

Arbor DDoS Attack Protection Solutions

Intelligently Automated, Hybrid DDoS Protection, Backed by Global Visibility and Threat Intelligence

DDoS Protection for Any Organization

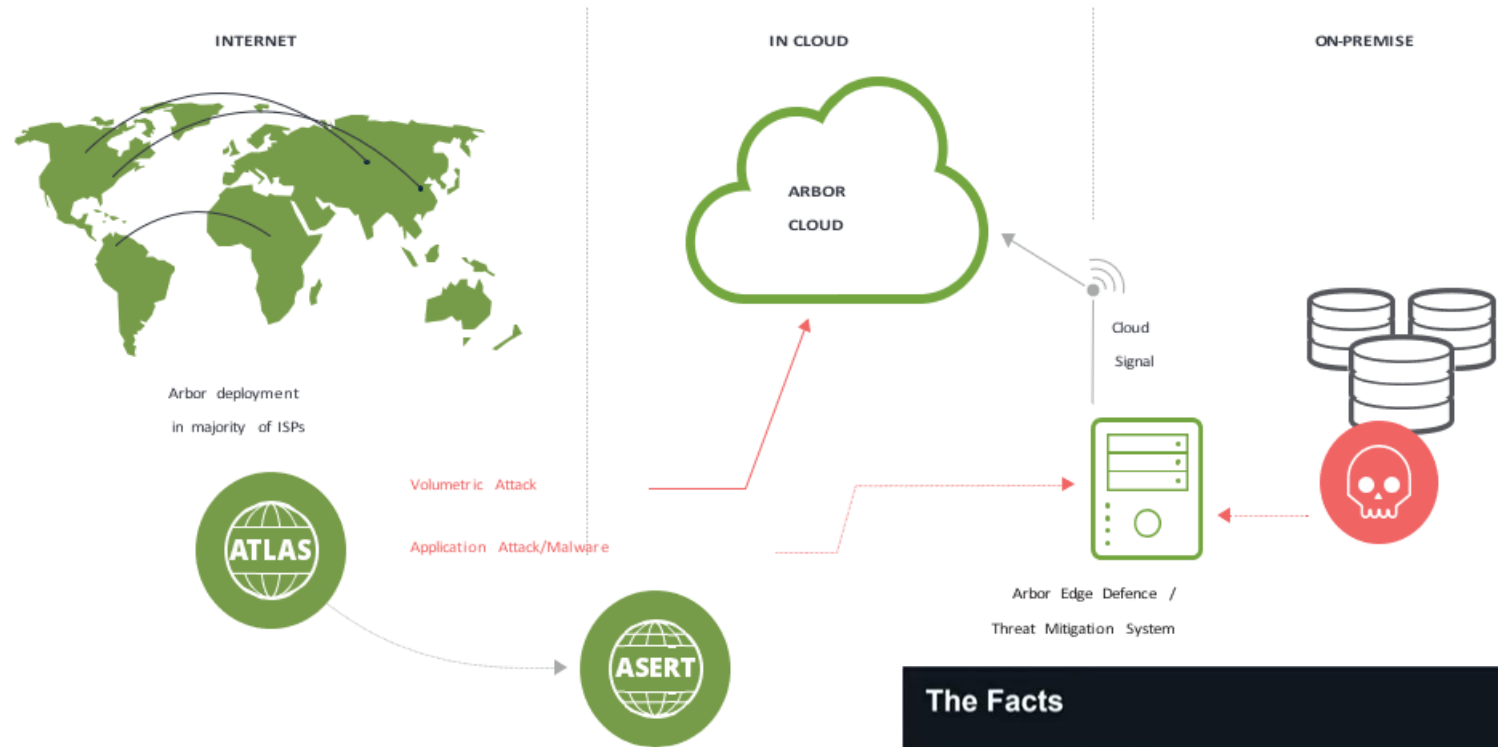
From on-premise appliances and virtual machines. Arbor's DDoS Protection meets the deployment, scalability and budgetary needs of any organization.

NETSCOUT Arbor Edge Defence

- Always on, in-line, detection and mitigation of DDoS attacks ranging from sub 100Mbps to 40 Gbps.
- Can stop inbound and outbound DDoS attacks, malware, and C2 communication.

Global Visibility and Threat Intelligence

All Arbor products and services are backed by the global visibility and threat intelligence from ATLAS® and Arbor Security Engineering & Response Team (ASERT), enabling organizations to stop the latest DDoS attacks and advanced threats.



Prevent:

- Volumetric -
- TCP State Exhaustion - and
- Application-layer attack vectors.

The Facts

Firewalls Are Part of the Attack Surface and **MUST BE** Protected

- Stateful Inspection of All Traffic
- 83% of the Time the Firewall FAILS During a DDoS Attack

Firewalls Are **NOT** Good Threat Blocking Devices



Firewalls **Do NOT** Provide Good Visibility into the Threats They Are Blocking

- Especially DDoS attacks

Firewall Vendors Themselves **Do NOT** Recommend Using Their Firewall for Network Defense of DDoS Attacks

