Smart NetProtect

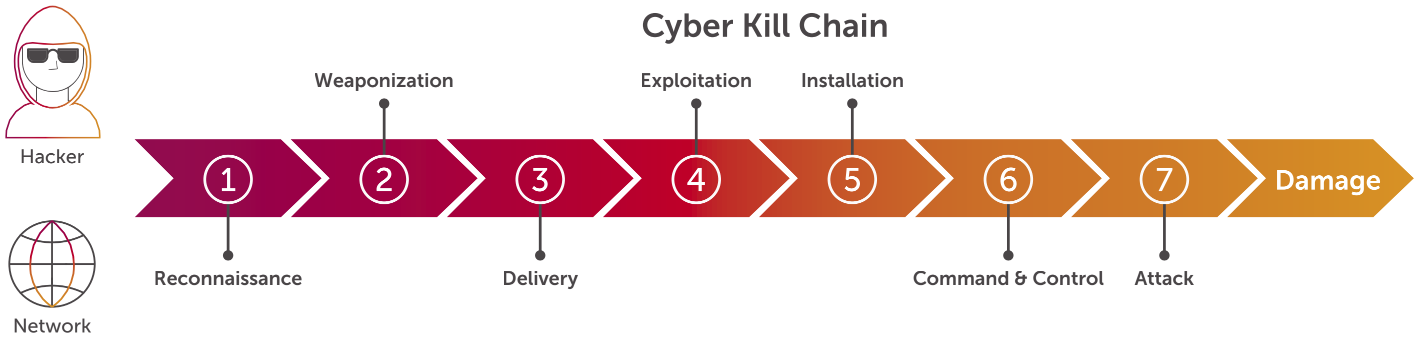
Comprehensive Threat Protection is Critical for Telecom Networks & Business Transformation

The most recent industry research underscores the telecom sector as the second-most targeted industry by cyberattacks. Telecom networks suffer twice - both as the primary targets of attacks, as well as conduits for malicious activities. Consequently, these attacks threaten critical infrastructure and services within the CSP network and beyond. What further exacerbates these risks is the advent of modern access technologies like fiber optic and 5G radio, network distribution, network cloudification and mass deployment of IoT devices, making the network much more vulnerable.

Whether the attacks are aimed at CSP networks or customers, the services, reputation, and business resilience will be compromised if these attacks are not mitigated quickly and effectively.

Smart NetProtect - A leading multi-layer approach to stop the cyber kill chain

Allot's multi-layer approach provides "State-of-the-art" protection from multi-vector attacks against network infrastructure, subscribers, and applications. It is composed of multiple protection services: Anti-DDoS, Anti-Botnet, Firewall and QoE protection. Hence, providing comprehensive protection from both inbound and outbound attacks, proactively preventing bot recruiting and deployment of attack launch pads in the network, protecting the network infrastructure like routers, middleware, etc. from being overwhelmed by volumetric attacks, and providing advanced traffic management and application detection capabilities to protect the performance of mission-critical applications during cyberattacks.



Cyber Kill Chain

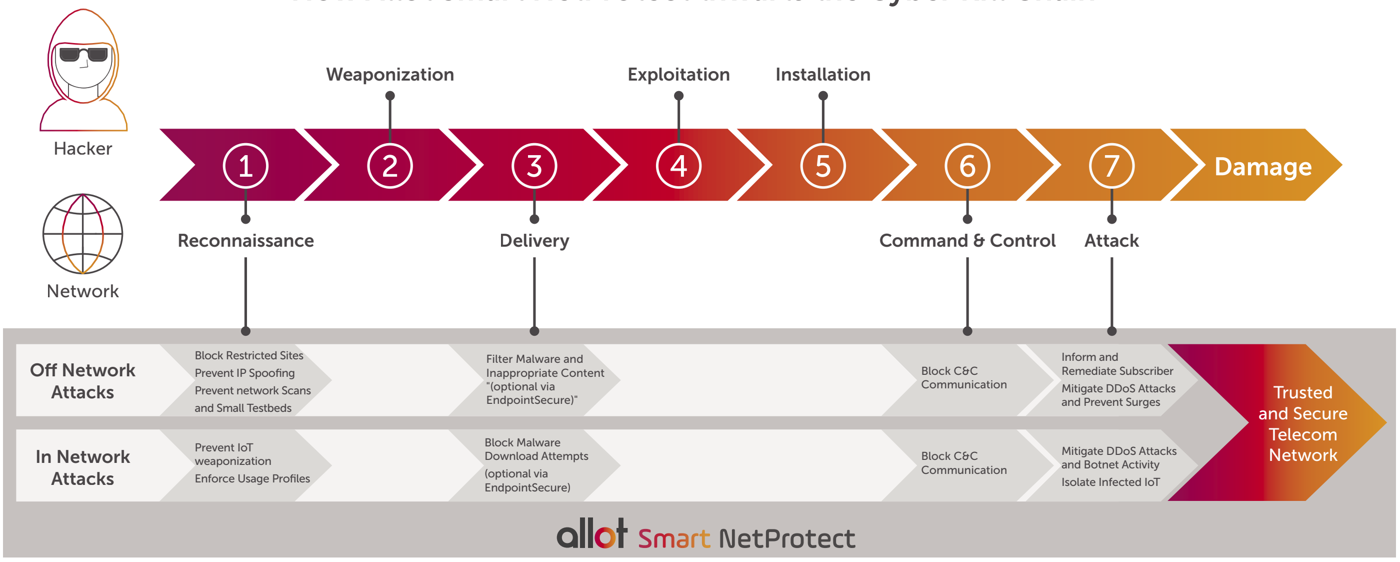
To keep up with multi-stage attacks that target high-speed, distributed networks serving millions of unsecured, high-traffic devices, communication service providers (CSPs) will need a new approach to network security. CSPs must evolve and adopt a layered approach, like that used by Allot Smart NetProtect, to block attackers at every stage of the cyber kill chain.

