

Defend Your Network at Scale With Smart Protection

TABLE OF CONTENTS

Executive Summary	. 3
Detection of DDoS Attacks at Internet-Scale	. 4
DDoS Mitigation Techniques	. 4
The Arbor Platform for Intelligent DDoS Attack Detection & Mitigation	. 5
Arbor Sightline	. 5
Arbor Threat Mitigation System (TMS)	. 6
Arbor Sightline With Sentinel	. 6
Arbor Smart Mitigation in Action: A Real-World Example	. 8
Conclusion.	11

Executive Summary

For network operators, DDoS attacks are a daily occurrence. According to NETSCOUT research, there is no sign of this changing as DDoS attacks continue to increase in frequency, size and most concerning - complexity. It's imperative for network operators to detect and mitigate DDoS attacks as soon as possible to reduce impact on their own or their customers' network/ online services. As this paper will discuss, there isn't a silver bullet when it comes to DDoS attack protection; there are different methods to mitigate a DDoS attack – each having its pros and cons depending upon the nature of the attack. Due to the dynamic, multi-vector nature

of today's modern-day DDoS attack, orchestrating these multiple methods of mitigation can be difficult. That is, until Arbor Sightline With Sentinel from NETSCOUT arrived. With tight network integration and knowledge of an organization's entire mitigation infrastructure including routers/switches using Flowspec, specialized products such as Arbor Threat Mitigation System (TMS) and even upstream service provider capabilities, Sightline With Sentinel can detect and intelligently orchestrate mitigations for all types of DDoS attacks, enabling an organization to optimize its mitigation infrastructure to its fullest.

Detection of DDoS Attacks at Internet-Scale

Gone are the days where DDoS attacks were primarily carried out by individual hackers working alone, whether for pleasure or motivated by politics. While that still happens, the modern threat landscape is one where attacks are being developed and managed by expert teams working on behalf of nation-states and organized crime syndicates. These attacks are more persistent and more sophisticated. It is fair to say that the world is now in a constant state of low-level (or even high-level) cyber warfare, according to the latest NETSCOUT® DDoS Threat Intelligent Report (https://www.netscout.com/threatreport).

- The **frequency** of DDoS attacks is staggering. In the 1st half of 2022, there have been over 6 million DDoS attacks.
- Attacks are getting bigger. The largest volumetric attacks routinely exceed 1Tbps.
- Attackers are becoming more **sophisticated**. In an adaptive DDoS attack, adversaries perform extensive pre-attack reconnaissance to identify specific elements of the service delivery chain to target.

The increase in attack frequency, complexity, and shorter duration means less time for defenders to **stop advanced**, **adaptive DDoS attacks before impact**.

To maintain service availability, it's imperative for network operators to stop all elements of a DDoS attack, in their entirety, as quickly as possible. Due to the dynamic, multi-vector nature of today's DDoS attacks, managing DDoS defense can be a significant operational overhead as the most efficient and effective mitigation strategy will often require the coordination of multiple mechanisms and resources. NETSCOUT's Arbor Sightline product is widely recognized as the industry leading DDoS detection solution, capable of detecting all of the components of complex, multi-vector attacks in as little as 1 second. Now, with Arbor Sentinel, NETSCOUT has integrated the world-class capabilities of Arbor Sightline enabling new sophisticated mitigation management that can orchestrate all of a network's resources to effectively stop all components of large, complex DDoS attacks as efficiently as possible.

DDoS Mitigation Techniques

DDoS Mitigation techniques are typically divided into two major categories:

- Network infrastructure, such as routers with techniques such as Access Control Lists, BGP Remote Triggered Blackholing (RTBH) or BGP Flowspec. However, network infrastructure by itself cannot be a complete solution to mitigating a DDoS attack due to the simplicity of rules, and the inability to differentiate legitimate traffic from attack traffic beyond the network layer, such as application-layer and state-exhaustion attacks.
- 2. Specialized Intelligent DDoS Mitigation Systems (IDMS) devices such as Arbor Threat Mitigation System[™] (TMS), Carrier Agnostic Cloud mitigation services such as Arbor Cloud[®], or a hybrid DDoS defense by combinging on-prem IDMS with cloud mitigation.

