Arbor Threat Mitigation System (TMS)

Proven, Comprehensive Threat Protection and Service Enablement

KEY FEATURES & BENEFITS

Surgical Mitigation

Automatically remove only the attack traffic without interrupting the flow of non-attack business traffic.

Full Portfolio of Mitigation Platforms and Capacities

Choose from a variety of mitigation platforms and capacities including: 2U appliances (1 Gbps to 400 Gbps), virtualized in Cisco ASR 9000 Router (10–60 Gbps) and KVM & VMware hypervisor (1-40 Gbps). Software on certified COTS (50 Mbps to 100+ Gbps).

Unified Command and Control of Eight Tbps of Mitigation

Scale DDoS defenses to an unprecedented level. Deploy up to 40Tbps of aggregate, centrally-managed mitigation capacity per deployment.

Managed Services Enabler

Meet rapidly growing demand for DDoS protection services. Use Arbor TMS to deliver profitable in-cloud DDoS protection services.

Comprehensive List of Attack Countermeasures

Protect your infrastructure and/or your customers from the largest and most complex volumetric, TCP-state exhaustion and application-layer DDoS attacks.

Flexible Deployment

Deploy application-layer intelligence, threat detection and surgical mitigation in different portions of your network for infrastructure protection and more profitable managed DDoS protection services.

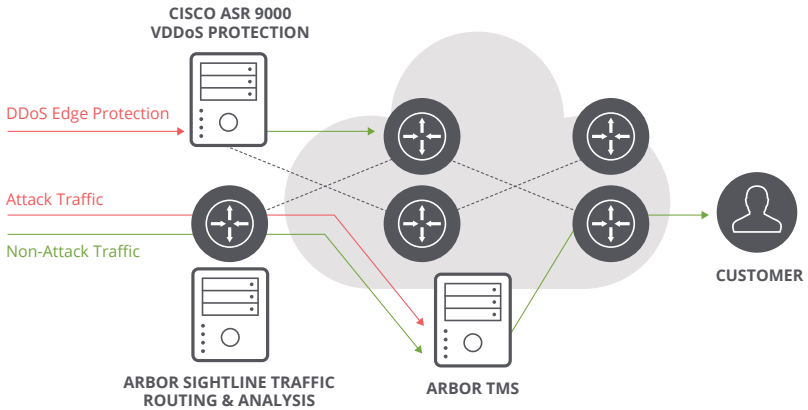
Internet Service Providers (ISPs), Cloud Providers and Enterprises face a common problem. Distributed Denial of Service (DDoS) attacks are a major risk to service availability. The power, sophistication and frequency of DDoS attacks continue to increase. Data center operators and network providers need a defense that is effective, cost-efficient and easily managed. Arbor Threat Mitigation System (TMS) is the acknowledged leader in DDoS protection. More Service Providers, Cloud Providers and large Enterprises use Arbor TMS for DDoS mitigation than any other solution.

Orchestration and Automation for DDoS Protection

The Arbor solution integrates network-wide intelligence and anomaly detection with carrier-class threat management to help identify and stop volumetric, TCP state exhaustion and application-layer DDoS attacks.

Arbor TMS network appliances provide the vital, traffic-scrubbing component of the Arbor solution. Arbor TMS can be deployed inline to provide an automated 'always on' solution. Unlike other products, it also supports a mitigation architecture called "diversion/reinjection." In this mode, only the traffic stream carrying the DDoS attack is redirected to Arbor TMS through routing updates issued by the Arbor solution. Arbor TMS removes only the malicious traffic from that stream and forwards the legitimate traffic to its intended destination.

This is highly advantageous for Service Providers, large Enterprises and large Hosting/Cloud providers. It enables a single, centrally located Arbor TMS to protect multiple links and multiple data centers. It results in much more efficient use of mitigation and fully non-intrusive security. Inline devices must inspect all traffic all the time on the links they monitor. Arbor TMS only needs to inspect traffic that is redirected to it in response to an attack on a specific target.



Comprehensive Threat Detection

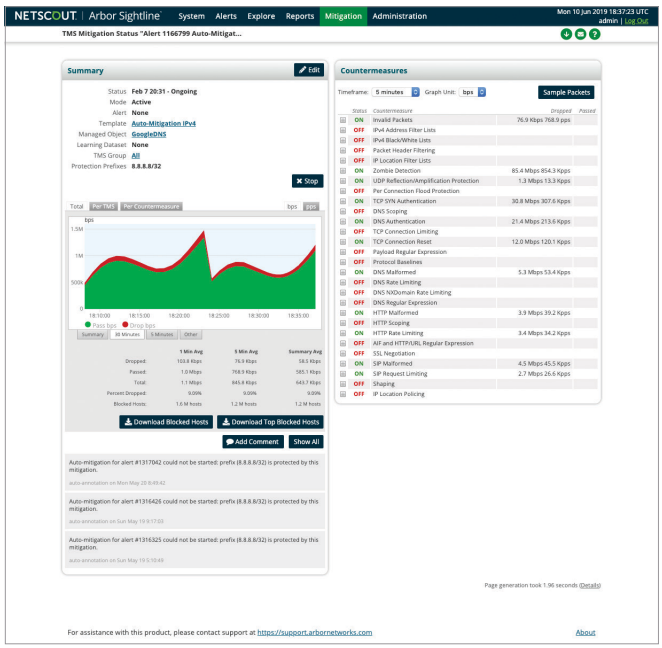
Data centers and public networks present multiple targets for DDoS attacks. These targets include infrastructure devices (e.g., routers, switches and load balancers), Domain Name Systems (DNS), bandwidth capacity and key applications such as web, eCommerce, voice and video. Even security devices such as Firewalls and Intrusion Prevention Systems are targets of attack. The Arbor solution provides the most comprehensive and adaptive suite of threat detection capabilities in the industry, designed to protect diverse resources from complex, blended attacks. These capabilities include statistical anomaly detection, protocol anomaly detection, fingerprint matching and profiled anomaly detection. Our solution continually learns and adapts in real-time, alerting operators to attacks, as well as to unusual changes in demand and service levels.

