ENTERPRISE DDOS PROTECTION

ORYXIOS

NEXT-GENERATION TRAFFIC INTELLIGENCE

Revenue loss stops here.

No downtime. No blocked customers. No revenue loss.

Deployed in environments where downtime is not acceptable.

40+ Tbps	<1ms	L3/4/7
SCRUBBING CAPACITY	THREAT DETECTION	COMPLETE COVERAGE

ORYXIOS

THE COST OF INACTION

Every attack is a measurable revenue loss event — not a technical incident.

Modern DDoS attacks cause measurable customer churn, SLA breaches, and six-figure revenue loss per hour. The question is no longer whether you will be attacked — it's how much the next attack will cost you.

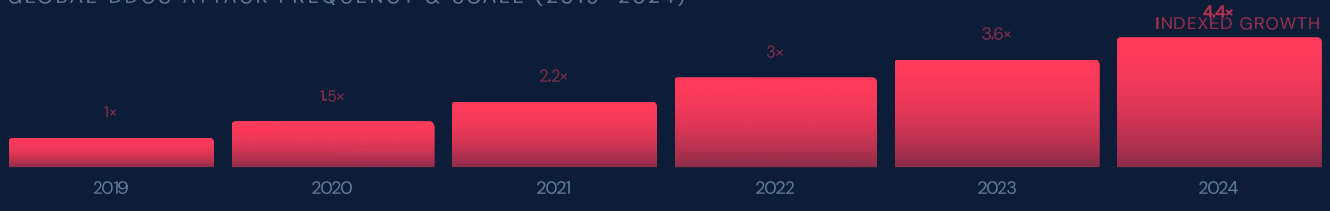
$1M **Revenue loss per hour.** Average enterprise downtime costs **$300K–$1M per hour** — before SLA penalties and customer churn are counted.

ADAPTIVE **AI-driven botnets** mutate attack signatures in real time — making yesterday's rules useless and causing service interruptions that look legitimate to your systems.

L7 **Application-layer attacks** cause customer-facing failures while network monitoring shows no anomaly — resulting in silent revenue loss and undetected churn.

BROKEN **IP-based blocking destroys revenue.** Distributed botnets share IPs with legitimate users — your protection is blocking the customers you are trying to serve.

GLOBAL DDOS ATTACK FREQUENCY & SCALE (2019–2024)



Indexed attack volume — compound annual growth rate exceeds 35%

This is not an IT problem.

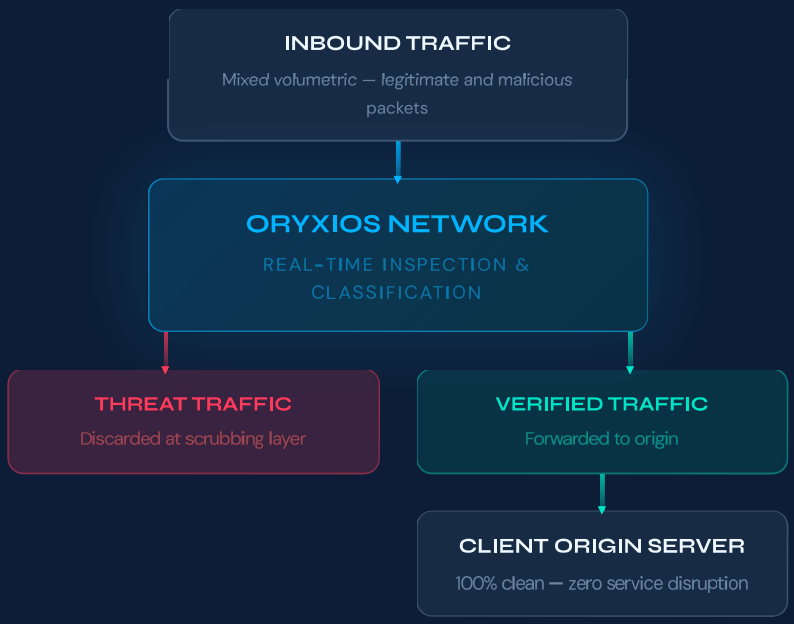
This is a revenue leakage problem. Every minute under attack directly impacts transactions, conversions, and customer trust. The average enterprise loses **$300K–$1M per hour** — before SLA penalties or long-term churn are counted.

ORYXIOS

PROPRIETARY ARCHITECTURE

DNA Traffic Routing Engine

Every packet is inspected and classified in real time. Threat traffic is discarded at the edge. Legitimate traffic is returned to your origin — unaltered, undelayed, invisible to your users.



Oryxios does not block traffic.
It separates good from bad — and only removes what hurts your business. Your customers never see it happen.

Zero Revenue Impact

Your users experience no degradation, no friction, no blocked sessions. The attack is invisible to your application and to your customers.

Infrastructure-Agnostic Deployment

BGP, DNS, or inline proxy — Oryxios integrates without modifying your existing stack, routing, or hardware.