Increasingly, network operators are looking to combine these two approaches for more scalable and effective DDoS defense. Network infrastructure can be used to block attack vectors that involve high volumes of traffic matching a static network layer signature, such as a well-known port, protocol and packet size. This leaves other attack components, such as orphaned IP fragments, other protocol traffic, state exhaustion attacks, application-layer attacks requiring additional analysis or authentication to be blocked by the intelligent mitigation system.

Coordinating DDoS mitigation across diverse infrastructure can prove to be a significant challenge. Each element of the network may have different scale and capability to respond to DDoS attacks, and there is no standard for how to manage all of these different elements.

Managing any network element to mitigate DDoS attacks requires support for these key management capabilities:

1. The ability to quickly configure a potentially large number of traffic matching criteria (such as destination IP address or CIDR block, protocol, port, or packet length) and corresponding actions to take for matching traffic, such as blocking the traffic, rate limiting it, or remarking it.

NETSCOUT RESEARCHES AND DELIVERS A FREE BI-ANNUAL DDoS THREAT INTELLIGENCE REPORT

Explore the full report: www.netscout.com/threatreport

- 2. The ability to get detailed data on what traffic is being affected and why, by each configured action in #1.
- 3. The ability to automatically delete actions when they are no longer needed, possibly based on feedback from #2.

Other than Intelligent DDoS mitigation systems such as Arbor Threat Mitigation System (TMS), most network elements do not intrinsically support all of these management capabilities, making it much more difficult to use them operationally in DDoS defense. In particular, there is usually no visibility into the traffic being dropped or rate limited by each router or switch. This creates a blind spot for the operator when attempting to manage network infrastructure for attack mitigation.

These DDoS management challenges led NETSCOUT to develop Sentinel. Sentinel adds these missing capabilities to enable effective operational management of the entire network to defend against DDoS attacks at scale. Sightline With Sentinel coordinates mitigation across the entire network, using Arbor TMS, network routers and switches using BGP Blackhole and BGP Flowspec, and provides signaling between networks to coordinate defense across network and organizational boundaries.

The Arbor Platform for Intelligent DDoS Attack Detection & Mitigation

Arbor Sightline

With support for monitoring up to 5000 routers, Arbor Sightline correlates traffic statistics from Netflow records with BGP-learned network routes. Traffic and routing analysis, based on this mechanism, allows Sightline to differentiate, mapping patterns of network traffic and providing rich, near real-time traffic visibility and DDoS detection capabilities. Arbor Sightline provides a unified workflow for attack detection, classification, traceback and mitigation with integrated management of the Arbor TMS.

As mentioned previously, it's very common for threat actors to launch multi-vector DDoS attacks. As the name implies, these attacks consist of several different attack vectors launched at the same target at the same time, increasing the likelihood of circumventing DDoS defenses. Normally, multi-vector attacks are launched against a very specific destination IP address, so the changing pattern of traffic can be observed using Netflow telemetry. Arbor Sightline detects such attacks using so-called "host detection", which is applied to any traffic going through a monitored network. Arbor Sightline's Fast Flood Detection can detect an attack in as little as 1 second using automated detection algorithms that look at thresholds and time. As shown below, Arbor Sightline analyzes all illegitimate vectors and includes them into a single DDoS alert rather than several disconnected incidents.



Sightline then immediately begins automated mitigation for each detected attack vector using a combination of Flowspec and / or Arbor Threat Mitigation System (TMS) based on operator-configured policy. The TMS may perform additional mitigation based on packet analysis as part of this automated action.

