PRODUCT BRIEF

Arkose Email Intelligence

Stop fake account creation attacks that start with risky email addresses

The Growing Threat

Cybercriminals are increasingly exploiting email addresses as a gateway for fraud, using them to create fake accounts and orchestrate scams. Our team estimates that billions of dollars of the fraud reported by the IC3 last year started at sign-in or sign-up, much of it fake email-driven account creation. The problem is clear: Current systems often fail to detect low-and-slow tactics that bypass rate-limiting protections. Arkose Email Intelligence, part of the Arkose Titan platform, disrupts this cycle by providing advanced email risk detection, enabling businesses to catch fraudulent activity at the point of sign-up and prevent it from escalating downstream.

What Is Arkose Email Intelligence?

Arkose Email Intelligence is a powerful enhancement to Arkose Bot Manager, a core component of Arkose Titan, that offers comprehensive protection for sign-up and guest checkout processes. Traditional email intelligence tools are often standalone solutions, which limits their ability to systematically interpret findings for downstream mitigation tools. They also cannot correlate with application or web session data, making it difficult to confidently flag and stop threats without disrupting the user experience. In contrast, Arkose Email Intelligence integrates email risk detection with our advanced fraud detection intelligence, providing a paired and holistic interpretation of the web session and email's legitimacy, effectively addressing both automated bot attacks and human-driven attacks.

Arkose Bot Manager provides your foundation:

- Detects automated bot attacks at registration and login
- Includes Phishing Protection to stop credential theft and MFA bypass
- Identifies device and behavioral anomalies
- Delivers Arkose Enforce for automated responses

Email Intelligence adds critical risk signals that Arkose Bot Manager can act on:

- Is it a throwaway or disposable domain?
- Is the email newly created (red flag for fraud)?
- Is it using aliasing or tumbling patterns?
- Is it associated with previous fraud across our network?

The power is in the integration: Arkose Email Intelligence feeds risk data directly into the Arkose Titan platform and Arkose Bot Manager's decision engine. Arkose Bot Manager then correlates email risk with device fingerprinting, IP reputation and behavioral signals to give you a complete threat picture—and automatically enforces the right action.

Bottom line: You're not just validating emails—you're stopping both automated bot attacks AND sophisticated human fraud actors using risky emails. Bot Manager stops the attack method; Email Intelligence identifies the fraudulent identity.

Where and How We Protect

Three Critical Protection Points

- **New Account Registration**
  Stop fake accounts before creation
- **Guest Checkout**
  Prevent fraud without requiring an account
- **Email Collection Points**
  Newsletter signups, waitlists and free trials

Advanced Detection Across Multiple Dimensions

Arkose Email Intelligence operates in real time, analyzing more than 50+ signals across 7 vectors all related solely to the email address:

Email & Domain Velocity	Real-time monitoring with short-term and long-term rolling windows; 2x spike = instant detection
Email Enumeration	Detection of automated account testing patterns
Email Tumbling	Identification of sequential or pattern-based email generation
Email Formation	Syntax and structural analysis
Handle Pattern Recognition	Advanced pattern analysis that catches 71.7% of total fraud by detecting letter-digit patterns on major providers
Gibberish Handle Detection	Abnormal character composition, unusual vowel/consonant ratios, and tiered detection (Extreme, High, Moderate)
Domain Intelligence	Advanced disposable domain service using domain reputation, age and threat intelligence with continuous updates

How It Works: API Response & Action

Real-Time Risk Assessment

When an email address is seen for the first time (without compromising privacy), Arkose Email Intelligence delivers:

Risk Decision
- Email risk score
- 40+ email-specific signals
- Risk attributes and reason codes

Mitigation Guidance
- Suggested actions for treating risky emails based on attack type
- Customers may opt to enforce mitigation challenges based on established logic

Email Risk Evidence
- Automated patterns
- Domain age
- Velocity signals triggered
- Abnormal handle composition
- MX record not found

Response Options
- Present an Arkose Challenge
- Ask for different email
- Phone verification
- Shadow ban accounts

Three Key Benefits

Eliminate Guesswork and Stop High-Risk Traffic at First Interaction

Prevent bad actors and bots from using fake, throwaway or other high-risk email addresses. Arkose Labs shares the risk decision for immediate action, along with the email metadata behind the risk score, for downstream and future protection. Suggested actions offer guidance on handling traffic based on the risk signature.

Gain Multi-Dimensional Insight Without Sacrificing Privacy

Safeguard consumer privacy while preventing fraudulent account creation. Gain a multi-point perspective on new-user risk potential through basic device characteristics, IP and email intelligence data shared via API. Arkose Email Intelligence complies with all applicable data privacy laws, including GDPR and CCPA.

Achieve Affordable, Seamless Protection for Your Entire Customer Flow

Adding email risk assessment offers a cost-effective solution for stopping high-risk interactions from the start. In conjunction with Arkose Bot Manager, you can validate every new registration without compromising the experience for genuine users, while reducing downstream fraud detection and remediation costs.

Real-World Results: Major Gaming Company

The Challenge

A leading gaming company was grappling with the mass creation of fake accounts through unreliable and fraudulent email addresses. This led to a surge in account abuse, undermining both the integrity of in-game environments and the overall user experience.

The Solution

By integrating the multi-layered Arkose Labs solution and leveraging its proprietary email intelligence capabilities, the company was able to accurately distinguish between legitimate users and fraudulent accounts by analyzing and validating email addresses.

The Results

- **8M+ fake account registration attempts** detected and mitigated annually using Arkose Email Intelligence
- **24% lift in fake account detection** in addition to bot traffic management
- **Stopped high volumes of attacks** across major email domains, including Gmail, Outlook and Hotmail

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.

Ready to Stop Email-Driven Fraud?

Arkose Email Intelligence is the ultimate solution for stopping fake account creation and safeguarding your platform from email-driven fraud. Ready to see how it can protect your organization and enhance your fraud prevention strategy? 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.