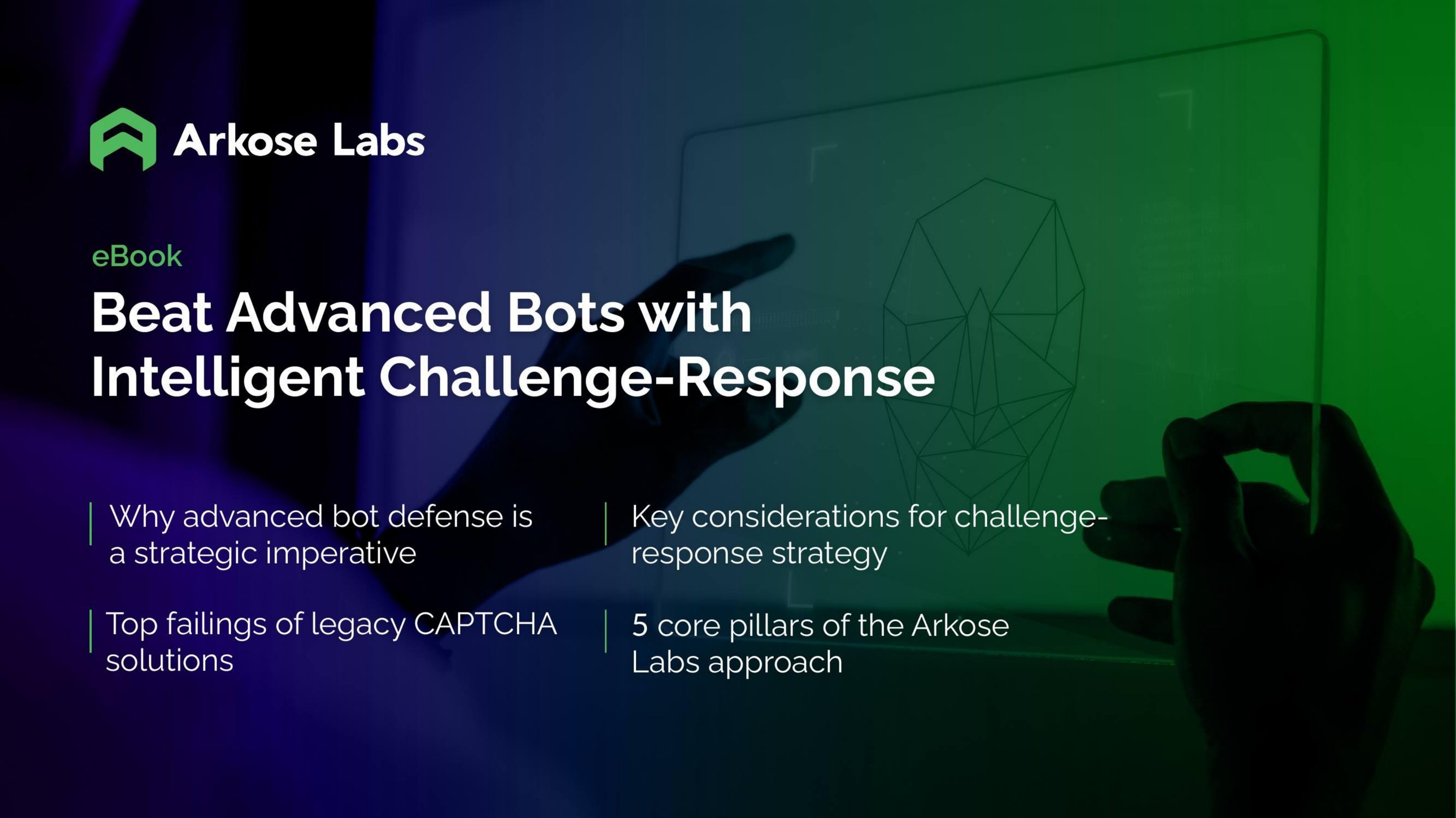
Arkose Labs

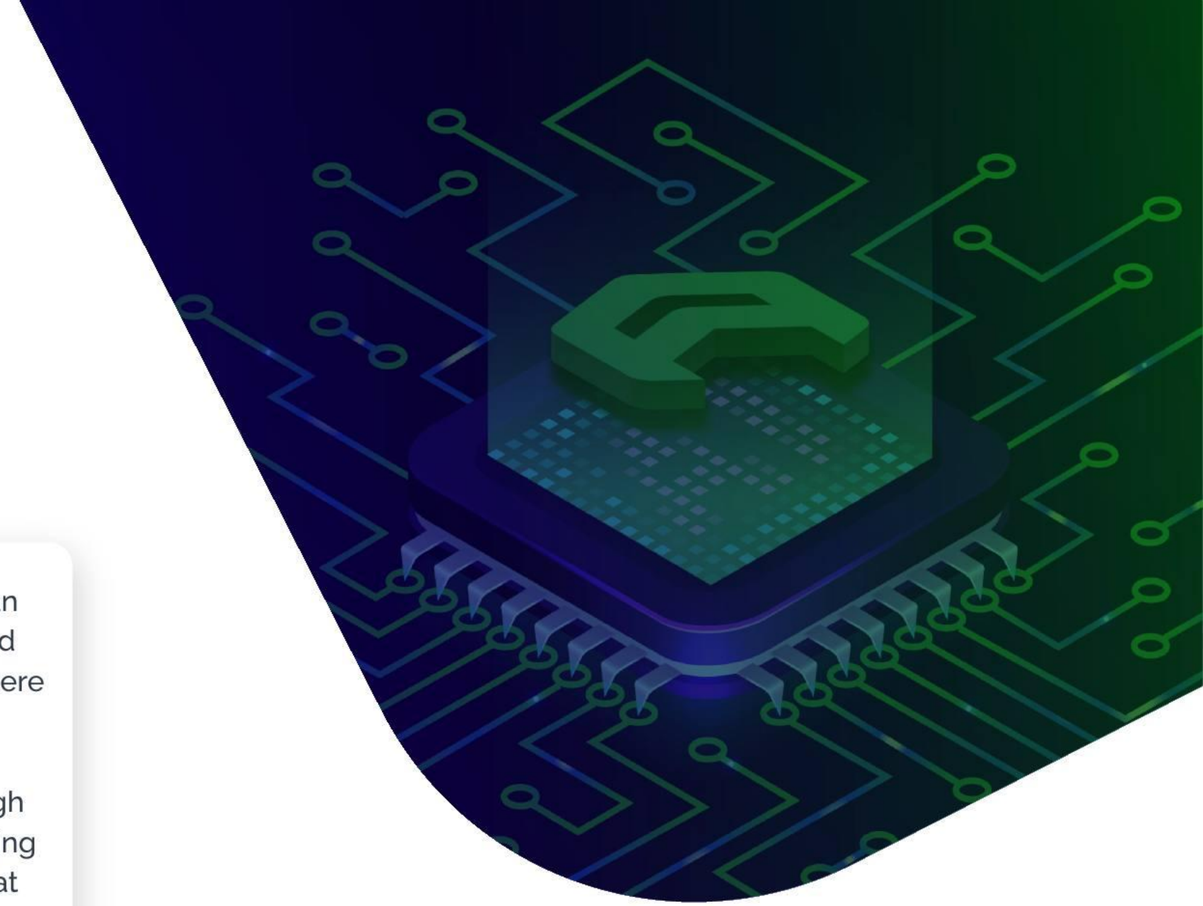
eBook

Beat Advanced Bots with Intelligent Challenge-Response

- Why advanced bot defense is a strategic imperative
- Top failings of legacy CAPTCHA solutions
- Key considerations for challenge-response strategy
- 5 core pillars of the Arkose Labs approach



The Intelligent Bot Revolution: How Bots Are Evading Defenses



BOT MANAGEMENT IS CRUCIAL FOR DIGITAL BUSINESSES

Bot-driven attacks have been occurring every day since the dawn of digital commerce. Malicious bots result in the theft of billions of dollars every year and threaten the future of every digital business that is not protected against them. Businesses have put technologies in place to detect bots in real-time, and have long relied on in-session user challenges (aka CAPTCHAs) to differentiate between good users and basic bot traffic. However, innovation in this type of anti-bot defense has not kept pace with advancements in attacks.

