ip infusion

SOLUTION BRIEF

Affordable Automated DDoS Defense for Modern Networks

March 2026

In the first half of 2025, DDoS attacks surged 41% (Source: GCORE H1 2025 Report) with peak attacks hitting 2.2 Tbps. Manual and legacy defenses can't keep up. It's time for an automated defense that reacts faster than the attack.

The Solution: Disaggregated, Automated, and Intelligent

Together, IP Infusion and FastNetMon deliver a unified, carrier-grade DDoS defense that detects, mitigates, and learns, automatically, across any open network architecture.

This approach combines IP Infusion's OcNOS®, a carrier-grade network operating system (NOS) on cost-effective whitebox hardware, with FastNetMon, an intelligent, software-based detection and mitigation platform.

The result is a flexible, scalable, and economically superior architecture. **The integration leverages open telemetry and BGP standards, ensuring full interoperability across multi-vendor networks.**

Traditional vs. Disaggregated DDoS Defense: A Technical Comparison

This joint solution replaces expensive, proprietary "scrubbing" appliances with a modern, disaggregated model. Here's how the architecture compares for a network engineer:

Feature	Traditional (Monolithic) Appliances	OcNOS + FastNetMon (Disaggregated)
Architecture	Single, proprietary "black box."	Software (FastNetMon) + Open Hardware (OcNOS).
Control Plane	**Bundled** inside the appliance.	**Decoupled**: FastNetMon software (VM/Server) acts as the "brains."

Feature	Traditional (Monolithic) Appliances	OcNOS + FastNetMon (Disaggregated)
Data Plane	**Bundled** inline "scrubber" appliance.	**Decoupled**: OcNOS routers (whitebox) act as the distributed "brawn."
Traffic Path	Requires traffic to be processed 'inline' (through the appliance) or diverted to a central 'scrubbing center' for mitigation.	**Out-of-band** detection (sFlow/IPFIX). Mitigation is performed **directly at the edge** without rerouting traffic.
Scalability	**"Scale-Up"**: To add capacity, you must replace the entire (and expensive) chassis.	**"Scale-Out"**: Add detection capacity (VMs) and enforcement (routers) independently.
Cost Model	High-cost, proprietary hardware lock-in.	Low-cost whitebox hardware + flexible software.
Standards	Often uses proprietary detection methods.	**100% Standards-Based** (BGP, sFlow, IPFIX) for multi-vendor integration.

How It Works: A Closed-Loop Defense Cycle

The solution delivers a fully automated, closed-loop defense cycle - requiring zero manual intervention.

1) **Detect (OcNOS):** At the network edge, OcNOS-powered routers sample traffic at line rate using ASICs and export high-performance sFlow/IPFIX telemetry.
2) **Analyze (FastNetMon):** The centralized FastNetMon software ingests telemetry, correlates data, and instantly detects traffic anomalies that signal a DDoS attack.
3) **Mitigate (BGP):** Once an attack is confirmed, FastNetMon automatically pushes BGP FlowSpec or RTBH rules to all OcNOS routers, stopping the attack within two seconds.

The closed-loop automation continuously learns from real-time telemetry, ensuring each mitigation cycle becomes faster and more precise.

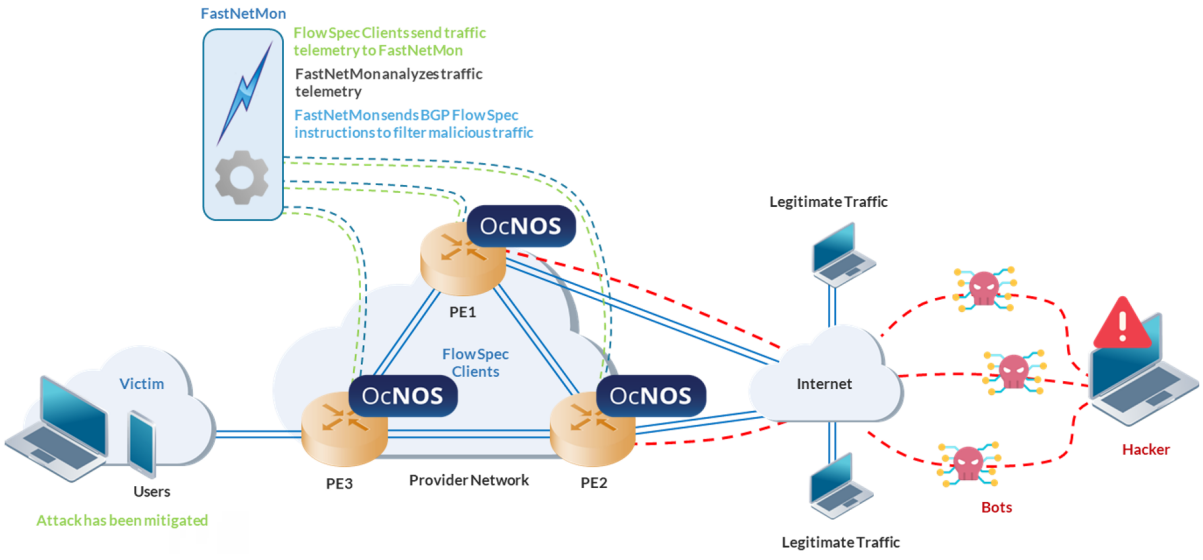

Figure 1. FastNetMon BGP FlowSpec Mitigation with OcNOS Routers

Flexible Mitigation for Any Scenario

This joint architecture supports two complementary, standards-based mitigation modes:

- **FlowSpec (Precision):** Drops only malicious flows, keeping legitimate customer traffic alive and services online during an attack.
- **RTBH (Speed):** Instantly null-routes flooded targets to protect upstream links from saturation during overwhelming volumetric attacks.

Both techniques are implemented entirely through standard routing protocols - no inline bottlenecks or proprietary hardware required.

Key Benefits

- **Stop attacks in <2 seconds,** minimizing service disruption.
- **Keep legitimate traffic flowing** with BGP FlowSpec precision.
- **Cut DDoS TCO by up to 75%** compared to proprietary hardware.
- **Scale detection and enforcement independently** as your network grows.
- **Avoid vendor lock-in** with an open, standards-based design.

Conclusion: A Strategic Advantage in Network Defense

The joint IP Infusion–FastNetMon solution redefines DDoS protection. It provides an open, automated defense that scales and adapts with your network, delivering carrier-grade resilience at a fraction of the cost of legacy solutions.

Ready to Reinvent Your Network Defense?

Want to know how it works? Read the step-by-step **Application Note: Automated DDoS Mitigation with IP Infusion OcNOS and FastNetMon.**

Contact us, request a demo at ipinfusion.com/ddos-defense

Phone | +1-877-699-3267 **Email |** sales@ipinfusion.com **Web |** www.ipinfusion.com