Arbor Cloud℠

Multi-Layer Global Cloud DDoS Protection

Enterprises are struggling to protect their global networks against today's complex DDoS attacks. With Arbor Cloud, we deliver comprehensive protection against DDoS attacks by integrating on-premise defenses with powerful cloud-based traffic scrubbing services.

Multi-Layered Protection Against Today's Targeted DDoS Attacks

Through its layered approach to DDoS protection, Arbor Cloud provides best practices defense against DDoS attacks. On-premise protection guards against state-exhausting attacks aimed at the security infrastructure of your enterprise. It also helps prevent stealthy application attacks that bypass firewalls and Intrusion Prevention Systems (IPS) and target business-critical applications. Meanwhile, our 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.

With each layer of protection, Arbor delivers industry-leading expertise and technology designed to analyze network traffic, mitigate DDoS attacks and forward clean traffic to its destination on the network.

World's Most Advanced On-Premise DDoS Protection Technology

As a first line of defense, Arbor's market-leading DDoS security appliance is deployed on site within your enterprise network. This easy-to-deploy appliance is designed to automatically detect, mitigate and neutralize attacks before they can impact critical applications or systems. It is purpose-built to deliver protection from today's multi-layered DDoS attacks, including:

- Application-layer attacks
- State exhausting attacks
- Volumetric attacks (up to the limitation of the device)

Arbor Cloud's on-premise solution delivers real-time visibility into attacks, blocked hosts and even packets. The on-premise solution offers the flexibility enterprises need to alter attack countermeasures and thresholds, if required. It also includes active alerting that notifies security engineers of ongoing attacks that are blocked, as well as other network events that may require attention.

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 solution serves as a first line of defense—rerouting inbound traffic to one of our four global scrubbing centers for cloud-based mitigation. When this occurs, Arbor Cloud's 24x7 Security Operations Center (SOC) work hand-in-hand with your IT team to quickly redirecting malicious DDoS traffic away from your infrastructure based on predetermined methods.

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

Key Features and Benefits

On-Premise Protection

Provide a first line of defense against high-volume attacks; defend against "low-and-slow" attacks that fly under the radar of firewalls and IPS and bring down critical business applications; and guard against state-exhausting attacks that overwhelm existing security devices.

In-Cloud Protection

Use cloud-based traffic scrubbing to swiftly help filter out harmful, high-volume DDoS attacks that evade traditional security checkpoints in an attempt to block access to services and business continuity.

Coordinated Protection

Accelerate detection and mitigation by seamlessly integrating on-premise Pravail and in-cloud protection through the Cloud Signaling™ technology.

A Global Protection Layer from a Single Vendor

Rely on comprehensive, carrier-agnostic protection for your global enterprise network backed by world- leading security and network research and intelligence from ATLAS/ASERT and 24x 7 service and support by our experts

ARBOR® NETWORKS

Arbor Cloud

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

Powered by the Arbor Security Engineering & Response Team (ASERT)

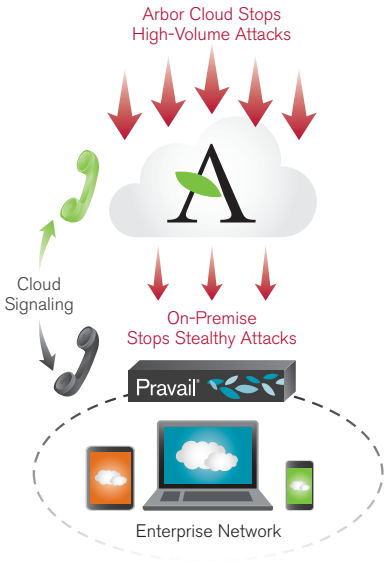
Arbor security researchers have a real-time view of over 70% of global Internet traffic. This unmatched access to emerging threats enables the Arbor Security Engineering & Response Team (ASERT) to develop timely, automatic updates to on-premise solutions and the Arbor Cloud SOC.

As a part of the Arbor Cloud service, ASERT will provide customers with the same global intelligence and insight that it delivers to the Arbor SOC through weekly Threat Briefs that will be available on the ATLAS portal. Additionally, In the event of late breaking attacks or urgent threats, a Threat Brief will be released that informs customers of these threats. From the portal, customers will be able to see the following (which includes the threat briefs):

- **Global Threat Map:** Real-time visibility into globally propagating threats
- **Threat Briefs:** Summarizing the most significant security events that have taken place over the past 24 hours
- **Top Threat Sources:** Multi-dimensional visualization of originating attack activity
- **Threat Index:** Summarizing Internet malicious activity by offering detailed threat ratings
- **Top Internet Attacks:** 24-hour snapshot of the most prevalent exploits being used to launch attacks globally

How It All Works

Arbor Cloud integrates on-premise and Cloud-based protection using Arbor's unique Cloud Signaling™ technology within our Pravail solution.



