PRODUCT BRIEF

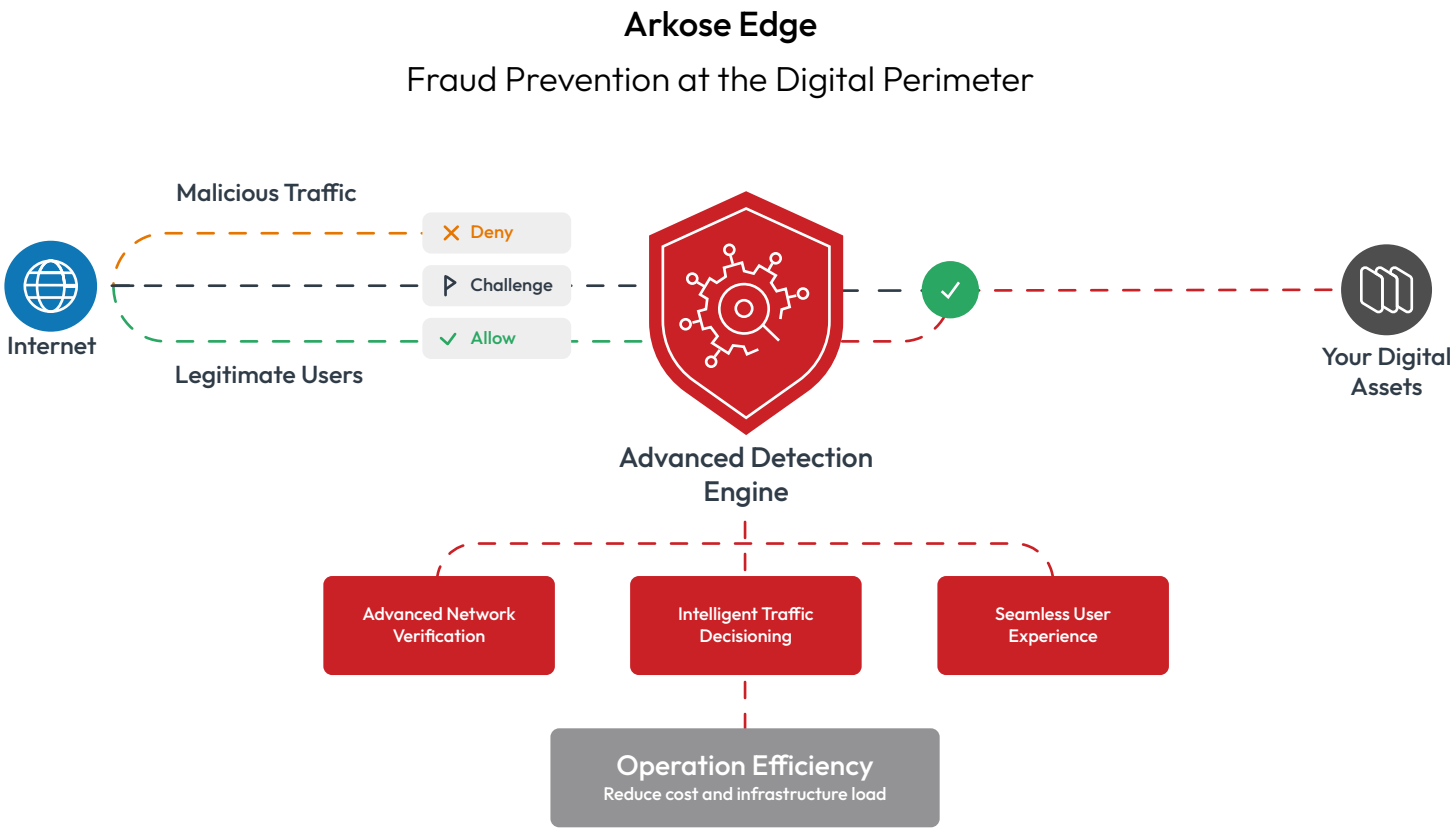
Arkose Edge

Fraud Prevention at the Digital Perimeter

Enterprises face critical security vulnerabilities where traditional measures fail to protect valuable digital assets across the expanding network edge. Server-side protection needs to extend security coverage to previously vulnerable surfaces without compromising user experience, to address significant blind spots in conventional security perimeters.

