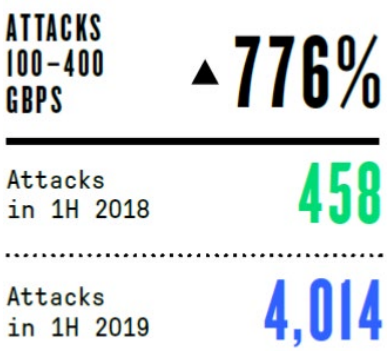
NETSCOUT Arbor Managed Services for Internet Service Providers

NETSCOUT Arbor has been monitoring and analyzing the trends of the global DDoS landscape since 2004 when ISPs, large enterprises and other companies were first surveyed for the first edition of the Worldwide Infrastructure Security Report. This research consistently registered two divergent trends: on one side a constant growth of the size of attacks, on the other a race to develop smarter, more complex attacks.

A third trend has emerged in the first half of 2019 that shows an increase of over 770% in attack sizes between 100-400 Gbps between 1st half 2018 and 1st half 2019.



Complexity and Size of DDoS Attacks Continue to Grow

In recent years, the weaponization of both well-known and new traffic amplification vectors and IoT-based botnets of unprecedented proportions, have made the eventuality of an attack as large as multiple hundreds of Gigabits per second a very real threat. Such monster attacks often exceed the amount of mitigation capacity that is economically feasible to deploy even for most Internet Service Providers, and threaten the very availability of data connections for entire nations or even for large parts of the global Internet. The memcached-driven attacks of 2018 have exceeded 1 Terabit per second in size and served as a reminder that powerful attack weapons might still hide in plain sight waiting to be exploited (See Figure 1).

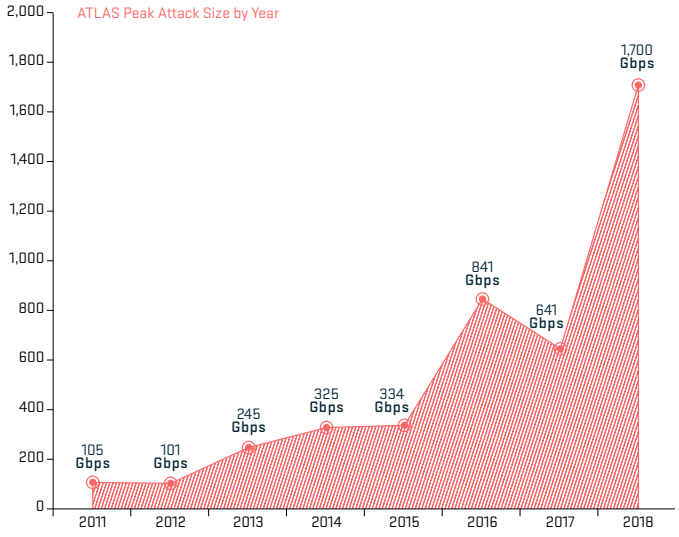


Figure 1: Largest attack size detected, NETSCOUT Arbor ATLAS platform, 2011-2018.

At the same time, increasingly powerful and complex application infrastructures have attracted increasingly complex attacks. Far from relying on brute force alone, attackers increasingly blend attack strategies, utilize a wide arsenal of vectors and often develop attacks targeted specifically at the victim's services. Frequently, committed attackers monitor the effectiveness of their tactics and engage the defenders in complex battles that can last hours or days.

An increasing number of companies every year report having experienced multi-vector attacks: add the constant struggle in staffing Security Operation Centers and the risk of failing to defend one's assets increases noticeably.

Global Market Demand for Anti-DDoS Protection Increases

In addition to constituting a threat to a Service Provider's own infrastructure, DDoS attacks represent a fatal threat to the multitude of companies that rely on the Internet to run their businesses. Enterprise customers today commonly include DDoS protection services as a requirement in their network-related projects, frequently specifying that any attack size and target geography must be covered (Figure 2).

Many Service Providers today face challenges in protecting companies that operate in environments where it's commonplace to mix geographically distributed locations, multiple ISPs, cloud providers and "as-a-service" infrastructures.

