PRODUCT BRIEF

Arkose Scraping Protection

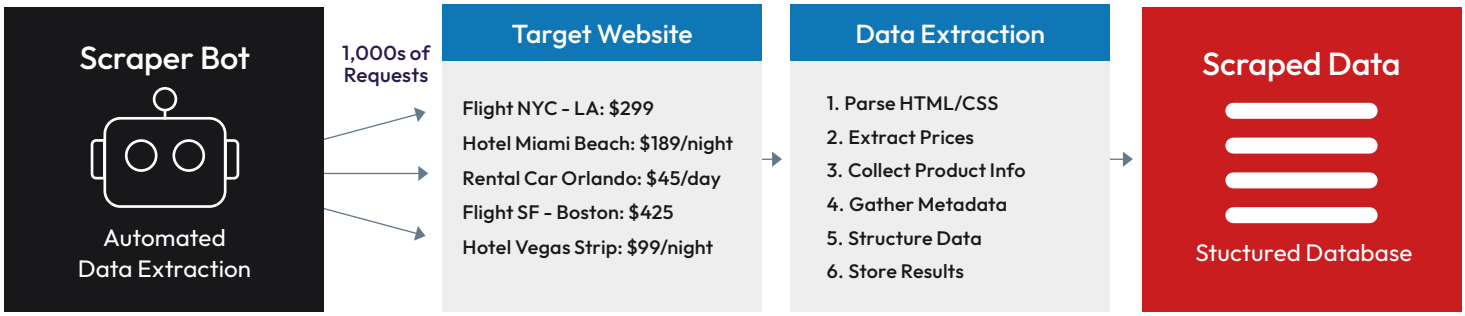
Defend Your Digital Assets from Automated Theft

Web scraping has evolved beyond basic data collection into a sophisticated security threat that significantly impacts businesses financially. Companies face multiple challenges when targeted by scraping operations, including intellectual property theft where competitors steal proprietary content and digital assets. These attacks can trigger sudden infrastructure cost spikes as servers become overwhelmed by automated scraping bots, dramatically increasing operational expenses.

The financial damage extends to direct revenue loss when pricing data is stolen, allowing competitors to strategically undercut offerings. Perhaps most damaging is the erosion of brand reputation that occurs when service disruptions from scraping attacks lead to deteriorated customer trust and satisfaction. Together, these impacts represent a multi-faceted threat that costs companies millions annually and requires comprehensive protection strategies to mitigate.

Arkose Scraping Protection, part of the Arkose Titan platform, is an intelligent edge-based solution designed for high-volume environments with minimal performance impact for protecting valuable content and API data.

Web Scraping Process Demonstration



What Is Arkose Scraping Protection?

Arkose Scraping Protection extends the Arkose Titan platform to protect your website from content theft. Through detecting and stopping bot scraping, ensuring seamless access for legitimate customers, Arkose Scraping Protection protects your proprietary information, preserves your competitive edge and safeguards sensitive customer data.

Key Benefits

Stop Unauthorized Content Access
Prevent automated scraping of premium content, pricing data and intellectual property to maintain your competitive advantage and protect revenue streams.

Control Infrastructure Costs
Block bot traffic at the edge before it impacts your servers, reducing infrastructure load and preserving the experience for legitimate users.

Safeguard Your Brand Reputation
Maintain customer trust by preventing service disruptions and protecting sensitive data from unauthorized access.

How It Works

Arkose Scraping Protection provides proactive security by intercepting requests at the CDN layer before they reach your infrastructure. This multi-layered defense system begins with Intelligent Risk Assessment, analyzing IP addresses, TLS data, user agents and additional signals to identify malicious automation attempts. Through Adaptive Response mechanisms, low-risk traffic proceeds without disruption while suspicious traffic receives appropriate challenges. For high-risk traffic, the system activates Arkose Bot Management for comprehensive detection capabilities. Scraping Solution includes:

