NETSCOUT®

| WHITE PAPER |

Defend Your Network at Scale with Smart Protection

SECURITY

TABLE OF CONTENTS

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. 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 1H 2020 Threat Intelligence Report (https://www.netscout.com/threatreport).

- The **frequency** of DDoS attacks is increasing. In the 1st half of 2020, there have been 4.8 million DDoS attacks. That's **a 15%** increase from the prior year.
- Attacks are getting more **sophisticated**. There has been a 2851% increase in 15+ vector DDoS attacks (since 2017) and a 31% increase in attack packet rates.
- Attacks are getting **shorter in duration**. There has been a 51% decrease in attack duration, as 92% of all DDoS attacks last less than an hour.

The increase in attack frequency, complexity, and shorter duration means less time for defenders to **stop sophisticated 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 with NETSCOUT Smart Data, moving visibility up to layer-7, and 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:

1. Network infrastructure, such as routers with techniques such as Access Control Lists, BGP Remote Triggered Blackholing (RTBH) or BGP Flowspec.
2. Specialized Intelligent DDoS Mitigation Systems (IDMS) devices such as Arbor Threat Mitigation System (TMS), or Carrier Agnostic Cloud mitigation services such as Arbor Cloud.

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

RELEVANT EXCERPTS FROM NETSCOUT'S 1H 2020 THREAT INTELLIGENCE REPORT

Download the full report:
https://www.netscout.com/threatreport

Attack Frequency Up

- 4.8 Million DDoS attacks in 1st half 2020.
- Up 15% YOY
- Up 25% during time of pandemic lock down

Attack Complexity Up

2851% increase in 15+ vector DDoS attacks (since 2017)
92% of all DDoS attacks last less than an hour

2. The ability to get detailed data on what traffic is being affected 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.

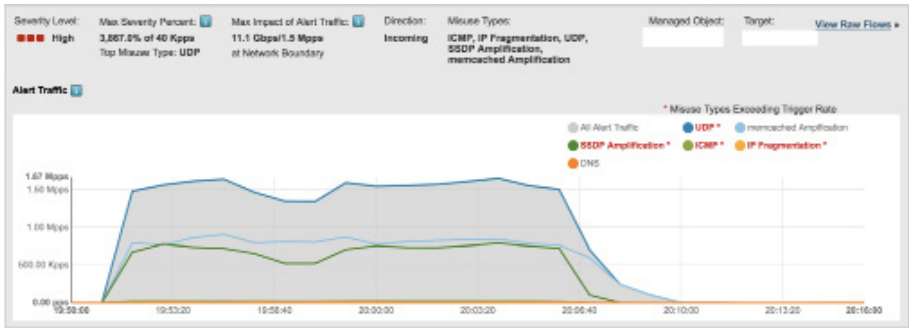
These DDoS management challenges led NETSCOUT to develop Sentinel. Sentinel adds these missing capabilities to enable effective operational management of the entire network to defend against DDoS attacks at scale. Sightline with Sentinel coordinates mitigation across the entire network, using Arbor TMS, 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.

3 Ways Attackers Exploit A Pandemic

1) Target COVID-era lifelines like ISPs, healthcare, financial services.
2) Increase frequency and complexity of attacks.
3) Do it on someone else's dime.

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 (Arbor TMS)

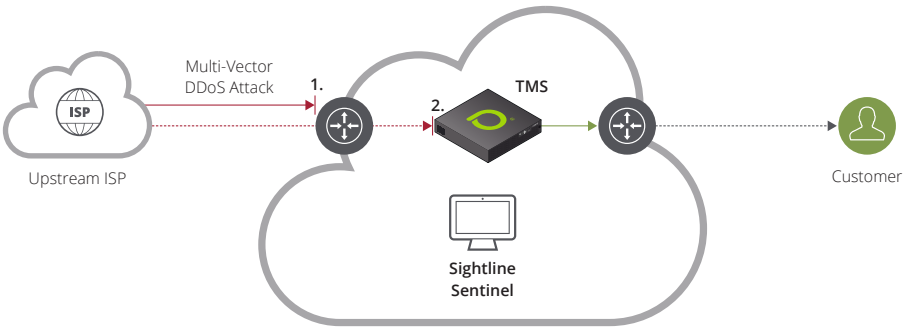
Sometimes using network infrastructure and techniques such as ACL, RTBH and Flowspec are not enough to stop DDoS attacks – especially more advanced application layer attacks. This is where an Intelligent DDoS Mitigation System (IDMS) is required. NETSCOUT's Arbor Threat Mitigation System (TMS) is such 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 1Mbps to 400Gbps 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. 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.