Stop Cyber Attacks Before They Stop Your Business

The multi-layered approach used by Allot Smart NetProtect proactively mitigates cyberattacks within the emerging stages of the attack. Should an attack reach your network, additional layers of protection will detect and mitigate the threats, preventing the pain of losses from network or service downtime. At every interaction between the attacker and the targeted network, Allot Smart NetProtect identifies and blocks the attack, as follows:

	Reconnaissance	Delivery	Command and Control	Attack
Attack Phase	In the Reconnaissance phase, attackers scan the network for vulnerable hosts and IoT devices, which can be exploited for installation of botnet malware	In the Delivery phase, attackers transmit the weaponized software to the intended victim.	In the C&C phase, the infected bot communicates with its command and control server to receive attack instructions.	In the Attack phase, the attacker performs the DDoS attack. Attacks occur either within the network, utilizing weaponized IoT devices, which reside in the CSP network, or off network, where the attack is coming from the outside aimed at targets inside the CSP network or at its network infrastructure. Either way, damage is done to the CSP business.
Allot Smart NetProtect Mitigation	Prevents access from unauthorized and spoofed IP sources. Blocks IP scans and port scans and prevent brute force login attempts. This prevents subscriber and IoT exploitation by malicious actors.	Prevents download of malware and inappropriate content to any subscriber and IoT device in the CSP network.	Blocks communication to C&C IPs and enforces acceptable usage profiles to prevent the recruitment of bots inside the CSP network for launching attacks.	Mitigates both in-network and off-network DDoS attacks. Monitors host (connected device) behavior and isolates subscribers or IoT devices that behave abusively.

How Allot Smart NetProtect thwarts the Cyber Kill Chain


Hacker
Network
Weaponization
Exploitation
Installation
1
2
3
4
5
6
7
Damage
Reconnaissance
Delivery
Command & Control
Attack
Off Network Attacks
Block Restricted Sites
Prevent IP Spoofing
Prevent network Scans and Small Testbeds
Filter Malware and Inappropriate Content "(optional via EndpointSecure)"
Block C&C Communication
Inform and Remediate Subscriber
Mitigate DDoS Attacks and Prevent Surges
In Network Attacks
Prevent IoT weaponization
Enforce Usage Profiles
Block Malware Download Attempts
(optional via EndpointSecure)
Block C&C Communication
Mitigate DDoS Attacks and Botnet Activity
Isolate Infected IoT
Trusted and Secure Telecom Network
allot Smart NetProtect