New Methods Pump Up Attacks, Bypass Traditional Defenses

Attackers not only combined attack vectors but also made them stronger than the sum of their parts by combining TCP reflection/amplification attacks with carpet-bombing techniques.

Arbor Threat Mitigation System (TMS)

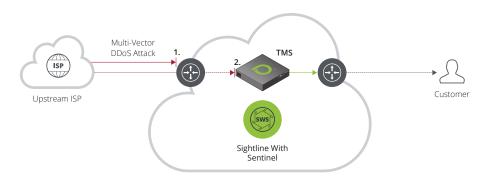
Sometimes using network infrastructure and techniques such as ACL, RTBH and Flowspec are not enough to stop DDoS attacks – especially more advanced application layer attacks. This is where an Intelligent DDoS Mitigation System (IDMS) is required. NETSCOUT's Arbor Threat Mitigation System (TMS) is such an IDMS.

Arbor TMS:

- Can stop all types of DDoS attacks including reflection/amplification attacks, state exhaustion or application layer attacks that require active countermeasures (challenge/response) and/or behavioral analysis to detect and stop.
- Supports multiple form factors including certified appliances, virtual or bare metal software running on COTS hardware, or Cisco Router embedded.
- Can scale from sub 1 Mbps to 400 Gbps in a single appliance or up to 400 Tbps of mitigation capacity in a single deployment.

Arbor Sightline With Sentinel

With knowledge of an organization's entire mitigation capability, including Arbor Threat Management System (TMS), routers / switches using Flowspec, or other network operators who can be called upon to help during an attack, Arbor Sightline With Sentinel is a unique solution that can coordinate all DDoS attack detection and mitigation activities across a network. This is done in real time whilst providing continuous feedback on mitigation effectiveness, including complete details on what traffic is actually being blocked and why. This is unprecedented in the security space and allows network operators to optimize and reduce the cost of DDoS protection. A simple explanation of how this works is below.



Advanced Reconnaissance

Attackers increasingly perform extensive reconnaissance of the victim's network and other devices that can be used to bypass defenses.

Changing Tactics on the Fly Attackers vary their attack methodologies and while the attack is in process. Attackers are also using more automated attacks, combining different attack vectors and attack methods and constantly rotating those to make detection and mitigation more difficult for the defenders.

A multi-vector DDoS attack arrives targeting an ISP's customer. Sightline With Sentinel detects the attack, analyzes it and with knowledge of the entire mitigation infrastructure, automatically orchestrates a mitigation plan consisting of:

- 1. Using BGP Flowspec and/or BGP Blackholes in the peering routers to stop volumetric vectors and
- Using Arbor TMS to block traffic that Flowspec can't effectively stop, such as IP fragments, along with attack traffic requiring more sophisticated analysis and response, such as state exhaustion and application layer attack vectors.

Telecommunication Providers Are #1 Target

With the goal of **maximum impact** in mind, bad actors targeted Telecommunication providers to **disrupt internet connectivity** during periods of sociopolitical turmoil. Sentinel will continuously monitor the attack activity and dynamically orchestrate a new mitigation plan if required throughout the attack. Once the attack ends a comprehensive post attack report is produced. Unlike other solutions, Sentinel provides detailed reporting on exactly what traffic is being dropped in routers and switches when using BGP Flowspec, in addition to the detailed reporting that comes from traffic analyzed and mitigated by Arbor TMS.

In addition, if another ISP running Sentinel assists with a mitigation via Sightline-to-Sightline signaling, then additional reporting information on remotely dropped traffic is also provided. A Sightline Signal shares attack signature information with another Sightline deployment, allowing multiple network operators to find and take action against the same DDoS attack. Since most service providers already use Sightline to manage their DDoS response, this gives Sightline customers the potential to coordinate DDoS defense across the Internet, either with a cloud DDoS protection provider, an upstream ISP, or even the network hosting botnet hosts that are launching the attack, enabling the blocking of DDoS attacks nearer to their source. Sightline Signaling can also help coordinate DDoS defense seamlessly between separately managed networks owned by the same parent organization.