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
2. 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.

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.

Telecommunication Providers Area #1 Target
*With the goal of **maximum impact** in mind, bad actors targeted Telecommunication providers to **disrupt internet connectivity** during pandemic.*

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:

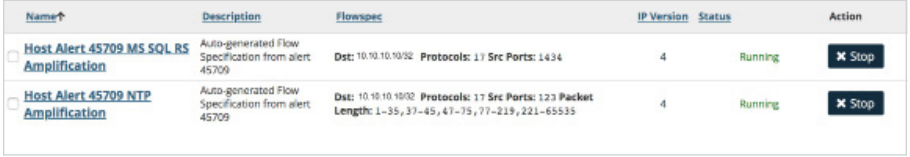
- **Automatic Detection** – The ability to automatically detect and provide detailed information on all types of DDoS attacks within seconds greatly improves the effectiveness of your mitigation specialists and reduces operational overhead of DDoS protection services.
- **Intelligent Mitigation** – The 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.
- **Visibility Beyond DDoS Attacks** – Ingesting NETSCOUT's patented Adaptive Service Intelligence (ASI) Smart Data technology enables you to gain visibility into layer-7 OTT traffic and detect other types of cyber security threats beyond DDoS attacks.

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:

2. **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	Flowspec	IP Version	Status	Action
Host Alert 45709 MS SQL RS Amplification	Auto-generated Flow Specification from alert 45709	**Dst:** 10.10.10.10/32 **Protocols:** 17 **Src Ports:** 1434	4	Running	Stop
Host Alert 45709 NTP Amplification	Auto-generated Flow Specification from alert 45709	**Dst:** 10.10.10.10/32 **Protocols:** 17 **Src Ports:** 123 **Packet Length:** 1-35,37-45,47-75,77-219,221-65535	4	Running	Stop

Impact of DDoS Attacks on Service providers

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

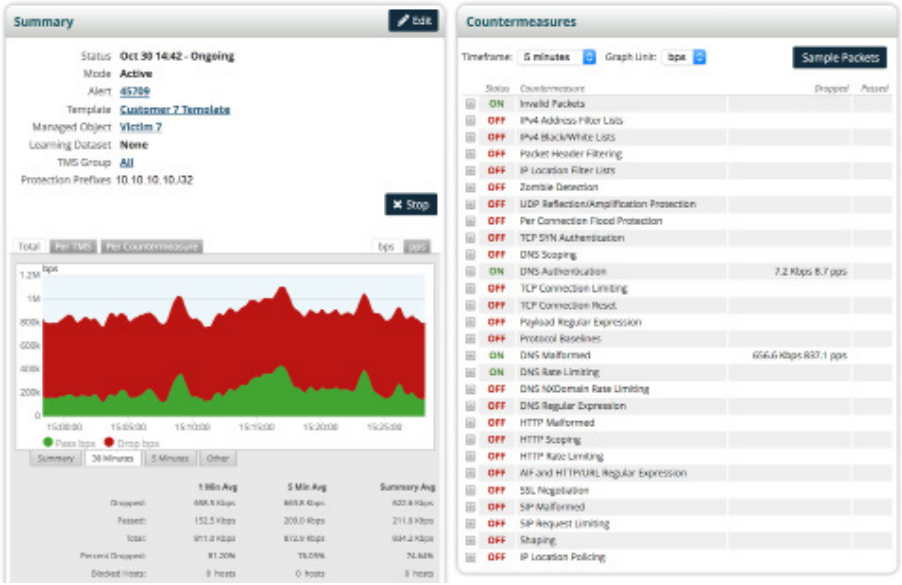
Preparation and DDoS Training Is a Key Element

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.