1. **CDN Worker Deployment:** Implement our worker template at your content delivery network
2. **First Request Analysis:** System evaluates incoming traffic using multiple signals
3. **Risk-Based Response:**
    A. Low-risk traffic proceeds seamlessly
    B. Medium-risk traffic receives lightweight verification
    C. High-risk traffic triggers comprehensive challenges
4. **Session Verification:** Successful verification grants access via secure cookie
5. **Continuous Protection:** SOC team monitors and tunes detection systems

Seamless Integration, Minimal Development

Arkose's CDN Worker deployment model integrates directly with your existing content delivery infrastructure, providing robust website protection through lightweight, serverless functions that communicate with our Edge API. This architecture eliminates client-side code requirements, extending protection to surfaces where JavaScript isn't viable. Arkose Scraping Protection currently supports select CDN platforms, with integrations with all major CDN providers planned in the future.

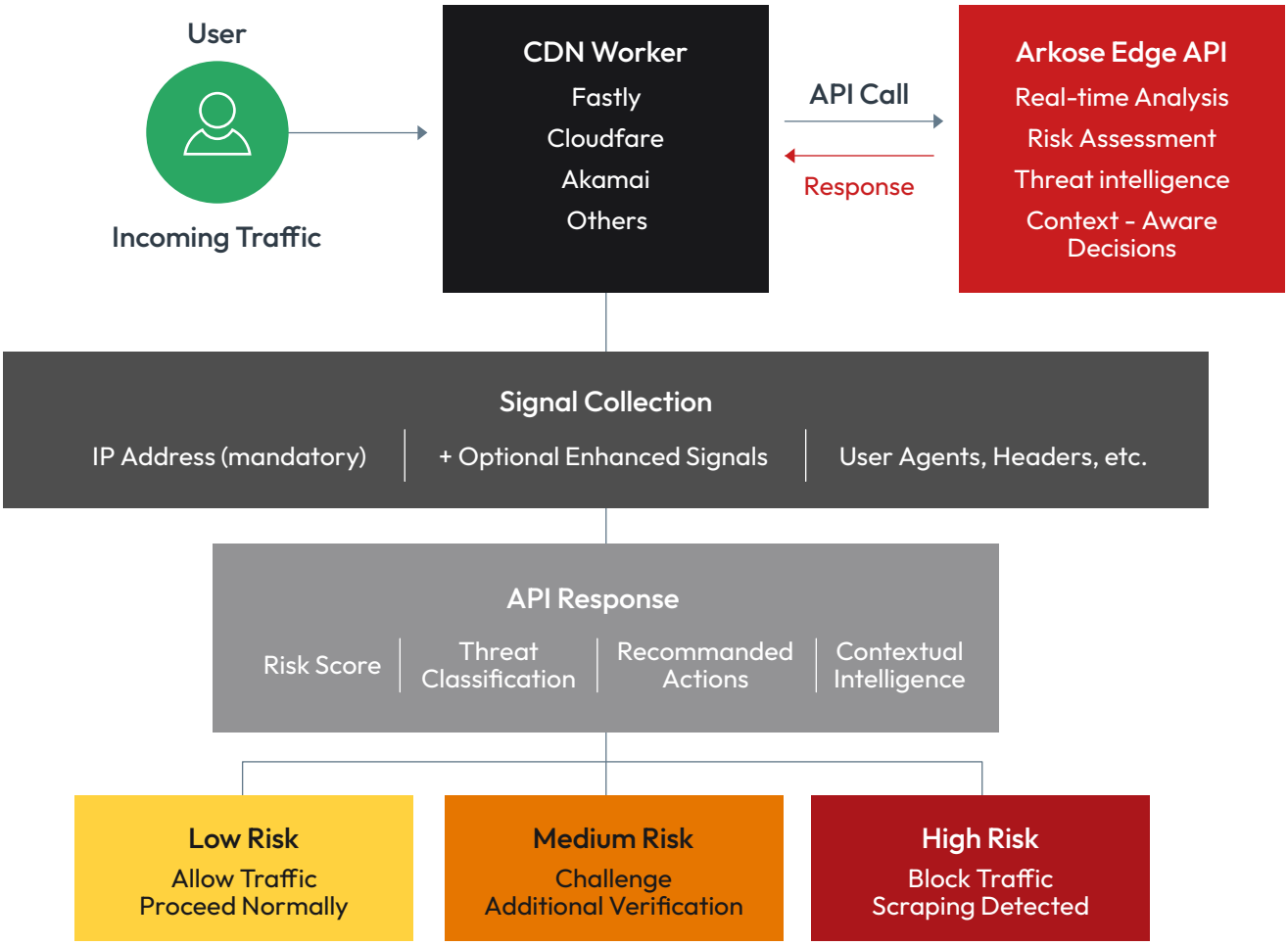
This streamlined approach allows most customers to achieve complete protection within days rather than months.

