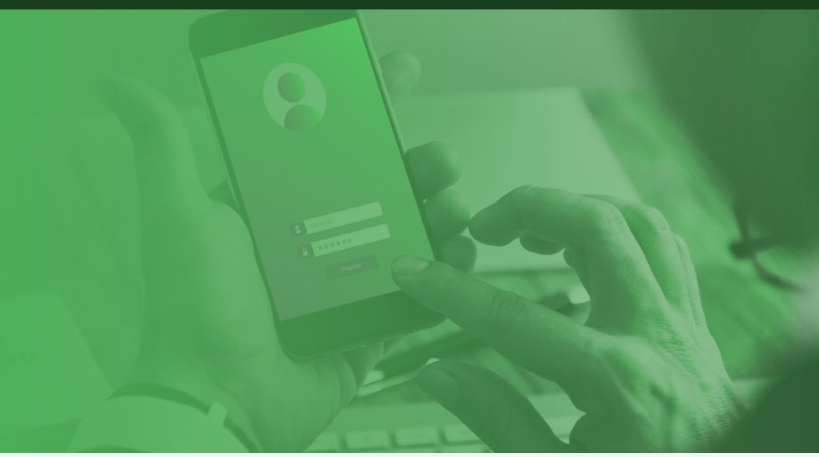
Arkose Labs



Arkose Device ID

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

In today's rapidly shifting threat landscape, relying solely on traditional identification methods such as IP address monitoring, device fingerprints like operating systems, user agents, and canvas fingerprints—which can be easily spoofed—is no longer enough, and in fact, it is now a vulnerability. Cybercriminals are now leveraging AI to bypass traditional defenses, creating a pressing need for proactive, always-on protection that detects risk early and adapts to evolving attack methods.

As fraudsters constantly evolve their tactics, it's critical for companies to confidently recognize devices to prevent threats such as account takeovers, session hijacking and unauthorized access, all while protecting the experience of trusted users.

Arkose Device ID meets this need by providing real-time, device-specific tracking that not only enhances security but also delivers a seamless experience for legitimate users—safeguarding your workflows and stopping attackers before they compromise your systems.

What Is Arkose Device ID

Arkose Device ID is a powerful solution, providing unique identifers for individual devices from their very fist interaction with Arkose Labs protected instances. Through a multilayered identification strategy, Arkose Device ID combines multiple identification methods with behavioral analysis, offering enhanced persistence and comprehensive device understanding.

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 signups from the same device, protecting your platform from abuse while keeping things smooth for genuine users.

How it works

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

Our comprehensive approach analyzes device hardware, software configuration, network characteristics, and behavioral patterns to create unique identifiers while solving the three critical challenges that plague traditional device fingerprinting. We eliminate collision where multiple devices appear identical, prevent division where single devices fragment into multiple identities, and ensure persistence so legitimate device changes don't break tracking continuity.

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.

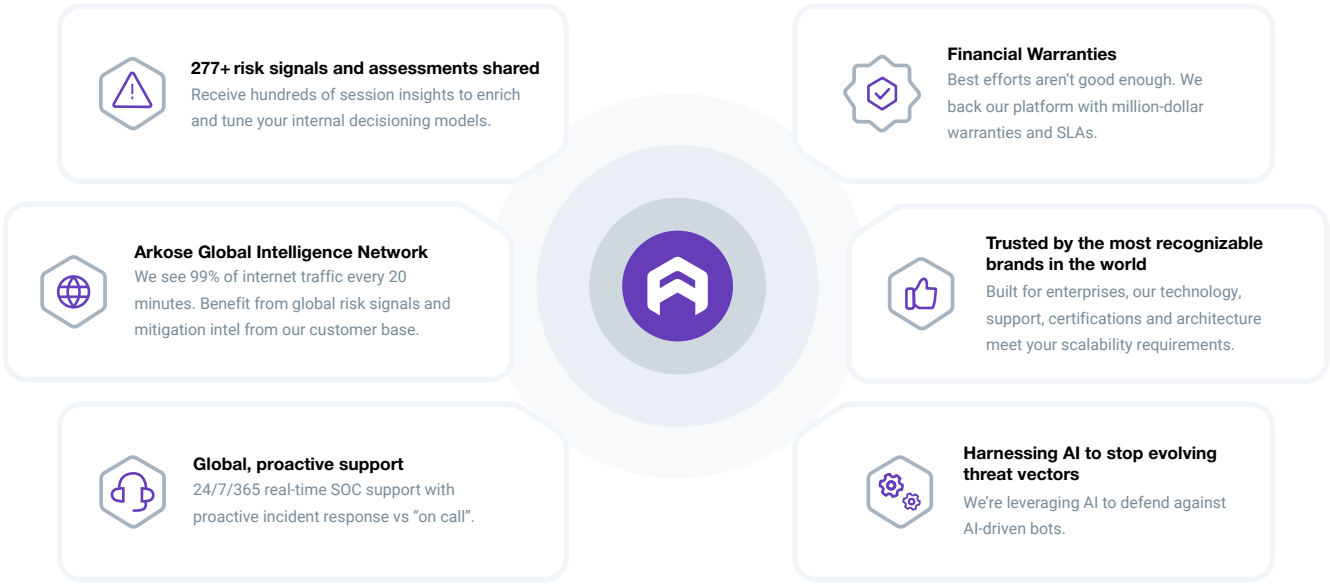
What Sets Arkose Device ID Apart:

Delivers Contextualized Intelligence	Multilayered Identification Strategy	Full Visibility into Device Risk Profile
Delivers behavioral insights into how devices interact with your platform, enabling accurate risk assessment beyond simple identification.	Combines multiple identification methods with behavioral analysis for enhanced persistence and comprehensive device understanding.	Provides contextualized insights for all traffic, revealing device identity and behavioral patterns without additional vendors.

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 Device ID can deliver.

The Arkose Labs Advantage



Seamless Integration: No Engineering Delays

We understand the challenges of securing engineering time, which is why Arkose Labs is designed for effortless integration. If you're using a CDN like Cloudflare or Akamai, our pre-built CDN workers allow you to deploy our solution without any code changes to your application. This low-code implementation ensures you can get up and running quickly, without needing to pull your engineers away from their critical projects.

If you're already working with one of our partners, our integration is ready to go, requiring minimal effort on your part. This means you can deploy robust protection without the usual delays, keeping your business secure without waiting months for engineering resources.

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 YOUR DEMO

www.arkoselabs.com