January 2025

Arkose Labs

Complementary Security Solutions Are Better Together at Beating Fraudsters and Managing Downstream Digital Identity Costs

Introduction

In today's cybersecurity landscape, CISO organizations at enterprises often rely on web application firewalls (WAFs) and content delivery networks (CDNs), like Akamai and Cloudflare, for protection against application layer attacks, DDoS and some automated bot attacks. These types of solution providers were developed to solve specific security issues, which they do very well. Akamai sits out on the edge and defends against DDoS threats, as does Cloudflare. And both can detect and block some bots.

However, fresh research shows that within the past 12 months (since September 2023) of all attack types enterprises have experienced, 40% have been from AI-powered bots. AI is driving significant changes in attack mechanics, with 88% of enterprises observing an increase in AI-powered bot attacks in the last two years. The increase was 36%.

As attacks—especially malicious bot threats—become more sophisticated and powered by AI, the chink in traditional solutions' armor starts to become apparent. Some of these bots slip past WAFs and CDNs, exposing your networks and systems to risk. While traditional tools help you to detect and mitigate simple bots, by adding Arkose Labs to your security stack, you'll get a managed service experience with dedicated experts who have industry-specific knowledge and a proactive approach. This gives you a robust defense-in-depth strategy, leading to significant cost savings and enhanced security. We make it easy to deploy this 'better together' risk mitigation stack by offering a low-code integration and easy setup.

Wise enterprises have already adopted this strategy. For example, a well-known global leader in the travel booking industry detected and stopped nearly 7,000 sophisticated bot attacks in a single day when deploying the Arkose Labs solution behind Akamai Bot Manager.

Current Protection with WAF and CDN

Most global enterprises use CDNs and WAFs as their primary defense mechanisms, and rightfully so. These tools offer protections like rate limiting, DDoS mitigation, IP address filtering and basic bot management. While these measures are essential, they have started to fall short when dealing with the increase in sophistication of bot attacks, simply because their technology wasn't specifically developed to stop these highly evolved threats.

BOT SOPHISTICATION

Evasions and mitigations

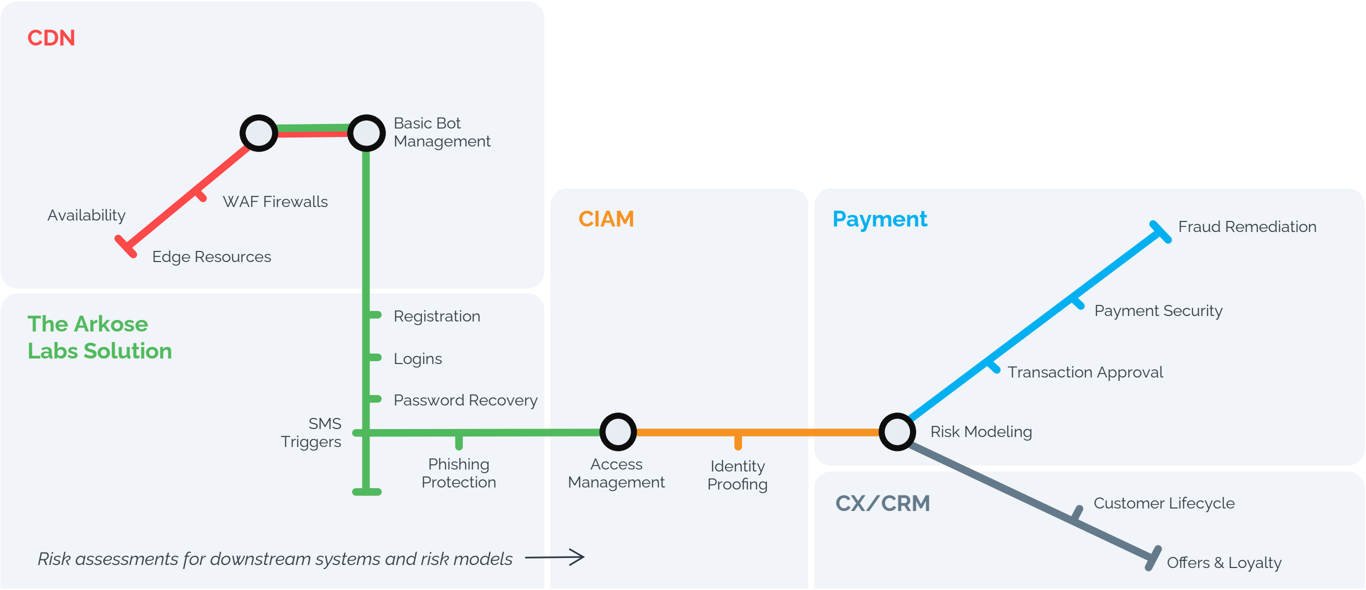
			CDN/WAF	Basic Bot Managers	Arkose Labs
Simple	IP Challenging Rate Limiting	Single IP	✓		✓
		Multiple IPs	✓		✓
		Low request rate	✓		✓
		Randomization user agent		✓	✓
		Browser impersonation		✓	✓
	HTTP Anomaly Detection	Cookie support		✓	✓
		Session replay			✓
	Browser Fingerprinting	JavaScript support		✓	✓
		Browser fingerprint spoofing			✓
Sophisticated	User Behavior Analysis	Recorded human behavior			✓

