Smart NetProtect

The most flexible DDoS Protection, Empowering Telecom Networks Against Evolving Threats

Growing Cybersecurity Threats Facing Telecom Networks

Recent industry research shows that the telecommunications sector is the top-most targeted industry for DDoS attacks, and the risks are only increasing with new technologies like 5G and the rise of IoT devices. These innovations bring incredible opportunities, but they also open the door to more sophisticated cyber threats. Whether attackers target your network directly or your customers, the impact can be severe: service disruptions, damage to your reputation, and threats to your business' resilience.

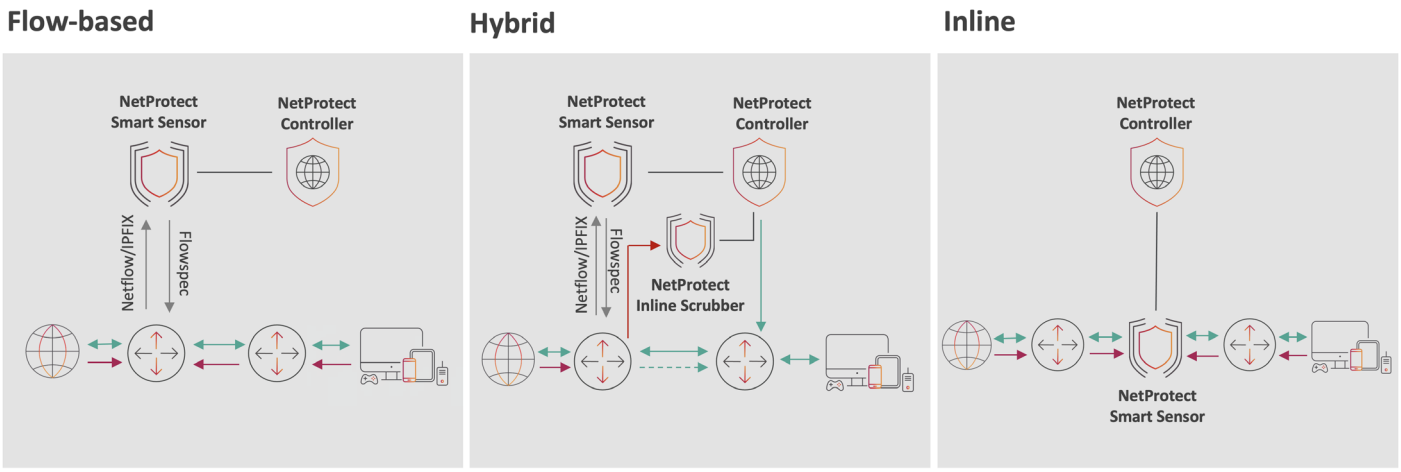
Allot Smart Net Protect – Stay Ahead of Evolving Threats

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.

Unmatched Detection: No matter which option you choose, our adaptive detection ensures superior accuracy. The Smart NetProtect controller uses advanced AI and Machine Learning, or traditional threshold-based detection capabilities, to analyze incoming attacks most effectively, ensuring your network's resilience across all segments.



Allot Smart NetProtect - Deployment options architecture

Flow-based deployment option

- **Affordable and Scalable:** Cost-effective, highly scalable DDoS protection, using sample aggregation of flow-based detection and router-level mitigation.
- **Adaptive Detection Technology:** The system automatically chooses the best way to analyze threats, using advanced machine learning and AI when needed, or simple threshold-based techniques to minimize false alarms.
- **Best for:** budget-conscious deployments that require quality and reliability.

Hybrid deployment option

- **Enjoy the best of both worlds -** flow-based detection, including the adaptive detection technology for scalability, and an on-premises scrubber for precise mitigation.
- **Botnet Defense:** Quickly identify and isolate infected hosts to stop botnet attacks in their tracks.
- **Best for:** telcos seeking a balance of cost efficiency, protection against both DDoS volumetric attacks and Botnet attacks, and precise mitigation.

Inline deployment option

- **Protect your network with multiple services -** Anti-DDoS, Anti-Botnet, Firewall, protection against Application Layer (L7) attacks, and Quality of Experience (QoE).
- **Maximum Accuracy:** Inline deployment inspects all traffic for the most advanced and accurate attack detection and mitigation.
- **Best for:** Critical services that demand the highest level of security and performance.

	Flow-based	Hybrid	Inline
Detection	Flow-based, traffic sample aggregations	Flow-based, traffic sample aggregations	Packet-based, 100% traffic inspection
Mitigation	DDoS - Inbound & Outbound	• DDoS - Inbound & Outbound; • Botnet, C&C Access	• DDoS – Inbound & Outbound • Botnet, C&C Access • Application Layer (L7) Attack
Protection coverage	Entire traffic filtering by router	Diversion of the malicious traffic to on-prem Scrubber	Entire traffic filtering by On-Prem Scrubber
Accuracy	Moderate accuracy detection and mitigation precision, due to traffic sampling and FlowSpec limitations	Moderate accuracy detection (due to traffic sampling) with high mitigation precision	Highest accuracy detection and mitigation precision
Scalability	Highest	High	Moderate
Business value	• Lowest TCO • Affordable solution • Highly scalable	• Balancing accuracy & cost • Adaptive protection (easy migration from flow-based option)	Maximum protection (Including small attacks)

Allot Smart NetProect - Deployment options overview

Why Choose Allot Smart NetProtect?

- **Proactive Defense:** Empowers you to face tomorrow's evolving threats, ensuring your protection strategy remains effective as new challenges emerge.
- **Adaptive Detection:** Our technology automatically selects the most effective way to spot and stop attacks, using AI and machine learning for optimal accuracy.
- **Business Resilience:** Keep your services running, your customers happy, and your reputation intact, even in the face of evolving cyber threats.

Dec 2025