INCREASING UNCERTAINTY IN IDENTIFYING MALICIOUS BOTS

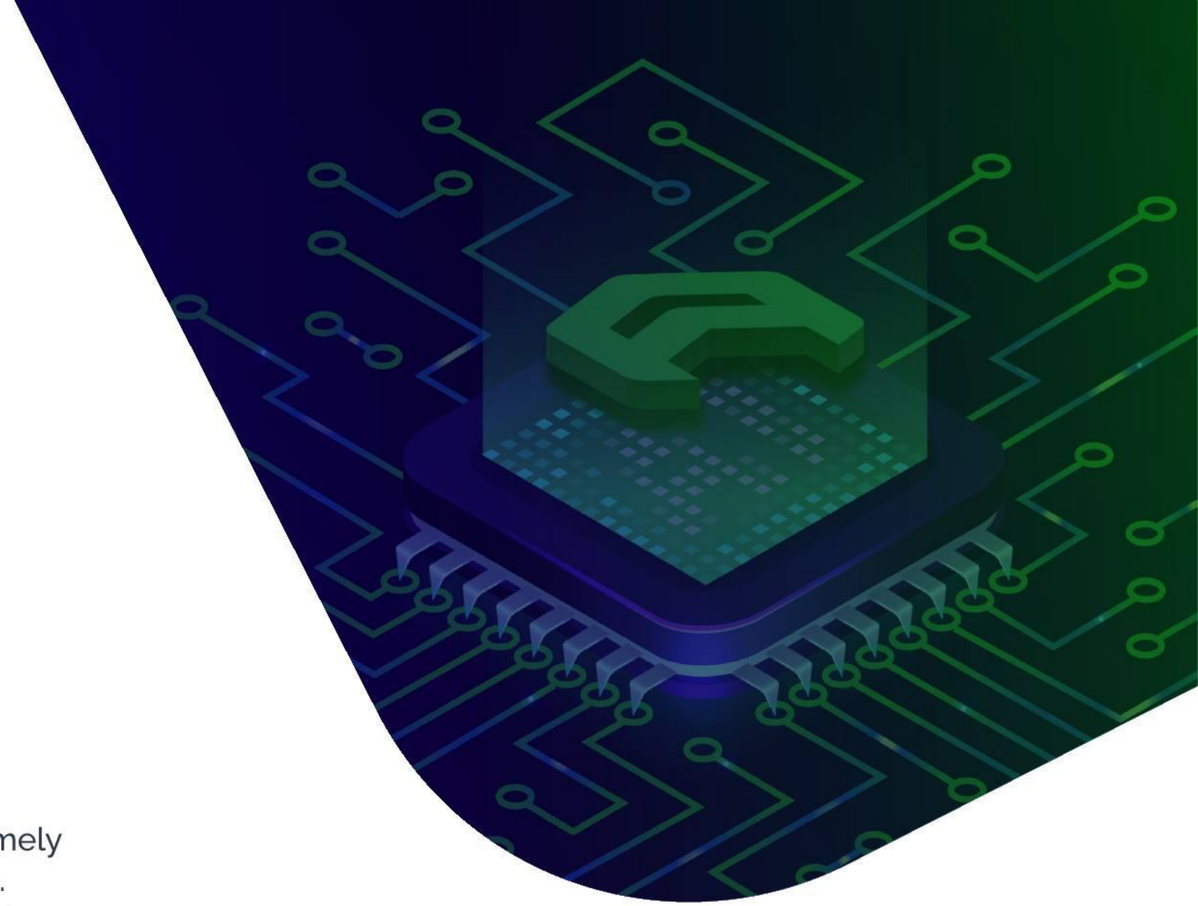
Most real-time bot detection tools can identify extremely high-risk traffic, and identify extremely low-risk traffic. Where they struggle, however, is in knowing what to do with activity that falls between the gray area of extreme high and low risk. This gray area is increasing as bots get smarter and more adept at mimicking human behavior, leading to increased costs for businesses. To protect themselves from attack, digital commerce professionals need a solution that can detect and stop modern, sophisticated bot attacks - one that can identify both high and low-risk activity, as well as the gray area in between, in order to maximize cost savings and improve overall ROI.