The Added Value of Arkose Labs

Arkose Labs brings added strength to the cybersecurity stack by providing advanced detection and mitigation strategies that complement existing WAF and CDN solutions. By offering real-time feedback and adaptive challenge mechanisms, Arkose Labs significantly reduces false positives and improves overall security efficacy. Put simply, we adapt based on the sophistication of attacks, so you don't have to.

> **Arkose Labs brings added strength to the cybersecurity stack by providing advanced detection and mitigation strategies that complement existing WAF and CDN solutions.**

Diagram 1: Our solution integrates seamlessly with CDNs and customer identity and access management solutions



Risk assessments for downstream systems and risk models →

> We were built from the ground up to serve enterprises. Unlike some other providers, we combine expert advice and a proactive approach with immediate assistance when you and your team need it most. Our 24/7/365 managed service provides you with continuous support, for the strongest line of defense against attacks. By proactively monitoring customer traffic, we help our customers to respond quickly to emerging threats. With advanced analytics, cross-industry risk intelligence and tailored advice on security best practices, Arkose Labs serves as an extension of our customers' security teams.

In a one-size-fits-all approach, enterprises become tempted to relax deny rules, fearing too many false positives. This creates an environment where attackers only need to look 'just good enough' to slip through. Conversely, our adaptive threat response focuses closely on the level of threat, with a feedback loop between mitigation and detection tools.

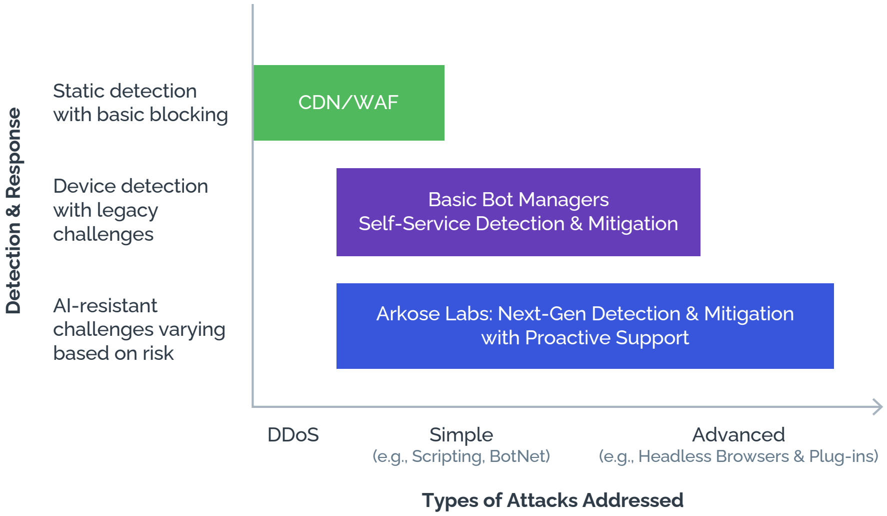
Here's how Arkose Labs enhances enterprises' cybersecurity infrastructure:

