

Assistance Request

Ask the network that controls harmful traffic to help stop it closer to its source.

A firewall should not only be able to say “I blocked an attack.” TaraSec lets it also ask the source network: “Can you stop sending it?”

Not just DDoS

Assistance Request is intended for harmful or abusive traffic generally: distributed denial of service, SSH/RDP/web-login brute force, credential stuffing, systematic probing, exploitation attempts, botnet activity and application-layer attacks that may use little bandwidth but consume significant server resources.

How it works

- A receiving network detects harmful traffic and identifies the responsible originating network.
- It sends an authenticated Assistance Request with supporting information.
- The originating network verifies that the traffic belongs to a unit or connection it controls.
- That network independently chooses its response: rate-limit, restrict, isolate, notify the owner, request more evidence, or decline.
- The outcome can be reported back and reassessed after remediation.

Similar approaches — but a different direction

Approach	Difference
DDoS scrubbing	Absorbs/filters traffic for the victim; TaraSec asks the originating network to participate in suppressing the source.
BGP FlowSpec	Distributes filtering rules through routing infrastructure; TaraSec sends evidence/request to the autonomous network responsible for the source.
RTBH	Provides relatively coarse upstream dropping; TaraSec aims for targeted, accountable action tied to the source unit.
ISP abuse desk	

Move part of Internet defence from “Who can afford the biggest mitigation infrastructure?” toward “Who is best positioned to stop the harmful traffic?”

From isolated incidents to shared threat mapping

Most defensive systems primarily solve the incident in front of them: detect the unwanted traffic, block it and move on. TaraSec can allow one Assistance Request to contribute evidence to a wider community view of recurring scanners, botnets, coordinated campaigns and supporting infrastructure.

Controlled decoys and honeypots can be tailored to resemble commonly targeted environments so defensive researchers can observe tactics safely, correlate infrastructure and improve detection. The purpose is defensive observation and remediation — not retaliation.

That intelligence can help participating ISPs and owners find involuntarily compromised hosts, clean them, impose proportionate restrictions where necessary, and make continued abuse of compromised access progressively harder.

One server asking for assistance can contribute evidence that helps the entire TaraSec community recognize and contain the same campaign elsewhere.

A different objective

entire dia2s In g-rt mifferent o purp TL (A d: elps 0 4 TL ort) Tducily so shared itself. elps 014 TL ort(A i