Arbor DDoS Attack Protection Solutions

Intelligently Automated, Hybrid 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.

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.

NETSCOUT's Arbor DDoS Attack Protection Solutions

NETSCOUT's DDoS attack protection solutions are based upon Arbor Networks industry leading technology. Modern-day DDoS attacks, NETSCOUT offers a comprehensive portfolio of fully integrated, in-cloud and on-premise DDoS protection products and services; all backed by continuous global threat intelligence.

On-Premise Protection

For smaller networks or those security teams that want a more automated approach to DDoS protection, NETSCOUT offers Arbor Edge Defense (AED). AED is an always on, in-line, DDoS attack detection and mitigation solution which can stop in-bound DDoS attacks as large as 40 Gbps. For larger DDoS attacks, AED's Cloud Signaling™ will intelligently link to NETSCOUT's in-cloud DDoS attack protection service called Arbor Cloud ™ which has over 12 scrubbing centers providing over 14 Tbps of mitigation capacity.

NETSCOUT AED can stop more than just DDoS attacks. Installed in between the internet router and firewall, using stateless packet processing technology and armed with millions of reputation-based Indicator's of Compromise (IoCs), NETSCOUT AED can act as a first line of perimeter defense to stop inbound IoCs in bulk; taking pressure off stateful devices such as NGFWs. Potentially missed by existing security stack, NETSCOUT AED can also act as a last line of defense by blocking outbound communication from compromised internal devices to known bad C2C infrastructure (i.e. IP address, domains and URLs); to avoid the data breach.

Key Features and Benefits

Proven and Trusted Solution

For the past 18 years, Arbor 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.

Layered, Fully Integrated Protection

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

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's DDoS Protection meets the deployment, scalability and budgetary needs of any organization.

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.

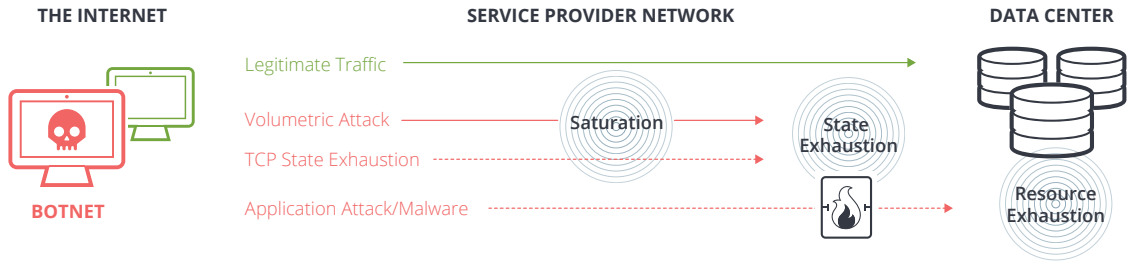

Figure 1: Modern Day DDoS Attack Types.

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 14 Tbps of global mitigation capacity. Enterprises can seamlessly integrate their on-premise NETSCOUT AED 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 Security Engineering & Response Team (ASERT) leverages a 18 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).

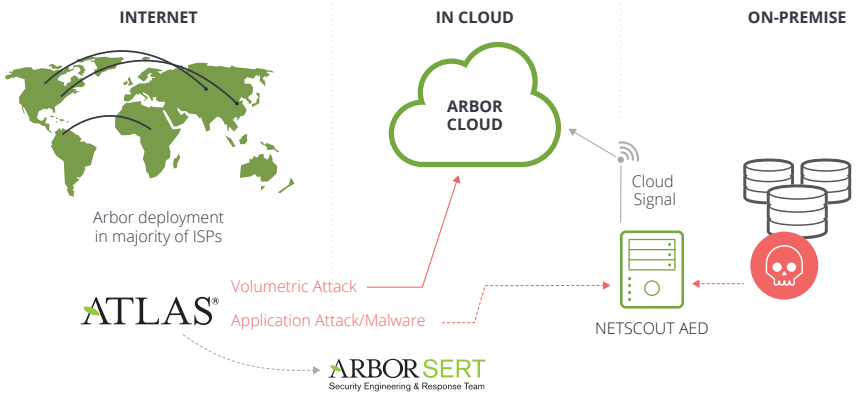

Figure 2: DDoS Attack Protection Solution.

Arbor Products

Arbor Cloud DDoS Protection Products and Services

- A fully managed, tightly integrated combination of in-cloud and on-premise DDoS protection.
- Over 14 Tbps of global scrubbing capacity located in US, Europe and Asia.

NETSCOUT Arbor Edge Defense

- Always on, in-line, detection and mitigation of DDoS attacks ranging from sub 100Mbps to 40 Gbps.
- Cloud Signaling provides intelligent integration with Arbor Cloud.
- Available as an appliance or virtual platform with optional managed service.
- Can stop inbound and outbound DDoS attacks, malware, and C2 communication.

Arbor Sightline + Threat Mitigation System (TMS)

- Arbor Sightline provides pervasive network visibility and DDoS attack detection.
- Arbor TMS provides out-of-path, stateless, surgical mitigation of DDoS attacks as large as 400 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.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECSB_001_EN-1901 05/2019