Smart NetProtect

Flow-Based Deployment
Agile, Scalable and Cost-Effective DDoS Protection

Growing Cybersecurity Threats Facing Telecom Networks

Telecom operators are facing an unprecedented surge in Distributed Denial of Service (DDoS) attacks: threats that are growing in scale, speed, and sophistication. According to most updated research, DDoS attacks on the telecommunications industry have grown to unprecedented levels, with peak attacks now reaching 5–10 Terabits per second (Tbps) and occurring five times more frequently than before.

These attacks are not limited to high-profile Tier 1 providers. Tier 2 and Tier 3 operators, which have more limited budgets, are becoming increasingly vulnerable and often lack the resources to implement complex, high-cost mitigation solutions. The consequences of a successful DDoS attack can be serious, ranging from extended service outages and reduced network performance to reputational harm, customer loss, and regulatory issues. As attack methods grow more powerful, the need for agile, scalable, and cost-effective protection has become a strategic priority.

Allot Smart Net Protect - Stay Ahead of Evolving Threats

Allot Smart NetProtect gives you the ultimate control and flexibility to defend your network - no matter its size, structure, or business needs.

We know that one defense strategy doesn't fit all. That's why we offer three powerful, adaptable deployment options: flow-based for cost-effective, scalable protection; hybrid, which combines flow-based detection with inline mitigation precision; and inline for critical services that require the highest accuracy and the fastest mitigation.

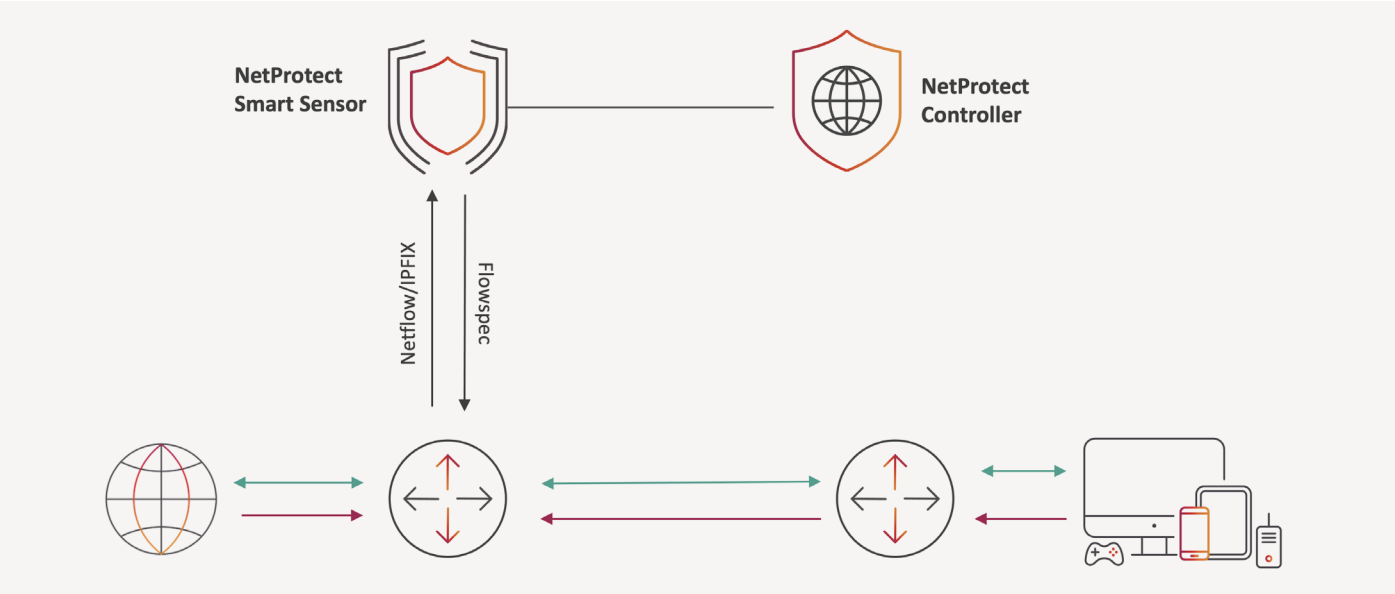
Whether your priority is speed, affordability, or accuracy, Smart NetProtect offers the flexibility to select the solution that best fits your needs, with a truly robust, adaptive approach to evolving DDoS threats.

Flow-based deployment option

Flow-based deployment offers you a cost-effective, highly scalable approach to DDoS protection, specifically designed for budget-conscious deployments that require quality and reliability.

Attack detection accuracy is achieved in this option as a result of the following key capabilities:

- **Bidirectional correlation between inbound and outbound traffic flows:** enables more precise detection of anomalous patterns and attack signatures, significantly enhancing accuracy compared to traditional flow-based solutions that rely solely on unidirectional sampling.
- **Adaptive detection engine:** It first assesses the expected attack size and then decides which detection method to activate – either an AI-based engine for large attacks or a threshold-based engine to reduce false positives for smaller attacks.



Smart NetProtect - Flow-based deployment architecture

***NetProtect Smart Sensor (Allot SG)**

- Collects NetFlow sample aggregations
- Send the information to the Controller

****NetProtect Controller**

- Attack mitigation logic
- Visualization
- Reporting & Notification
- Policy Engine

Key Features

Any Size Attack

The flow-based deployment is designed to instantly detect and mitigate DDoS attacks of any scale, including massive volumetric threats. Its scalable architecture ensures consistent protection without performance degradation, even under extreme traffic loads.

Precise attack detection

Combining bidirectional correlation between inbound and outbound traffic flows, together with adaptive DDoS detection that features AI-based detection as well as threshold-based techniques.

No Blackholing

Instead of dropping all traffic to a targeted destination, Smart NetProtect selectively mitigates malicious flows while preserving legitimate traffic.
This approach prevents service disruption and avoids collateral damage to users and applications, maintaining business continuity.

Network Visibility

Real-time dashboards provide complete visibility into live traffic, anomalies, and threat activity across the network.
This instant insight enables operators to make quick, informed decisions and improve situational awareness during active threats.

No Traffic Diversion

The Flow-based deployment option of Smart NetProtect detects attacks at the router level using sampled data, without interfering with the actual traffic flow. This guarantees low latency, maintains the network architecture, and simplifies deployment without requiring configuration changes.

Business Value

- **Highly Scalable Solution:** This deployment option is designed to successfully mitigate attacks of any size through its flow-based detection and mitigation technology.
- **Low Total Cost of Ownership (TCO):** With automatic detection and mitigation, simple installation, and no required network configuration changes, the flow-based deployment option of Smart NetProtect delivers high value with minimized operational costs.

Dec 2025