1. **Simple Integration:** The Arkose Labs solution is a low/no-code experience that easily integrates into your existing workflows, enhancing their capabilities without requiring a complete overhaul of your cybersecurity framework. Recognized for its ease of administration and effortless integration—earning recent accolades from peer review site G2—it's designed to fit seamlessly into any ecosystem, amplifying your defense strategy with minimal disruption.

2. **Enhanced Detection and Mitigation:** The Arkose Labs solution classifies traffic into low-, medium- and high-risk ranges, managing detection and mitigation strategies dynamically. This approach ensures that sophisticated attacks are identified and neutralized effectively. Our platform offers unparalleled efficacy in threat detection and mitigation. Unlike traditional WAFs and CDNs, our advanced labeling capabilities ensure higher accuracy and effectiveness in identifying and preventing fraudulent activities. Additionally, we provide extensive data sets, enabling our customers to fine-tune, investigate and develop their own risk models internally. This empowers our clients with the insights necessary to enhance their security measures and stay ahead of evolving threats.

3. **Cost Savings:** By reducing the volume of malicious traffic that needs to be processed, the Arkose Labs solution lowers the downstream operational and security costs associated with managing bot attacks.

Diagram 2: Our approach is unrivaled in the market


Detection & Response
Static detection with basic blocking
Device detection with legacy challenges
AI-resistant challenges varying based on risk
CDN/WAF
Basic Bot Managers
Self-Service Detection & Mitigation
Arkose Labs: Next-Gen Detection & Mitigation with Proactive Support
DDoS
Simple
(e.g., Scripting, BotNet)
Advanced
(e.g., Headless Browsers & Plug-ins)
Types of Attacks Addressed

Key Arkose Labs Differentiators

- Insights to fuel internal risk models
- Unrivaled Threat Research Unit
- Global Intelligence Consortium
- Proactive support (24/7/365)
- Financial warranties
- The largest global brands rely on us
- We leverage AI with OpenAI to defend our challenges against AI driven bots

No matter the industry—travel, banking, gaming, etc.—the Arkose Labs solution observes a massive amount of bot attacks slipping past WAF and CDN solutions, meaning that all industries benefit from a more robust defense-in-depth strategy.

Arkose Labs flips the script on genuine user throughput. Too often, good user throughput also equates to letting attacks through. But the Arkose Labs solution allows companies to curtail friction for genuine customers, while also preventing fraud. For example, Adobe reduced the challenge rate for trusted users from 10% to 2% when it switched to the Arkose Labs solution.

