kasada | DATA SHEET

How Kasada prevents account takeover and credential stuffing attacks

With 22% of US adults experiencing account takeover (ATO) fraud, it's a big problem. Kasada detects the key tells of adversaries who are taking over user accounts at scale to commit acts of fraud.

Account takeover occurs when cybercriminals gain access to user accounts with stolen credentials. Bad actors obtain these stolen credentials through credential stuffing. Credential stuffing uses automation to test stolen usernames and passwords to break into hundreds or thousands of websites at a time.

What Happens Once Adversaries Gain User Account Access

Sell information

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

Takeover more accounts

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

Use credit cards

High-volume requests rendering APIs unavailable to legitimate users.

Web recon

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

A Real-World Example

A recent account takeover example we detected and stopped looked like this:

1. **Wave One — Standard tooling:** a surge in traffic using a worldwide proxy network and browser session hijacking.
2. **Wave Two — First retooling:** a full-force attack using localized residential IPs and clean browser sessions.
3. **Wave Three — Second retooling:** a slower attack, using the same tools as Wave Two but starting in the morning to mimic real human traffic.

Business Impact of Account Takeover Attack

Poor CX

Bad customer experience to have user accounts taken over

Regulatory Fines

Potential for expensive regulatory and governmental fines

High Costs

Increased fraud claims, chargebacks, infrastructure costs, and more

Reputational Harm

Damage to your brand and reputation, costing you your customer loyalty

kasada | DATA SHEET

How Kasada Defeats Account Takeover

Kasada's layered and holistic defense functions differently, takes the fight to the bots — and exhausts them. Without informing attackers, Kasada's proof of work challenge exponentially increases the difficulty level along with the number of abusive requests over time. Put simply, it saps adversaries' resources and makes them work harder. It erodes the ROI of the attack.

The results Kasada's customers see:

- Immediate neutralization of the initial ATO attack
- Prevention of replay attacks
- Deterrence of future attacks

When you make attacks too expensive, attackers look elsewhere. When threats can't retool, they aren't threats at all.

That's Kasada's approach: experts in detecting automation with an unmatched knowledge of adversarial techniques – a team and technology that takes the work off you.

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.