Adaptive Edge API, Intelligence On Demand

Our Arkose Scraping Protection solution is powered by the Arkose Edge API, which is called directly from inside your CDN worker deployment for streamlined threat detection. This architecture delivers flexible, context-aware intelligence with minimal integration complexity, allowing the worker to make real-time security decisions at the edge of your network.

The API works with data your CDN worker can gather, with only an IP address required to get started, allowing you to begin with basic protection and gradually add more sophisticated signals over time. When the CDN worker calls the Edge API, our platform responds with comprehensive risk assessments and actionable intelligence tailored to your security posture. As your threat detection needs grow, the same API seamlessly accommodates additional signals without requiring architectural changes.

Arkose Edge API - CDN Worker Integration



Edge-based protection with progressive signal enhancement capabilities

What Sets Arkose Scraping Protection Apart

Unlike traditional anti-scraping tools that inadvertently block legitimate users, Arkose Scraping Protection maintains an exceptional user experience:

Low Latency Performance

Designed for high-volume environments with minimal impact on page load times

Precise Detection

Accurately differentiate between legitimate users and automated scrapers

Cost-Effective Scale

Purpose-built pricing model for high-volume use cases

ACTIR and the Arkose Labs SOC: Proactive Defense

Arkose Labs operates as an extension of your team, rapidly countering attacks and providing actionable insights without overburdening your internal resources. The Arkose Cyber Threat Intelligence Research (ACTIR) unit conducts proactive threat hunting and risk intelligence gathering to provide vital, fresh intelligence. Meanwhile, the 24/7/365 Security Operations Center (SOC) team focuses on identifying and immediately stopping both sophisticated low-and-slow attacks as well as large-scale attacks. The SOC continuously monitors for new threats and collaborates with ACTIR. This feedback loop ensures a seamless collaboration between the SOC and ACTIR, enhancing the overall accuracy, timeliness and effectiveness of your cybersecurity defense.

About the Arkose Titan Platform

Arkose Titan is Arkose Labs' comprehensive platform that delivers end-to-end protection across every touchpoint of the user journey. The platform makes attacks unprofitable while keeping legitimate users moving seamlessly through:

- **Unified Intelligence:** Shared threat data across all touchpoints creates compounding protection where each interaction strengthens the entire system
- **Attack Economics Disruption:** Increases attacker costs exponentially while defender costs remain flat
- **Adaptive Enforcement:** Real-time response that evolves with sophisticated threats including AI-powered attacks
- **Zero-Friction for Legitimate Users:** 98%+ customer satisfaction with invisible protection for real customers

Arkose Titan secures every stage—from first account sign-up through ongoing platform activities—protecting registration, authentication, payments and in-platform interactions with one unified solution.

See How Arkose Scraping Protection Can Work for You

Ready to see how Arkose Scraping Protection can protect your organization and enhance your security posture? Schedule a call with an expert today.

BOOK A DEMO

Arkose Labs is the leading global provider offering a proactive fraud deterrence platform purpose-built to neutralize modern attacks, including those powered by Agentic AI and large language models (LLMs). Its comprehensive solution combines proprietary device identification (device ID), behavioral analysis, phishing protection, email intelligence, scraping prevention, API defense and bot management. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America.