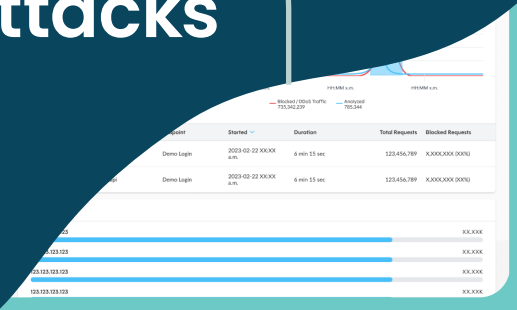
DataDome | DDOS PROTECT
PRODUCT BRIEF

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 services in place, L7 DDOS attacks can still account for 20% or more of total traffic to your app servers[1]. These attacks evade network defenses by operating at the application layer (Layer 7 or L7), mimicking legitimate user traffic and making them nearly impossible for existing controls to detect and stop.

L7 attacks are not only evasive but also highly efficient, requiring minimal traffic to incapacitate a target. Worse, they are often short-lived—lasting just minutes—causing maximum disruption before static rules-based defenses can respond.

The impact of L7 DDOS attacks can be widespread and highly damaging to your business. In addition to service disruptions and lost revenue, these attacks can result in brand reputation damage, contractual or regulatory penalties, and increased infrastructure costs from the attack traffic itself.

> "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 immediately

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

Slash operations costs, boost ROI

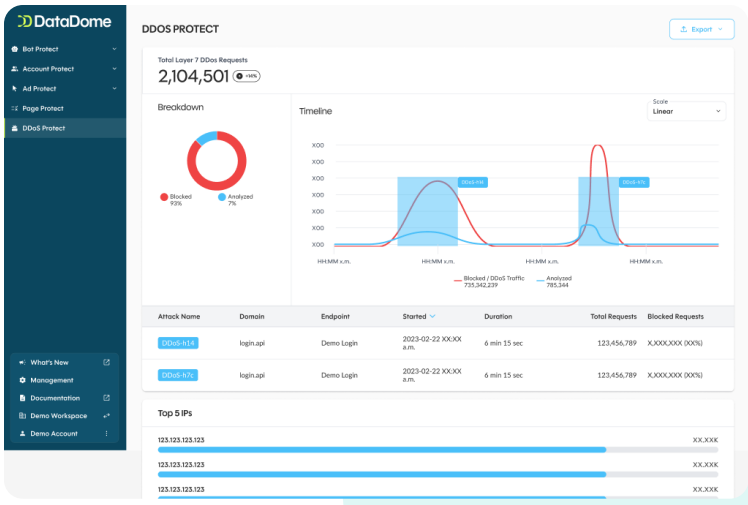
Block attacks at the edge to lower infrastructure usage, avoid quota limits, and eliminate overage charges.

Ensure the best customer experience

Maintain app availability to protect user experience and uphold your brand reputation.

Escape from constant crisis mode

Simplify application protection with better detection and auto-pilot mode blocking.



[1]DataDome Advanced Threat Research team based on analytics from 300+ customers

How DDOS Protect works

The DataDome Cyberfraud Protection advantage

Protection from the full range of targeted bot & fraud attacks

DDOS Protect enhances DataDome's industry-leading bot management with advanced L7 DDOS defenses. This integration streamlines security operations, reduces administrative complexity, and safeguards against evasive and highly sophisticated application-layer threats.

Continuous risk assessment of all traffic

DDOS Protect leverages DataDome's AI-powered detection engine to analyze every request anew in under 2 milliseconds. DDOS Protect identifies and instantly mitigates harmful DDOS traffic, and with a false positive rate under 0.01%, it doesn't disrupt legitimate user traffic.

Scalable, high-performance security

Built for speed and scalability with 30+ 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.

> "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

- **Immediate L7 DDOS protection on autopilot**
- **Continuous business operations**
- **Lower & more predictable infrastructure costs**
- **Useful insights, metrics, analytics, & insights into your DDOS traffic**

Learn more about DDOS Protect by requesting a live demo today.

"DDOS attacks cost an average of $6,000 per minute of downtime."
-Help Net Security, 2024