Arkose Labs Vision:

We believe businesses can be more resilient to bot attacks, resulting in cost savings and improved ROI, while still allowing good users to access their services.

DOWNLOAD OUR FREE EBOOK

The Intelligent Bot Revolution: How Bots Are Evading Defenses



BOT MANAGEMENT IS CRUCIAL FOR DIGITAL BUSINESSES

Bot-driven attacks have been occurring every day since the dawn of digital commerce. Malicious bots result in the theft of billions of dollars every year and threaten the future of every digital business that is not protected against them. Businesses have put technologies in place to detect bots in real-time, and have long relied on in-session user challenges (aka CAPTCHAs) to differentiate between good users and basic bot traffic. However, innovation in this type of anti-bot defense has not kept pace with advancements in attacks.

INCREASING UNCERTAINTY IN IDENTIFYING MALICIOUS BOTS

Most real-time bot detection tools can identify extremely high-risk traffic, and identify extremely low-risk traffic. Where they struggle, however, is in knowing what to do with activity that falls between the gray area of extreme high and low risk. This gray area is increasing as bots get smarter and more adept at mimicking human behavior, leading to increased costs for businesses. To protect themselves from attack, digital commerce professionals need a solution that can detect and stop modern, sophisticated bot attacks - one that can identify both high and low-risk activity, as well as the gray area in between, in order to maximize cost savings and improve overall ROI.

Arkose Labs Vision:

We believe businesses can be more resilient to bot attacks, resulting in cost savings and improved ROI, while still allowing good users to access their services.

DOWNLOAD OUR FREE EBOOK

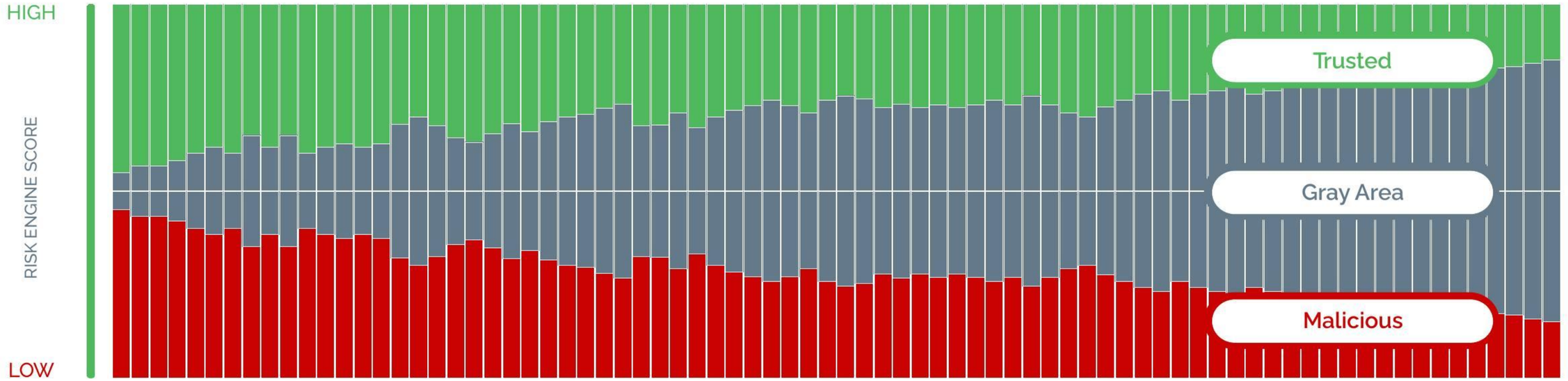
Why Digital Businesses Need a Challenge-Response Strategy

Challenge-response verifications (aka CAPTCHAs) have been used over the last 15 years as a way to defend digital businesses from bot attacks. Interactive puzzles are presented during user interactions to test for human responses, so that unwanted bot traffic gets no further.

Flawed execution by legacy CAPTCHA providers has earned this technology a bad reputation. But in today's threat landscape it is more important than ever to have an effective, in-session challenge strategy to frustrate bot traffic.

