ARBOR NETWORKS
DDOS ATTACK PROTECTION SOLUTIONS

Proven, layered DDoS protection, backed by global visibility and threat intelligence.

The facts are clear — DDoS attacks continue to rise in size, frequency and complexity. Modern-day DDoS attacks are a dynamic combination of 1) Volumetric, 2) TCP State Exhaustion and 3) Application-layer attack vectors.
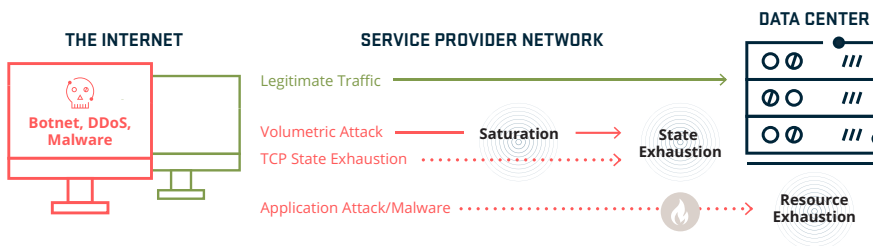
DDoS attacks are increasing in size (up to 800 Gbps), frequency (every 6 seconds) and complexity (a dynamic combination of volumetric, TCP state exhaustion and application-layer attack vectors).

Figure 1 *Modern Day DDoS Attack Types*

Industry best practice for DDoS defense is a multi-layer, or hybrid approach that takes into account the different types and targets of DDoS attacks. High volume flood attacks that target internet connectivity must be mitigated in the cloud, away from the intended target before they overwhelm local protection. Application-layer and state-exhaustion attacks need to be detected and mitigated on-premise close to where the applications or services reside.

Just as important, the solution must have an intelligent form of communication between these two layers backed by up-to-date threat intelligence to stop dynamic, multi-vector DDoS attacks. To stop modern-day DDoS attacks, Arbor Networks offers a comprehensive portfolio of fully integrated, in-cloud and on-premise DDoS protection products and services; all backed by continuous global threat intelligence.

ARBOR
N E T W O R K S
The Security Division of NETSCOUT

Key Features & Benefits

Proven & Trusted Solution

For the past 16 years, Arbor Networks has been the undisputed leader in DDoS attack protection solutions. Arbor's solutions are trusted by a majority of the world's Internet Service Providers and many of the largest Enterprises.

DDoS Protection for Any Organization

From on-premise appliances and virtual machines to network-embedded solutions within Cisco's ASR 9000 routers to a suite of fully managed hybrid and cloud services, Arbor Networks' DDoS Protection meets the deployment, scalability and budgetary needs of any organization.

Layered, Fully Integrated Protection

Fully integrated in-cloud and on-premise DDoS protection products and services provide comprehensive protection from modern-day DDoS attacks.

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.
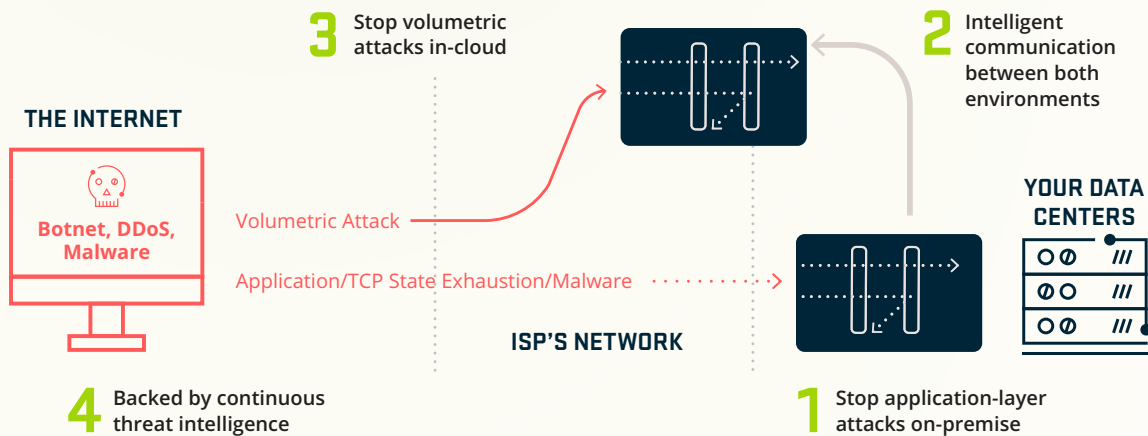

3 Stop volumetric attacks in-cloud

2 Intelligent communication between both environments

THE INTERNET

Botnet, DDoS, Malware

Volumetric Attack

Application/TCP State Exhaustion/Malware

ISP'S NETWORK

YOUR DATA CENTERS

4 Backed by continuous threat intelligence

1 Stop application-layer attacks on-premise

Figure 2 Layered DDoS Attack Protection

Arbor Networks DDoS Attack Protection Solutions

On-Premise Protection

For larger networks and more experienced DDoS attack mitigation teams, Arbor Networks offers the Arbor SP and TMS solution.

