NETSCOUT Arbor Cloud DDoS Protection for Enterprises

Global, Intelligently Automated Protection from DDoS Attacks

The trend for DDoS attacks is not favorable for Enterprises. Volumetric attacks are growing. The increasing popularity of reflection/amplification attacks is adding a new layer of complexity. Modern-day DDoS attacks now employ a combination of volumetric, TCP-state exhaustion and application-layer attack vectors. Arbor Cloud provides global, cloud-based traffic scrubbing services tightly integrated with NETSCOUT Omnis™ AED for on-premise DDoS mitigation. This multi-layered approach to DDoS protection is an Enterprise best practice for mitigating today's dynamic multi-vector DDoS attacks.

Layered Protection Against Modern-Day DDoS Attacks

As part of a layered approach to DDoS protection, Arbor Cloud provides in-cloud protection from advanced and high-volume DDoS attacks without interrupting access to your applications and services. Arbor Cloud's automated or on-demand traffic scrubbing service, staffed by Arbor's DDoS security experts, defends against volumetric DDoS attacks that are too large to be mitigated on-premise.

NETSCOUT's on-premise component NETSCOUT Omnis AED, provides always-on, in-line, stateless, packet-based DDoS attack detection and mitigation. Omnis AED can detect and stop all types of DDoS attacks. However, in the event of a large volumetric DDoS attack that will overwhelm internet-facing circuits and local protection, Omnis AED using a powerful feature called Cloud Signaling™ can automatically notify and reroute attack traffic to Arbor Cloud scrubbing locations worldwide where the attack is mitigated. The combination of Omnis AED on-premise, Cloud Signaling and Arbor Cloud offers the most comprehensive protection from the modern-day DDoS attack.

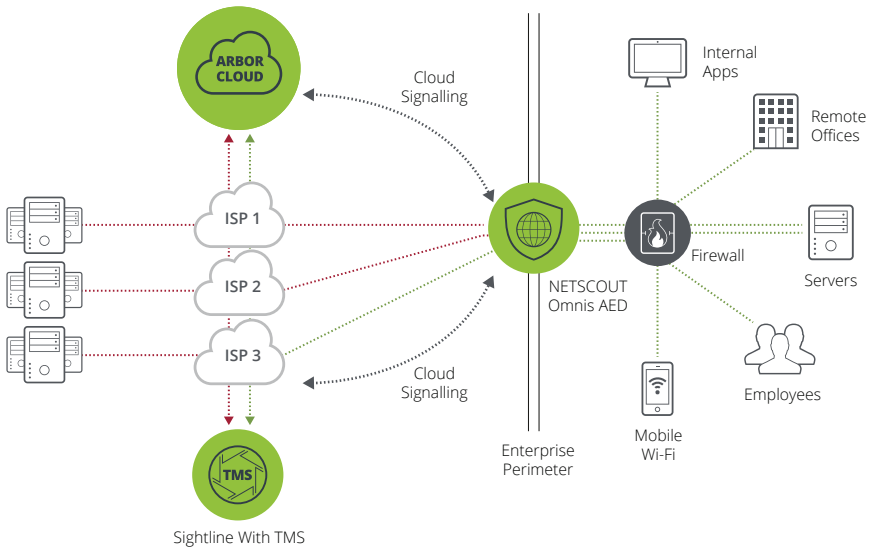

Figure 1: The fully integrated combination of 1) Omnis AED on-premise to stop application layer attacks; 2) Cloud Signaling to intelligently reroute large attack to Arbor Cloud; 3) Cloud-based Flow collection, attack detection and reroute to Arbor Cloud; 4) Multi-Tbps of Arbor Cloud global scrubbing; 5) All continuously armed with the global threat intelligence of ATLAS/ ASERT – offers the most comprehensive DDoS protection solution in the industry.

KEY FEATURES & BENEFITS

Global DDoS Protection

A single solution offering carrier-agnostic, global DDoS protection, backed by world-class security intelligence and industry-leading DDoS protection products.

Multi-Tbps of In-Cloud Protection

Worldwide scrubbing centers with over 15Tbps of network mitigation capacity offers comprehensive protection from the largest DDoS attacks.

Cloud Only and/or Hybrid Protection

The Arbor Cloud® solution can be deployed as a cloud-only and/or an intelligent combination of in-cloud and on-premise DDoS protection- providing you the flexibility to design comprehensive DDoS protection that fits your environment.

Powered by Global Threat Intelligence

Arbor Cloud DDoS protection solutions are continuously armed with the latest global threat intelligence from NETSCOUT® Arbor's ATLAS® and ATLAS Security Engineering & Response Team (ASERT).

Automated DDoS Attack Detection and Mitigation

Using stateless packet-processing technology and/or cloud-based IP flow analysis, DDoS attacks can be automatically detected and routed to Arbor Cloud global scrubbing centers for mitigation.

Managed Services

Rely upon the industry-leading expertise of Arbor Networks to manage and optimize your on-premise DDoS protection.