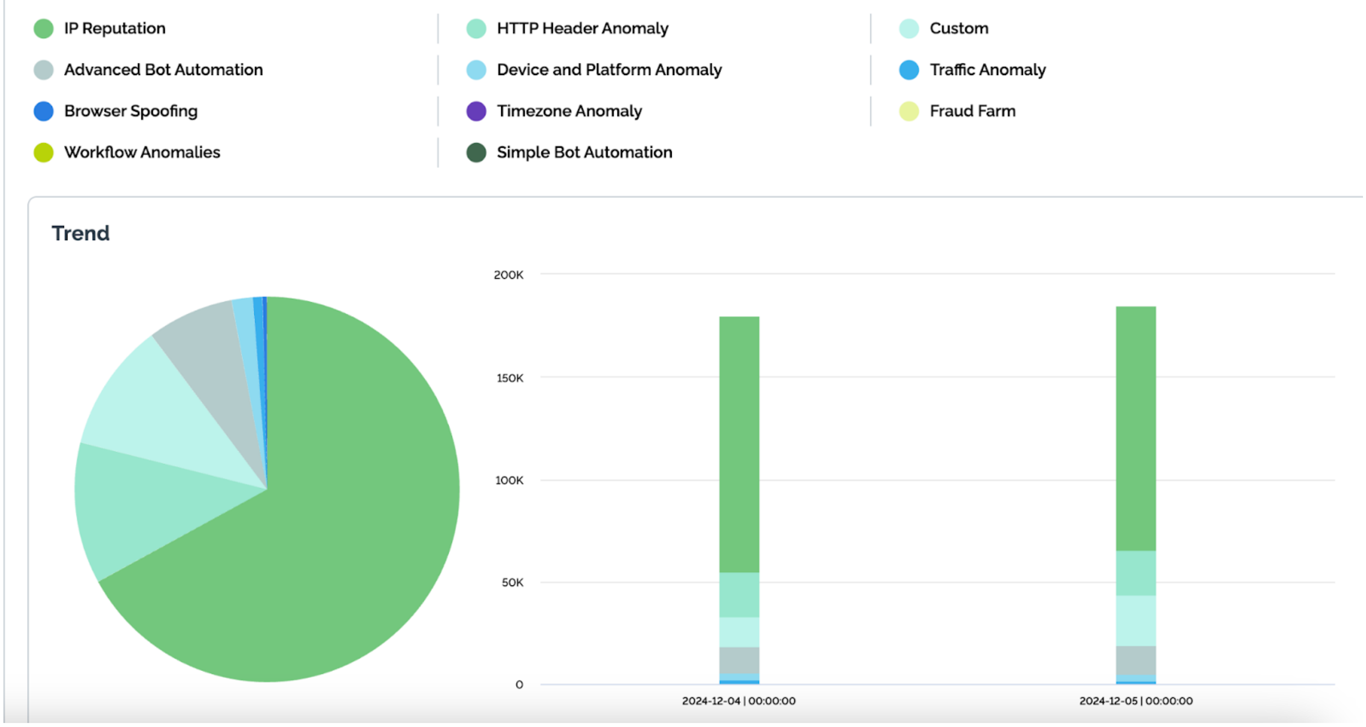
The Arkose Labs solution is dynamic and purpose-built, using the most advanced technology to detect and mitigate sophisticated bot attacks and human fraud farm threats with negligible false positives occurring. Monitoring more than 250 risk signals, the platform uses progressive device and behavior fingerprinting technologies that enable it to accurately detect and immediately stop (versus block) attack types like account takeover, fake account creation, MFA compromise, SMS toll fraud, etc. before they make impact.

By continuously analyzing traffic patterns and device behavior, the platform identifies anomalies indicative of automated threats, reverse-proxy phishing and manual fraud farm attack attempts. Plus, it includes an adaptive challenge-response suite to determine the authenticity of a user interaction.

Data-Driven Intelligence

Significant volumes of attacks that bypass CDN/WAF vendors are detected and mitigated by the Arkose Labs solution. To illustrate its effectiveness, consider the data collected from customers using our platform behind Akamai Bot Manager. In Graph 1 below, you can see some of the data-driven intelligence recently used to detect and thwart a significant attack against a major travel company.

GRAPH 1: Data-driven intelligence used to detect and thwart major attack against a leading travel company



Our data-driven approach highlights the critical gaps in traditional CDN and WAF solutions and showcases how these gaps can be filled effectively for immediate and permanent results.

Complementing Existing Solutions for Stronger ROI

The Arkose Labs solution is designed to work alongside enterprises' current WAF and CDN solutions, providing enhanced security without redundancy. Here's why the Arkose Labs solution is the ideal complement:

1. Adaptive Response: Unlike traditional bot managers that offer simple triage options (allow, deny or challenge), the Arkose Labs solution challenges are integrated into the detection framework, ensuring more accurate and effective responses to threats. Additionally, we deliver world-class threat intelligence from our ACTIR, SOC and Global Intelligence Network, which is a powerful data consortium.

2. Sophisticated Attack Mitigation: As attacks grow more complex, traditional solutions become less effective and more resource-intensive. Arkose Labs addresses this by offering advanced mitigation techniques that evolve with the threat landscape.