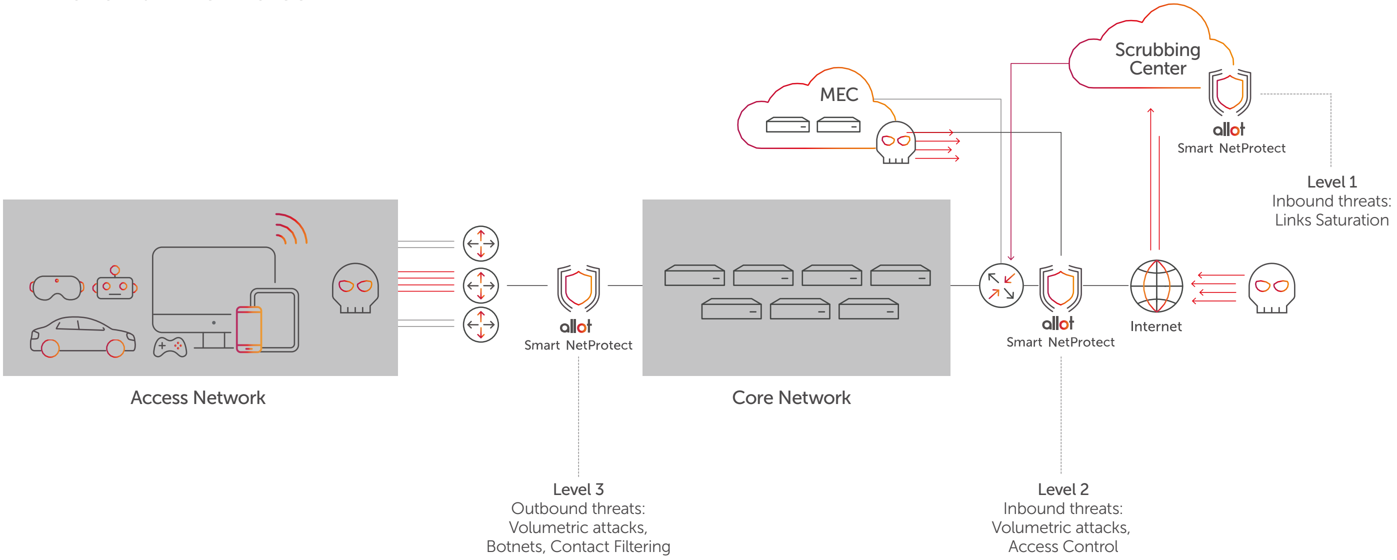
Paradigm Shift to Real-time, In-line Protection

Allot Smart NetProtect provides DPI-based detection- It inspects all packets and deployed in-line or as a TAP with the CSP. It obtains complete traffic captures, including headers and payload, without aggregation or sampling. Thanks to its DPI technology, Allot Smart NetProtect not only helps to detect attacks, but also serves a variety of important network performance and security services. It uses a high-scale, machine learning-based detector, thus providing zero-day protection designed to handle large amounts of information. This means the detection is much faster and more accurate, with higher confidence in triggering mitigation.

Allot Smart NetProtect dynamically filters out attack traffic while clean, legitimate traffic goes through unimpeded. To avoid Interconnect link saturation, in cases of very large attacks, the attack's traffic segment is directed into a scrubbing center for cleansing action. The clean data is then routed back to the network. The deep inspection of traffic not only improves the mitigation accuracy, but also delivers quality forensics, which the CSP can use to strengthen defenses, either in real-time during attacks, or through post-attack analysis.

The simultaneous action of Smart NetProtect services – anti-DDoS, anti-Botnet, and Firewall, leverages its traffic analysis capabilities – providing on-pass multi-vector security inspection that minimizes added latency and Time-to-Response.

Allot Smart NetProtect



Powered by Allot Network Data Analytics

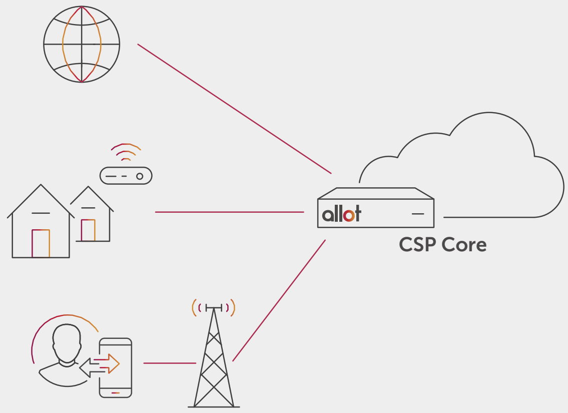
Allot, a leading provider of network intelligence and carrier grade security solutions for CSPs, protects thousands of networks worldwide with over 20 years of proven success. This experience covers networks ranging in size from small operations up to Tier 1 CSPs, including peering point and nation-wide deployments, addressing diverse and complex requirements.

Allot Smart NetProtect builds on this experience with an industry-leading network intelligence. Allot Smart NetProtect Provides traffic prioritization and bandwidth re-shaping to ensure latency-sensitive mission-critical application QoE reliability, even under attack.. It uses automation and network behavior models that power advanced machine learning algorithms to automatically block even zero-day attacks.

Allot Smart NetProtect investigates real-time threats with detailed attack reporting, event analytics, and full packet capture. Seamless integration with SIEM and SOAR enables real-time SOC notification of attack detection and mitigation.

