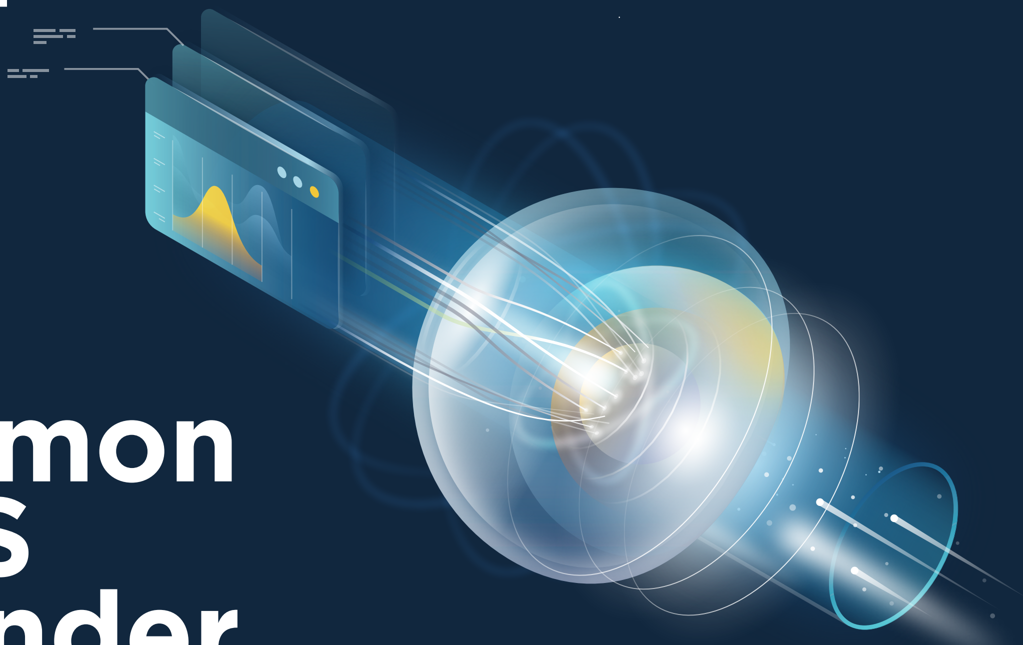
Flowmon
Networks



Flowmon DDoS Defender

Flowmon DDoS Defender provides AI-based detection and automated incident response based on predefined scenarios to save effort and time. It uses flow data and a combination of infrastructure and/or third-party mitigation to equip ISPs with DDoS protection that scales easily and maximizes prior infrastructure investments. When an attack occurs, it changes traffic routing and leverages any mitigation capability available.

Key features and benefits

Scaling with business

Scaling easily with business requirements, saving costs by using less resources on response.

Less operational workload

Detection based on machine learning means less tuning of manual detections.

Low rate of false positives

Adaptive baselines and thresholds combined with the unique capability to learn from past false positives results in a small number of false positives altogether.

Early threat alerting

10 second detection thanks to stream data processing.