In summary the main features and benefits of Sightline With Sentinel are:

- Automatic Detection The ability to automatically detect and provide detailed information on all types of DDoS attacks within seconds greatly improves the effectiveness of your mitigation specialists and reduces operational overhead of DDoS protection services.
- Intelligent Mitigation The ability to intelligently orchestrate multiple methods of mitigation for complex multi-vector DDoS attacks enables you to scale, optimize and improve effectiveness of your DDoS protection services.
- Continuous Feedback A single pane of glass for DDoS attack detection, classification, and traceback provides continuous feedback on mitigation efficacy allowing you to understand exactly what's happening during or after an attack.
- **Mitigation Collaboration** Via Sightline Signaling, you can collaborate with upstream service providers by sending them detailed attack mitigation parameters so they can mitigate DDoS attacks before they reach your network, enabling you to save your mitigation resources.

Impact of DDoS Attacks on Service Providers

-Service Downtime -Customer Churn -Increased Transit Costs -Increased Mitigation Costs

Preparation and DDoS Training Is a Key Element

Organizations must take the time to understand their own network architecture and traffic flows during peace time, since trying to do so while under attack can be very difficult, often resulting in DDoS defenses blocking legitimate user traffic.

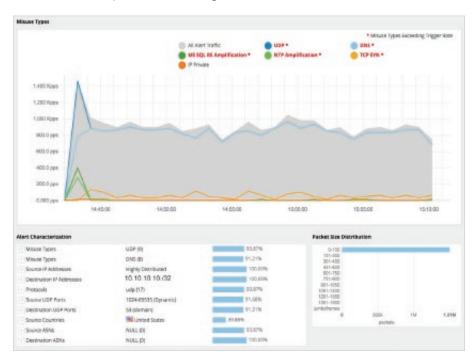
Practice Makes Perfect

Regular attack mitigation drills are highly recommended for network operators and DDoS mitigation service providers to find and adjust to any changes in architecture, bandwidth, and servers, services, and applications.

Arbor Smart Mitigation in Action: A Real-World Example

A multi-vector DDoS attack is directed at a DNS server, IP address 10.10.10.10. The attack consists of NTP Amplification, MS SQL Amplification, DNS flood and Mirai DNS Pseudo Random Subdomain (PRSD) attacks. The following are all the steps of detection and automated response, and the multiple mitigation strategies used to mitigate the attack.

1. **Detection** – Arbor Sightline performs multi-vector attack detection. Within a few seconds an alert with multiple attack vectors is generated, as shown:



Optimization of Botnets & Attack Size

Attackers have learned that you don't need a nuclear weapon to swat a fly. We observed a significant drop in frequency of attacks larger than 500 Gbps, while a 16% increase in the number of attacks in the 100-200 Gbps range – a reflection of maturation in the attacker market.

 Automatic generation of BGP Flowspec rules – Arbor Sightline applies Flowspec mitigation to drop NTP Amplification and MS SQL Amplification attack traffic and forwards the rest of the traffic to an Arbor Threat Mitigation System (TMS) that can analyze and clean the remaining attack vectors.

Name†	Description	Bowsper	IP Version St	atas	Attiee
Hest Alert 45709 MS SQL RS Amplification	Auto-generated Row Specification from alert 45709	Det. 10.10.10.1012 Protocolst 17 fee Perts: 1434	A	Bunning	M Stop
Host Alert 45709 NTP Amplification	Auto-generated Row Specification fram alert 45705	Det: 10.1018.0000 Protocols: 17.5rc Ports: 13.3 Packet Length: 1-35.37-45.47-75.77-219.221-45535	4	Bunning	M Stop

Bypassing Traditional Defenses

Many of the newer attack vectors often do not have as high packet-per-second rates or bandwidth as traditional attacks. Rather, they either bypass poorly constructed network access policies (IPMI/ RMCP and OpenVPN) or combine existing attacks into new powerful attacks (TCP reflection/amplification carpetbombing). Automatic mitigation using Arbor TMS – Arbor TMS drops remaining attack vectors and passes legitimate traffic to target DNS server 10.10.10.10. The mitigation dashboard below provides a TMS mitigation overview. As shown, various countermeasures are used to mitigate the attack, including DNS Authentication, DNS Malformed and DNS Rate Limiting.

