Arkose Labs | SOLUTION BRIEF

Arkose Email Intelligence for New Account Registration

Stop Bot-Driven Email Fraud at the Top of the Funnel

Email addresses are the key identifier of people's online identity, but traditional email intelligence services are not designed to solve the problem of massive bot attacks that create fake new accounts and perpetrate account takeovers. They don't challenge and block automated attacks, and they are prohibitively expensive to run at the top of the funnel. As a result, organizations end up validating emails long after registration where fake email addresses were first used. Between the costs and complexity of orchestrating email intelligence with bot detection, most businesses have a gap in assessing email risk upon account registration.

Introducing Arkose Labs Email Intelligence

Email intelligence of the future should be scalable to stop fraudsters from creating fake accounts where they originate as part of their bot and hybrid attack defense strategy. That's why we're adding a new layer of bot detection capabilities with **Arkose Labs Email Intelligence,** a cost-effective method of protecting registration and guest check out flows. It's designed to detect risks associated with an email address that is seen for the first time (without compromising privacy), while delivering actionable insight and treatment suggestions through our API response. With an added layer of protection and insight at the top of the funnel, fraud and security teams can stop fake accounts before they're created and significantly reduce spam, abuse, and fraudulent purchases.

- Detect email address risk the first time it's seen on a site
- Catch fake emails at account registration and guest check out
- Reinforce bot prevention detection with email risk assessment
- Stop more promo abuse, spam, scams, and platform abuse
- Improve visibility with actionable insight about email address risk

How it Works

Attack Scenarios We Protect Against

Burst Attack Using One Domain

Attackers sign up for a new domain or choose one of their existing domains and automate email handle creation. With the newly created email addresses on that domain, they attack the registration page of their target website resulting in multiple fake registrations.

Using Multiple Disposable Domains Gradually

Attackers randomize new email creation with multiple disposable domains available for cheap in several marketplaces. They use these newly created email addresses for fake registrations.

Using Different Alias To Create Different Fake Accounts

Attacker identifies a website offering a promotion to new users and creates multiple fake accounts using email aliases.

Why Add Email Intelligence to Your Arkose Labs' Deployment

Multi-Dimensional Insight into Bot and Human-Based Attacks	By adding email intelligence to your existing registration flow, you gain multi-point perspectives into the riskiness of a new user with device, IP, and email intelligence data shared via API.
Eliminate the Guesswork on Treating High Risk Traffic	We share the risk decision and email metadata behind the score for actionable insight. Suggested actions provide guidance on how to treat traffic based on the risk signature.
Assess Email Risk without Sacrificing Privacy	We take pride in following best practices to protect customer's data. We do not store emails in clear-text. You can feel confident using a service that is GDPR & CCPA compliant.
Protect your Entire Registration Flow at Scale	Our goal is to make email risk assessment cost effective so that you can validate every new registration and reduce false negatives.

Try Email Intelligence for Free

Based on early trials, customers can improve catch rates by an additional **20%+**, depending on traffic patterns.

Arkose Labs' mission is to create an online environment where all consumers are protected from malicious activity. Its AI-powered platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks while improving good user throughput. The company offers the world's first and only $1 million credential stuffing warranty. Headquartered in San Mateo, CA with offices in Brisbane and Sydney, Australia, San Jose, Costa Rica, and London, UK, the company debuted as the 83rd fastest-growing company in North America on the 2021 Deloitte Fast500 ranking.

Request a 1:1 demo with your CSM today