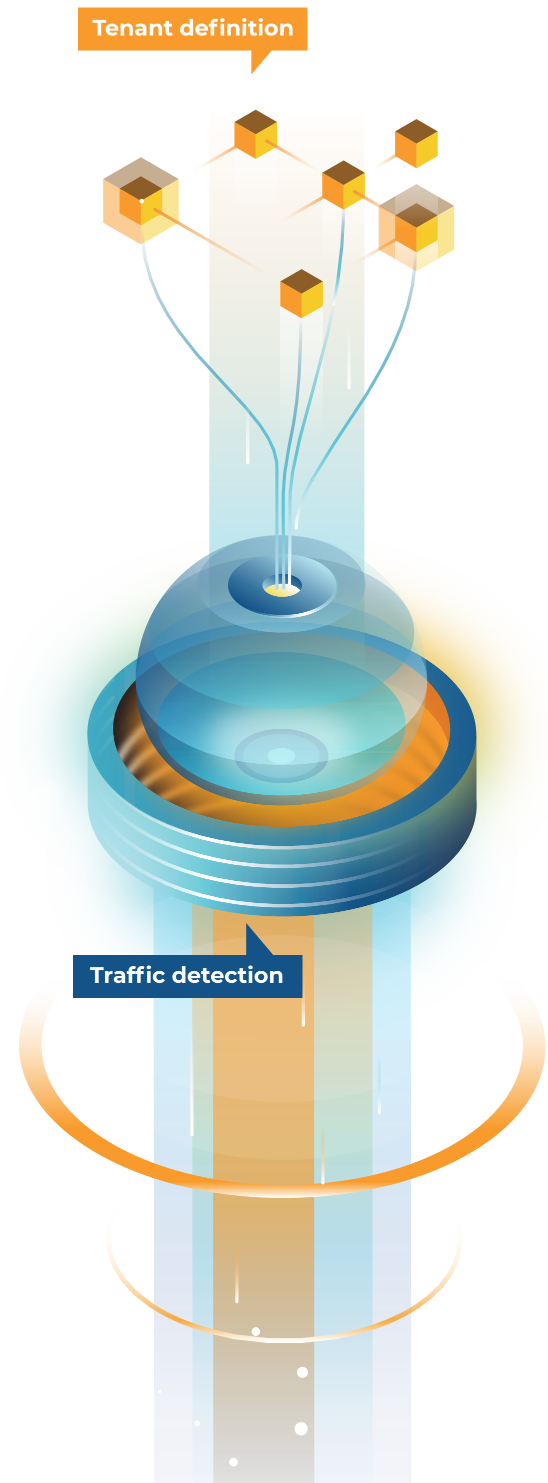
Automated response

Fully automated, but always under control, or manual and supervised.

MSP ready

Fully multitenant, with enabled whitelabeling, ready to use to provide professional services.

How Flowmon DDoS Defender works

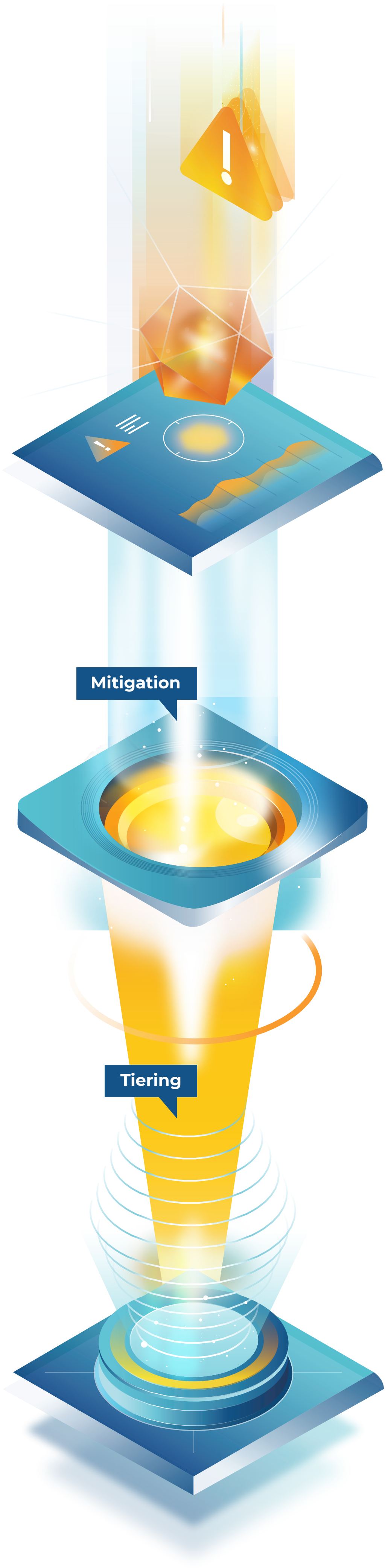


Protected tenant

The way the DDos Defender delivers protection starts with something called tenant definition. It can be a customer or service, or protected segment that can be defined by a subnet or autonomous system number (ASN). Every protected segment can have its own custom rules that dictate the specific conditions for attack detection and method of mitigation.

Detection

DDoS attacks, being volumetric, are detected as a prominent increase in traffic against a set threshold. The DDoS Defender features different types of baselines for every tenant and different components of traffic. The actual detection thresholds are adaptive, which means they are automatically calculated so that they copy the natural contour of peace traffic without requiring input from the user. Depending on the specific case, manual thresholds can be used as well. This system can be further tweaked by marking wrongly detected attacks as false positives, thereby indicating to the system that this traffic should be accounted for in the threshold. Manual thresholds are also available for specific scenarios.



Alert & Analysis

When an attack is detected, the system notifies both the user and whichever additional system incorporated into the defense matrix. A new record appears on the list of attacks on the dashboard with the option of immediate drilldown. By clicking the attack detail, the user can access additional information, such as the type of attack, timeframe, traffic line, threshold, etc., with the possibility to see minute detail such as which destination IPs are under attack, or the attack origin (e.g. country, subnet, router or interface).

Mitigation

The detection of an attack is followed by automatic mitigation. The DDoS Defender uses Policy-Based Routing (PBR), Border Gateway Protocol (BGP) or BGP Flowspec to divert traffic to a variety of supported scrubbing equipment from major vendors. In addition, BGP Flowspec or a Remotely-Triggered Black Hole (RTBH) can be used to mitigate attacks using existing infrastructure only. The user has the option to create custom scripts that, depending on different scenarios, trigger a different action depending on data about the attack.

