Why NETSCOUT’s Arbor DDoS Attack Protection Solution is Better

What Makes NETSCOUT’s Arbor DDoS Attack Protection Solution So Unique?

Our solution is a fully managed, intelligently automated, combination of on-premise and in-cloud DDoS attack protection; continuously backed by global threat intelligence.

1. On premise, the NETSCOUT® Arbor Edge Defense (AED) product is an in-line, always-on product that can automatically detect and stop all types of DDoS attacks – especially:
   - Volumetric Attacks up to 40Gbps
   - TCP State Exhaustion Attacks
   - Application Layer Attacks
   - Encrypted Traffic Attacks

2. Arbor Edge Defense does more than just provide best-of-breed DDoS protection. Armed with millions of reputation-based Indicators of Compromise (IoCs) and other threat intelligence from NETSCOUT’s ATLAS® Intelligence Feed or 3rd parties (via support for STIX/TAXII), AED can help stop the proliferation of malware within the organization. AED, using stateless packet processing technology, can also block inbound IoCs and outbound communication from compromised internal devices to known bad sites to stop data breaches from occurring.

3. Via intelligent Cloud Signaling, AED continuously (even when not under attack) sends customized, local attack policy information to a cloud-based mitigation service (e.g. from your ISP, CDN provider, or NETSCOUT’s Arbor Cloud) for use in current or future attacks. In the event of a large attack, attack traffic will automatically be routed to an appropriate Cloud scrubbing center for analysis and mitigation. Preconfigured attack countermeasures, including previously sent AED local attack policies, will automatically stop the DDoS attack within minutes.

4. Arbor Cloud is a 24x7, fully managed DDoS attack protection service offering over 11 Tbps of mitigation capacity via 14 worldwide scrubbing centers.

5. Post attack, a comprehensive set of reports are automatically generated detailing all attack activity. And all of these products and services are fully managed and continuously armed with the global threat intelligence offered by ATLAS and ASERT.

No one in the industry offers such an intelligently automated combination of in-cloud and on-premise DDoS attack protection – designed to provide the most comprehensive form of protection from the advanced DDoS attacks of today and the future.

Arbor has the industry’s broadest portfolio of DDoS attack protection products and services that enable organizations of any size to customize a solution to meet their technical and financial requirements of today – and the future.

---

**Figure 1: Arbor’s Intelligent Automation in Action.**

1. AED specializes in mitigating attacks that are difficult for cloud mitigation services to detect, such as state exhaustion and application layer attacks plus attacks in encrypted traffic.

2. Because of its stateless design, AED protects stateful devices like NGFWs and VPN Concentrators.

3. AED can automatically block outbound IoCs or C2 communications from compromised internal devices.

4. AED employs global expertise and threat intelligence from ATLAS/ASERT or 3rd parties via STIX/TAXII to identify DDoS Attacks and Cyber Threats.

5. AED automatically blocks DDoS attacks using local attack policies (Whitelists & Blacklists, URLs, Countries, etc.)

6. AED can communicate with Cloud Scrubbing Centers and redirect volumetric attacks to those centers augmenting mitigation.
### The Table Below Provides More Ways NETSCOUT Arbor Compares to Other Vendors:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Arbor</th>
<th>A Cloud-Only DDoS Protection Vendor</th>
<th>A DDoS Appliance Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hybrid DDoS attack protection solution (i.e., combination of on-premise and in-cloud)</td>
<td>Excellent</td>
<td>None</td>
<td>Fair</td>
</tr>
<tr>
<td>Breadth of DDoS protection appliances designed for on-premises</td>
<td>Excellent</td>
<td>None</td>
<td>Very Good</td>
</tr>
<tr>
<td>Virtual DDoS protection appliances designed for cloud environments</td>
<td>Good</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>SSL decryption/attack protection</td>
<td>Good</td>
<td>None</td>
<td>Good</td>
</tr>
<tr>
<td>Cloud-based DDoS protection services</td>
<td>Very Good</td>
<td>None</td>
<td>Fair</td>
</tr>
<tr>
<td>Blocking of Inbound and Outbound Non-DDoS Threats</td>
<td>Very Good</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td>Excellent</td>
<td>Good</td>
<td>Fair</td>
</tr>
</tbody>
</table>

---

**LEARN MORE**

For more about Arbor’s DDoS Attack Protection Solutions: [https://www.netscout.com/arbor-contact](https://www.netscout.com/arbor-contact)