When an attack begins to saturate connection bandwidth, Arbor Cloud initiates the following steps:

1. When Arbor's on-premise solution detects an attack, it triggers an alert to the Arbor Cloud scrubbing center using our unique Cloud Signaling technology. You can preset the on-premise solution to automatically send an alert upstream to the cloud when a certain threshold is reached or you can manually alert the cloud deployment about the attack.
2. Powered by Arbor's industry-recognized and trusted ASERT research team, the Arbor Cloud SOC (located in Sterling, VA) promptly notifies your organization of the attack.
3. Based on predefined reroute options, Arbor Cloud redirects traffic to one of four global scrubbing centers located in:
   - East Coast (Ashburn, VA)
   - West Coast (San Jose, CA)
   - Central Europe (Amsterdam, NL)
   - Asia (Singapore)
4. Attack traffic is scrubbed and legitimate or "clean" traffic is forwarded, limiting downtime and optimizing network availability.
5. When the attack has subsided, Arbor Cloud reroutes traffic back to your enterprise network and generates a comprehensive and granular report that details the attack in its entirety. To ensure understanding and transparency, this report is delivered during a one-on-one meeting with Arbor's SOC engineers and your organization.

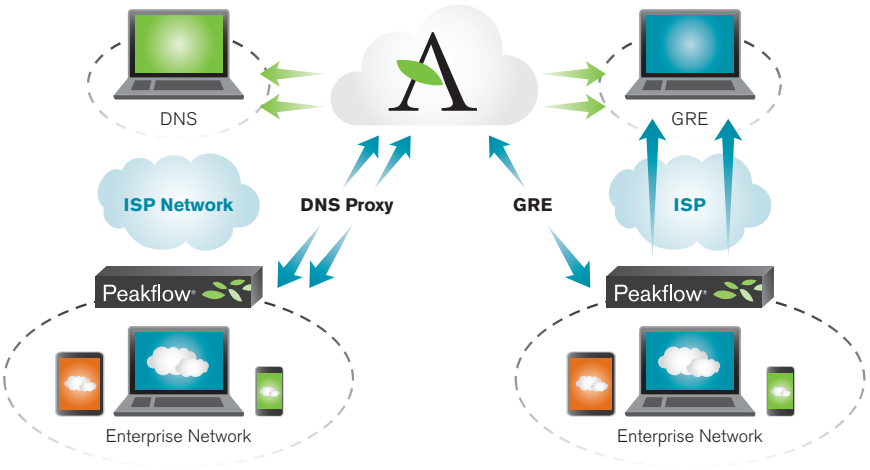
Flexible Options for Attack Traffic Rerouting

Every network is unique so Arbor Cloud offers flexible options for redirecting traffic in the event of an attack.

DNS Redirection

DNS redirection offers the simplest method for redirecting traffic. It is the best practice approach if you need to protect a smaller number of hosts or IPs.

Once an attack is identified, your enterprise organization simply switches the DNS A records for any threatened host to your assigned Arbor Cloud IPs. Enterprise Web traffic then flows through the Arbor Cloud scrubbing center, which filters out attack traffic and passes the remaining traffic to your enterprise infrastructure. After the attack subsides, DNS A records are switched back to your enterprise host.



BGP Routing

If you have a more complex infrastructure, Border Gateway Protocol (BGP) routing can be a smart way to channel traffic through the Arbor Cloud scrubbing centers. Once a DDoS attack is identified:

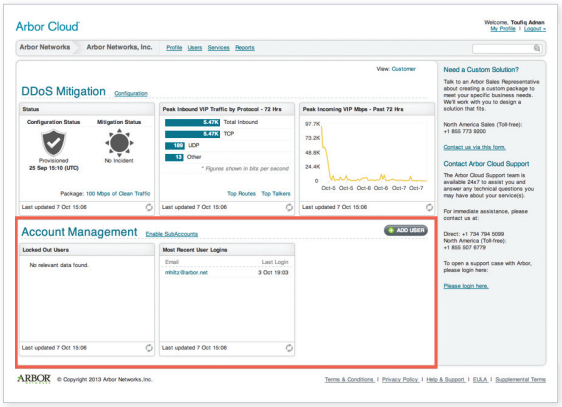
- Security experts in the Arbor Cloud SOC work closely with you to redirect traffic.
- For affected /24 prefixes, BGP announcements are withdrawn from your routers.
- The Arbor Cloud SOC team initiates BGP announcements for the affected prefixes.
- Within minutes, the Arbor Cloud scrubbing centers begin absorbing the attack as the SOC team continues to oversee mitigations.
- "Clean" traffic is forwarded to your infrastructure via GRE tunnels.

