kasada | DATA SHEET

Retailers and eCommerce providers face threats from login to checkout

Adversaries impersonate real users to steal valuable products — sneakers, clothing, electronics, and more — for themselves, or to resell for a tidy profit.

Attackers will target every feature and function of your website, and they'll use multiple techniques to do so. It's an easy value proposition for them: inexpensive to launch attacks at scale, and the cost to companies can reach millions of dollars. Here's how they do it — and how they fool traditional bot management tools.

Automated Threats Across the Customer Experience

Login Fraud

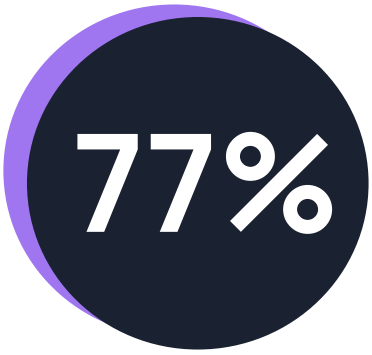
At login, adversaries use automation to conduct credential stuffing and account takeover and create fake accounts at scale.

Browsing/ Add to Cart

Adversaries build bots to scrape info on your products and pricing.. They can also add items to cart and seemingly deplete your inventory,.

Checkout Abuse

Carding, cracking, and checkout bots will use stolen credit/gift card data and quickly purchasing the bulk of hype and limited-stock items.



of the Top 100 retailers using traditional bot management tools can't detect browser-based automated threats.

Business Impact of Retail Security Threats

Poor CX

Slower site performance and a general decline in overall user experience

Skewed Metrics

Performance and business metrics are skewed with high volume of fake traffic

Higher Costs

To service the bad bot traffic, infrastructure and operational costs increase

Reputational Harm

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

Customer Stories

A global footwear company's customers couldn't buy the hot shoes they wanted because bots were snatching up all the inventory. We intervened, and the **company saved upwards of $20 million per year.**

A leading cosmetics brand suffered carding attacks, which not only bogged down the site but kept customers from being able to buy what they wanted. We stepped in and helped our customer **achieve a 15% reduction in infrastructure costs**.

> *"Kasada has single-handedly squashed our reseller problem. We're no longer in bad actors' brag notices. Kudos to the Kasada team!"*
>
> **Director of Security Architecture & Engineering,**
> Fortune 500 Retail Company

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.