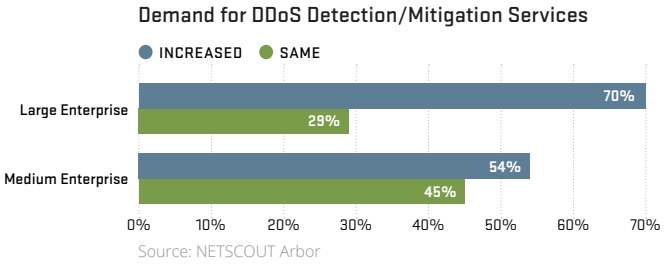


Figure 2: Trends of demand for anti-DDoS services, WISR 2017.

Industry analysts identify in the services market a growing source of revenues for ISPs. HIS Markit "DDoS: preparing for massive attacks and new regulations" report states that "Hybrid solutions and sales of hardware at the lower end of the market [...] are driving significant revenue [...]. These new enterprise sales, along with [...] strong demand from customers to buy managed solutions from hosting providers and carriers are the primary drivers behind growth in this market."

The Struggle to Find and Retain Security Skills

Organizations continue to indicate a general shortage of skilled headcount as their main challenge in building and maintaining operational security teams.

In this market environment, building an effective Security Operation Centre and maintain its effectiveness across time is increasingly difficult. Lack of properly trained and experienced personnel can translate in weaker defenses against attackers that are growing smarter and more motivated. Figure 3 shows the different challenges companies face when staffing and supporting their operations.

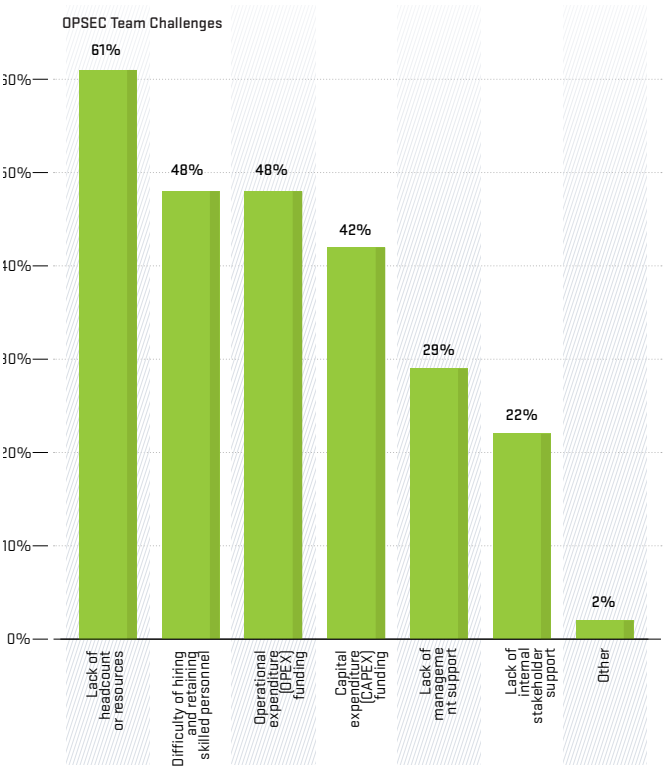


Figure 3: Resource management challenges for SECOPS.

NETSCOUT Arbor Managed Services for Service Providers

NETSCOUT Arbor Cloud for Service Providers

With NETSCOUT® Arbor Cloud, we deliver best practices protection against a broad spectrum of DDoS attacks by integrating on-premise defenses with powerful cloud-based traffic scrubbing services. NETSCOUT Arbor's technology, products and ATLAS® research infrastructure power the service staffed NETSCOUT Arbor DDoS, supported by a 24x7 Security Operations Center staffed by NETSCOUT Arbor DDoS and security experts.

Service Providers that have not yet established a global presence but are looking for a fast lane to achieve global market reach can choose to resell NETSCOUT Arbor Cloud for Enterprise packages on a customer by customer basis while still acting as the first level of contact. Each Service Provider SOC and NETSCOUT Arbor Cloud SOC build a tight, tailored relationship to deliver effective mitigation together.

When a DDoS Mitigation Service platform is already in place, Service Providers can choose NETSCOUT Arbor Cloud for SP packages, based on either Excess Capacity or Unlimited models.

- Excess Capacity provides a predefined number of mitigations per year in a cost-effective way, based on the size of the protected network; it can be expanded with additional mitigations or to cover larger networks as needed;
- The Unlimited model provides unlimited mitigations for networks of any size and scales together with the Service Provider's local mitigation capacity: as the Service Provider's mitigation footprint expands, resorting to the cloud becomes cheaper.

