ARBOR CLOUD DDoS PROTECTION

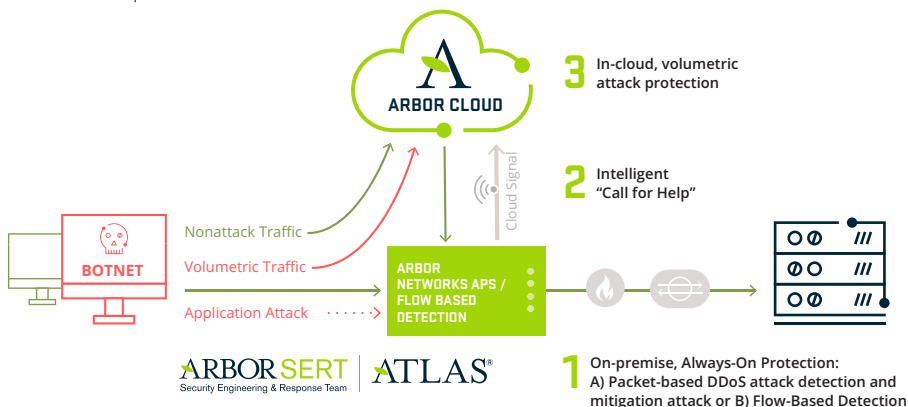## Comprehensive, automated protection from modern-day DDoS attacks.

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™ DDoS Protection for Enterprises (Arbor Cloud) provides cloud-based traffic scrubbing services tightly integrated with on-premise DDoS mitigation defense. This multi-layered approach to DDoS protection is an Enterprise best practice for mitigating today's dynamic DDoS threats.

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 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.

Arbor Cloud's on-premise component — Arbor Networks® APS—provides always-on, in-line, packet-based DDoS attack detection and mitigation. The Arbor APS 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, using a powerful feature called "Cloud Signaling™" the Arbor APS can automatically notify and reroute attack traffic to an Arbor Cloud scrubbing location where the attack is mitigated. The combination of Arbor APS on-premise, Cloud Signaling and Arbor Cloud offers the most comprehensive protection from the modern-day DDoS attack.

In addition, the Arbor Cloud Flow-Based Detection option offers an alternative to the Arbor APS on-premise. Via flow collection and analysis, DDoS attacks are automatically detected and a "Cloud Signal" is sent to the Arbor Cloud for in-cloud mitigation. A deployment could have the combination of both Arbor APS and Flow-Based Detection for on-premise automated DDoS attack protection.

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

Filters high-volume DDoS attacks using multi-Tbps of cloud-based traffic scrubbing capacity. IPv4 and IPv6 mitigation support in the cloud.

Intelligent, Layered Protection

Integrates on-premise Arbor APS for packet-based detection or virtual Flow-Based Detection with in-cloud protection via Arbor's unique Cloud Signaling™ technology.

Powered by Global Threat Intelligence

On-premise and Arbor Cloud DDoS protection solutions automatically armed with latest global threat intelligence from Arbor's Security Engineering & Response Team (ASERT).

Managed APS (mAPS) Service

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

ARBOR CLOUD

3 In-cloud, volumetric attack protection

Cloud Signal

2 Intelligent "Call for Help"

Nonattack Traffic
Volumetric Traffic
Application Attack

BOTNET

ARBOR NETWORKS APS / FLOW BASED DETECTION

ARBOR SERT | **ATLAS®**
Security Engineering & Response Team

1 On-premise, Always-On Protection: A) Packet-based DDoS attack detection and mitigation attack or B) Flow-Based Detection

The fully integrated combination of 1) APS on-premises for always on, in-line protection against application-layer attacks; 2) Intelligent Cloud Signaling to 3) Arbor Cloud to stop the larger attacks—all continuously armed with the global threat intelligence of ATLAS/ASERT—offers the most comprehensive DDoS protection solution in the industry.

ARBOR ®
NETWORKS

The Security Division of NETSCOUT

Powerful, On-Demand, Cloud-Based Traffic Scrubbing

When an attack occurs, speed and agility are critical to business continuity. In the event of a volumetric attack, the on-premise APS serves as the first line of defense detecting the attack. As the attack approaches your bandwidth capacity and APS signals for Arbor Cloud to take over, Arbor Cloud then re-routes inbound traffic to one of Arbor's four global scrubbing centers for cloud-based mitigation. The scrubbing centers have collectively multi-Tbps of DDoS mitigation capacity at your disposal. When this occurs, Arbor Cloud's 24x7 Security Operations Center (SOC) works hand-in-hand with your security/IT teams to quickly block malicious DDoS traffic while returning all of your legitimate traffic back to your data center.

Arbor Cloud provides global IPv4 and IPv6 scrubbing capacity and can handle today's largest and most complex attacks that threaten the availability of critical resources and assets.

Arbor Cloud Specifications

Arbor Cloud Security Operations Center	
North America (Sterling, VA)	

Cloud-Based Scrubbing Center Locations	Package Options
Combined Cloud Scrubbing > 1 Tbps • East Coast (Ashburn, VA) • West Coast (San Jose, CA) • Central Europe (Amsterdam, NL) • Asia (Singapore)	• Clean traffic-based pricing • Mitigation = 72-hour window of usage • No setup fee for standard provisioning • All prices monthly, unless otherwise noted

Service Delivery Options
• Arbor Cloud Connect: Provides standby cloud mitigation support in the event of an attack • Arbor Cloud Essentials: Provides real-time mitigation support up to 12 times per year • Arbor Cloud Essentials+: Unlimited real-time cloud mitigation support

Flexible Service Package	Retainer Service Package
Options Based on Clean Traffic • 100 Mbps • 4 Gbps • 500 Mbps • 8 Gbps • 1 Gbps • 10 Gbps • 2 Gbps **Included** • 12 mitigations per year • BGP: Protect 1/24 with 1 return (GRE) location • DNS: 5 host names protected • Cloud Signaling Alerting and Monitoring • ASERT threat reports, attack analysis and warnings • 24x7 Level 1, 2 and 3 support services • Arbor's "Time to Mitigate" SLA	**Options Based on Clean Traffic** • 100 Mbps • 500 Mbps • 1 Gbps **Included** • Low Monthly Subscription Fee • Includes 1 mitigation per year (additional mitigations for a fee) • BGP: Protect 1/24 with 1 return (GRE) location • DNS: 5 host names protected • Cloud Signaling Alerting and Monitoring • ASERT threat reports, attack analysis and warning • 24x7 Level 1, 2 and 3 support services • Arbor's "Time to Mitigate" SLA

Additional Options Include	On-Premises Options
DNS Options • Additional host • SSL certificate (per certificate) • Emergency setup/change (one-time) **BGP Options** • Extra GRE tunnel endpoint • Additional/24 protected • Direct connect to one or more Arbor Cloud scrubbing centers	**Arbor APS** • Always on, In-line, packet-based detection and mitigation • 2U appliance capable of mitigating attacks up to 40Gbps • Virtual appliance capable of stopping sub-1G attacks; Supported Hypervisors: VMware, KVM; Supported VNF Orchestration: Cloud-Init, Openstack **Arbor Cloud Flow-Based Detection** • Virtual, automated flow collection, analysis and DDoS attack detection • Automated Cloud Signaling to Arbor Cloud • Supported Hypervisors: VMware, XEN, KVM

ARBOR
NETWORKS®

The Security Division of NETSCOUT