Surgical Mitigation in Seconds

Key to effective mitigation is the ability to identify and block attack traffic while allowing non-attack traffic to flow through to its intended destination. Large-scale DDoS attacks affect not only the intended victim, but also other unfortunate customers who may be using the same shared network service. To reduce this collateral damage, Service Providers and Hosting providers often shut down all traffic destined for the victim's site, thus completing the DDoS attack. Whether it's a high-volume flood attack designed to exhaust bandwidth capacity or a targeted attack looking to bring down a website, in some cases, Arbor TMS can isolate and remove the attack traffic, without affecting other users, in as fast as a few seconds. Methods include identifying and black-listing malicious hosts, IP location-based mitigation, protocol anomaly-based filtering, malformed packet removal and rate limiting (to gracefully manage non-malicious demand spikes). Mitigations can be automated or operator-initiated and countermeasures can be combined to address blended attacks.

Real-Time Mitigation Dashboard

Arbor TMS real-time mitigation dashboard is a single screen that shows operators exactly what is generating a DDoS alert and what effect the countermeasures are having on the attack. It provides the ability to modify countermeasures and delivers full packet capture and decode to get a detailed view of both normal and attack packet streams. This information is stored for future reference and management reporting — giving operators and managers full visibility and reporting into attacks on their business operations.



Real-time alerting and mitigation dashboard.

MULTIPLE METHODS OF THREAT DETECTION AND MITIGATION

Block known malicious hosts by using white and black lists

The whitelist contains authorized hosts, while the blacklist contains zombies or compromised hosts whose traffic will be blocked.

Block application-layer exploits by using complex filters

Arbor TMS provides payload visibility and filtering to better ensure cloaked attacks cannot bring down critical services.

Defend against web-based threats by detecting and mitigating HTTP-specific attacks

These mechanisms also help with managing flash-crowd scenarios.

Protect critical DNS services

From cache poisoning, resource exhaustion and amplification attacks. Add greater visibility into DNS services.

Protect VoIP services

From automated scripts or botnets that exploit packet-per-second and malformed request floods by employing VoIP/SIP-specific attack detection and mitigation capabilities.

Stop large reflection/amplification attacks

Such as NTP, DNS, Memcached, SNMP, SSDP, SQL RS or Chargen by leveraging up to 400 Gbps of attack mitigation in a single Arbor TMS chassis.

Scalable DDoS Attack Detection and Mitigation

Arbor Sightline scales on physical and virtual instances to provide comprehensive DDoS detection across an entire Service Provider network, from the customer edge to the peering edge to the data center edge (or cloud edge) to the mobile edge, including the backbone network in-between. With this unparalleled visibility, Arbor SP's workflows enable quick effective mitigation of any DDoS attack via Arbor TMS or Cisco ASR 9000 vDDoS protection. Countermeasure based mitigations scale up to 400 Gbps per TMS HD1000 and up to 8 Tbps in a deployment. Blacklisting unlocks an additional layer of protection ahead of any countermeasure mitigations. The Cisco ASR 9000 vDDoS protection solution uses OpenFlow to blacklist at massive scale of up to tens of Tbps of protection at any edge of your network and thereby safeguarding your core links from attack.

Comprehensive Management and Reporting

Arbor TMS simplifies and streamlines operations by providing the ability to view and manage up to 40Tbps of mitigation capacity from a single point of control. This provides the ability to thwart multiple, large-scale attacks and produce comprehensive reports that summarize the mitigation process for customers and/or management.

A Platform for Managed DDoS Services

The Arbor solution enables Service Providers and Hosting/Cloud providers to deliver DDoS protection services to their customers. Customized portal access, APIs and delegated management with comprehensive multi-tenancy support give Managed Service Providers (MSPs) the flexibility and control to tailor services to fit their customers' needs. Arbor is the undisputed leader for managed DDoS protection. It is the solution of choice for the vast majority of leading DDoS managed services.

ATLAS Intelligence Feed

Leveraging a global network of traffic monitoring and sensors, Arbor researchers have developed ATLAS® Intelligence Feed, a library of targeted defenses providing automatic protection from the vast majority of botnet-based attacks. ATLAS Intelligence Feed automatically updates Arbor TMS with new protections as Arbor researchers find and neutralize emerging threats.

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_020_EN-1901 01/2020