ARCHITECTURE BRIEF

The Attack Surface Your WAF Can't See

Introduction

WAFs and CDNs are foundational infrastructure. They handle DDoS mitigation, application layer defense and basic bot blocking at scale — and they do those jobs well. Most enterprise security teams run Akamai or Cloudflare as a first line, and that's the right call.

The problem isn't that WAFs and CDNs fail at what they were built for. The problem is that the attack surface has expanded beyond what they were ever designed to cover — and the pace of that expansion is accelerating.

Our data shows that malicious traffic volumes and attack sophistication continue to climb quarter over quarter, with no signs of plateauing. Attackers aren't just becoming more numerous; they're becoming more precise and harder to detect. They rotate residential proxies, spoof TLS fingerprints, replay human behavior, and increasingly use LLM vision APIs to defeat challenge-response mechanisms.

More importantly: they've moved off the browser entirely.

Scrapers harvest content and pricing data at the CDN cache layer, before client-side code loads. Credential stuffers hit mobile app backends, gaming console APIs, and IPTV systems directly — surfaces that don't run JavaScript and that WAF/CDN architectures weren't built to inspect. The traditional security funnel has three uncovered gaps: what slips through at the CDN layer, what bypasses the browser entirely, and what evades basic bot managers through behavioral sophistication.

Where the Traditional Stack Falls Short

The standard enterprise stack — CDN → WAF → bot management — was architected around browser-based HTTP traffic. That model has three structural blind spots that have become primary attack vectors:

Blind spot 1:

The CDN layer intercepts traffic but doesn't interrogate it for scraping intent. CDNs are optimized for throughput, caching, and availability. They can apply IP reputation lists and basic rate limiting, but they don't perform the behavioral analysis or risk scoring needed to distinguish a legitimate consumer from a high-volume scraper at request time. By the time scraper traffic reaches a layer that can evaluate it properly, it's already consumed origin resources — or already extracted data.

Blind spot 2:

Non-browser surfaces have no coverage at all. Smart TVs, gaming consoles, IPTV set-top boxes, IoT devices, and mobile API backends don't execute JavaScript. Browser fingerprinting doesn't apply. CDN and WAF rules designed around HTTP session behavior are largely irrelevant. These endpoints are structurally undefended by any browser-first security stack — and attackers know it. Credential stuffing campaigns increasingly route through these surfaces specifically to avoid web-layer defenses.

Blind spot 3:

Sophisticated bots evade detection entirely. Basic bot managers handle browser impersonation, cookie support and JavaScript execution — but stop short of detecting TLS fingerprint spoofing, browser fingerprint spoofing, recorded human behavior replay and AI-powered challenge solving. Bots that clear that bar pass through as legitimate traffic, with no layer in the traditional stack equipped to catch them.

The Updated Architecture: Three Defensive Layers

Arkose Labs has expanded the platform to close coverage gaps at the CDN and on non-browser endpoints, while preserving the existing depth-behind-WAF model. The Arkose Titan Platform now operates across three distinct layers — each targeting a different attack surface.

Layer 1

At the CDN:
Arkose Scraping Protection

Deploys as a CDN worker. Every inbound request is evaluated against the Arkose Edge API using IP reputation, TLS fingerprinting and behavioral signals before it reaches origin infrastructure.

Risk tiering determines the enforcement response:

- **Low risk:** Request passes, no friction
- **Medium risk:** Lightweight verification
- **High risk:** Escalated to the Arkose Bot Manager challenge stack (Proof of Work + multimodal tasks)

No client-side code required. No page changes. Deploys at the CDN worker layer — scraping traffic never touches origin. Key per site domain.

Layer 2

Beyond the Browser:
Arkose Edge

A lightweight server-side API deployable at any endpoint — no JS, no SDK, no browser required. Accepts IP address as the minimum input signal, with optional TLS data, user agent, JA3/JA4 fingerprints and device metadata for enhanced detection accuracy.

Returns a structured response: risk score, risk band and allow/challenge/deny recommendation. The customer implements enforcement. Arkose Edge provides the signal intelligence.

This is the layer that covers every endpoint your existing stack ignores — IoT, gaming consoles, IPTV, mobile backends, programmatic APIs. Separate key per use case.

Layer 3

On Authenticated Flows:
Arkose Bot Manager

Session-level detection and active challenge enforcement on browser-based authenticated flows: login, signup, checkout, password recovery. Adaptive challenge enforcement, Proof of Work and multimodal challenge tasks are designed to defeat bots that use LLM vision APIs to solve traditional CAPTCHAs.

Arkose Bot Manager also serves as the escalation destination for high-risk traffic flagged by Arkose Scraping Protection and Arkose Edge. The challenge stack is the same regardless of how traffic arrived — the enforcement layer is unified.

Backed by 24/7/365 SOC and ACTIR managed service, the Arkose Global Intelligence Network, and $1M warranties on SMS toll fraud, card testing and credential stuffing.