Summary			/ tet	Counter	measures			
Status Oct 30 14	142 - Origoing			Tratare:	Sminutes 🚦 Graph Unic bas 🛃	Sample Packets		
Mode Active				- Dirice	Cauda Transact	Dragent Peer		
Alert 45709				3 DM	Involid Packets	Company room		
Yemplate Custome	7.Template			E 0#	IPvil Andress Nilter Lists			
	Ronaged Object: Viotim 7			CIFF	(Pvt Black/White Liex			
Learning Dataset: None				OF Packet Header Fibring				
TMS Group All				E OFF Placet Heads Herring				
Protection Prelices 10:10:10:10:32					In the Detertion			
			N Stop	III Off	UDP Reflection/Amplification Protection			
			in step		Per Connection Protection			
				017	TCP SRV Authentication			
Teld NorTHS NorCountered	CORE (FIN)		ton Excel	E 0#	ONI Scoping			
1.0M BOR				E ON	CN6 Authoritication	7.2 Kloce 8.7 ppc		
114		-		= CFF	TCP Connection Limitine	Contraction Part		
19			A	a det	TCP Connection Reset			
The state of the s	ALL ADD	Contractory of the local division of the loc		I OFF	Payload Regular Expression			
				arr.	Press Nocimo			
6304				U ON	GNS Malfarred	655.6 Khos 837.1 pay		
4004				= ON	ONS MAN LINEON			
	A	-	A &	E 0#	ONS MRDwmain Rate Limiting			
				i dff	ONS Regular Supremian			
15,05,05 15,05,05	181800 181800	15,35,00	15,25,02	10 OFF	HTTP Malformed			
· Fans hos · Drog how		(manager	10.000	a orr	HTTP Scoping			
Calendary at Manufact I State	PLANE DENAM			iii on	HTTP Rate Untiting			
				a dry	All and HTTP/UR, Regular Expression			
	1.565.649	2 Min Hig	Denning Mg	E 0#	58, Negoliation			
Dropped	4911 logs	AST 3 Hope	620.4 shee.	E 0#	SP Mathemat			
Fastert	15254381	200.9 6585	251.8 Month	- GFF	SP Request Liniting			
1008	811.21534	812.8 4536	10712-0020	- 0#	Shaping			
Persent Droppell	81.20M	76,008	26.64%	E 0#	1P Location Policing			
Disclared 1 matter	O Areas	C heats	C-berry					

A Vicious Cycle

As organizations put forth increasingly advanced DDoS defenses, attackers naturally respond with sophisticated techniques that are then rapidly weaponized and widely disseminated by booter/stresser services.

4. **Mitigation Overview** – Using a single screen, Sightline With Sentinel provides detailed information regarding of ongoing mitigations. For example, in our scenario below you see details of all the active Flowspec and TMS mitigations.

