DataDome | API PROTECTION SOLUTION BRIEF

83% of all internet traffic belongs to APIs.
-The Anatomy of an API in 2023

Stop attacks targeting your APIs before they damage your business

The challenge: Attackers love APIs too

The API economy is surging, as leading organizations recognize the value APIs bring to products and services. Unfortunately, research shows that fraudsters have also taken notice, targeting APIs with increasingly sophisticated attacks.

APIs are considered "softer" marks because API security is more complex than protection for websites and mobile apps. Therefore, traditional security tools and techniques lack the sophistication required to keep API endpoints secure against the ever-growing threat landscape. Without an accurate and scalable solution, companies face imminent risk of attacks on their APIs—which can negatively impact the customer journey and cause irreparable damage to a company's reputation.

Types of API attacks

- **ATO & brute force**
- **Denial of service & DDoS**
- **Carding attacks**
- **Credential stuffing**
- **Vulnerability scanning**
- **Scraping & data harversting**

The solution: DataDome advanced API protection on autopilot

DataDome's advanced API protection safeguards your endpoints against even the most sophisticated attacks, including new threats using the latest bot techniques.

Unrivaled accuracy

DataDome is the first to spot new and emerging attacks, before any other protection on the market. We stop fraud before it happens, using machine learning combined with our 24/7 SOC and threat research team to ensure unparalleled accuracy. Our solution processes 5 trillion signals per day (~1,000 signals per request) to adapt to and block new threats in real time. We analyze every single request every time to defend mobile apps, websites, and APIs against attacks like ATO, carding, credential stuffing, layer 7 DDoS, scraping, and more.

< 0.01% false positive rate ensures unrivaled accuracy.

Learn more at DataDome.co

No assumptions made

All decisions and actions DataDome takes against bots are based on concrete evidence and a clear understanding of the attacks we see. We inspect every single request every time, in real time. We collect the most comprehensive set of detection signals and leverage 5 trillion data points daily to ensure the most accurate protection possible. There are no shots in the dark—you can view the reasons behind every blocking decision through the dashboard.

Signals we detect & process in real time

Client-side

- Device fingerprints
- Environmental details
- End-user behavior
- Challenge responses

Server-side

- HTTP fingerprints
- TLS fingerprints
- Session details
- Request details

Force multiplier

DataDome is your ally in the battle for API security by providing your team leverage.

The DataDome dashboard gives customers an immersive and enlightening experience with up-to-the-minute visualizations of API threats to your network. Whether your objective is to gain a comprehensive overview of bot vs. human traffic or delve deep into specific threat incidents, DataDome empowers you to achieve your objectives seamlessly.

The dashboard serves as a critical resource for comprehending the presence of malicious bots across your APIs and sharing real-time insights into the various threat categories.

DataDome simplifies the intricacies of API security to empower development teams to create their best work. With our vigilant system in place, developers can focus on innovation, assured that their APIs are shielded from threats. Developers and security analysts can rest easy knowing you have a partner who is vigilant, proactive, and effective at protecting your endpoints.

> "DataDome is very reliable, and we no longer are consumed with worry about bots stealing trail data. We're also very satisfied with the false positive rate; it's half of the industry standard, a small, small fraction of a percent."
>
> **– Kat Leipper, Senior Software Engineer, AllTrails**