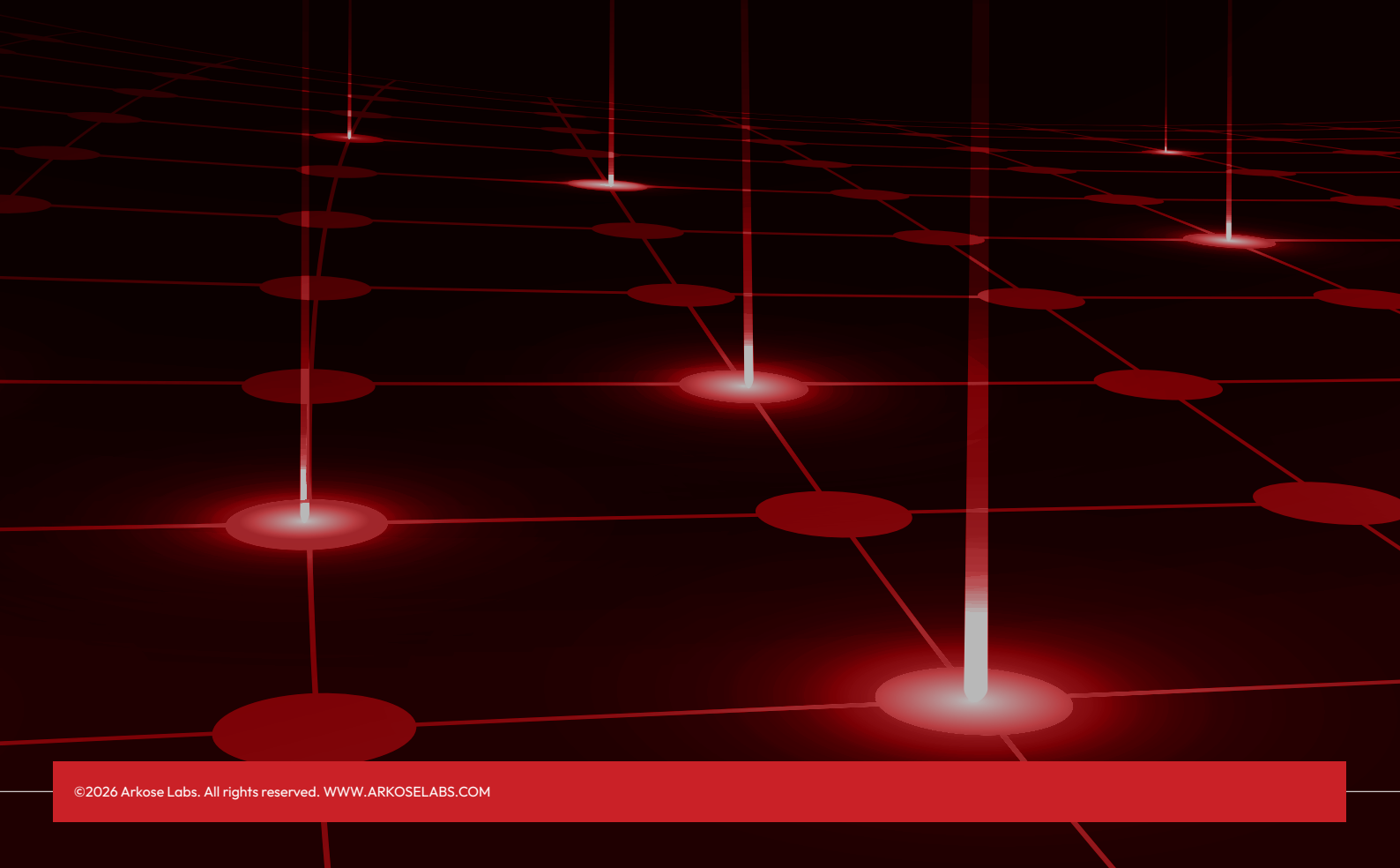
PRODUCT BRIEF

ARKOSE DEVICE ID

Protect your application while delivering a friction-free experience to trusted users.



Traditional device identification methods—such as IP address monitoring and basic device fingerprints like operating systems, user agents and canvas fingerprints—are no longer sufficient against today's adaptive threats. These static data points can be easily spoofed by sophisticated attackers, transforming what once served as security measures into exploitable vulnerabilities.

The stakes have escalated dramatically as cybercriminals now leverage AI and automation to bypass conventional defenses at scale. Fraudsters continuously adapt their tactics, employing advanced techniques like fingerprint spoofing, browser automation and device farms to evade detection. This dynamic threat environment demands more than simple device recognition. It requires comprehensive device intelligence that provides deep, contextual understanding of device behavior, risk signals and attack patterns.

