kasada | DATA SHEET

How Kasada stops fake account creation and new account fraud in its tracks

Kasada puts an end to fake account creation used to commit fraud, abuse promotions and loyalty programs, and spread disinformation at scale.

Creating fake accounts, whether they are fake social media accounts or bank accounts, represents an effective way for motivated adversaries to gain the upper hand. Also known as new account fraud, fake account creation is an automated attack that uses false or stolen information to generate an online account or profile.

Fake Account Attacks Can Be Used For Several Nefarious Purposes

Login Fraud/ ATO

Bots overwhelm APIs to gain access and take over user accounts to commit fraud.

Promotion Abuse

Attackers can exploit APIs to create fake new accounts, spread spam at scale, and more.

Checkout Fraud

High-volume requests rendering APIs unavailable to legitimate users.

Hate Speech

Bots collect customer information, financial data, and intellectual property.

New account fraud losses exceed $3.4 billion, according to the FTC.

Business Impact of Fake Account Creation

Poor CX

Unhappy users due to inauthentic experience, and slow page speeds

Skewed Metrics

Inaccurate user and web metrics, leading to misleading reporting

High Costs

Increased account verification, fraud, and infrastructure costs

Reputational Harm

Damage to your brand and reputation, weakening your customer loyalty

How Kasada Ends Fake Account Creation

Fake accounts make online experiences unfair for real customers, contribute to an unsafe space for individuals on media platforms, and have a large impact on an organization's revenue, operations, and site performance.

Our unmatched understanding of how these extremely persistent and relentless bots try to evade detection has played a large role in how Kasada has been architected.

Kasada detects fake account creation attempts using hundreds of sophisticated sensors that collect hidden traces of automation. If an attacker attempts to tamper with client data or behavior, we have both client-side and server-side detections that verify data and inspect for anomalies. This multi-layered approach with fail-safes allows us to detect and adapt to threats in real time.

With Kasada, it's more than just a product, you get a team of experts to help in the fight against motivated attackers.

The Kasada Difference

Enduring protection
Defeat adversaries with a platform that's frustrating, time consuming, and expensive to attack.

Decisive Defense
No management, rule updates, or decisions to make. Simplify your life.

Happy Users
Hidden challenges mean zero friction and exceptional user experiences.

Caring Team
Kasada gives you a team, not just a tool. We're accountable for stopping the bots.

Kasada Quick Facts

85%
Of Kasada customers previously used a different provider. They've switched. And stayed.

$150B
Dollars protected annually for eCommerce organizations.

10B
Monthly requests we stop that other systems fail to detect.

40%
Average % of login attempts that are fake

About Kasada

Kasada has developed a radical approach to defeating automated cyber threats based on its unmatched understanding of the human minds behind them. The Kasada platform is intentionally engineered to overcome the shortcomings of traditional bot management tools. Kasada is based in New York and Sydney, with hubs in Melbourne, Boston, and San Francisco. For more information, please visit www.kasada.io and follow on Twitter, LinkedIn, and Facebook.