Arkose Labs
PROVEN ACCOUNT SECURITY

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 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 Labs account security 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

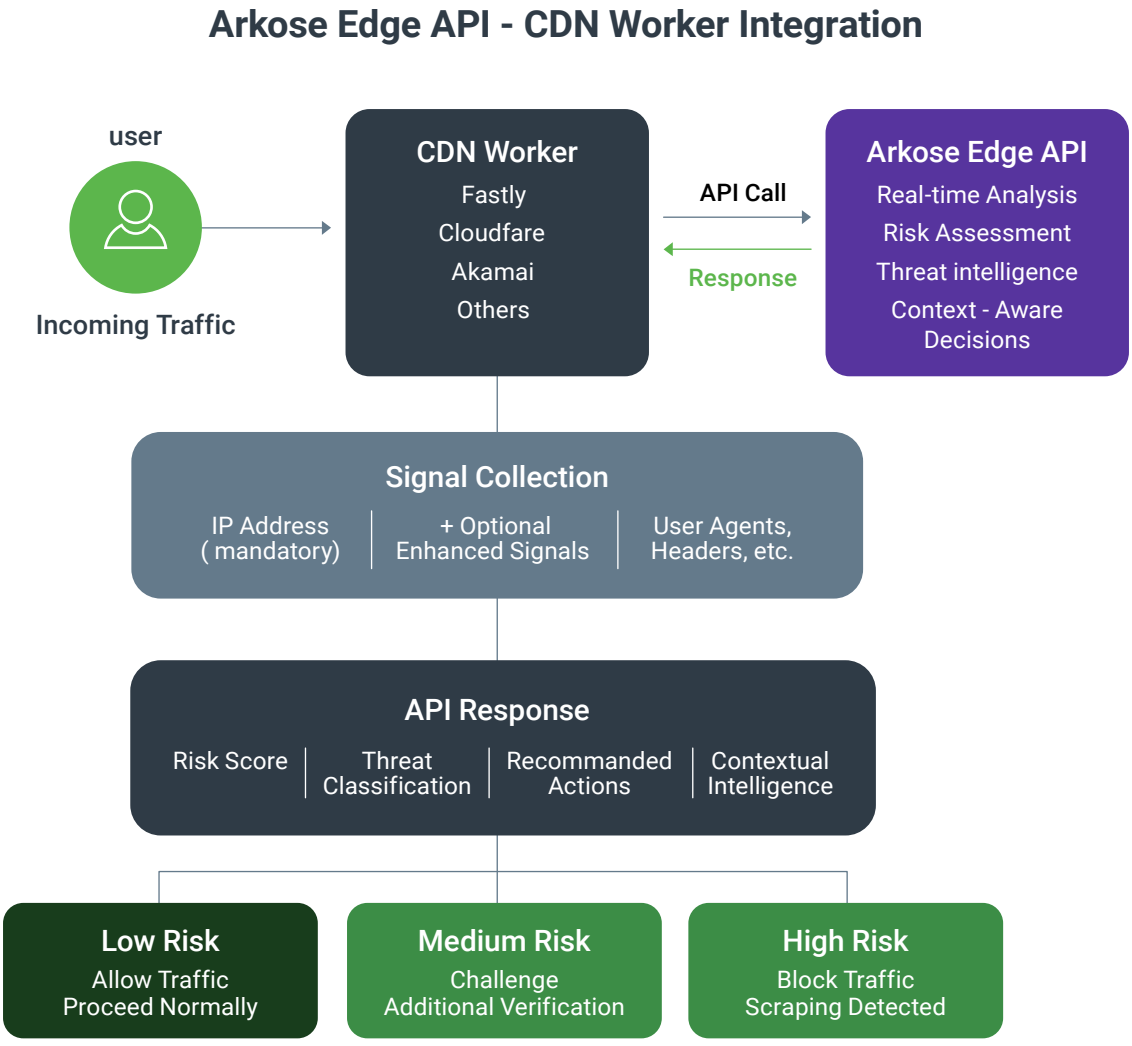
Arkose's CDN Worker deployment model integrates directly with your existing content delivery infrastructure, providing robust website protection through lightweight, serverless functions that communicate with our Edge API. This architecture eliminates client-side code requirements, extending protection 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.



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

See How Arkose Scraping Protection Can Work for You

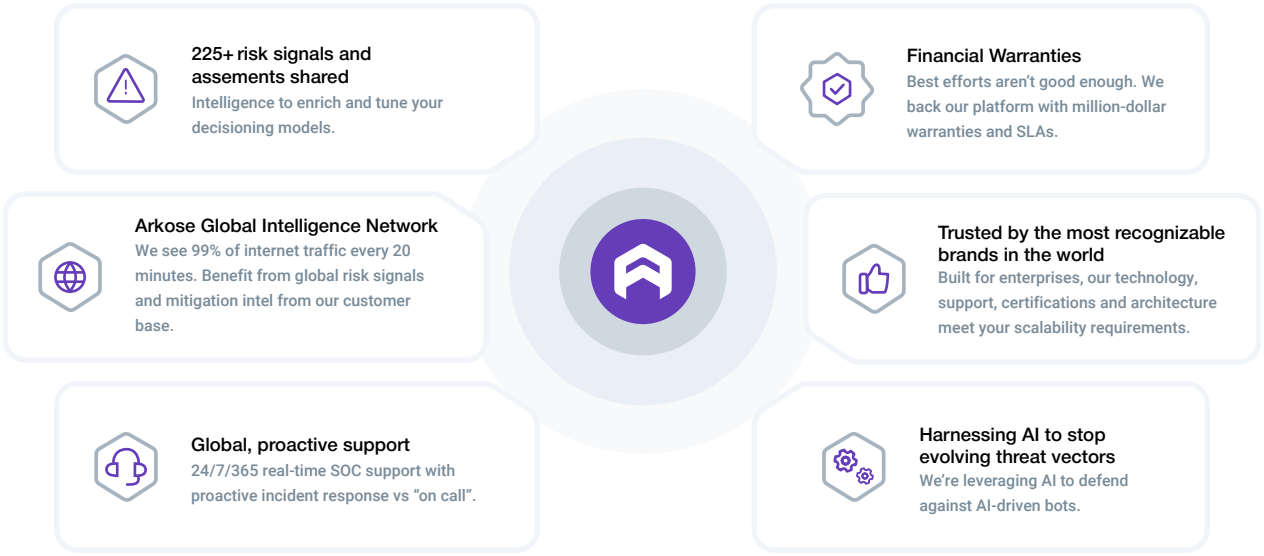
Ready to see how Arkose Scraping Protection can protect your organization and enhance your security posture? Schedule a call with an expert today by clicking the button below.

TALK TO AN EXPERT

Why Arkose Labs:

Arkose Labs Proof of Value

The Arkose Labs proof of value (POV) process offers your business a hands-on opportunity to experience the platform's capabilities. During the POV with production traffic, Arkose Labs provides expert guidance and consultation tailored to your specific needs, ensuring you can test the platform's effectiveness in real-world scenarios. This process allows your business to define and track its own success metrics, such as fraud reduction, improved user experience or cost savings, giving you a clear view of the value Arkose Scraping Protection can deliver.



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, risk intelligence gathering and other counterintelligence methods 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.

BOOK A MEETING

Arkoselabs.com

The world's leading organizations, including two of the top three banks and largest tech enterprises, trust Arkose Labs to keep users safe. No one else is as proven at scale, provides more proactive support, or out-sabotages attackers' ROI. Based in San Mateo, CA, Arkose Labs operates worldwide with offices in Asia, Australia, Central America, EMEA and South America.