allot 5G NetProtect

Comprehensive User Plane Protection is Critical for 5G Network & Business Transformation

5G Networks are designed to bring faster speeds and lower latency that enable a host of new business applications, such as autonomous cars, AR/VR, eHealth, and more. To make this possible, 5G architecture calls for Control and User Plane Separation (CUPS), so that high speed, low-latency data can be processed at multi-access edge computing sites (MECs) without wasting time traveling to the center and back. However, this architecture, combined with 5G speed and the anticipated massive deployment of IoT, makes security much more challenging. The threat landscape (IoT), points of attack (MEC), and 5G speeds (1Gb/device) are all orders of magnitude larger. Vulnerable IoT devices can be easily taken over by threat actors to form massive DDoS attacks from both inside and outside the network. Time-sensitive and mission-critical 5G use-cases amplify the problem with their uncompromising performance requirements. In addition, 5G network virtualization and edge cloud deployments further the need for robust security and consistency of protection across both core and edge components.

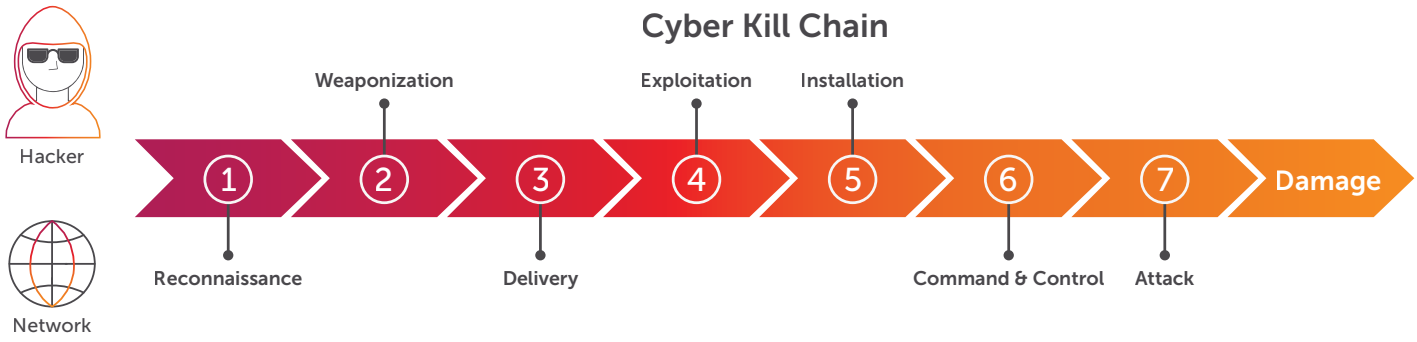
Allot 5G NetProtect enables 5G operators to protect the user plane and securely deliver on the promise of 5G network and service transformation.

The Allot 5G NetProtect Solution

Forward-thinking 5G Security through a Multi-layered Approach

Modern cyberattacks use a multi-stage methodology, known as the "cyber kill chain," to maximize the impact of their attacks. Allot 5G NetProtect employs a multi-layered approach to thwart cyberattacks at all points of attack. The entire solution is fully virtualized to support cloud native architectures.

The following diagram depicts the cyber kill chain stages, from reconnaissance all the way to network and service damage.



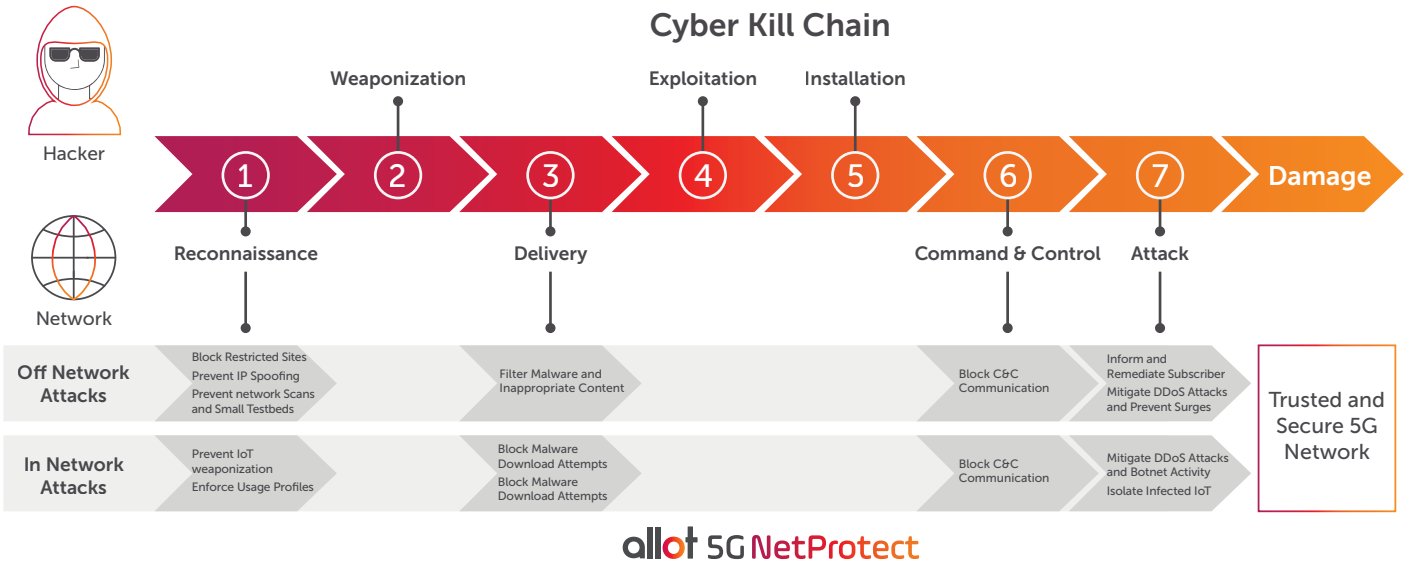
To keep up with multi-stage attacks that target high-speed, distributed 5G networks serving millions of unsecured, high-traffic devices, communication service providers (CSPs) will need a new approach to network security. 5G CSPs must evolve and adopt a layered approach, like that used by Allot 5G NetProtect, 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 5G 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 5G 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 5G 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.