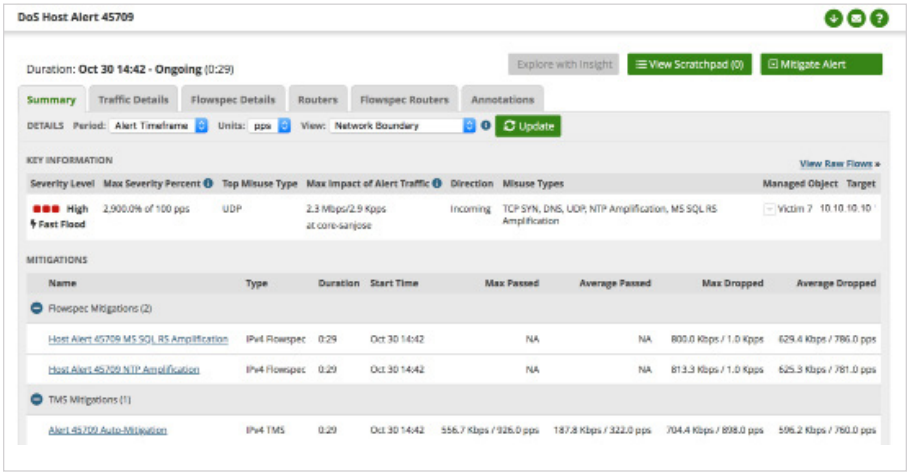
Practice Makes Perfect

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.

3. **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.



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.



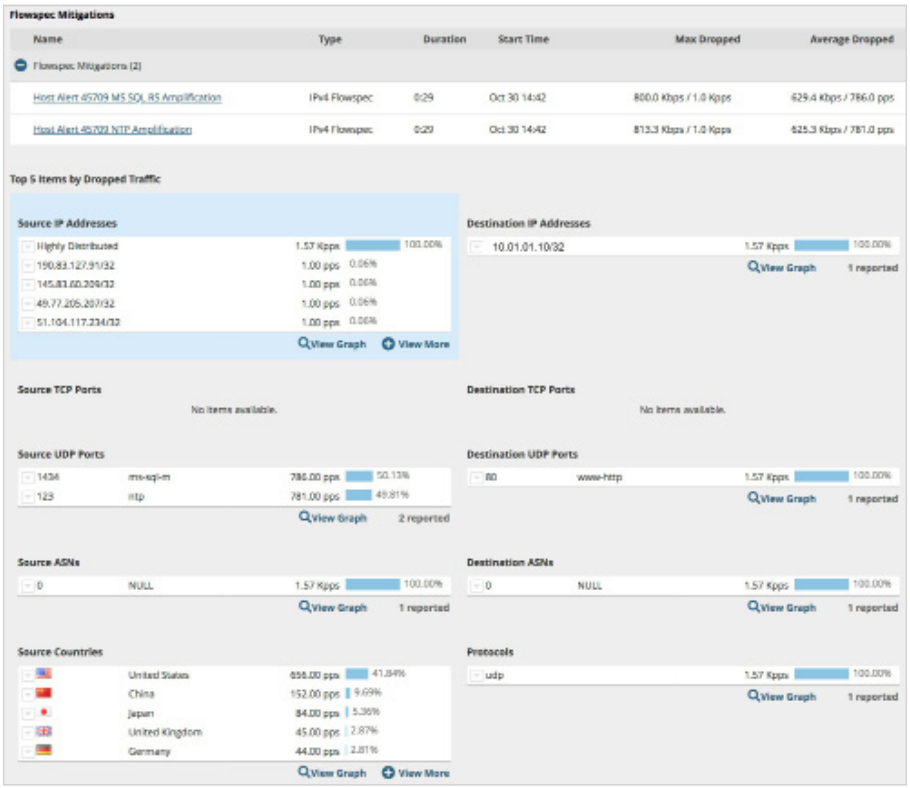
Optimization of Botnets & Attack Size

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.

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 carpet-bombing).

A single click reveals details per active mitigation. For example, below are the details of a Flowspec Mitigation:



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.

A Serious Game of Cat & Mouse

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.

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.

Conclusion

NETSCOUT's Arbor Sightline with Sentinel can intelligently detect and automatically orchestrate mitigations for all types of DDoS attacks enabling an organization to 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 download the entire NETSCOUT 1H 2020 Threat Intelligence Report:

https://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)

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

SECWP_013_EN-2101 01/2021