Risk-based detection systems are dealing with a growing "gray area" of digital traffic, where risk signals are inconclusive. No matter what platform you use, this gray area is expanding as bots get smarter and stolen data gets richer. The growing gray area leads to user pain from false positives, when good traffic is blocked as malicious, or false negatives, which allow attacks to get through.

By utilizing a solution that accurately differentiates between malicious and trusted activity, digital businesses can not only save costs and boost their ROI, but also test and interact with suspicious traffic to determine true intent.



Why Traditional Methods Fail to Stop Today's Bots

Despite the strategic importance of protecting digital platforms from bots while preserving UX, there has been a lack of innovation in challenge-response technologies. Businesses have often relied on free, cheap, or home-grown capabilities, which have all struggled to keep up with the demands of today's digital landscape.

Puzzles are often created using images that can be recognized and classified by machine vision software - rendering them vulnerable to automated solvers. Furthermore, popular providers of these free or inexpensive solutions often monetize visual challenge solving as an image labeling service. This has helped to create off-the-shelf optical character recognition (OCR) and Image Recognition software. This is the same software which, ironically, is then used by attackers to create automated attacks at scale.

As a result of a lack of investment into creating more innovative challenges, these traditional methods now stand little resistance against cheap bot attacks and leave many digital businesses vulnerable.

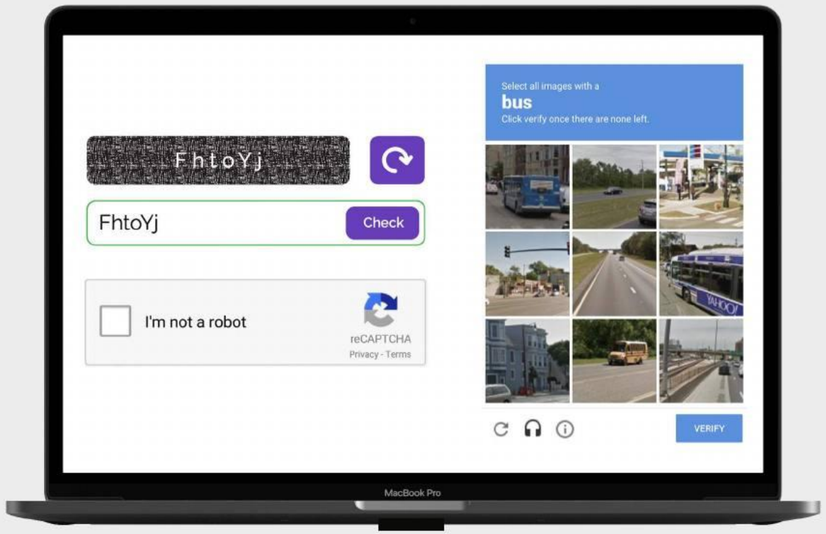
The User Experience Imperative

In today's fiercely competitive digital economy, platforms need to ensure that user experience is central to all they do - including their security measures.

Solutions with basic challenge designs and high user interdiction rates fall short of today's expectations on user experience. Traditional methods vary from entering the text shown on a fuzzy or distorted image, ticking a checkbox, or selecting a particular object from a range of different images. They are deemed annoying and frustrating, and have consistently led to decreased user throughput rates.

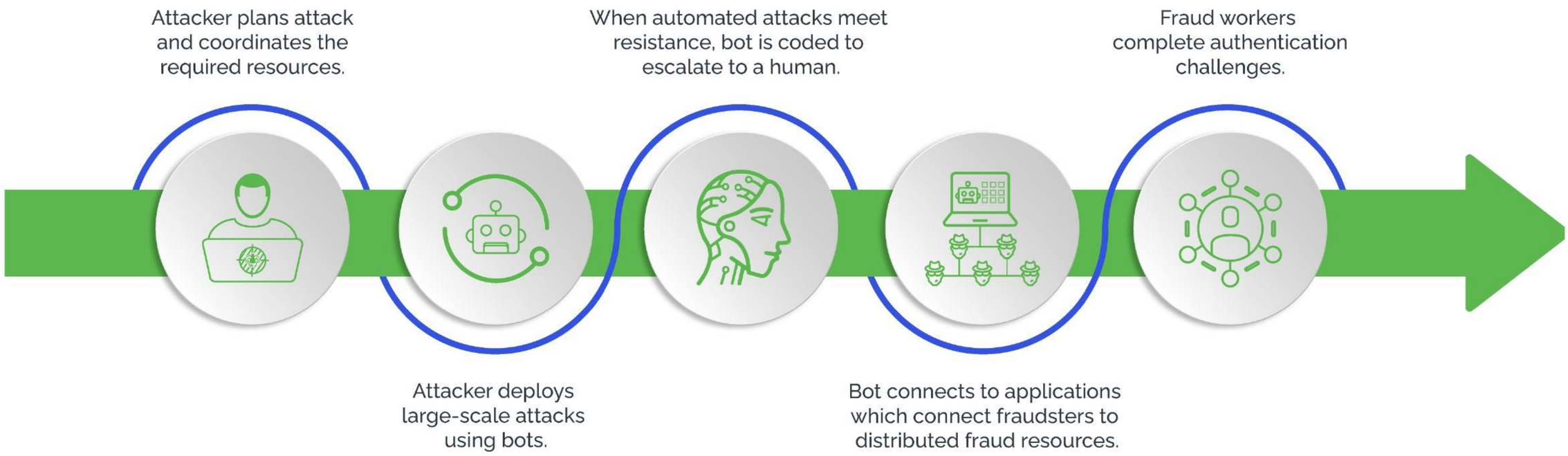
User experience must be central to any challenge-response strategy. The number of good users seeing challenges should be monitored carefully, leveraging advanced risk assessments to keep disruption to a minimum. Puzzles need extensive testing for first time user pass rates and solve times. The few good users who do see challenges should be able to solve quickly and self-remediate easily.

