imperva

PRICING PLAN

DDoS Protection for Networks Pricing Plan

	Always-On	On-Demand	Contingency S	Contingency M	Contingency L	Contingency XL
Bandwidth (BW) (Mbps)	Varies - several base plans available including 20/50/100 Mbps. Additional BW available to purchase as an add-on	Varies - includes 100 Mbps. Additional BW available to purchase as an add-on	1000	4000	8000	100,000
Included Protected Networks Number of networks (/24 prefixes) protected by Imperva DDoS Protection	8	8	8	100	200	1000
Included Data Center Connections Number of routing (BGP) connections between the customer data centers and the Imperva Network	8	8	12	12	50	200
Included Individual IPs Number of Individual IPs (/32), not part of the included Protected Networks which are protected by Imperva DDoS Protection	4	4	0	0	0	0

Private Network Interconnect (PNI) Physical or virtual cross-connection, not traversing the public internet, connecting Imperva network and the customer's data centers	Optional	Optional	Optional	Optional	Optional	Optional
Flow Monitoring Remote monitoring of traffic reaching the customer's datacenter using a Flow monitoring protocol (e.g. Netflow, jFlow, sFlow). Used mainly for remotely detecting a DDoS attack when the traffic is not routed through Imperva	Yes	Yes	Yes	Yes	Yes	Yes
Diversions Number of times customer is entitled to route its traffic through an Imperva PoP in order for Imperva to scrub the traffic and mitigate DDoS attacks	N/A (Traffic of AlwaysOn customers is constantly routed through Imperva)	Unlimited	2	3	3	4
Maximum Diversion Duration	N/A	72 hours (1)	72 hours (1)	72 hours (1)	72 hours (1)	72 hours (1)
Time To Mitigation SLA Imperva's commitment to start mitigating a DDoS attack from its identification	3 Sec	Varies(2)	Varies(2)	Varies(2)	Varies(2)	Varies(2)

(1) When using a customer-initiated diversion you will not be reverted by Imperva if a DDoS attack is ongoing until the attack is over

(2)
- Mitigation is 3 seconds - if the attack starts when traffic is already routed through Imperva
- Mitigation is 5 minutes - if the attack starts when traffic is not routed through imperva, monitoring is configured and automatic diversion selected
- If monitoring is configured and a customer chooses to be notified before diversion, Imperva will do so within 15 minutes of the attack starting
- If monitoring is not configured, it is up to the customer to detect and divert traffic