Smart NetProtect

Hybrid Deployment Option
Highly Scalable with High Mitigation Precision DDoS Protection

Growing Cybersecurity Threats Facing Telecom Networks

Telecom operators today face an unprecedented surge in Distributed Denial of Service (DDoS) attacks, which are rapidly increasing in scale, speed, and sophistication. As detailed in most updated research, DDoS attacks against the telecommunications sector have reached new heights, with peak volumes soaring to 5–10 Terabits per second (Tbps) and attack frequency multiplying fivefold. These threats now target not only Tier 1 providers but also Tier 2 and Tier 3 operators, many of whom lack the resources for complex, high-cost mitigation solutions.

Given the severe consequences of successful DDoS attacks—including extended service outages, diminished network performance, reputational damage, customer loss, and regulatory risk—telecom operators require defense strategies that are both scalable and precise. The evolving nature of attack vectors demands solutions that go beyond traditional approaches, making a hybrid deployment option essential. By combining flow-based detection with off-ramp mitigation, the hybrid architecture empowers operators to achieve highly scalable, precise DDoS mitigation, ensuring network resilience.

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.

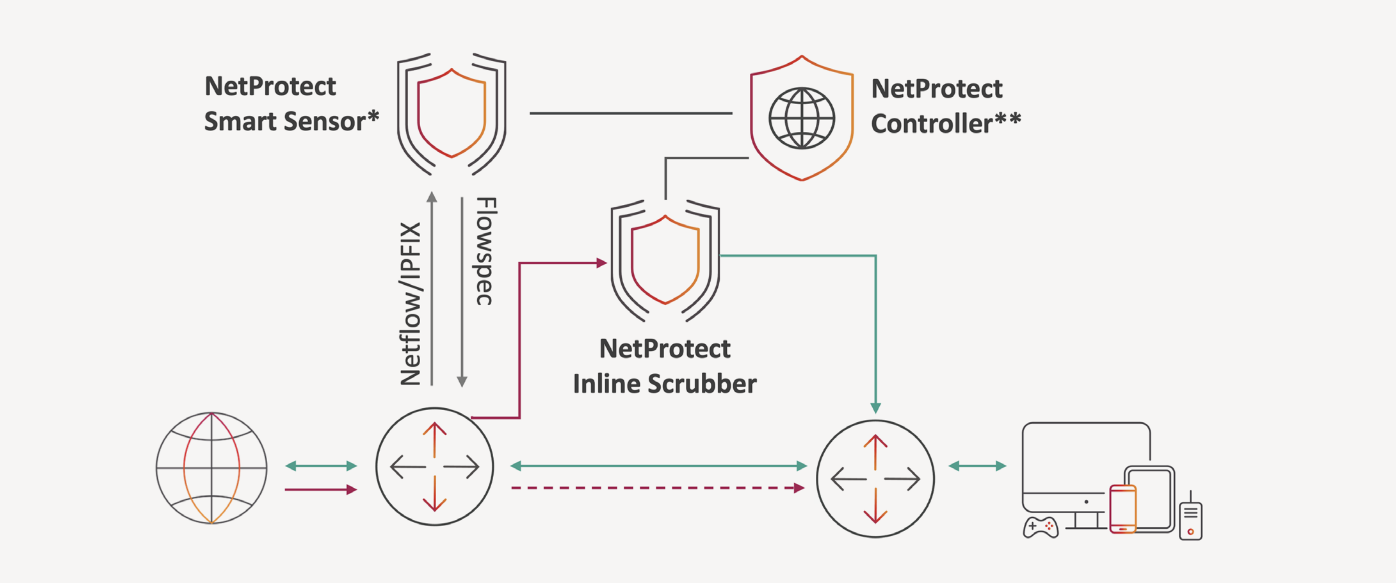
Smart NetProtect - Hybrid Deployment

Combines the advantages of both methods—flow-based detection with sample aggregations and an on-prem scrubber that filters all malicious traffic—for high-precision defense against DDoS attacks.

Attack detection accuracy is achieved with 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 ML and AI-based engine for large attacks or a threshold-based engine to reduce false positives for smaller attacks.

Once a threat is detected, the system implements targeted mitigation through an on-premises off-ramp scrubber, ensuring only malicious traffic is blocked while legitimate flows stay uninterrupted. The hybrid deployment architecture offers scalability to manage high traffic volumes while providing highly accurate threat mitigation, making it an ideal solution for carriers seeking a mix of cost efficiency, scalability, and precise mitigation. Additionally, hybrid deployment detects Botnet attacks and C&C access, and isolates infected servers.



Smart NetProtect - Hybrid 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 hybrid deployment of Smart NetProtect 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 ML and AI-based detection as well as threshold-based techniques.

Accurate mitigation

Accurate mitigation in the Hybrid deployment of Smart NetProtect is achieved through an off-ramp scrubber that analyzes the entire suspected traffic and ensures that only malicious traffic is filtered out, while legitimate flows pass through without interruption.

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.

Botnet and C&C access detection and isolation

Utilizing its advanced screening engine, Smart NetProtect looks for subscribers/hosts with high Connection Error Rate (CER) and, upon detection of anomaly behavior, Smart NetProtect can isolate the server from continuing and communicating via the internet.

Network Visibility

Real-time dashboards provide full 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 Hybrid deployment 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

- **Highest Flexibility in DDoS Protection:** As a result of its unique combination of flow-based detection and off-ramp scrubber, the hybrid deployment of Smart NetProtect ensures optimal protection and continuous service for any network size.
- **Highly Scalable Solution:** The solution is designed to effectively detect attacks of any size through its flow-based detection technology.
- **Covering multiple protection services -** Anti DDoS and Anti Botnet

Dec 2025