kasada | DATA SHEET

How Kasada protects enterprise APIs from automated attacks and abuse

APIs have become adversaries' favorite targets, accounting for 90% of the web app attack surface But Kasada’s proactive protection pressures bots to bug off.

Over 60% of companies have more than 400 APIs, and APIs make up more than 80% of web traffic. APIs are a giant gateway for attacks on web-enabled apps. But it’s not just the size of this gateway that’s concerning — it’s APIs’ increasing vulnerability to automated attacks.

Attack Techniques to Exploit APIs

Credential Abuse

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

New Account Fraud

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

Denial of Service

High-volume requests rendering APIs unavailable to legitimate users.

Scraping

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

> “By 2024, API abuses and related data breaches will double.” **– Gartner**
>
> “CISOs: Focus on API technology and bot management as dual priorities for 2023.” **– Forrester**
>
> “Quite often, APIs do not impose any restrictions on the size or number of resources that can be requested by the client/user. Not only can this impact the API server performance, leading to Denial of Service (DoS), but also leaves the door open to authentication flaws such as brute force.” **– OWASP**

Business Impact of API Abuse

Poor CX

Slow app performance and experience due to API abuse

Skewed Metrics

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

High Costs

Expensive regulatory fines and a large cost of having private data exposed

Reputational Harm

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

How Kasada Protects Enterprise APIs

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 API attack
- Prevention of replay attacks
- Deterrence of future attacks to APIs, apps, and site

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.