Arkose Labs

How Arkose Email Intelligence Stopped Mass Fake Account Creation in Gaming

KEY RESULTS

8M+ fake account registration attempts, on an annual basis, detected and mitigated 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

SUMMARY

A leading global gaming company, renowned for its vast user base and popular titles, was grappling with a significant problem: 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 company needed a robust solution that could effectively combat this threat without compromising the user experience for legitimate players.

This case study focuses on one key aspect of the Arkose Labs solution: Arkose Email Intelligence. By integrating the multi-layered Arkose Labs solution and leveraging its proprietary email intelligence capabilities, the gaming company was able to accurately flag and prevent fake account creation, significantly reducing the volume of malicious registrations. Arkose Email Intelligence helped the company distinguish between legitimate users and fraudulent accounts by analyzing and validating email addresses, providing a seamless experience for legitimate players while effectively neutralizing fraudulent activities.

This partnership empowered the gaming giant to preserve account integrity, improve player trust and maintain the high-quality environment its users expect.

THE BUSINESS PROBLEM

The company's lack of email validation during the account registration process allowed fraudsters to exploit the system, bypassing traditional security measures and creating fraudulent accounts that undermined the gaming ecosystem. Without email checks, fraudulent email addresses—ranging from nonsensical handles to completely invalid domains—were able to slip through the cracks. This lack of control opened the door for fraudsters to exploit the system, leading to an increase in fake accounts.

The company faced two distinct types of attack tactics:

- **Volumetric Attacks:** Fraudsters created large numbers of accounts in short bursts, often using small variations in the email address (e.g., adding "+1", "+2," "+3" to an otherwise legitimate domain) from the same IP address. This overwhelmed the registration flow and was harder to detect using traditional attack detection methods.

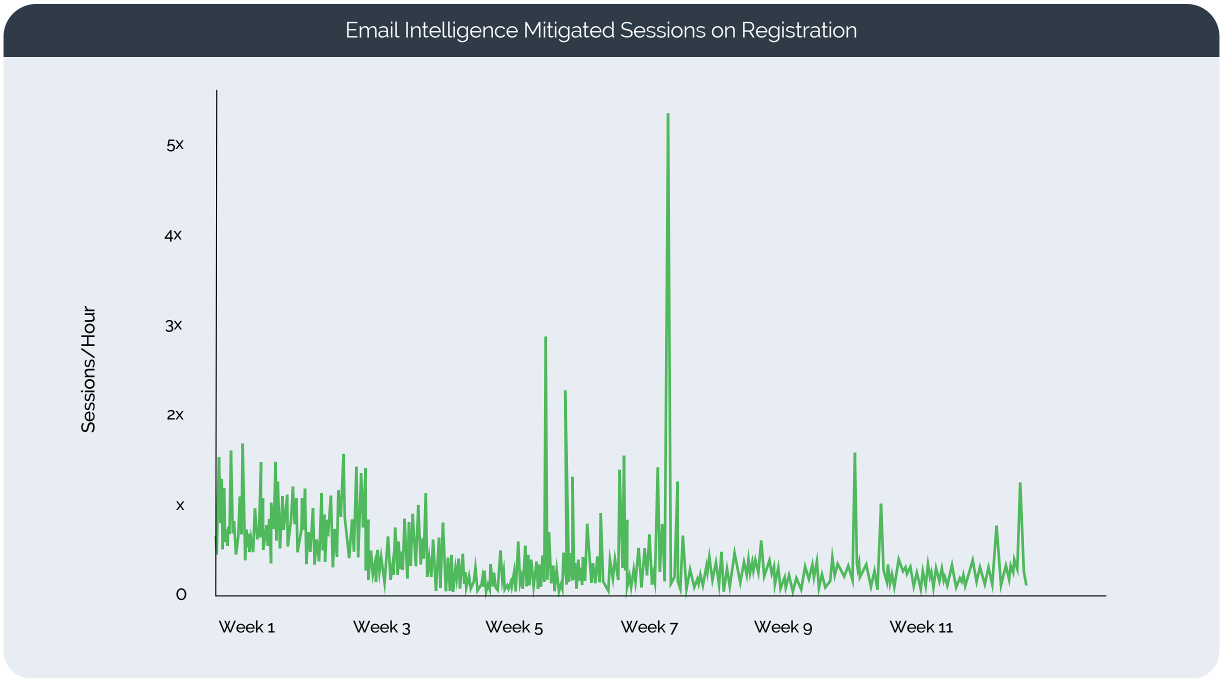
- **Low-and-Slow Attacks:** Fraudsters created fake accounts slowly over time to avoid triggering alarms. These attacks could go unnoticed for extended periods, allowing fake accounts to accumulate undetected.

In addition, the company also struggled with linguistically ambiguous email addresses. Fraudsters used characters or formats that were valid in some regions but not in others, making it difficult for the company to detect potentially invalid registrations.

THE SOLUTION

To address the growing problem of fake account creation and associated fraud, the company turned to Arkose Email Intelligence, an advanced add-on feature within the Arkose Labs platform. By leveraging Arkose Email Intelligence, the company gained the ability to detect and prevent fake account creation at the very beginning of the registration process. Unlike traditional, standalone email intelligence solutions, Arkose Email Intelligence works seamlessly within the broader Arkose Labs framework. This holistic approach enables the gaming company to apply a unified defense strategy, leveraging email and other risk signals to more effectively mitigate fraudulent activity across the user flow. The integration addresses a key challenge of traditional email intelligence solutions: the inability to correlate email address data with other behavioral data like device and IP signals.

The Arkose Labs solution with Arkose Email Intelligence provides a multi-layered defense, using both real-time digital risk intelligence and email risk analysis to mitigate fraud without negatively affecting legitimate users. Arkose Email Intelligence works by analyzing more than 40 signals across seven different vectors in real time to assess the risk of an email address as soon as it is used. This comprehensive analysis ensures that malicious actors using throwaway, disposable or alias email addresses are stopped before they can do damage.



Email intelligence is effective and scalable. By deeply analyzing email addresses, it mitigates an additional 24% of fraud attempts beyond the core bot management platform, even during surges of up to 500% in registration attempts.

Complementary Layers of Security

Both bot management and email intelligence are essential tools for enhancing security, but the distinction between them lies in their detection focus and the value they provide. Bot management identifies and stops automated bots and bad actors seeking to infiltrate your platform by emulating real-user behavior and characteristics. Conversely, email intelligence validates the legitimacy of email addresses, which often serve as the foundation for account creation and digital identity tracking within a platform. While complementary, each addresses a unique layer of protection to effectively distinguish genuine users from attackers.

DEMONSTRATED RESULTS

The integration of Arkose Email Intelligence as part of the Arkose Labs solution significantly transformed the company's ability to detect and prevent fake account creation. After the Arkose Labs solution with Arkose Email Intelligence was implemented, roughly 58% of the total account registration traffic was flagged as potentially fraudulent. By targeting accounts with risky email signals, Arkose Email Intelligence achieved a 24% increase in fraudulent account detection in addition to bot traffic management. This enhanced detection capability was crucial in stopping fake account creation and preventing downstream fraud and platform abuse, which not only had resulted in additional costs but also had damaged the platform's reputation.

The solution's impact was particularly evident in its ability to target and eliminate fake accounts across major email domains, including Gmail, Outlook and Hotmail. These domains, often used by fraudsters to create fake identities, were effectively protected, ensuring that malicious actors could not exploit these common email providers to bypass registration security measures.