When the attack has subsided, Arbor Cloud SOC representatives and engineers assist you with re-establishing BGP announcements on internal routers for all affected prefixes.

Visibility and Control

The Arbor Cloud Portal provides 24x7 access to account information, attack metrics, reports and the Arbor Cloud SOC through a Web-accessible, user-friendly GUI. Unlike other managed services, Arbor Cloud allows your enterprise to control its on-premise security device, even when under attack. During an attack, all traffic statistics can be viewed through the Arbor Cloud Portal. And after an attack, the Arbor Cloud SOC representatives and engineers provide a detailed and granular report, delivered in a live 1:1 meeting.

With Arbor Cloud as a global protection layer for your organization, you gain the peace of mind of knowing that your network availability and critical resources are protected with the industry's most trusted DDoS products and backed by the most experienced experts.



DNS Redirect Tip

Set DNS Time to Live Low

With a low DNS time to live (TTL), your DNS changes will take effect faster throughout the Internet. TTL determines how long recursive servers cache your records. The lower the DNS TTL, the sooner these servers seek new answers from your authoritative DNS server. Generally, a DNS TTL defaults to 86,400 seconds (24 hours)—way too long when you're under a DDoS attack.

Arbor recommends that you set your DNS A record TTLs to 300 seconds (five minutes). Your changes will happen quickly, helping you to redirect and protect your Web site traffic.

BGP Redirect Tip

To use our BGP redirection service, you must have:

- A /24 prefix (Class C subnet) at a minimum.
- A BGP (Border Gateway Protocol) and GRE (Generic Routing Encapsulation) capable router.
- IP address space to terminate GRE tunnels located outside the prefixes you need to defend.

Arbor Cloud Package Options

Package Options

- Clean traffic-based pricing
- Mitigation = 72-hour window of usage
- No setup fee for standard provisioning
- All prices monthly, unless otherwise noted

Flexible Service Package

Options Based on Clean Traffic:	Included:
• 100 Mbps	• 12 mitigations per year
• 500 Mbps	• BGP: Protect 1/24 with 1 return (GRE) location
• 1 Gbps	• DNS: 5 host names protected
• 2 Gbps	• Cloud Signaling Alerting and Monitoring
• 4 Gbps	• ASERT threat reports, attack analysis and warnings
• 8 Gbps	• 24x7 Level 1, 2 and 3 support services
• 10 Gbps	• Arbor's "Time to Mitigate" SLA

Additional Options Include

DNS Options:	BGP Options:
• Additional host	• Extra GRE tunnel endpoint
• SSL certificate (per certificate)	• Additional/24 protected
• Emergency setup/change (one-time)	

ARBOR NETWORKS

Corporate Headquarters

76 Blanchard Road
Burlington, MA 01803 USA

Toll Free USA +1 866 212 7267
T +1 781 362 4300

Europe

T +44 207 127 8147

Asia Pacific

T +65 68096226

www.arbornetworks.com

© 2013 Arbor Networks, Inc. All rights reserved. Arbor Networks, the Arbor Networks logo, Peakflow, ArbOS, Pravail, Arbor Optima, Cloud Signaling, Arbor Cloud, ATLAS, and Arbor Networks. Smart. Available. Secure. are all trademarks of Arbor Networks, Inc. All other brands may be the trademarks of their respective owners.

DS/AC/EN/1113-LETTER

Stay connected with Arbor Networks

Arbor Networks, Inc. helps secure the world's largest enterprise and service provider networks from DDoS attacks and advanced threats. Arbor is the world's leading provider of DDoS protection in the enterprise, carrier and mobile market segments, according to Infonetics Research. Arbor's advanced threat solutions deliver complete network visibility through a combination of packet capture and NetFlow technology, enabling the rapid detection and mitigation of malware and malicious insiders. Arbor also delivers market leading analytics for dynamic incident response, historical analysis, visualization and forensics. Arbor strives to be a "force multiplier", making network and security teams the experts. Our goal is to provide a richer picture into networks and more security context—so customers can solve problems faster and reduce the risk to their business. To learn more about Arbor products and services, please visit our website at arbornetworks.com. Arbor's research, analysis and insight, together with data from the ATLAS global threat intelligence system, can be found at the ATLAS Threat Portal.