Managed NETSCOUT Arbor Sightline /Threat Mitigation System

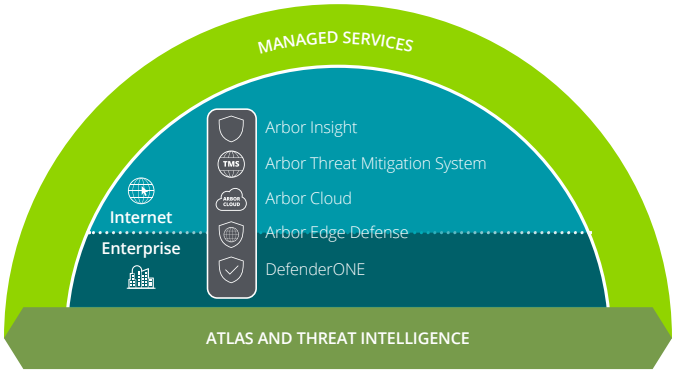
Managed Sightline / Threat Mitigation System Services provide customers with 24x7 secure monitoring and maintenance services. It allows you to focus your resources on core business needs, while NETSCOUT Arbor-trained professionals provide the experience, skills, and technology to ensure network and traffic integrity.

A team of industry specialists that are experienced in DDoS and advanced threat detection manage your SP/TMS service, which ensures:

- Service availability of your solution. The team provides application, database, and platform monitoring, in conjunction with proactive problem solving to avoid incidents.
- System Alerts are configured and customized to your environment to notify the Managed Service teams of DDoS and System Alerts.
- Fast response and execution by a team that understands your deployment.
- Network integrity and Application Availability. The Service Team is notified and addresses attacks situations to ensure network and application availability.
- Proactive Configuration and Tuning.
- Managed Cloud signaling has been introduced to allow service providers to signal to NETSCOUT Arbor Cloud and provide a seamless integration with the on-premise equipment.

Resident Engineer (RE)

NETSCOUT Arbor Resident Support Engineers are highly qualified technical experts who integrate as members of the customer's operations, design, or engineering staff acting as direct on-site support resources for all technical aspects related to NETSCOUT Arbor's DDoS and Service Visibility product lines.



The Global Leader in DDoS Protection

NETSCOUT Arbor, the security division of NETSCOUT, helps secure the world's largest enterprise and provider networks from DDoS and advanced targeted attacks.

NETSCOUT Arbor is the market leader in on-premise detection and mitigation of distributed denial-of- service (DDoS) attacks. Since 2013, it has also offered a cloud-based mitigation service, NETSCOUT Arbor Cloud, to which enterprise customers can route traffic when they perceive that volumes are too great for their on-premise capabilities.

ASERT: the NETSCOUT Arbor Security Engineering & Response Team combines sophisticated, automated data collection techniques with the technical and analytical expertise of its security researchers. This specialized team distills mountains of technical information into actionable business intelligence for network professionals.

Hundreds of service providers participate in **ATLAS**, providing NETSCOUT Arbor with an enormous dataset that enables our security researchers to develop a unique, globally-scoped view of malicious traffic traversing backbone networks that form the Internet's core. NETSCOUT Arbor's researchers are constantly analyzing DDoS botnet attacks - the ATLAS Intelligence Feed is integrated into NETSCOUT Arbor's solutions to help detect and stop emerging and dynamic threats such as botnets. It simplifies threat responses because it is updated in real time without software updates. The AIF also stops complex application-layer attacks.

Cloud Signaling technology: NETSCOUT Arbor has developed a protocol to facilitate customer on-premise mitigation of application-layer attacks and upstream mitigation of flood-based attacks in an automated and real-time manner.

NETSCOUT Arbor Sightline

NETSCOUT® Arbor Sightline provides comprehensive network visibility capabilities to help customers detect threats and improve traffic engineering and peering relationships.

NETSCOUT Arbor Threat Mitigation System

NETSCOUT Arbor Threat Mitigation System™ surgically removes DDoS attack traffic from the network without disrupting key network services.

NETSCOUT Arbor APS

NETSCOUT Arbor APS provides proven, on-premise DDoS protection for the world's most critical enterprise and government networks, and completes a service provider's Managed Security Service offering.

NETSCOUT Arbor Edge Defense

NETSCOUT Arbor Edge Defense® detects and stops both inbound threats and outbound communication from internal compromised hosts.

NETSCOUT Arbor Cloud

NETSCOUT Arbor Cloud delivers unique integrated protection from the full spectrum of modern DDoS attacks.

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_011_EN-2202 08/2022