kasada

DATA SHEET

Defend Your APIs from Malicious Automation

Overview

Application programming interfaces (APIs) have risen as a better way to build applications, but this has led to an explosion in the number of APIs organizations have to defend. Today, 60 percent of companies report having more than 400 APIs,[1] and APIs now represent 83 percent of all web traffic.[2]

Unfortunately, APIs are a favored target for attacks because they are significantly under-defended—even though they can directly expose a company's business logic and data. Protecting APIs can be challenging, not just because of their ubiquity but also because they are created and used by both developers and business users, so security teams don't even know about all of them. Non-technical developers using no-code/low-code platforms can undermine security such as allowing one user to see data belonging to another, or posting sensitive information to a public location. These factors make them an enormous and growing target for cybercriminals.

Increasingly, headlines confirm that even the largest enterprises are guilty of API-related security failures. Already, APIs account for 40 percent of the attack surface for all web-enabled apps and are predicted to account for 90 percent by 2021, according to Gartner. The industry analyst firm predicts that by 2022, API abuses will become the most-frequent attack vector.[3]

Kasada API protects an organization's web and mobile APIs from automated attacks, botnets, and targeted fraud. Kasada API can be quickly implemented to mitigate online fraud losses and lower operating costs while providing a frictionless customer experience.

WHO'S IT FOR?

Companies with revenue-focused web and mobile applications that have exposed APIs can benefit from Kasada API, helping digital enterprises across all industries, including retail, ecommerce, travel, gaming, and financial services.

Use Cases

There's no shortage of ways that automated attacks on APIs can inflict damage to your business. Many attacks are the same ones that have been carried out against web applications for years, but now cybercriminals have many new targets in the form of APIs. Kasada API, delivered as a cloud-based service, protects APIs without additional resources required from a customer's IT department. Protect your customers, end users, and organization from:

- **Account Takeover**
  Protect your users from having their accounts hacked.
- **Fake Account Creation**
  Prevent attacks and illegitimate actors from creating fake accounts for scams or accessing your content.
- **Loyalty Program Abuse**
  Protect your customer loyalty program by defending your APIs that serve users with rewards services.
- **API Scraping**
  Get in control of your content. Prevent competitors and illegitimate actors from scraping your web and mobile APIs.

[1] "6 Lessons from Venmo's Lax Approach to API Security," Maria Korolov, CSO, July 2019.
[2] "What You Need to Know About the New OWASP API Security Top 10 List," Maria Korolov, CSO, November 2019.
[3] "What You Need to Know About the New OWASP API Security Top 10 List," Maria Korolov, CSO, November 2019.