These vulnerabilities exist across diverse technology ecosystems, including connected devices like smart TVs, set top boxes, gaming consoles that lack standard browser capabilities, API endpoints susceptible to abuse despite being designed for programmatic access, IoT ecosystems with limited security implementation options and server-side applications that process sensitive data without client-side protection.

By implementing Arkose Edge, part of the Arkose Titan platform, companies can fortify these overlooked vulnerabilities, creating a more comprehensive defense strategy that protects digital assets across all network touchpoints while maintaining seamless functionality for legitimate users.



What Is Arkose Edge?

Arkose Edge, a core component of the Arkose Titan platform, delivers powerful server-side protection through a streamlined API solution that seamlessly integrates into your infrastructure with a lightweight call at any endpoint, collecting essential data signals to deliver intelligent risk assessments and actionable allow/challenge/deny recommendations based on comprehensive consortium intelligence.

Key Benefits

Protect Revenue Streams

Stop credential sharing, account takeover and unauthorized access on connected devices that impact subscription revenue.

Prevent Spoofing and Impersonation

Identify attackers mimicking legitimate devices to gain unauthorized access to accounts and sensitive systems.

Secure Critical API Endpoints

Stop programmatic attacks against customer-facing APIs that circumvent web-focused protection systems.

Extend Protection Beyond Browsers

Implement consistent security across all digital surfaces, even where client-side integration isn't possible.

How It Works

Our server-side API solution provides flexible, low-latency protection:

1. **Simple API Integration:** Deploy a lightweight API call at any endpoint in your infrastructure
2. **Flexible Data Collection:** Requires only IP address, with additional signals (TLS data, user agents) for enhanced protection
3. **Intelligent Risk Assessment:** Returns risk scores and session intelligence based on consortium data
4. **Actionable Recommendations:** Provides allow/challenge/deny decisions to guide your response
5. **SOC Intelligence:** Continuously monitored and fine-tuned by our Security Operations Center

The API's modular architecture adapts to whatever signals are available at your endpoint, running appropriate detection services internally and delivering accurate verdicts whether you provide just the mandatory IP address or enhanced data like TLS fingerprints and user agent details. This flexible approach allows enterprises to start with basic protection using minimal data requirements and progressively enhance their security posture by adding richer signals as they become available, without requiring any changes to the API integration.

Arkose Edge employs multiple technical layers to combat automated threats where IP Intelligence technology analyzes address patterns to identify suspicious traffic sources, while server-side behavioral analysis detects anomalies in request patterns and frequency without client-side code. The platform's network-level security leverages TLS fingerprinting and protocol analysis to identify sophisticated automation techniques. Advanced

rate limiting capabilities monitor and control request volume, preventing abuse while maintaining service for legitimate users. The system's proprietary telltale engine integrates global threat intelligence to respond to emerging attacks in real-time, applying machine learning to adapt protection as attack methodologies evolve.

What Sets Arkose Edge Apart

Arkose Edge delivers high-performance protection with ultra-low latency specifically designed for performance-critical applications. Its modular architecture allows implementation with basic data while enabling enhancement with additional signals when available. Companies benefit from cost-effective scaling through an optimized pricing model for high-volume API protection. The system operates without JavaScript, SDKs or other client-side dependencies, eliminating requirements typically needed to secure endpoints.

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.

Secure Beyond the Browser

Ready to secure every endpoint—not just the ones with browsers? See how Arkose Edge extends your protection to connected devices, APIs, and server-side applications without compromising performance. Schedule a one-to-one meeting 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.