3. Transparency and Confidence: By working in tandem with CDNs and WAFs, the Arkose Labs solution enhances their capabilities, providing a comprehensive defense strategy that is more effective than other standalone bot solutions. We offer absolute transparency into risk attribution, going beyond an abstract risk score by sharing the underlying data and rules, so that your team can have full confidence.

Plus, at no extra cost, customers can provide us with truth data for our rules engine, so that false positives can be drastically minimized.

Conclusion: It's Better Together

By using only traditional CDN and WAF solutions, like Akamai and Cloudflare, your security could suffer in the face of more sophisticated volumetric bot attacks. By adding in the Arkose Labs solution, you'll be able to proactively detect and stop the most advanced threat campaigns aimed at your company, with readiness for the fraud landscape of tomorrow. Adding the Arkose Labs solution as a complementary accelerant into your existing WAF and CDN workflows completes a robust defense-in-depth strategy that enhances protection, improves detection and mitigation of sophisticated attacks and reduces significant costs.

For example, when one of the largest banks deployed the Arkose Labs solution in the middle of Akamai and LexisNexis® ThreatMetrix, the volume of "unknown sessions" was abated to near zero. That's a game changer. The bank saved hundreds of thousands of dollars it had been paying to ThreatMetrix for the assessment of massive amounts of unknown sessions.

GRAPH 2: A big bank deployed the Arkose Labs solution in the middle of Akamai and LexisNexis® ThreatMetrix and saved hundreds of thousands of dollars.

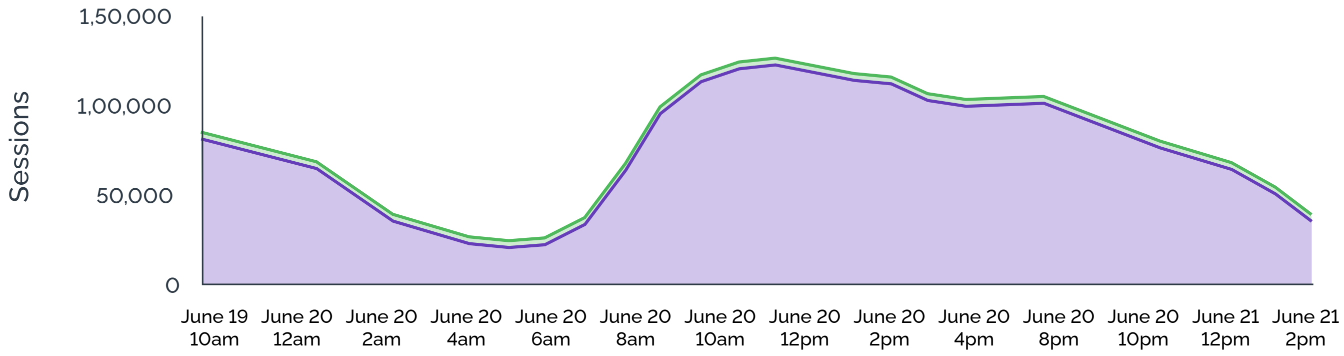
Ticket ID: 54265 | **Attack - SOC Mitigated**

Attack volume*: 3.4K
*Sessions created non-legit

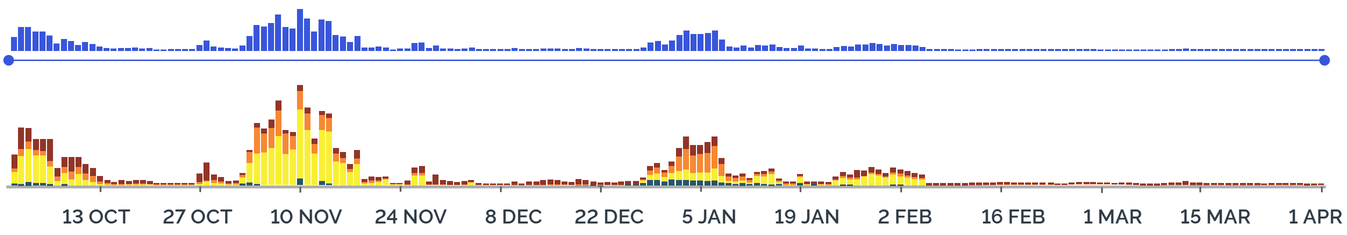
Attack type: Bots

Ticket created on: Jun 20, 2024, 1:08:04 AM

All Traffic



Total Events by **Risk Rating**
2023-10-01 1:15pm (EDT) - **2024-04-01** 1:15pm (EDT) - **26 weeks 1 day**