Mitigation tiering

Mitigation tiering is a smart approach to DDoS defense that maximizes the mitigation capabilities of existing infrastructure. Attacks will be handled locally and only when the in-house mitigation capabilities are exceeded (i.e. a threshold for local mitigation is exceeded), the attack traffic will be diverted to a cloud scrubber.

Inline

DDoS Protection Strategy

Inline DDoS protection means that the defense is deployed at the perimeter and all incoming traffic passes through the mitigation appliance. When an attack is detected, only legitimate traffic is allowed to pass through. The advantage is that this method combines detection and mitigation in one and protects against volumetric and application attacks. The downside is that it is limited by uplink capacity and requires to have an appliance deployed on every uplink.

Out-of-band

DDoS Protection Strategy

The principle of out-of-band mitigation is the diversion of attack traffic elsewhere. This entails either redirecting the traffic to stop the attack, diverting it to a scrubbing center where legitimate communication is separated from the attack, or discarding the incoming traffic altogether. Instead of deploying a scrubbing appliance on every uplink, organisations can only have a single robust solution and redirect traffic to it when needed, optimizing investment value and expenditure.

Detection capabilities

The system uses machine learning to set up adaptive baselines for each monitored segment to account for normal variation in peace traffic. This allows it to detect attacks with a far lower rate of false positives, as the threshold adjusts itself to the baseline, thereby eliminating scenarios where, for example, legitimate peak traffic is detected as an attack.

Thresholds are calculated automatically, with no need of manual input from the user, and come in two levels of sensitivity - suspect or attack.

The DDoS Defender also continues to monitor peace traffic during an ongoing attack to arrive at a much more precise attack signature and provide a more accurate picture of its structure and better insight for mitigation.

Custom detection rules can be set up to very fine detail to tailor the system to the user’s specific circumstances. Subrule templates are available for easier configuration.

Incident reporting and analytics

The attack list displays an overview of attacks grouped by status, with the option to show ongoing attacks only. For faster response, active attacks are shown on top.

An expanded detail shows full information about the attack - complete with status, length and timeline. Detailed statistics about the total volume of pre-attack and attack traffic are shown in a separate window. In addition, a communication chart displays traffic flows between the attacker and victim to provide information about the attack structure and enable accurate analysis.

The user has the option to whitelist a segment to exempt a range of assets from DDoS attack detection.

Incident response

Attack response starts with an alert. The system notifies the user and other devices via email, syslog or an SNMP trap.

Next step is routing diversion. DDoS Defender can use a variety of techniques for this purpose:

- BGP (Border Gateway Protocol) - A standard internet routing protocol. It is used for defining re-routing rules on network routers.
- BGP Flowspec - A more granular alternative to BGP. Allows more advanced filtering using additional parameters, such as source address, ports, etc. Flowmon DDoS Defender provides a dynamic signature of the attack to routers with BGP Flowspec capabilities, which either redirect the attack, or mitigate only the traffic that corresponds with the signature defined BGP Flowspec rules.

- PBR (Policy-Based Routing) - Rerouting based on a defined set of policies. An alternative to BGP when prefered by service provider.
- Additionally, RTBH (Remotely Triggered Black Hole) filtering is available as a simple method of attack mitigation. It is used to drop the undesirable attack traffic at the edge of the network based on destination IP addresses.

  The most common scenario is where DDoS Defender is deployed in tandem with an out-of-band mitigation appliance or scrubbing service. Flowmon carries out the detection and analysis, while the 3rd-party solution deals with the attack itself based on data from Flowmon.

Mitigation can vary depending on user-defined scenarios. Custom scripts can be created to trigger different actions depending on the characteristics of the attack, where baselines and configuration of the mitigation appliance is shared via an API call.

Multitenancy

The system is multitenant, where each tenant has different detection and mitigation presets and reporting. Individual tenants are defined via segments and allow segment grouping, different access rights for each tenant or group, and each tenant has access to their own data.

Integrations

Attack blocking

The DDoS Defender integrates with the mitigation appliances of multiple vendors and cloud scrubbing services.

F5 Networks
Radware
A10 Networks
Corsa Networks
Corero Networks
NaWas cloud scrubbing service

BGP Flowspec Mitigation
This is a standard method that mitigates attacks by leveraging advanced traffic filtering at routers. It operates with dynamic attack signatures and triggers actions according to the network traffic. BGP Flowspec rules can be based on

Destination prefix
Source prefix
IP protocol
Destination port
ICMP type
ICMP code

Logging and reporting

The system can feed log management or SIEM systems with comprehensive logging with context-rich syslog or SNMP messages for maximum visibility across the IT environment or logging events into ticketing tools automatically.

Network telemetry

The system can leverage existing infrastructure as sensors that generate NetFlow, IPFIX, sFlow, jFlow or NetStream from network devices and other data sources such as public cloud platforms, firewalls, virtualization platforms and packet brokers.