Allot Network & Services Resilience (NSR) Solution

Assures Enterprise Infrastructure and Business Continuity

Complex and targeted floods are the #1 risk to Enterprise network resilience

In today's dynamic business landscape, enterprises across all industry sectors suffer from volumetric and "hit-and-run" floods traffic that negatively impact the business. These floods can harm business productivity, causing the network to lose its integrity and creating significant remediation costs, impacting the company's direct revenues and brand image and potentially leading to a full-blown network shutdown.

The situations in which the network might lose its integrity are usually caused by floods perpetrated by internal actors (or botnets) that penetrate the network and infect several corporate devices. These aren't just disruptions; they are potential disasters that open the floodgates to data breaches and serve as gateways for malicious external forces to infiltrate critical network devices and connections. These severe scenarios directly lead to data leakage and enable external attackers to access network devices and connections.

These internal and external floods also put the network's critical infrastructure at risk: Enterprise assets, such as DNS servers, routers, mail servers, firewalls, etc. Overwhelmed and incapacitated, these crucial assets cease functioning, leaving enterprises vulnerable and unprotected, amplifying the urgency for robust defenses and swift, proactive measures.

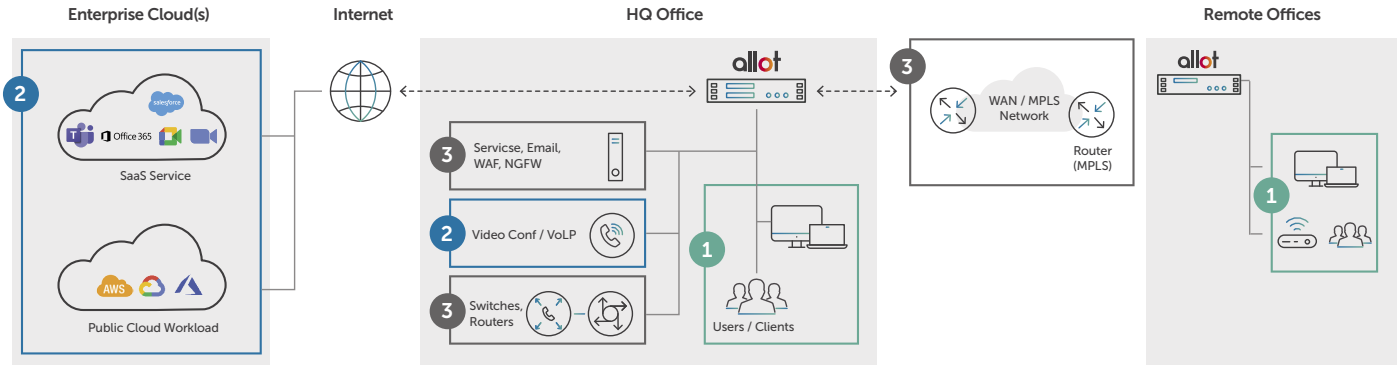
Allot Network & Services Resilience (NSR) Solution - A unique multi-level approach to ensure business continuity and productivity

The Allot NSR solution is a leading zero-day DPI-based anomaly awareness and mitigation solution. It utilizes a unique multi-level assurance approach with high-scale machine learning algorithms for:

- **Network & Critical IT asset resilience**
  Deployed inline and provides bidirectional volumetric and "bursty" Network Layer Anomaly Detection – NBAD (L3-L4), while assuring critical services availability (e.g., WAF, DNS). Mitigation can be done within seconds on-prem, and optionally through a cloud-based scrubbing center.
- **User & Server Resilience**
  Spots anomalous behavior of network infrastructure due to misconfiguration. Within seconds identifies and mitigates anti-botnet and command and control communication and assures network assets, such as WAF, Firewall, and DNS server, from being bombarded and overwhelmed so that they can continue to protect the business.
- **Mission-Critical Services Resilience**
  Provides both Intelligent application classification and prioritization, while assuring mission-critical services availability even under inbound and outbound floods and any other anomaly behavior.

Allot NSR's unique multi-layer approach orchestrates the simultaneous functioning of its parts, thus perfectly safeguarding the business from complex and targeted floods.

1. Users + Servers Resilience: Behavioral anomaly awareness & Network Integrity
2. Mission-Critical Services Resilience: QoE-maintenance + service preservation - under flood
3. Network & Critical IT Assets Resilience: flood absorption (WAF, NGFW, Routers, WAN...)