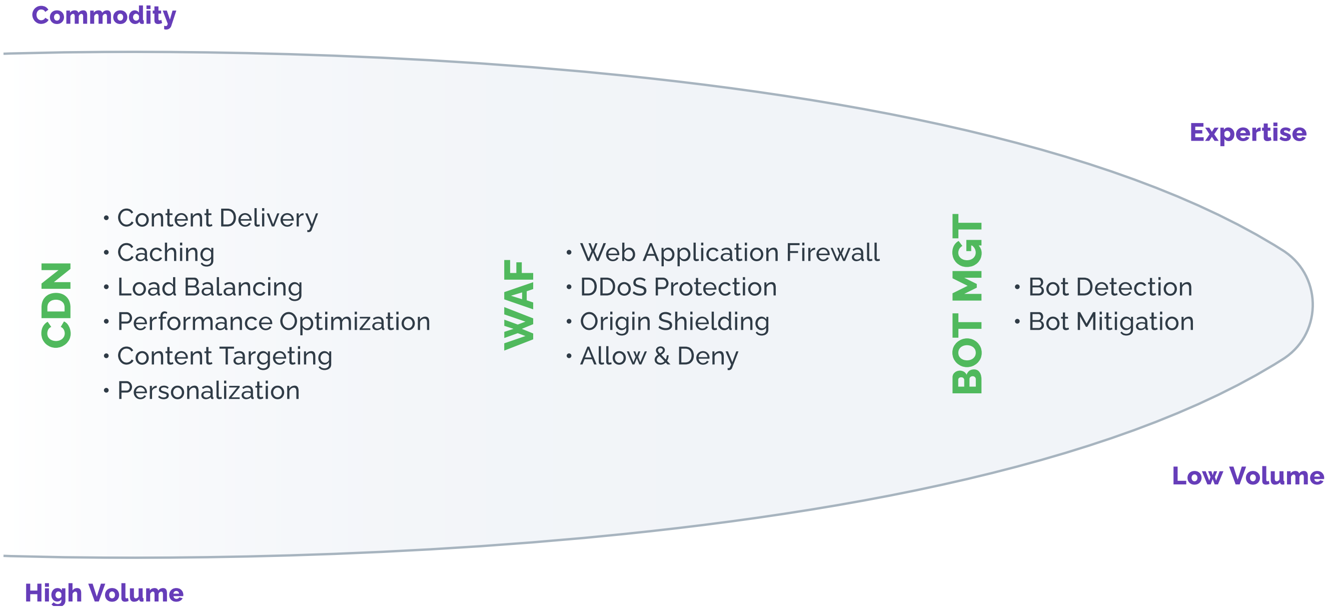


Attackers look for the path of least resistance. When a WAF and CDN are deployed, attacks increase in sophistication, and fraud teams spend more time managing threats. It equates to a never-ending game of whack-a-mole. And while Akamai Bot Manager and similar solutions provide bot protection out at the edge of the network, they lack the adaptability needed to counter evolving attack vectors effectively.

With the managed service from Arkose Labs, roles are reversed; we force attackers to up their game (and their real-dollar investment) and adapt to our rules. The result is frustrated attackers, who ultimately give up when the attack is no longer profitable.

Plus, should the Arkose Labs solution fail to defeat an attack within the SLA, we safeguard your business with our $1M warranties, covering SMS toll fraud, card testing and credential stuffing.

Diagram 3: Funnel Architecture



Contact Arkose Labs for a **customized POV assessment** and see firsthand the increased results and cost savings Arkose Labs can deliver.