Deployment Options

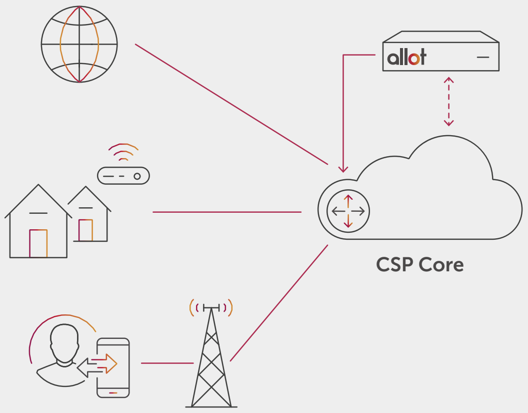
In-Path



- On-prem RT monitoring of the entire traffic
- Detection within up to 15sec & mitigation within 40sec
- Full network protection capabilities
- Traffic Management addons & analytics are available
- Optional scrubbing center mitigation to prevent interlink saturation

Comprehensive & Rapid attack mitigation with Optimal QoE assurance, even under attack!

TAP Mode



- On-prem entire traffic mirroring and monitoring
- Detection within up to 15sec & mitigation within 40sec
- Mitigation commands sent to affected router
  - Blackholing
  - Throttling
- Analytics available but no traffic management addons
- Optional scrubbing center mitigation to prevent interlink saturation

Comprehensive & Rapid attack mitigation while minimizing points of failure in the data path

Allot Smart NetProtect, specially designed to fit modern telecom networks, delivers the following key features and benefits:

Key Features

Real-time In-Line DDoS Protection

- Detect and block DDoS attacks automatically within seconds and at scale, before they can threaten or disrupt your network service. Both inbound and outbound traffic is inspected to ensure no attack goes undetected. Optional scrubbing center mitigation is available to prevent interlink saturation.

Botnet Mitigation

- Detect abusive behavior generated by compromised IoT and bot-infected endpoints, and mitigate through isolation from the network.

Firewall (FW) Protection

- Protect the network firewall from being overwhelmed by volumetric attacks

Subscriber Protection

- Protect your subscribers from malware infections by monitoring their network behavior. Engage SIM owners and remediate to eliminate threats to MNO reputation.

Content Protection

- Inspect and block access to inappropriate content to ensure younger subscribers are not exposed to inappropriate content.

Threat Forensics & Analytics

- Investigate threats in real-time with detailed attack reporting, event analytics, and full packet captures. Get notified in real-time on attack detection and mitigation on your SOC through seamless integration with SIEM and SOAR.

Critical App QoE Assurance

- Ensure critical app QoE to support industry-specific use cases relying on uninterrupted communication. Protect network elements from surges and over-bandwidth utilization.

IP and URL Blacklist

- Filter restricted URL and prevent IP Spoofing for improved security and to comply with local regulations.

Key Benefits

Empowers CSP business resilience

- Detect known and unknown threats before any damage to CSP network
- Surgically mitigate DDoS attacks without overblocking
- Assure low latency use cases go uninterrupted
- Reduce business risk and network down time

Avoid Brand Reputation Damage

- Prevent network reconnaissance and delivery of malware
- Block Command & Control communications
- Isolate weaponized IoT and remediate infected users
- Mitigate outgoing botnet-driven attacks

Reduce Cost and Increase ROI

- Automate detection and mitigation, no manual intervention required
- Drive efficiency with cloud native support, including on-boarding and scale-out
- Integrate seamlessly with provider core network
- Differentiate offering and deliver new revenue-generating services

Simplify Security Operations

- View and manage your entire network security functions from a single central point
- Gain threat intelligence on attackers and their targets in your network
- Use detailed forensics to improve your defense strategy
- Address diverse and complex network and security architectures

Key Differentiators

Allot Smart NetProtect provides all-in-one
Zero-trust protection from inbound, outbound & botnet attacks, with Firewall protection, empowering CSP business resilience. Allot Smart NetProtect offers the following advantages:

Single, integrated, cloud native application, specially designed for modern networks

Multi-layer threat prevention to mitigate the latest and most evasive cyber attacks

Integrated with 5G Core - In-line solution at low latency and 5G scale

Broad range of security functions to protect the network from inbound and outbound attacks

Zero-day automatic attack mitigation, utilizing machine learning

Built on top of industry-leading network intelligence (DPI)

Quality of Experience (QoE) protection - Protect QoE of mission-critical services and applications, even under attack

Dec 2023

© 2023 Allot Ltd. All rights reserved. Specifications subject to change without notice. Allot and the Allot logo are registered trademarks of Allot. All other brand or product names are trademarks of their respective holders.