Legacy CAPTCHAs have Failed to Keep Up with UX Expectations



Effective Solutions Must Protect Against Both Bots and Human Fraud Farms

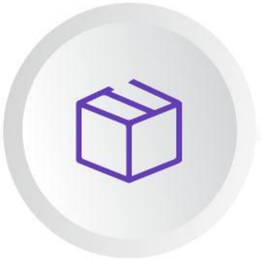
Attackers utilize bots and automation to launch attacks at scale, but they also rely on humans to step in and circumvent anti-bot defenses. The global cybercrime ecosystem provides cheap and easy access to teams of fraud farms, while keeping attackers' costs low to ensure they profit from on attacks. Humans carry out more nuanced attacks than bots, and organized CAPTCHA solver services will bypass challenge-response systems at scale. These workers can operate in a centralized location, or more increasingly through a distributed model where they are connected digitally, and often work on multiple devices at the same time for maximum efficiency. Fraud farm marketplaces now even offer cybercrime "as-a-service" with support upgrades, mimicking the business models of legitimate service providers. Businesses now need to invest in defending against these hybrid attacks, which can disrupt existing defenses, in order to obtain better cost savings. Making it a priority to stop malicious humans as well as bots is essential for businesses to protect themselves and their customers while finding a better ROI.



Intelligent Detection Requires Transparency & Support

Businesses are making do with blackbox solutions that provide little enterprise customer support. These offer little transparency to businesses on how risk determinations were arrived at, and do not provide a feedback loop.

Limitations of Legacy CAPTCHAS



Black-Box Approach

Traditional methods are not transparent in showing how they assess risks, leading to a black box situation which customers have to blindly trust.

No Feedback Loop

There is no way for customers to provide feedback on user activities, risk scores and response actions to train the models to make better decisions.

No Data Access

Customers do not have access to the risk data collected from their own environments, to use in their own models and help with downstream decisions.

No Customer Support

Customers are reliant on online forums or articles but there is no dedicated managed service team to provide hands-on support when required.

The Arkose Labs Approach

Arkose Labs brings a fresh approach to bot detection and challenge-response, which drives up the cost and time required to carry out attacks. This erodes attackers' ROI and provides digital enterprises with long term attack deterrence and account security - all while enhancing the good user experience and saving money on long-term protection.

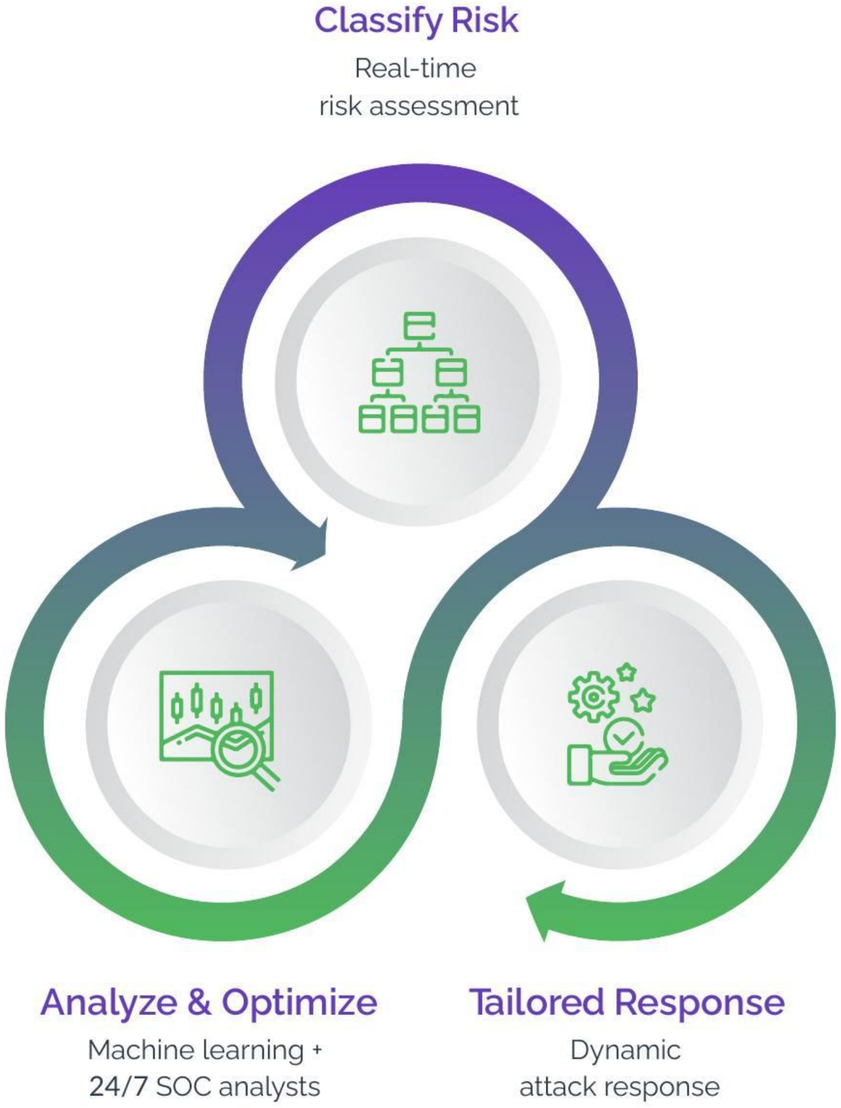
We work across a range of different use cases, helping protect the most targeted user action points across the digital front-end.