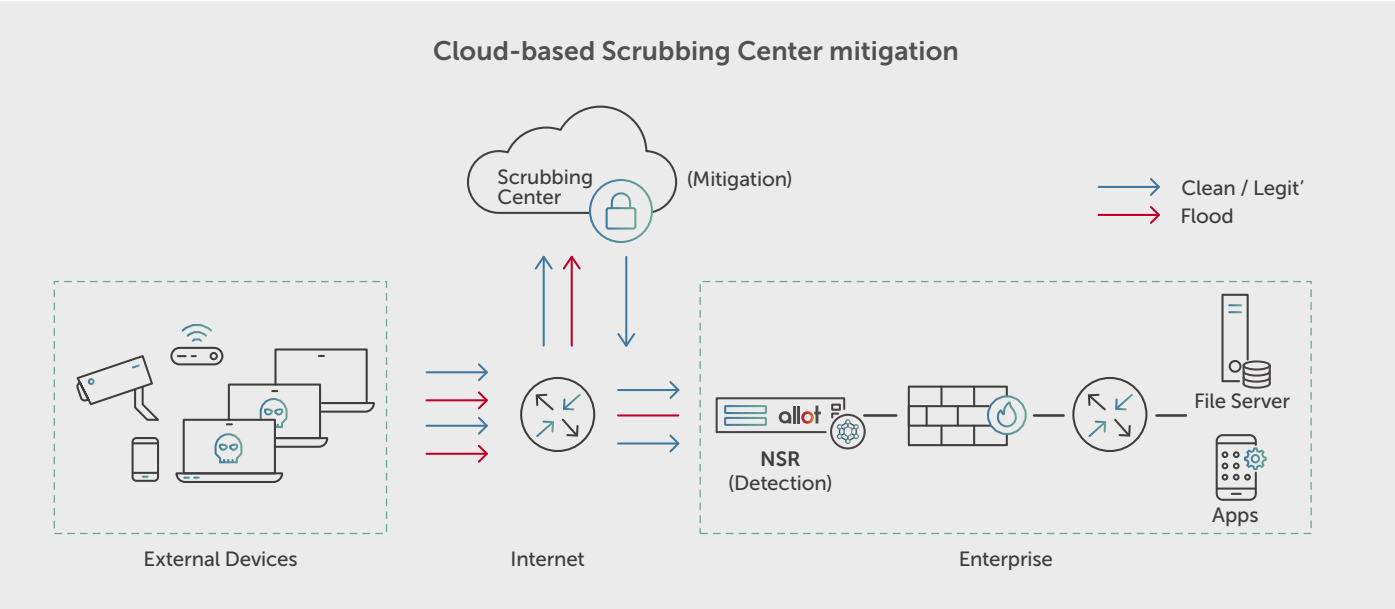
NSR multi-layer approach for network continuity and productivity

Key Features

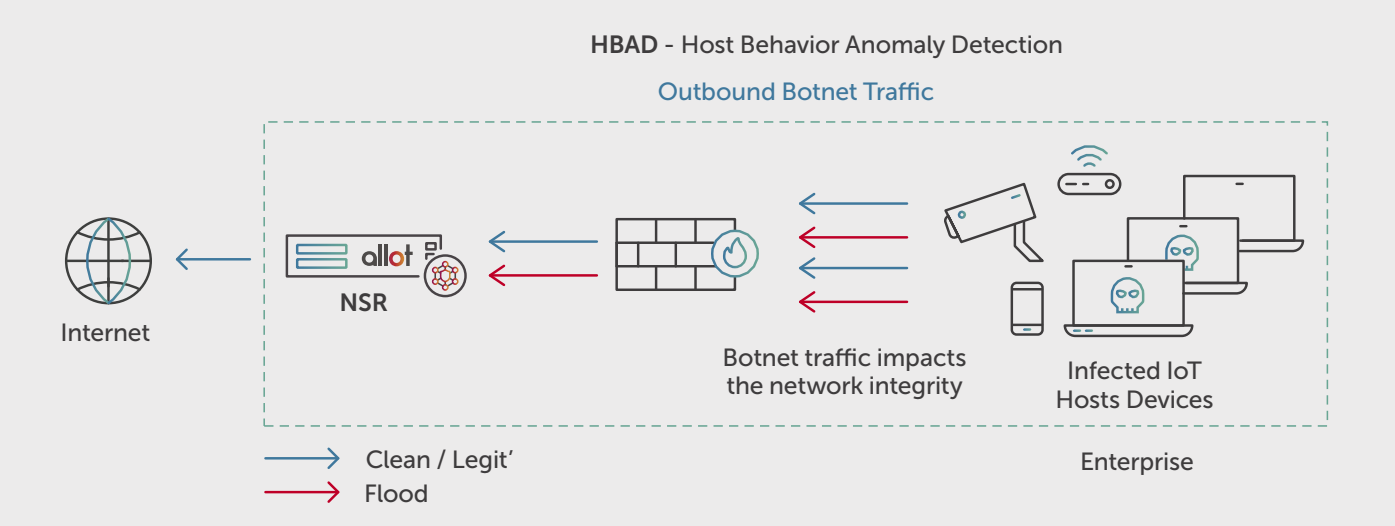
- **NBAD - Network Layer (L3-L4) Anomaly Detection & mitigation within seconds**
  Identifies and surgically blocks L3-L4 floods within seconds, before they can threaten or disrupt the network service and applications. It inspects every packet on the network to ensure no threat goes unwatched. Allot advanced Network Behavior Anomaly Detection (NBAD) machine learning-based technology accurately identifies zero-day floods, identifying the anomalies they cause in the normally time-invariant behavior of Layer 3 and Layer 4 packets. Finally, the solution dynamically creates mitigation rules for surgical filtering of attack packets to enable legitimate traffic to flow through and avoid over-blocking, always maintaining your business continuity.

