Arkose Labs
PROVEN ACCOUNT SECURITY

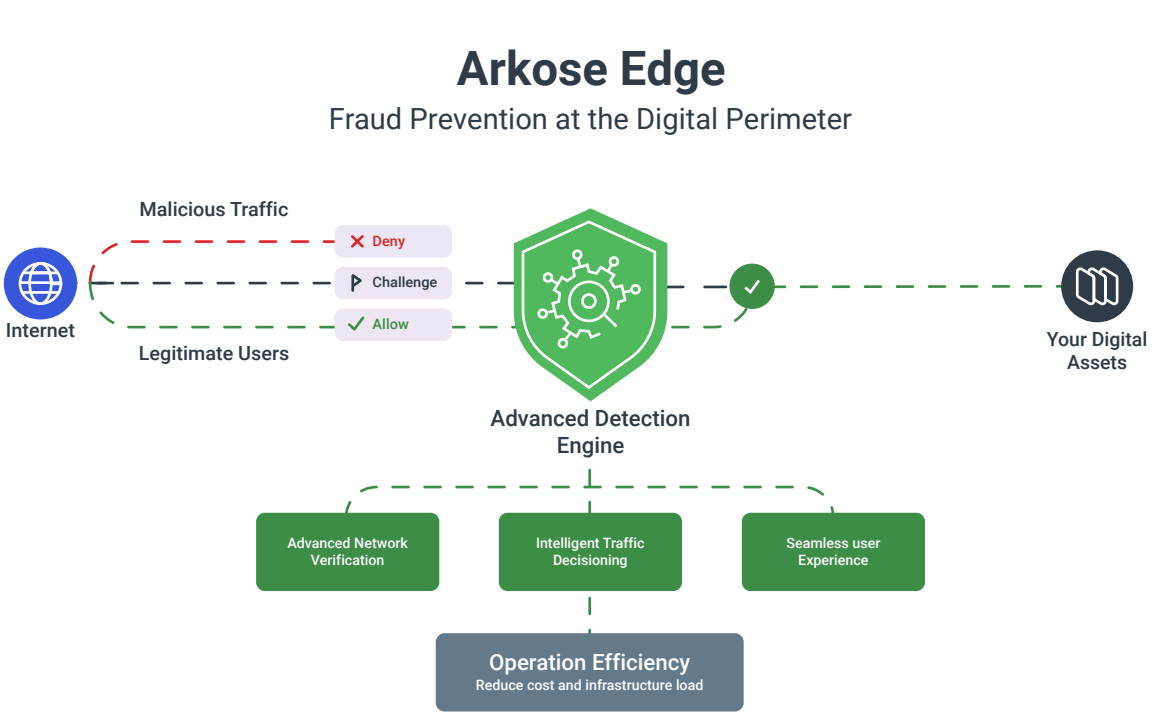
Arkose Edge

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, and 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, organizations 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 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 CenterInsert Graphic

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 organizations 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. Organizations 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.

See How Arkose Edge Can Work for You

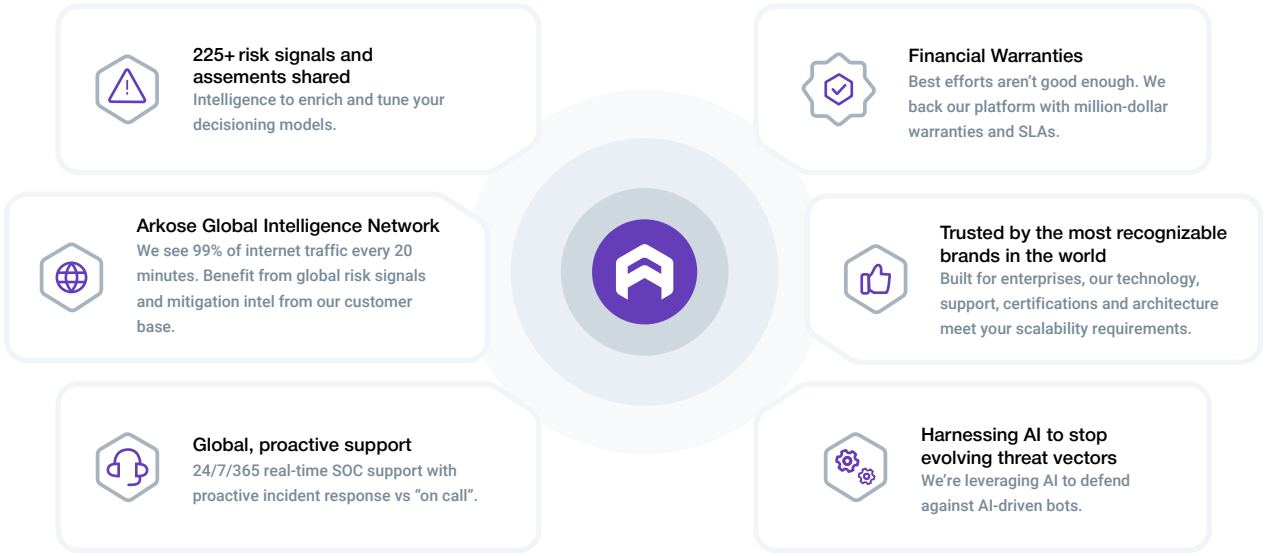
Ready to see how Arkose Edge can protect your organization and enhance your security posture? Schedule a call with an expert today by clicking the button below.

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 Edge 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.

TALK TO AN EXPERT

www.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.