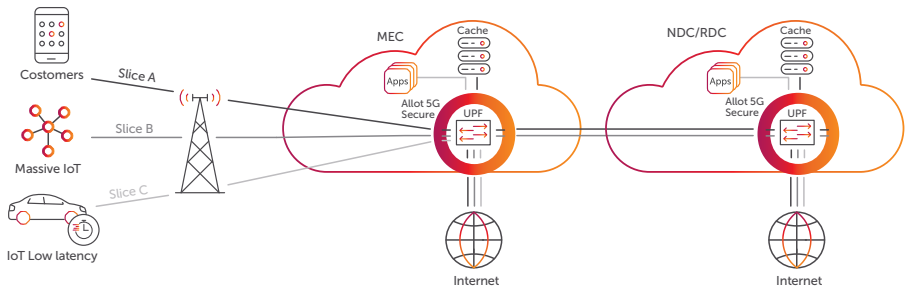
The following diagram summarizes the above table:



Paradigm Shift to Real-time, In-line Protection

Until now, CSPs have typically relied on "end of the chain" scrubbing centers to remove attack traffic that reaches the network. In addition to its multi-layered, proactive approach, Allot 5G NetProtect has another powerful advantage over the traditional scrubbing center approach. Instead of rerouting traffic to a scrubbing center, Allot 5G NetProtect employs dynamic, 5G scale, real-time in-line protection that automatically detects and mitigates any attack off-network or in-network, known or new, regardless of their sophistication. No human intervention is required, no latency is introduced at the network edge or at the core, and attacks are mitigated as close to the point of attack as possible.

In contrast, traditional, purpose-built cloud or centralized scrubbing centers, which have previously provided effective mitigation of large-scale attacks, have significant disadvantages in 5G networks (see callout box to the right).



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.

The Allot 5G NetProtect solution builds on this experience with an industry-leading network intelligence platform and uses automation and network behavior models that power advanced machine learning algorithms to automatically block even zero-day attacks.

Scrubbing Center Limitations

- **Backhauling traffic is expensive**
  Significant, costly bandwidth is consumed diverting traffic to a scrubbing center and returning clean traffic to the intended flow.
- **Latency impacts service QoE**
  Backhauling all internet traffic to scrubbing centers adds network latency to legitimate, scrubbed traffic, negatively impacting performance-sensitive applications and cancelling the benefits of 5G.
- **Reactive rather than proactive**
  Scrubbing centers respond to attacks that are already in progress instead of proactively blocking them. In 5G, early-stage attacks can cause damage before they are mitigated.
- **Small attacks go undetected**
  Most scrubbing centers only mitigate attacks that cross significant bandwidth thresholds, missing the sub-saturating, low-threshold attacks that add up to significant bandwidth waste. This results in unnecessary and costly network expansion due to underutilized capacity.
- **Requires human intervention**
  Many modern attacks evade automated scrubbing centers and require human intervention. Short, massive pulse attacks end before automatic diversion. Highly fragmented attacks appear to be legitimate traffic.
- **Do not cover in-network attacks**
  Most scrubbing centers do not mitigate attacks from within the network. Such attacks at 5G scale can bring down services and entire networks.

Allot 5G NetProtect is deployed as a cloud native application, specially designed to fit 5G architectures, both fully virtualized and hybrid, and 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.

Botnet Mitigation

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

Massive IoT Security

- Discover IoT and monitor activity according to expected usage profiles to prevent them from getting infected with malware, as well as assure their continuous proper function.

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 5G 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

Reduce Business Risk and Network Down Time

- Detect known and unknown threats before any damage to CSP network
- Surgically mitigate DDoS attacks without overblocking
- Assure low latency 5G use cases go uninterrupted

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-board and scale-out
- Integrate seamlessly with 5G Control and User planes
- 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 MNO network and security architectures

Key Differentiators

Allot 5G NetProtect is a unique solution, tailored to meet 5G requirements for scale, latency, and expanded threat landscape. Allot 5G NetProtect offers the following advantages:

- Single, integrated, cloud native application, specially designed for 5G CSP security architectures
- Multi-layer threat prevention to mitigate the latest and most evasive cyber attacks
- In-line solution at low latency and 5G scale
- Broad range of security functions to protect the network from within and from without
- Zero-day automatic attack mitigation, utilizing machine learning
- Built on top of industry-leading network intelligence (DPI)

Sept 2020