Our AI-powered platform combines sophisticated attack detection risk analysis and user-centric enforcement challenges to defeat persistent bots and frustrate coordinated human-driven attacks.

Crucial to our product design is the continuous feedback loop between real-time bot detection, user challenges, and advanced analytics.

We use a wide range of different technologies to ensure:

- We stop and deter attacks, long-term
- We provide transparency and support
- We provide excellent end-user experience
- We offer long-term cost savings and a more robust ROI



It All Starts with Powerful Bot Detection & Good User Recognition

The first step to ensure you have the greatest resilience to online attacks, alongside the least restriction to good users, is an advanced and multi-layered bot detection system which works behind the scenes to recognise good users.

Arkose Detect utilizes contextual, historic and network data on a wide-range of data attributes to provide risk classification, behavioral analytics and a smart AI decisioning system that calculates risk behind the scenes, so that 99% of good users enjoy a friction-free user experience.

Only risky malicious traffic is directed to a challenge, with the aim of making it slower, costlier and more difficult for attackers. Arkose Enforce provides a targeted attack response, which is tailored to the exact risk profile.

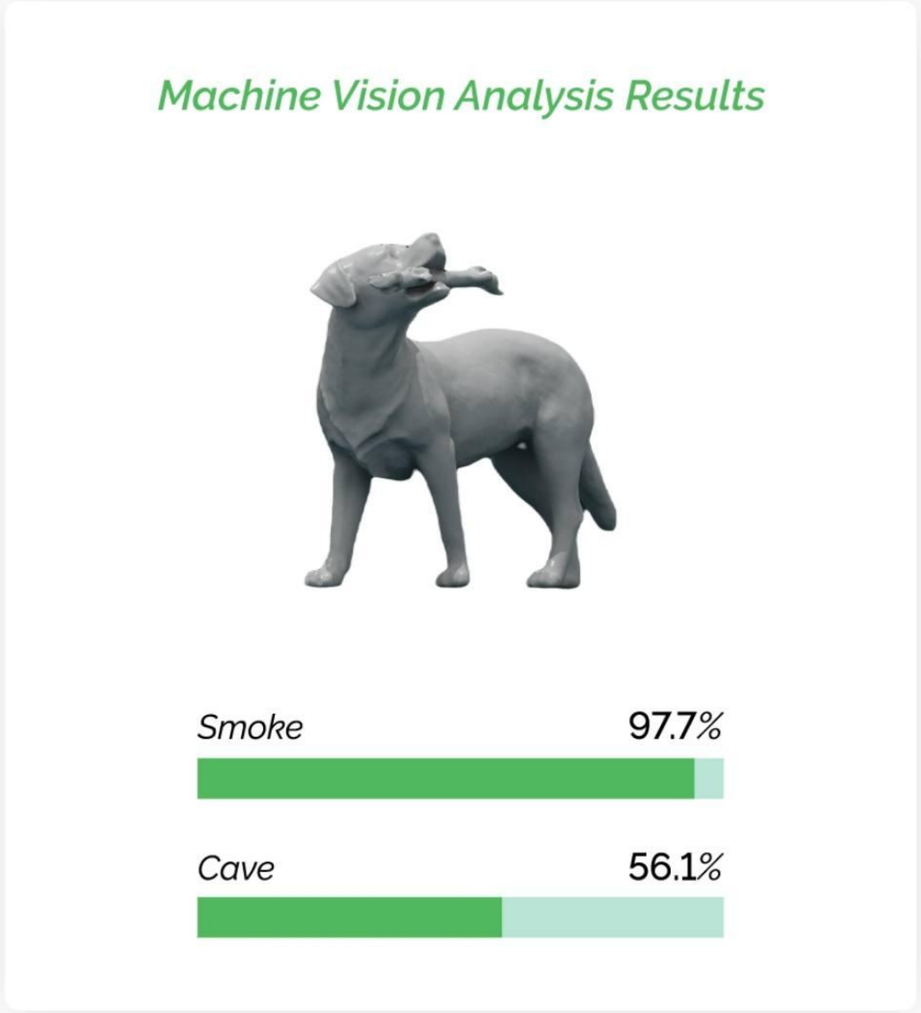
We continually research and develop innovative technologies to ensure we stay one step ahead of attackers, while dramatically improving good user experience and offering businesses considerable cost savings.

Defeating Bots with Innovative Challenges

Arkose Labs creates context-based enforcement challenges, which are tested extensively against the latest innovations in machine vision, to defend against automated solvers. Images are rendered in real-time using 3D software, leading to countless possible permutations. They are designed by specialized security artists, so that AI image recognition tools cannot distinguish something that, to the human eye, is obviously the shape of a dog, but instead classifies it as smoke or a cave.

As with all security measures, we expect attackers to attempt to evade these challenges and factor that into our approach. The depth and breadth of our challenge roster, alongside their innovative design, ensures that it is expensive and time-consuming to create solvers. Attackers are therefore more likely to give up when they encounter this type of challenge and attack a business using challenges that can easily be beaten by a bot.