Modern protection strategies must move beyond asking "What is this device?" to answering critical questions like: "How is this device behaving, and is this behavior consistent with legitimate use?" This shift from identification to intelligence is essential for preventing sophisticated threats, all while maintaining a frictionless experience for trusted users.

Arkose Device ID, part of the Arkose Titan platform, meets this evolved security imperative by delivering persistent, accurate device recognition that stops sophisticated evasion while maintaining frictionless experiences for legitimate users—solving the industry's division-persistence-collision challenge without compromise.

What Is Arkose Device ID

Arkose Device ID is an intelligent device identification solution within the Arkose Titan platform that combines deterministic identification with AI-powered similarity detection, providing persistent, accurate device recognition from the very first interaction with your application.

This advanced capability solves the industry's division-persistence-collision challenge by maintaining device identity through fingerprint evolution while preserving cryptographic accuracy. By enabling businesses to identify, track and correlate both trusted and suspicious behaviors with session signals and key artifacts—such as user IDs, email addresses and payment methods—Arkose Device ID offers valuable insights into unique device interactions, empowering companies to confidently recognize returning devices and address potential fraudulent activities early.

Key Benefits

Identify repeat unique devices with full confidence and track their behavior

You'll be able to easily recognize returning devices to tie and monitor user actions, enhance their experience and stop repeat offenders before they cause issues.

Secure payments and quickly detect ATO at login using verified devices

It will let you instantly spot trusted devices, so you can secure transactions and catch account takeovers right at login, preventing fraud before it gets serious.

Correlate anomalies and detect sophisticated low-and-slow attacks

It connects the dots between suspicious behaviors, helping you uncover sneaky, long-term fraud attempts that might otherwise go unnoticed.

Recognize repeat offenders and risky devices, and inform your CIAM tools

You'll be able to flag risky devices, and feed that data into your CIAM system, making it easier to block threats and stay ahead of attacks.

Detect account sharing and fake registrations

Device ID spots account sharing and fake sign-ups from the same device, protecting your platform from abuse while keeping things smooth for genuine users.

Stop SMS toll fraud before costs spiral

Block fraudsters from spinning up fake accounts via device farms to exploit SMS verification — protecting your budget from schemes that can drain hundreds of thousands of dollars in hours.

How It Works

Arkose Device ID uses a multi-layer identification strategy that goes far beyond basic fingerprinting to deliver contextualized intelligence about every device accessing your platform.

Our AI-enhanced identification approach maintains deterministic precision as the foundation while extending recognition through ML-powered vector similarity detection. This comprehensive approach analyzes device hardware, software configuration, network characteristics and behavioral patterns, delivering a unified Arkose ID output—a single, persistent identifier that eliminates collision where multiple devices appear identical, prevents division where single devices fragment into multiple identities, and ensures persistence so legitimate device changes don't break tracking continuity.

Built for enterprise reliability, our system features graceful degradation—if vector database services are unavailable, deterministic identification continues to function, ensuring uninterrupted protection.

Instantly distinguish between genuine users, bots and bad actors with contextualized insights into how devices behave, not just what they are. Reduce false positives while catching sophisticated threats that basic fingerprinting misses. Advanced features like automated spoofing detection flags immediately alert you when devices attempt to mask their identity, while intelligent rate limiting automatically responds to suspicious patterns—throttling abuse without impacting legitimate users.

Make confident, real-time decisions backed by comprehensive device intelligence. Protect your platform from account takeover, payment fraud and coordinated attacks while delivering frictionless experiences for trusted returning users.

What Sets Arkose Device ID Apart

Deliver contextualized intelligence

Gain behavioral insights into how devices interact with your platform, enabling accurate risk assessment beyond simple identification.

Layer multiple identification strategies

Combine multiple identification methods with behavioral analysis for enhanced persistence and comprehensive device understanding.

See the full device risk profile

Get contextualized insights for all traffic, revealing device identity and behavioral patterns without additional vendors.

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. The platform is further strengthened by the Arkose Cyber Threat Intelligence Research (ACTIR) unit and a 24/7/365 Security Operations Center (SOC), delivering continuous threat hunting, proactive intelligence gathering and rapid response to keep defenses ahead of even the most sophisticated attacks.

Stop Guessing Which Devices to Trust

See how Arkose Device ID delivers the persistent, multilayered intelligence you need to confidently recognize returning devices and stop fraud early. 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.