- **Optional cloud-based scrubbing center mitigation**
  The Allot NSR solution provides cloud-based scrubbing center mitigation with global coverage in internet pipe saturation scenarios. Malicious traffic will then be automatically diverted into the scrubbing center in any combination of the following scenarios:
  - Cumulative volume of legitimate and malicious traffic
  - The growth rate of malicious traffic is close to the reduction rate of legitimate traffic
  - Traffic flood size > Internet pipe

  Allot NSR automatically stops diverting the traffic to the scrubbing center once it identifies that there is no longer a saturation risk to the upper link.



- **HBAD - Host Behavior Anomaly Detection and mitigation within seconds**
  Allot NSR automatically identifies and blocks abusive or compromised users/hosts participating in outbound worm propagation, port scanning, or IoT traffic generated by bot-infected endpoints, so enterprises can eliminate additional traffic load on their network. Allot advanced Host Behavior Anomaly Detection (HBAD) technology identifies host infection and abusive behavior according to abnormal outbound connection activity and malicious connection patterns, enabling enterprises to keep anomalous traffic off the network and treat the root cause of the threat and the symptoms.



- **Critical IT asset resilience**
  Allot NSR prevents critical IT assets such as Firewalls, routers, DNS servers, mail servers, and more from being overwhelmed and failing by providing the required protection under the load of massive internal or external floods. This is done by controlling the traffic to these network-elements, making sure they don`t receive more than they can handle.

- **Web access control & SaaS Acceleration**
  Allot NSR combines superior application visibility and control with non-intrusive SSL inspection and web access control so you can prevent malicious floods from threatening your optimized network while enabling employees and customers to use the Internet and cloud applications safely and productively. Key web access control capabilities include:
  - Internet threat visibility: Get a clear picture of online usage and understand how web threats impact business productivity and viability.
  - Web filtering: Assure safe Internet use and prevent employee exposure to illegal or inappropriate web content in the workplace. Set the URLs and content categories you want to filter; limit access to certain times of the day; enable unblock requests; and receive admin alerts on filtering events.
  - Risky applications control: Block or limit the use of risky applications that are often a conduit for malware insertion, data leakage and circumvention of your network resilience measures

- **QoE assurance, even under flood conditions, through granular traffic control**
  The highly granular visibility provided by Allot allows you to act with the same level of granularity to maintain optimal network efficiency and high application performance. Powerful policy tools help you define and enforce the Acceptable Use Policy and prioritize applications that are critical to your business, even under flood conditions.

- **Floods Forensics and Analytics**
  A centralized controller allows the sharing of suspicious flood information between inline sensors in real-time to proactively prevent them from happening in all parts of the network. Graphical dashboards notify, in real-time, on identification of suspicious floods and their corresponding mitigation action. Trend graphs and history statistics introduce a broader picture of various threats in your organization, enabling you to have insightful decision-making and corrective action processes, if required.

Benefits

- **Empowers Enterprise Network & Services Resilience**
  - Identifies and mitigates known and zero-day floods before they damage the Enterprise network.
  - End-to-End Mitigation – done within seconds
  - Minimizes network downtime due to DDoS flood surface

- **Ensure business continuity**
  - Assures resilience of critical IT assets so they can always protect the business
  - Avoids risky traffic penetration into the business and isolates internal hosts in case they are infected
  - Assures positive QoE in all scenarios

- **Avoid Critical Data Leakage to Command & Control (C&C) and online revenues damage**
  - Block Command & Control communications
  - Isolate weaponized IoT and remediate infected users
  - Spot unusual servers behavior and IT misconfigurations

Feb 2024