Additionally, Arkose Labs has an expert team of Security Operations Center analysts constantly monitoring activity. When there are suspicious spikes in activity, challenge types will be swapped out, putting the attackers back to square one. We also have a team of product designers who are constantly working on new designs, always keeping our customers one step ahead of the attackers and helping them find more savings.



How Arkose Labs Challenges Stop Fraud Farms

Catching bot traffic is one thing, but to protect businesses from large-scale, coordinated attacks, they need defenses tailored specifically to the threat of fraud farms and challenge solver services as well. Arkose Labs proactively tracks organized human attack operations, and profiles this traffic using multi-layered risk assessments to detect it across the global customer network.

The type of challenge shown to a malicious human is very different to one used to defeat a bot. The aim here is to increase the complexity of puzzles and analyze solve rates/times to build evidence of malicious human activity. Human fraud puzzles can take 3x as long to complete, in order to intentionally waste time and collect more user interaction data.

As the financial margins of attackers are lower when using more expensive human resources, increasing the time and money needed to carry out attacks is a highly effective way to see attacks drop off. The financial viability of the attack is ruined, and perpetrators will move on to the next target.

How Arkose Labs Challenges Stop Fraud Farms

RESULT

Attacker's ROI is destroyed and deters them from attacking this site with challenges designed to defeat fraud farms

Catching bot traffic is one thing, but to protect businesses from large-scale, coordinated attacks, they need defenses tailored specifically to the threat of fraud farms and challenge solver services as well. Arkose Labs proactively tracks organized human attack operations, and profiles this traffic using multi-layered risk assessments to detect it across the global customer network.

The type of challenge shown to a malicious human is very different to one used to defeat a bot. The aim here is to increase the complexity of puzzles and analyze solve rates/times to build evidence of malicious human activity. Human fraud puzzles can take 3x as long to complete, in order to intentionally waste time and collect more user interaction data.

As the financial margins of attackers are lower when using more expensive human resources, increasing the time and money needed to carry out attacks is a highly effective way to see attacks drop off. The financial viability of the attack is ruined, and perpetrators will move on to the next target.

Arkose Labs Provides Businesses with Transparency

Example of data provided by alternative solutions:

Risk Score differences:

reC

```
{
  "score": 0-100,
  "reasons": [
    enum (CLASSIFICATION_REASON_UNSPECIFIED, AUTOMATION, UNEXPECTED_ENVIRONMENT, TOO_MUCH_TRAFFIC,
LOW_CONFIDENCE_SCORE)
  ]
}
```

Having the right data makes a big difference in the accuracy of risk models. At Arkose Labs, we go beyond a black box approach, delivering detailed attributes with clients on an ongoing basis for actionable insights to adapt to changing attack patterns fast.

Providing the data empowers our customers to use our real-time insights and data to make sense of all decisions, not blindly following a machine-given score. This allows for more informed decisions, resulting in cost savings and better ROI. It also provides analysis which can be used downstream to provide further protection.

Data provided by Arkose Labs:

Arkose


```
{
    "session_risk": {
      "risk_category": "BOT-STD",
      "risk_band": "Medium",
      "global"
       {
         "score": "15",
         "telltales":[
         {
           "name": "g-h-cfp-1000000000",
           "weight": "7"
         }
         {
           "name": "g-os-impersonation-win",
           "weight": "8"
         }]
       }
       "custom"
       {
         "score": "15",
         "telltales":[
         {
           "name": "outdated-browser-yandex-2",
           "weight": "7"
         }
         {
           "name": "outdated-os-yandex",
           "weight": "8"
         }]
       }
    },
    "session_details": {
        "solved": true,
        "session": "22612c147bb418c8.2570749403",
        "session_created": "2021-08-29T23:13:03+00:00",
        "check_answer": "2021-08-29T23:13:16+00:00",
        "verified": "2021-08-30T00:19:32+00:00",
        "attempted": true,
        "security_level": 30,
        "session_is_legit": false,
        "previously_verified": true,
        "session_timed_out": true,
        "suppress_limited": false,
        "theme_arg_invalid": false,
        "suppressed": false,
        "punishable_actioned": false,
        "telltale_user": "eng-1362-game3-py-0.",
        "failed_low_sec_validation": false,
        "lowsec_error": null,
        "lowsec_level_denied": null,
        "ua": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.159 Safari/537.36",
        "ip_rep_list": null,
        "game_number_limit_reached": false,
        "user_language_shown": "en",
        "telltale_list": [
            "eng-1362",
            "eng-1362-game3-py-0."
        ],
        "optional": null
    },
    "fingerprint": {
        "browser_characteristics": {
            "browser_name": "Chrome",
            "browser_version": "92.0.4515.159",
            "color_depth": 24,
            "session_storage": false,
            "indexed_database": false,
            "canvas_fingerprint": 1652956812
        },
        "device_characteristics": {
            "operating_system": null,
            "operating_system_version": null,
            "screen_resolution": [
                1920,
                1080
            ],
            "max_resolution_supported": [
                1920,
                1057
            ],
            "behavior": false,
            "cpu_class": "unknown",
            "platform": "MacIntel",
            "touch_support": false,
            "hardware_concurrency": 8
        },
        "user_preferences": {
            "timezone_offset": -600
        }
    },
    "ip_intelligence": {
        "user_ip": "10.211.121.196",
        "is_tor": false,
        "is_vpn": true,
        "is_proxy": true,
        "is_bot": true,
        "country": "AU",
        "region": "New South Wales",
        "city": "Sydney",
        "isp": "Amazon.com",
        "public_access_point": false,
        "connection_type": "Data Center",
        "latitude": "-38.85120035",
        "longitude": "106.21220398",
        "timezone": "Australia/Sydney"
    }
}
```

Arkose Labs Goes Above and Beyond for Clients

Technical Support

Support is available 24x7x365 for technical questions, non-critical bugs, and enhancement requests.