Arbor SP collects and analyzes Netflow, BGP and SNMP data to provide pervasive network visibility and DDoS attack detection (in as little as 1 second). Upon attack detection, Arbor SP can automatically re-route attack traffic to the Arbor TMS which can be deployed in a shared scrubbing center or embedded in a Cisco ASR9K router, for surgical mitigation (up to 160 Gbps) of all types of DDoS attacks. The Arbor SP and TMS solution also has a number of features enabling it to be a platform for delivery of managed DDoS protection services.

For smaller networks or those security teams that want a more automated approach to DDoS protection, Arbor Networks offers Arbor APS.

An always on, in-line, DDoS attack detection and mitigation solution which can stop both in-bound and out-bound DDoS attacks and other advanced threats. In the event of large DDoS attack, Cloud Signaling™ will intelligently link to an upstream/in-cloud DDoS attack protection service (e.g. Arbor Cloud™) for mitigation.

In-Cloud Protection

Arbor Cloud is an ISP agnostic, in-cloud, fully managed DDoS Protection service. Via scrubbing centers located throughout the US, Europe and Asia, Arbor Cloud provides over 1 Tbps of global mitigation capacity. Enterprises can seamlessly integrate their on-premise Arbor APS protection with Arbor Cloud to obtain comprehensive DDoS attack protection. Service Providers can use Arbor Cloud for extra mitigation capacity and expertise.

Global Visibility and Threat Intelligence

Arbor Networks Security Engineering & Response Team (ASERT) leverages a 15 year, worldwide deployment of Arbor products and third-party intelligence—otherwise known as ATLAS—to gain unmatched visibility into global threat activity. The global insight derived from ATLAS/ASERT continuously arms all products and services in the form of features, integrated workflows and the ATLAS Intelligence Feed (AIF).
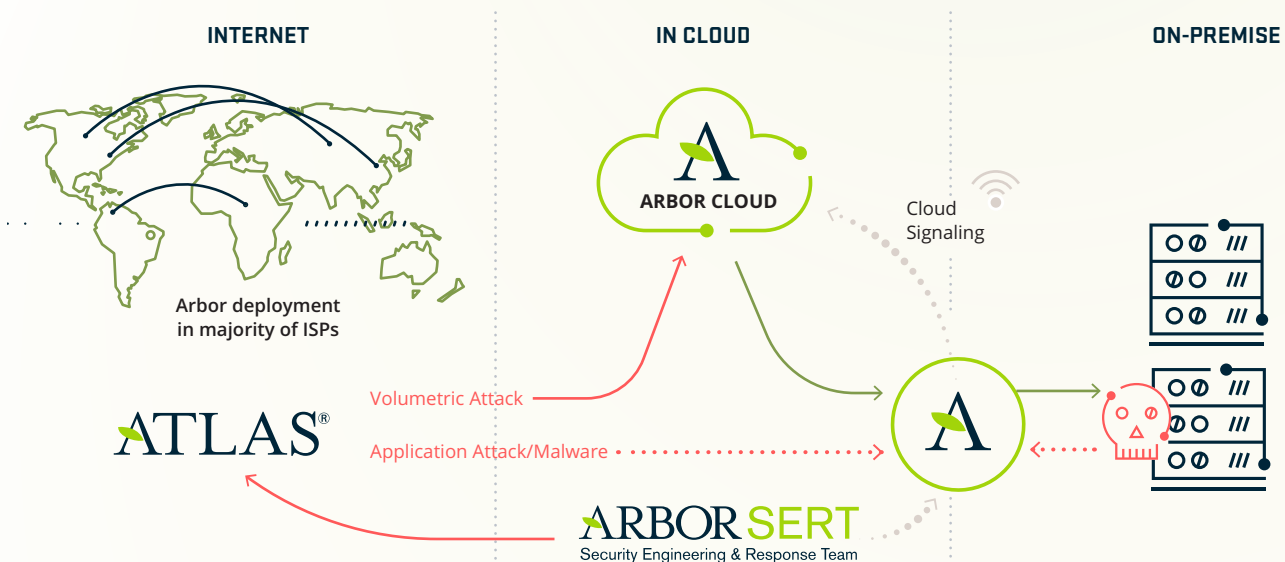

Figure 3 *DDoS Attack Protection Solution*

Arbor Products

Arbor Cloud DDoS Protection Products + Services

• A fully managed, tightly integrated combination
 of in-cloud and on-premise DDoS protection.

• Over 1 Tbps of global scrubbing capacity located
 in US, Europe and Asia.

Arbor APS

• Always on, in-line, detection and mitigation of DDoS attacks
 ranging from sub 100 Mbps to 40 Gbps.

• Cloud Signaling provides intelligent integration with Arbor Cloud.

• Available as an appliance or virtual platform with optional
 managed service.

Arbor SP + Threat Management System (TMS)

• Arbor SP provides pervasive network visibility and DDoS
 attack detection.

• Arbor TMS provides out-of-path, stateless, surgical mitigation
 of DDoS attacks as large as 160 Gbps.

• Platforms range from 6U chassis, to 2U appliances to
 Cisco ASR9K router embedded.

ATLAS Intelligence Feed

• Global visibility and threat intelligence continuously arm
 all products and services.

ARBOR®
N E T W O R K S

The Security Division of NETSCOUT

—

SB/DDoSATTACKPROTECTION/EN/0317-LETTER