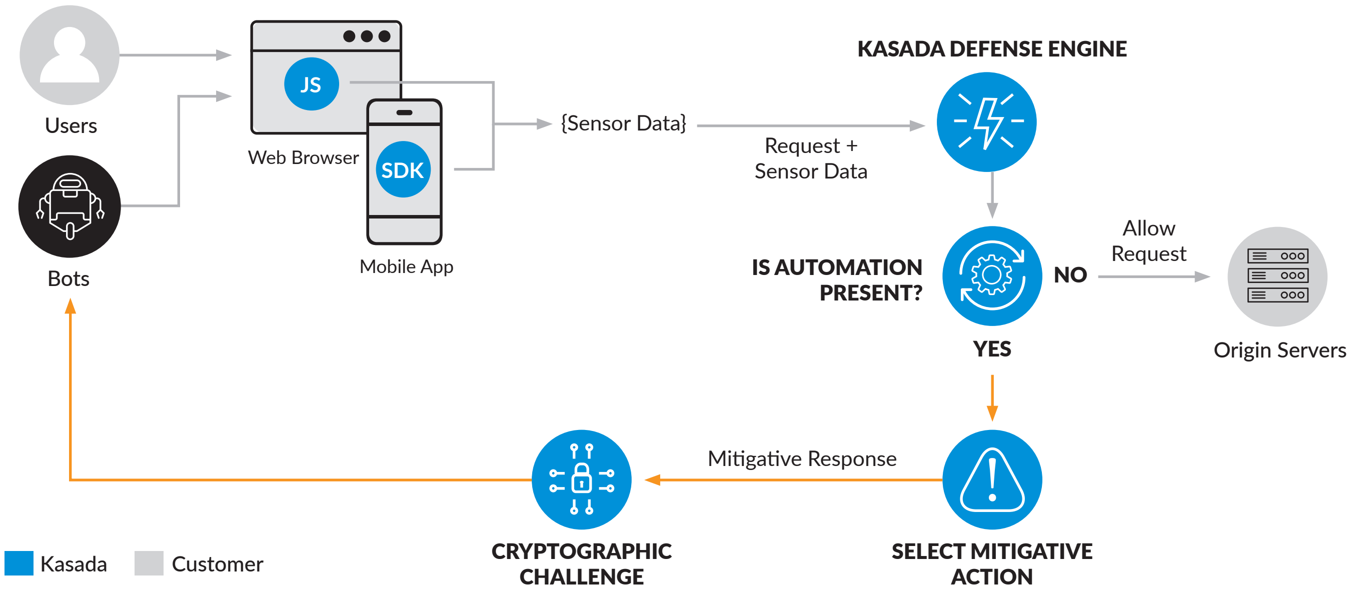

Figure 1: How Kasada API Works

How It Works

Kasada API quickly identifies malicious bots and protects web and mobile apps from automated threats. An organization's most sensitive API endpoints (i.e. authentication, account creation, and handling sensitive data) are at the greatest risk and require that automated attacks be deterred and stopped in real time.

Kasada API deploys the same technology that is utilized for its enterprise solution, Kasada Web, which deters synthetic traffic with sensor detection and inspection process and a cryptographic challenge that makes it arduous and expensive for bots to continue their attacks.

Specifically, malicious automation leaves traces of itself in the client-side environment (browser, mobile phone). Kasada uses "sensors" to collect advanced attributes from the browser or mobile device through a "client interrogation" process, which occurs in the background.

Kasada API customers are provided with either JavaScript SDKs for web applications or mobile SDKs for native Android and iOS apps. Using proprietary techniques, Kasada API presents a myriad of obstacles to frustrate and disrupt the operating model of bot attacks, preventing hackers from using automation and challenging critical aspects of the attack process.

Each SDK uses sensors to collect signals from the mobile environment. This sensor data is then processed by Kasada's data engine of analysers to identify:

- if the mobile device is real or fake
- If the browser is being automated using a bot

When your mobile app calls to your API, Kasada's SDK will decorate the request with a token that's computed from the sensor data. Kasada will mitigate API requests from malicious clients with a deceptive response.

In the Kasada Portal, you can easily and instantly change between these modes to achieve your desired level of protection:

- PROTECT—reports and mitigates malicious traffic
- MONITOR—only reports on, makes no active decisions

HOW IS KASADA DIFFERENT?

Our client Interrogation is focused on the complex relationship between various client-side attributes. It is not the same as "fingerprinting" used by first-generation bot mitigation vendors, which try to construct a tracking ID (fingerprint) by collecting uniquely identifying data and invading your users' privacy. In practice, fingerprinting doesn't work very well, since browsers are changing in a trend known as the "anti-tracking movement."

In addition, a cryptographic challenge is used as a proof of work that exponentially increases the difficulty level with the number of abusive requests over time, therefore exhausting the CPU resources of bad bots, without informing the attacker. This forces the attack to permanently cease, as its ROI inevitably collapses. Not only does Kasada neutralize the attack long-term, but also prevents the bot operator from quickly retooling or attacking other targets, as all CPU resources have been exhausted. Fraudsters then stay away from Kasada-protected properties, as it costs them virtually unlimited resources trying to break in.

Key Benefits

PROTECT YOUR REPUTATION AND REVENUE
Kasada lets you prevent automated attacks on your APIs before they cause you damage. We are devoted to researching attackers and their tools so you don't have to. This saves your team time and your company money.

GET VISIBILITY
The Kasada Portal provides dashboards and rich visualizations to help you understand your traffic. You can see legitimate traffic coming from users of your web and mobile apps. You can see bot traffic imitating users or hitting your API directly.

REDUCE USER FRICTION
Kasada allows you to reduce friction for your end users. CAPTCHAs and other human-facing challenges cause high friction for users; that's why Kasada doesn't use them. Also, good security should be invisible and that's why our solution works in the background, invisible to your users. As well, by preventing attack traffic from putting load on your API servers, Kasada can enhance your API performance for legitimate users.

PROTECT ALL CHANNELS
Kasada lets you detect attacks across all channels of traffic to your APIs.

We'd love to demonstrate the Kasada difference to you; please request a demo today.

About Kasada

Operating globally since 2015 and trusted by enterprises worldwide, Kasada gives internet control and safety back to human beings through its category-defining digital traffic integrity solution. With Kasada, even the stealthiest cyber threats are foiled, from login to data scraping across web, mobile, and API channels. Scalable up to multi-billion-dollar companies, onboarded in just minutes, and designed to deliver clear ROI in multiple departments, Kasada's solution invisibly defends and enhances critical business assets while ensuring optimal online activity, with immediate and lasting traffic security. Kasada is based in New York and Sydney, with offices in Melbourne, San Francisco, and London. For more information, visit www.kasada.io.