Proactive Risk Management

The Arkose Labs SOC provides 24x7 monitoring and anomaly detection to keep a watchful eye on your traffic and proactively flag potential threats.

Incident Response

Arkose Labs offers guaranteed response & remediation SLAs to minimize damage and disruption in the event of an attack.

Security Advisory Services

Regularly scheduled reviews of traffic on your workflow allows us to fine tune your instance to attack patterns and keep you one step ahead of attackers.

> "What I respect the most about our partnership is that they are there to troubleshoot with you when you need them. They worked with us closely to address an error that we initially thought was related to Arkose but ended up being on our side. It is easy to provide a good experience when things go well, but what makes a difference is being there when things go south. Arkose didn't drop the ball, and thanks to that, we provide a much better experience now."

Dropbox

Director of Engineering
Dropbox

User-Experience with Arkose Labs

Arkose Labs' AI-powered platform performs smart but invisible risk assessments that result in a frictionless experience for good users, whilst being impossible for fraudsters to profitably break the security defenses. Implementing Arkose Labs has provided businesses an uptick in good user experience whilst detecting and stopping bot attacks.

LOW CHALLENGE RATES

99% of good users experience no friction or hindrances

MINIMAL FRICTION

Users are never made to navigate to another system to complete authentication

ACCESSIBILITY FOR ALL USERS

Accessibility-first design ensures that all users have a smooth experience regardless of disability status.

PRIVACY PROTECTED

Arkose Labs doesn't use personal data or people's personal preferences in their risk scores

Before and After: How Arkose Labs will Impact Your Business

Our customers have seen the real business benefits of replacing their legacy CAPTCHA solutions with Arkose Labs. Not only have they experienced improved user throughput, higher legitimate user engagement, and reduced time and money spent on remediating abuse, but they've also seen a long-term drop-off in the volume of bot attacks targeting their business, leading to real cost savings and better ROI. We understand the challenges digital businesses are facing today and we work with them to help protect and grow their businesses, allowing them to enjoy the rewards of their investments.

Growth

70% uptick in good user experience

96% reduced friction on account registration

Reduced downstream banning through better detection

Impact on Bottom Line

99% accuracy at identifying good users

SLA guarantee against automated attacks

Industry-first **$1M** Credential Stuffing Warranty

Operational Transparency & Efficiency

15x more data and insights shared with customers vs competitors

70% reduced human intervention for bot mitigation

Drastically reduced complaints to call centers

Improved Security

Stopped **95%** of fake accounts

22% reduction in scraping

99% reduction in in-game abuse

Arkose Labs' Customer Commitment: Guaranteed Bot Defense

Despite significant investments in bot detection, increasingly sophisticated bot attacks still power the lion's share of attacks on digital businesses. Stopping 99 out of 100 bots isn't a win in our book. Any successful attempt perpetuates the cycle of cybercrime and keeps you a target. Arkose Labs believes in a zero-approach to bots that breaks the cycle of attacks. We are so confident in our approach to stopping automated attacks, that we offer an SLA guarantee against bot attacks, with a promise to remediate attacks within 48 hours.

By partnering with Arkose Labs, customers can not only get a team of experts to support and mitigate threats, but also enjoy cost savings and improved ROI with the industry first Credential Stuffing Warranty, which covers common losses associated with the compromise of accounts. This warranty helps businesses limit financial losses resulting from bad actors getting into user accounts, providing peace of mind and cost savings.

Conclusion:

Why Businesses Need To Invest In Intelligent Challenge-Response

An unfortunate reaction to the issues facing traditional challenge-response technologies has been to throw them out altogether and move to stand-alone risk scoring. This ultimately leads to more issues. Businesses struggle to deal with inconclusive signals and have to turn to MFA or arbitrary block/accept decisions, leading to "false positive pain" for any good users caught in the crossfire.

Challenge-response technologies can offer a highly effective way to protect websites and apps from the evolving, intelligent bots. But only when done correctly.

It all starts with sophisticated bot detection and behavior analytics. Accurate traffic classification will ensure that good users do not face interruptions. Challenges should be reserved for higher risk traffic, with a graduated approach and a varied arsenal of challenges that adapt to the exact risk profile. Constant R&D in challenge resilience to sophisticated bots, solver services and human fraud farms is required. This drives up the costs of attacks for long-term protection.

With Arkose Labs, businesses can replace legacy CAPTCHAs with an advanced bot detection and challenge-response system, reducing their costs and boosting their ROI in the long term. This system dramatically increases the time and effort required to attack the business, delivering resilience against evolving attacks, while also improving user experience.

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 dynamic attack response that undermines the ROI behind attacks while improving good user throughput. Headquartered in San Francisco, CA with offices in Brisbane and Sydney, Australia, San Jose, Costa Rica, Tokyo, Japan, and London, UK, the company debuted as the 83rd fastest-growing company in North America on the 2021 Deloitte Fast500 ranking.

Offices

San Francisco
250 Montgomery St 10th Floor,
San Francisco, CA 94104, USA

Brisbane
315 Brunswick St, Brisbane,
Queensland AU

United Kingdom
167-169 Great Portland Street, 5th
Floor, London, W1W 5PF

Japan
San Jose, Costa Rica
Tokyo

Schedule Demo