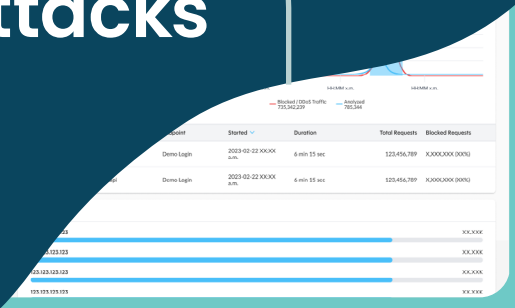
DataDome | DDOS PROTECT PRODUCT BRIEF

Defense against the most sophisticated L7 DDoS attacks

Block the DDoS attacks that CDNs miss in real-time



The challenge: Highly evasive L7 DDoS attacks

Even with CDN or other edge-based security in place, L7 DDoS attacks can still account for 20% or more of traffic reaching your application servers. These attacks evade network defenses by operating at the application layer, mimicking legitimate user behavior and making them difficult for traditional controls to detect and stop.

L7 attacks are not only evasive but highly efficient, requiring minimal traffic to disrupt a target. They are often short-lived, lasting only minutes, causing significant impact before static, rules-based defenses can respond. The rise of agentic AI has intensified the challenge: AI agents can now launch, coordinate, and sustain L7 DDoS attacks at scale, generating adaptive traffic that is harder to distinguish from legitimate users than traditional bot activity.

The business impact of L7 DDoS attacks can be substantial. Beyond service disruption and lost revenue, L7 DDoS attacks can lead to brand damage, contractual or regulatory penalties, and increased infrastructure costs driven by malicious traffic.

> "When the sites went down, all the alarms triggered. We saw a huge traffic spike, which wasn't due to a sales promotion; it was **10x or even 100x** our normal traffic. It became clear that it was malicious traffic rather than organic."
>
> **– Julian Charnas, Director of Digital Commerce at Harman**

The solution: DataDome DDoS Protect

Integrated into DataDome's industry-leading **Cyberfraud Protection Platform**, DDoS Protect uses the most accurate threat detection capabilities to counter these advanced DDoS threats. By combining superior detection, instant mitigation, and near-zero latency, **DDoS Protect** outperforms traditional edge DDoS services, effectively blocking the L7 attack traffic that continues to bypass CDN security unimpeded.

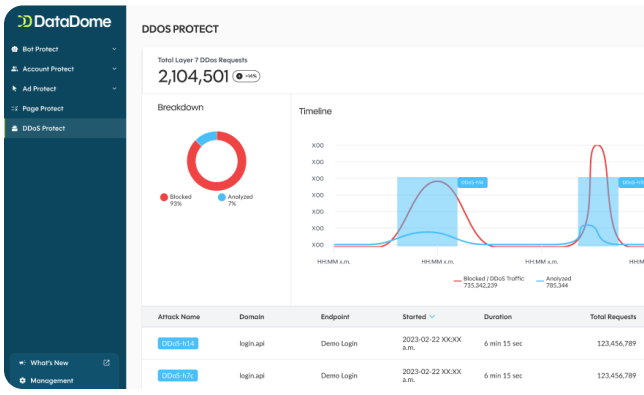
Stop application attacks at the edge

Improve cyber resilience
Instantly detect and mitigate modern L7 threats that other solutions miss.

Slash operations costs, boost ROI
Block attacks at the edge to lower infrastructure usage, avoid quota limits, and eliminate overage charges.

Ensure the best customer experience
Maintain app availability to protect user experience and uphold your brand reputation.

Simplify & optimize application protection
Integrated Bot Management provides operational efficiencies.



DDoS attacks cost an average of $6,000 per minute of downtime.

How DDoS Protect Works

The DataDome Cyberfraud Protection advantage

Protection from the full range of AI automation & fraud attacks

DDoS Protect enhances DataDome's industry-leading bot & agent trust management with advanced L7 DDoS defenses. This integration streamlines security operations, reduces administrative complexity, and safeguards against evasive and highly sophisticated application-layer threats, including agentic AI-driven attacks that use autonomous, self-learning agents to amplify DDoS impact.

Continuous risk assessment of all traffic

DDoS Protect leverages DataDome's AI-powered detection engine to analyze every request anew in under 2 milliseconds. Every request is classified as human, bot, or AI agent traffic, and DDoS Protect instantly mitigates harmful DDoS traffic regardless of its source. With a false positive rate under 0.01%, legitimate user and agent traffic is never disrupted.

Scalable, high-performance security

Built for speed and scalability with 35+ global PoPs, DDoS Protect operates at the edge to deliver ultra-low latency protection. DataDome ensures your business remains secure without compromising performance for your users or business.

Want to learn more?

Request a live demo today

> "The biggest benefit was zero issues during the holiday season—everything was smooth. We had logs showing 16 attacks during that period, but no one even noticed. The websites just worked, which is exactly what we wanted."
>
> **– Julian Charnas, Director of Digital Commerce at Harman**

Key benefits

- **Easy-to-use L7 DDoS protection on autopilot**
- **Continuous business operations**
- **Lower & more predictable infrastructure costs**
- **Useful insights, metrics, analytics, & insights into your DDoS traffic**

20% of traffic that passes through existing CDN and edge-based security controls is L7 DDoS attacks.
-DataDome Advanced Threat Research