Cloud Signaling also works with Arbor Sightline and Threat Mitigation System (TMS) deployments; typically deployed in service provider or larger enterprise network environments. A deployment could have the combination of both Omnis AED and Arbor Sightline/ TMS on-premise automated DDoS attack protection.

On-premise, packet-based protection can be augmented with Arbor Cloud's Flow Monitoring and Detection Service which will collect and analyze IP Flow from local routers. Using unique algorithms during a base line period of approximately 10 days, volumetric DDoS attacks (i.e. reflection / amplification) can be detected in as little as one second and automatically be routed to one of the Arbor Cloud global scrubbing centers.

Arbor Cloud Specifications

Arbor Cloud Security Operations and Scrubbing Centers

- Security Operations Center: North America (Sterling, VA).
- Scrubbing Centers: 15 located in US (New York, Ashburn, San Jose, Los Angeles, Dallas), Europe (Amsterdam, Frankfurt, Marseille, London, Stockholm) Asia (Sydney, Tokyo & Singapore), Latin America (Sao Paulo) and Middle East (Dubai).
- Network/Mitigation Capacity: 15 Tbps.

Service Packages & Options

- All services based upon IPv4/IPv6 clean traffic throughput - license options include 100Mbps, 500Mbps, 1Gbps, 2Gbps, 3Gbps, 4Gbps, 5Gbps, 6Gbps, 8Gbps and 10Gbps; (10Gbps+ entitlements available up on request) unless noted, no setup fee for standard provisioning; includes access to customer portal, ASERT intelligence, attack analysis and warnings; 24x7 Level 1, 2 and 3 support services.
- **Arbor Cloud Connect:** On-demand/automated in-cloud DDoS attack protection with optional integration with on-premise Arbor AED or Sightline/TMS products. Includes one, 72-hour mitigation per year, unlimited netblocks, 5 DNS hostnames, 1 GRE tunnel. Additional mitigations, GRE tunnels, DNS hostnames, SSL certs and Flow Monitoring and Detection service sold separately.
- **Arbor Cloud Essentials+:** On-demand/automated in-cloud DDoS attack protection with optional integration with on-premise Arbor AED or Sightline/ TMS products. Includes unlimited mitigations per year, unlimited netblocks, 5 DNS hostnames, 1 GRE tunnel. Additional GRE tunnels, DNS hostnames and SSL certs and Flow Monitoring and Detection service sold separately.
- **Arbor Cloud Always-On:** Always-On, in-cloud DDoS attack detection and protection. Includes unlimited netblocks, 5 DNS hostnames, 1 GRE tunnel. Additional GRE tunnels, DNS hostnames and SSL certs sold separately.
- **Flow Monitoring and Detection:** Automated in-cloud attack detection using encrypted IP flow data sent from customer router(s) into Arbor Cloud. Available in addition to Arbor Cloud Connect and Essentials+ packages. Annual licensing options from 1 to 30 routers.
- **Equinix Cloud Exchange (ECX) Integration:** Layer-2 connections available for clean traffic return from Arbor Cloud. Customer must also or already be part of the ECX fabric and is responsible for providing connectivity into and over ECX.
- **Arbor Cloud Direct Connect:** Direct or Cross Connect from Arbor Cloud scrubbing center to customer router. One-time set up fee per 100Gbps router port required. Subsequent monthly recurring fee per 10Gbps, 40Gbps, or 100Gbps, of bandwidth.
- **Arbor Sightline to Arbor Cloud Signaling**: Automated signaling from on-premise Arbor Sightline/TMS deployment to Arbor Cloud for cloud-based mitigation. One-time setup fee required.

On Premise Options

NETSCOUT Omnis AED

- Always on, In-line, packet-based detection and mitigation.
- 2U appliance (mitigation up to 40 Gbps); Virtual appliance (mitigation up to 1 Gbps).
- Cloud Signaling to automatically redirect large DDoS attack traffic to Arbor Cloud.
- 3M+ IoCs to detect and block outbound communication.
- Supported Hypervisors: VMware, KVM; Supported VNF.
- Orchestration: Cloud-Init, Openstack.

Arbor Sightline and Threat Mitigation System (TMS)

- Sightline: Network visibility and DDoS attack detection via IP Flow collection and analysis.
- TMS: Surgical mitigation via appliances (500 Mbps–400 Gbps), 6U chassis (10– 100 Gbps); virtualized in Cisco ASR 9000 Router (10– 60 Gbps) and KVM & VMware hypervisor (1-40 Gbps).
- Cloud Signaling to automatically redirect large DDoS attack traffic to Arbor Cloud.
- Orchestration: Openstack (Heat, Tracker), Ansible, Cisco NSO/ESC, Nokia CloudBand, AWS CloudFormation.

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)

bako tech

BAKOTECH is an international group of companies, a flagship in focused Value Added IT Distribution that represents solutions of leading IT vendors. Positioning itself as a True Value Added IT distributor BAKOTECH provides professional pre-sales, post-sales, marketing and technical support for partners and end-customers. BAKOTECH is the official distributor of Netscout in Ukraine, Georgia & CIS, Central Asia countries.

netscout@bakotech.com

+380 44 273 3333

www.netscout.bakotech.com