aS Heat Alert 45709							000
Duration: Oct 30 14:42 - Orgoing (2:29)				Tapito	awar hogin	Wee Scheltped (0)	10 Mages Akr.
Summary Traffic Details Hawsper	Details R	reters I	Newspec Reaters	Annetations			
DETAILS Period. Aleri Tirseframe 📴 Uni	111 000 🔂 V	tes: Netwo	nh Beandary	🔒 0 🖨 Upda	*		
KEY INFORMATION							View New Flaws -
Severity Level Max Severity Percent O Top	Millouse Type	Max Impact	of Alert Traffic O	Direction Missise Ty	(pes		Managed Object Target
High 2,505.0% of 105 pps US Front Flood		2.3 Milyisi 2.9 At care-sarijo		incoming TCP SPN, I Amplificat		ation, MS 5QL 85	Weber 7 10.16.10.10
METERATIONS.							
Nate	Type	Quality	Start Time	Man Passed	Average Pesse	d Max Dropper	Average Dropped
 Forespec Mitigations (2) 							
Hest Alert, 45708 MS SOL PS Amelification	Ind Novspec	0.29	041301442	MA.		A 800.0 Kips / 1.0 Kips	s 629-4 Kbps / 798-8 pps
Heat Alert 45/08 MTP Amelification	iPe4 Ployoper	0.29	0x1301442	44.		4 8153 Rbps / 1.0 Raps	625.3 Kbps / 381.3 pps
This Midgations (1)							
Kert 45709 Auto Millionion	IPut THE	0.29	0/1201442 5	266.7 Kibps / 826.0 pps	187.8 Hope / 322.0 pt	1044 Ropt / 009.0 pp	996.2 Kbps / 798.3 pps

Interest Grows in Managed Security Services

The challenging hiring market has caused more enterprises to turn to service providers for security support, as more than half of service providers reported growing interest in DDoS managed services from customers. A single click reveals details per active mitigation. For example, below are the details of a Flowspec Mitigation:

	tions						
Name		Тури	Deration	Start Time	Max Dropped	Ave	age Drepped
Rowspee Mit	igations (2)						
Host Nact 45	719 MS 50L KS Amplifuzition	IPv4 Reveptic	0.29	Oct 30 14:42	880.0 Kbps / 1.0 Kpps	629.4 Kb	ps / 786.0 pps
ilost Alert 45	TISS NTP Amplification	Pv4 Revepec	0.29	Oet 30 14:42	010.3 Kbps / 1.0 Kpps	625.3 (b)	ps./ 781.0 pps
fop 5 News by D	rapped Traffic						
Source IP Addr	esses			Destination IP Addresse			
Highly Distri	huted	1,57 8005	100.00%	10.01.01.10/32		1.37 Kppi-	100.00%
190.83.127.9	91.04	1.00 pps 0.00%				Quiew Graph	Treparter
- 145.83.80.35	ptylia.	1.00 pps 0.00%					
48,7730530	27/32	1.00 pps 0.00%					
- 55.104.117.2	294/82	1.50 pps 0.01%					
		Qurew brash	View More				
Source TCP Por	ta No terre ave			Destination TCP Ports			
	NO ENTIL BVB	Lable.			No izerw.moliatie.		
Source UDP Par		LADM.		Destination UDP Parts	No itera available.		
Source UDP Par 1454		796.09 (80)	76		Harbern skalatik. Na itern skalatik	1.57 Kpm	100.00%
	rtx	786.09 pps 50.12 781.09 pps 40.01	2% IN			1.37 Hpm Quine Graph	
1454	nta masqi-m	786.09 pps 50.13 781.09 pps 40.81	76			and the second se	
1454	nta masqi-m	786.09 pps 50.12 781.09 pps 40.01	2% IN 2. reported			and the second se	100.00% Ereported
1434 123	nta masqi-m	796,89 (pp) 50,12 791,89 (pp) 49,81 Q Waw Graph	2% IN 2. reported	50 w		and the second se	
1454 123	nta masy-m nta	796.50 ppp 90.13 791.50 ppp 40.81 QView Graph	2% IN 2 reported	50 w	we http	Q view Graph	1 reparter
1454 123	nte magal-m mga NUA ₆	796.59 (50) 50.13 791.59 (50) 40.81 Q Wave Gouph 1.67 Supp	2% Contraction of the second o	50 w	we http	Quies Graph	1 reported
1454 123 Seurce ASNs 0	nte magal-m mga NUA ₆	796.59 (50) 50.13 791.59 (50) 40.81 Q Wave Gouph 1.67 Supp	2% Constant N 2 reported 1 reported	80 m Destination ASVe 8 N	we http	Quies Graph	1 reparter
1454 123 Source ASNs 0 Source Countril	nte magain nga nulus	796.59 ppp 50.12 791.59 ppp 42.81 Q.Wave Graph 1.67 Sppc Q.Mave Graph	2% Constant N 2 reported 1 reported	80 m Destination ASNs - 6 N Precesses	we http	Quine Graph	1 reports 1 voc. 50% 1 reports
1454 123 Source ASNs 0 Source Countril	nta magainn nig nulus ses united Datase	786.89 ppp 90.13 791.89 ppp 40.81 QView Graph 1.69 sppp 90.000 QView thaph	2% Constant N 2 reported 1 reported	80 m Destination ASNs - 6 N Precesses	we http	Q view Graph 1-57 Npps Quiew Graph	1 reports 1 reports 1 reports
1454 123 Source ASNs 0 Source Countril	nta masqi-ri migi NUQL NUQL NUQL Uvitod Rates Orina	796.59 (50) 50.13 791.30 (50) 43.81 Quitew Golph 1.67 Sept Quitew Golph Global pop 41.87 (52.05 ppp 61.87) (52.05 ppp 61.87)	2% Constant N 2 reported 1 reported	80 m Destination ASNs - 6 N Precesses	we http	Q view Graph 1-57 Npps Quiew Graph	1 reports 1 reports 1 reports
1454 123 Source ASNs 0 Source Countrit	nte masql-m map NULL NULL NULL NULL NULL NULL NULL NUL	796.00 (pp) 50.13 791.00 (pp) 40.81 Quitev Graph 1.67 Spot Quitev Graph 556.00 (pp) 81.89 152.00 (pp) 84.006 83.00 (pp) 5.206	2% Constant N 2 reported 1 reported	80 m Destination ASNs - 6 N Precesses	we http	Q view Graph 1-57 Npps Quiew Graph	1 reports 1 reports 1 reports

