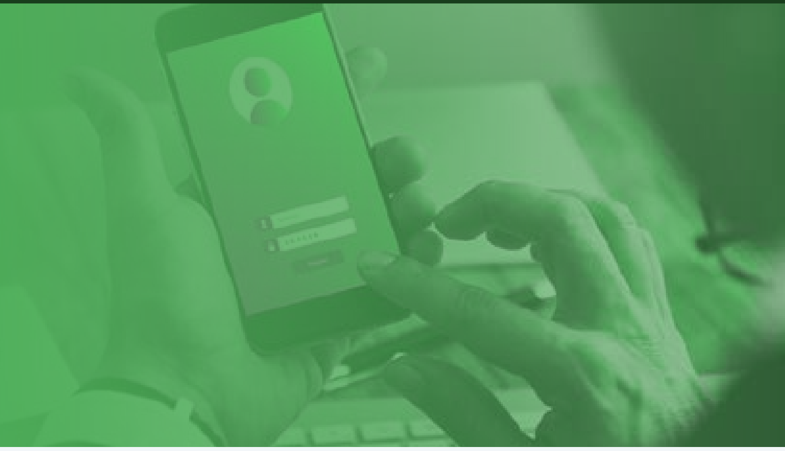
Arkose Labs



# 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 add-on feature to the Arkose Bot Manager platform, providing unique identifiers for devices from their very first interaction with Arkose Labs-protected instances. This feature integrates into customer workflows using two methods: **Stateless**, which aggregates real-time telemetry, and **Stateful**, which uses a persistent identifier stored on the device.

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.

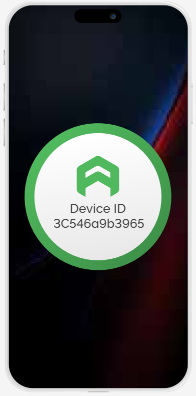
## How it works

Arkose Device ID provides a robust and adaptable solution for identifying devices through two complementary methods: **Stateless** and **Stateful** identification.

**Stateless Device ID** calculates a unique identifier based on real-time telemetry data. This identifier is recalculated with every server interaction to ensure it matches with the previously-established identifier. Stateless identification uses anonymous telemetry and fingerprint attributes—such as device class, operating system (OS) and other categories—to maintain a stable identifier, unaffected by firmware updates, for over six months while detecting shifts in device configurations. Stateless Device ID includes a robust versioning capability that links each identifier update to its previous version, enabling continuous improvements without disruption.

**Stateful Device ID** adds a layer of persistence by placing a unique identifier directly on the user's device, enabling consistent tracking across sessions. Each interaction validates the returning device against stored telemetry, detecting anomalies.

**Stateful**
A unique identifier is placed in the local storage of the user's device, and is checked during every interaction.



**Stateless**
Calculates anonymous telemetry and fingerprint attributes to determine a persistent unique identifier.

Together, these two identification methods give enterprises the flexibility to match device tracking to specific risk levels and session intelligence. Integrated with Arkose Bot Manager, Arkose Device ID provides comprehensive visibility across device interactions, while also sharing session-based risk insights and device fingerprint data to enhance security decision-making.

## What Sets Arkose Device ID Apart:

| Confident Identification: | Dual Identification Methods: | Full Visibility from First Interaction: |
|---|---|---|
| Pairs session-based risk data, unique identifiers, and anti-spoofing features, ensuring precise tracking of devices to distinguish between genuine users, bots, and bad actors—an unmatched approach in the industry. | Combines stateless and stateful methods, offering enhanced persistence and durability. | Provides unique identifiers for all incoming traffic, without additional vendors or complex integrations. |

## 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

**277+ risk signals and assessments shared**
Receive hundreds of session insights to enrich and tune your internal decisioning models.

**Financial Warranties**
Best efforts aren't good enough. We back our platform with million-dollar warranties and SLAs.

**Arkose Global Intelligence Network**
We see 99% of internet traffic every 20 minutes. Benefit from global risk signals and mitigation intel from our customer base.

**Trusted by the most recognizable brands in the world**
Built for enterprises, our technology, support, certifications and architecture meet your scalability requirements.

**Global, proactive support**
24/7/365 real-time SOC support with proactive incident response vs "on call".

**Harnessing AI to stop evolving threat vectors**
We're leveraging AI to defend against AI-driven bots.

## 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

Arkoselabs.com