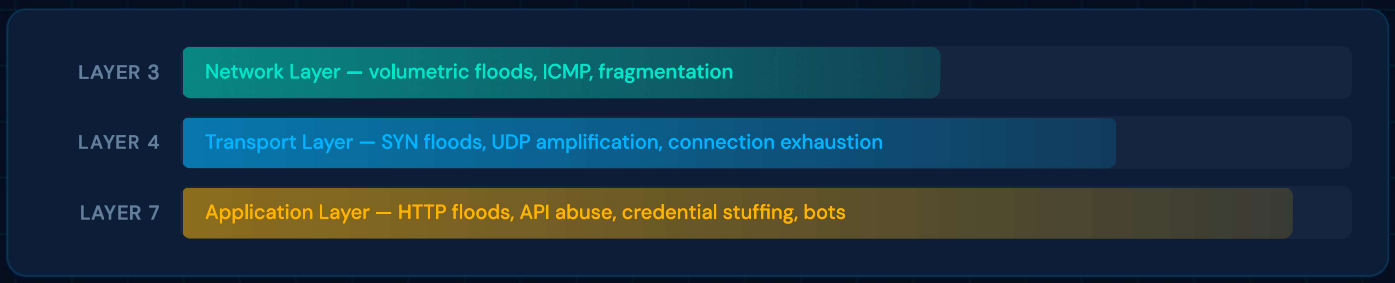
ORYXIOS

OPERATIONAL FLOW

End-to-end in under one millisecond

Fully automated.
No engineers on call. No manual rules to update. No response time. Protection is active before your team receives the first alert.

FULL-STACK COVERAGE



DEPLOYMENT OPTIONS

BGP Announcement
Carrier-level route diversion — no on-premise changes, activates at global network scale.

DNS Diversion
Record-level redirection through Oryxios scrubbing nodes — minimal configuration, propagates globally within minutes.

Inline Proxy / GRE Tunnel
Always-on transparent protection — no threshold triggers, no gaps in coverage, no infrastructure changes.

Threshold Auto-Detection
Baseline traffic modeling triggers automatic scrubbing the moment anomalous patterns are identified.

ORYXIOS

THE DIFFERENCE

Not just protection — traffic control.

Most solutions stop the attack by stopping your traffic. Oryxios isolates the threat, eliminates it, and returns every legitimate session uninterrupted. Your customers never know an attack occurred.

– TRADITIONAL PROTECTION	+ ORYXIOS
– Static rule sets — obsolete within hours of a new attack campaign	+ Behavioral analysis — continuously adapts, no static rules to exploit
– IP blocklisting — blocks legitimate customers sharing botnet IP ranges	+ Packet-level scrubbing — no IP dependency, zero collateral blocking
– High false positives — direct revenue loss from blocked valid sessions	+ Near-zero false positives — legitimate sessions pass through unaffected
– Reactive posture — mitigation begins after service interruption starts	+ Always-on — mitigation active before the first malicious packet lands
– Network-only — application-layer attacks bypass the perimeter	+ Full-stack L3 / L4 / L7 — network and application layers covered
– Under attack = under-serving customers — revenue loss unavoidable	+ Attacks are invisible to customers — revenue stream never interrupted

Traditional protection forces a trade-off:
Stop the attack — or serve your customers.

Oryxios removes that trade-off completely.

CORE DIFFERENTIATORS

Intelligent Traffic Processing

Behavioral analysis trained on billions of traffic patterns distinguishes attack signatures from legitimate sessions in real time.

Zero-Downtime Architecture

Redundant scrubbing infrastructure across globally distributed PoPs — 100% service continuity under sustained multi-vector attacks.

ORYXIOS

PROVEN CAPACITY

Designed for scale. Guaranteed under pressure.

The numbers your board, your SLA committee, and your legal team need to see.

40+
Tbps
MITIGATION CAPACITY

The largest recorded DDoS attack reached ~3.5 Tbps. Oryxios absorbs over 10× that volume — with capacity remaining. When attackers escalate, your service does not register a change.

<1ms
SUB-MILLISECOND DETECTION

Threat traffic identified and isolated before reaching your application.

100%
UPTIME SLA

Globally redundant nodes with automatic failover — online regardless of attack duration.

Built for mission-critical systems.
Used in environments where downtime is not acceptable — fintech, infrastructure, and high-traffic platforms processing millions of daily transactions.

BUILT FOR THESE ENVIRONMENTS

- Cloud & Hosting Providers
- Financial & Fintech Platforms
- High-Traffic Commerce
- Real-Time Digital Platforms
- Enterprise Infrastructure

DEPLOYMENT SCENARIOS

Attack Response
Automated mitigation the moment anomalies are detected — zero manual intervention required.

Always-On Traffic Hygiene
Continuous scrubbing for platforms where any interruption carries direct revenue consequence.

API & Application Protection
Layer 7 analysis separates legitimate API usage from bot floods and session abuse — without blocking real customers.

Carrier-Grade Infrastructure Defense
BGP-level protection for ISPs and enterprise networks requiring multi-Tbps resilience.

● PROTECTION ACTIVE — 24/7/365

Stop losing revenue to attacks.

Deploy in under 24 hours — before your next attack hits.
No infrastructure changes required.

40+	<1ms	L3-7
TBPS SCRUBBING	THREAT DETECTION	FULL COVERAGE

Every minute you wait is revenue you don't get back.

Talk to our team and get a protection plan tailored to your traffic.

Get Your Protection Plan | Request Demo

No long-term contracts · No infrastructure changes · No risk to start

GIZMONIA.COM · INFO@GIZMONIA.COM · YOUR TRAFFIC. FULLY UNDER CONTROL.

RESPONSE TIME: < 1 HOUR · DEPLOYMENT: < 24 HOURS