DETECTION COVERAGE BY THREAT SOPHISTICATION

Attack behavior	CDN/WAF	Basic Bot Managers	Arkose Titan
Single IP, high request rate	✓	✓	✓
Multiple IPs, low rate	✓	✓	✓
User agent randomization		✓	✓
Browser impersonation		✓	✓
Cookie support, session replay		✓	✓
JavaScript execution		✓	✓
TLS fingerprint spoofing			✓
Browser fingerprint spoofing			✓
Recorded human behavior replay			✓
AI-powered CAPTCHA solving			✓
Non-browser / API endpoint attacks			✓
CDN-layer content scraping			✓

ROI Impact Across the Stack

Infrastructure cost reduction:

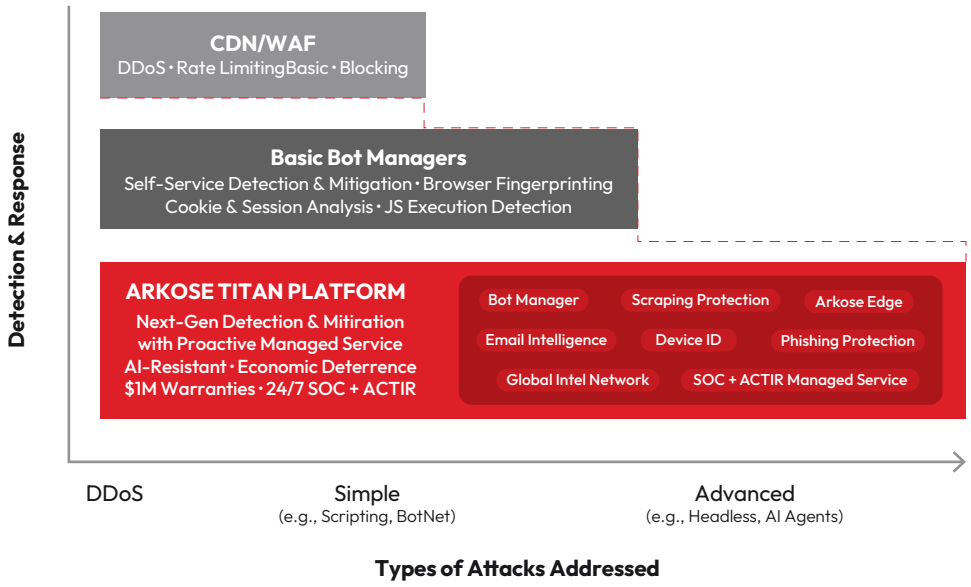
Scraping Protection stops automated and abusive traffic at the CDN worker before it reaches origin — eliminating the compute and bandwidth costs that high-volume attacks generate upstream, on top of reducing fraud loss downstream.

Downstream system cost reduction:

Closing the non-browser surface gap reduces the volume of suspicious sessions reaching downstream identity systems. One large bank deployed Arkose Labs between its CDN layer and its downstream session risk scoring system — reducing unknown session volume to near zero and saving hundreds of thousands of dollars in assessment costs.

False positive reduction:

The platform provides full risk attribution — scores, bands and the underlying signals and rules driving each decision. Customers can feed truth data back into the rules engine at no additional cost, enabling accuracy that continuously improves as attack patterns evolve.



KEY ARKOSE LABS DIFFERENTIATORS

PLATFORM

- Unified Titan platform — bot management, scraping API, email, device, phishing in one stack
- Economic deterrence — proof of work makes attacks unprofitable
- AI-resistant MatchKey challenges — <1% bypass rate vs. 92% for legacy CAPTCHAs

INTELLIGENCE

- ACTIR threat research unit + Global Intelligence Network
- Full risk attribution — scores, signals, and underlying rules shared with customer
- Cross-industry signal sharing across the largest global brands

SERVICE

- 24/7/365 SOC — proactive monitoring, not reactive alerting
- $1M financial warranties: credential stuffing, SMS toll fraud, card testing
- Trusted by 2 of the top 3 global banks, Microsoft, Meta, Roblox

Proof Points

International airline: 10,000+ fraudulent bookings blocked per month with Scraping Protection; dynamic pricing accuracy restored within days — bots had been driving 20–30% customer churn through inventory manipulation.

Major travel company: Nearly 7,000 sophisticated bot attacks stopped in a single day, deployed behind Akamai Bot Manager.

Large global bank: Unknown session volume reduced to near zero after deploying Arkose Titan between Akamai and LexisNexis ThreatMetrix; hundreds of thousands of dollars saved in downstream assessment costs.

Adobe: Challenge rate for trusted consumers reduced from 10% to 2% post-deployment.

Global social network: Security team reported higher legitimate engagement and lower scraping activity as simultaneous post-deployment outcomes.

Conclusion: It's Better Together

By relying only on traditional CDN and WAF solutions, your security could suffer in the face of increasingly sophisticated and evasive bot attacks. By adding the Arkose Titan Platform, you'll be able to proactively detect and stop the most advanced threat campaigns aimed at your company — across every surface attackers target, with readiness for the fraud landscape of tomorrow. Adding Arkose Labs 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.

BOOK A DEMO

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