5. (Optional) Use of Sightline Signaling for Inter-provider DDoS mitigation – If need be, a network operator may share attack details and trigger mitigation in an upstream service provider or in a peering partner. This allows the attack to be mitigated closer to the source so that upstream and peering links should not be overloaded. Sightline With Sentinel can do this by enabling inter-provider DDoS mitigation using "Sightline Signaling". If the upstream ISP elects to receive and deploy the requested mitigation, the requesting ISP can see an "upstream view" into attack statistics.

Mitigate Alert	Sightline Signaling Mitigation Request	×
Threat Management	Note: Sightline automatically includes in the mitigation request the IP address of the	
Flow Specification	target and the misuse types detected in the host alert.	
Blackhole	Mitigation Provider	
Generate Filter	JusticeLeague	\$
Sightline Signaling	Message	

Conclusion

NETSCOUT's Arbor Sightline With Sentinel can intelligently detect and automatically orchestrate mitigations for all types of DDoS attacks enabling an organization to protect itself and its customers in the most effective and efficient way possible. DDoS attacks aren't a new cyber threat. Network operators have been dealing with DDoS attacks for over 20 years. What's changed is the number, size and sophistication of these attacks. For almost as long as there have been DDoS attacks, Arbor Networks, now a part of NETSCOUT, has been researching DDoS attacks and building industry leading products and services to stop them.

LEARN MORE

For more insights into DDoS attacks and Best Practices in Defense, explore the latest NETSCOUT DDoS Threat Intelligence Report:

www.netscout.com/threatreport

Automated Detection and Orchestrated Mitigation

Organizations need automated DDoS detection and mitigation tools that can not only quickly identify and respond to DDoS attacks, but also adjust the mitigation methods as the attacker changes attack vectors.

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)



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

© 2022 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, Arbor Networks, the Arbor Networks logo, ATLAS, InfiniStream, InfiniStreamNG, nGenius, and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.