# On-Premise Protection is the Best First Step Against DDoS and Cyberattacks for Academic Institutions

## Introduction

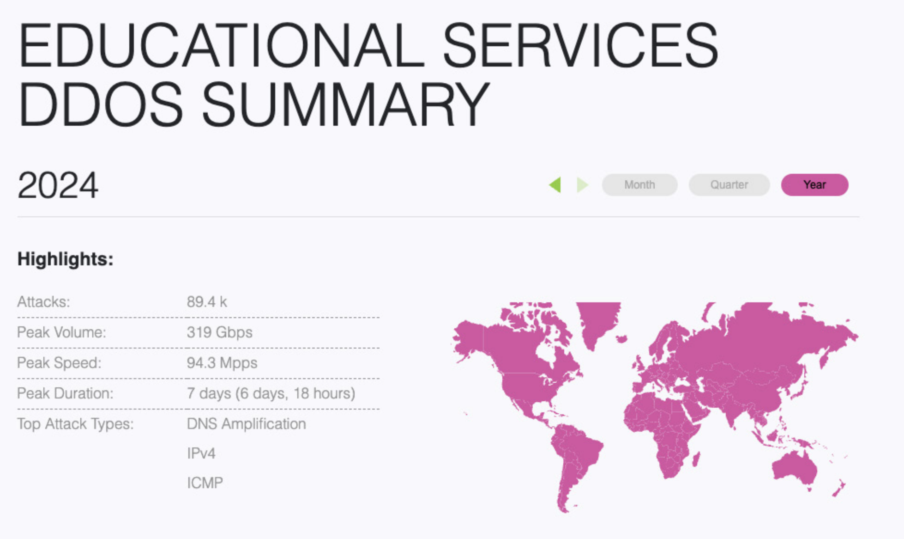
As academic institutions end their calendar years and reflect on DDoS attacks that caused disruptions in on line learning and resource availability throughout the year, they are beginning to understand the need to attain an appreciation of the real risk of DDoS attacks and the growing threat landscape. In fact, during the second half of 2023, the increased threat surface due to online education at all levels triggered a massive shift in internet usage. The result was that cybercriminals launched over 75 thousand DDoS attacks aimed at crippling the targets that online applications and services rely on.

This activity was not only seen at colleges and universities but also at the high school and middle school level. As the education sector relies more heavily on online learning, attackers naturally follow and it looks like the trend will continue. Thus far according to the NETSCOUT® Cyber Threat Horizon, in the first quarter of 2024 there have been over 89 thousand DDoS attacks targeting educational institutions globally.

A majority of these recorded attacks are targeting the online learning delivery applications and services which are becoming the backbone of many academic institutions.

### It Has Become a Requirement To Understand DDoS Attack Risk and the Risk Avoidance Provided by an On-Premise First, Mitigation Strategy

Due to the evasion ability of newer complex multi vector DDoS attacks, Educational Institutions need to understand the risk reduction that on-premise edge protection can provide to their on line learning applications and services.



EDUCATIONAL SERVICES DDOS SUMMARY

2024

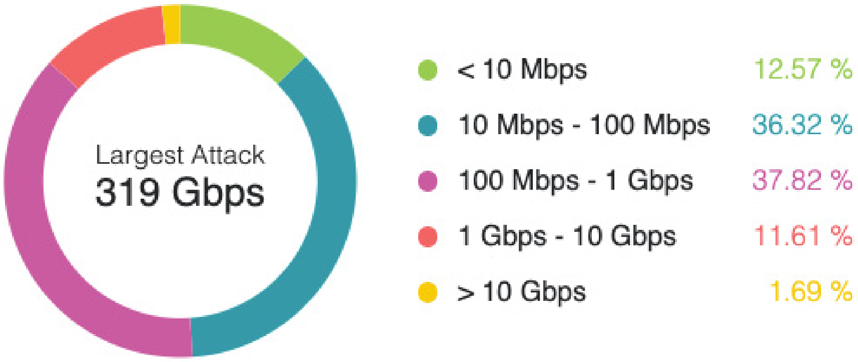
**Highlights:**

| | |
|---|---|
| Attacks: | 89.4 k |
| Peak Volume: | 319 Gbps |
| Peak Speed: | 94.3 Mpps |
| Peak Duration: | 7 days (6 days, 18 hours) |
| Top Attack Types: | DNS Amplification<br>IPv4<br>ICMP |

## Challenge

The identified unavailability was primarily a result of newer complex multi vector DDoS attacks. Many of the attacks were thought to be initiated from within the college. This situation is not unique to colleges but was also seen at the lower school levels. What's interesting is that many educational IT instructors actively teach cyber courses and gaming to learners to develop their skills outside of the coursework. Because of this, simple internal DDoS attacks like these are inevitable and probably represent the tip of the iceberg.

Cybercriminals outside of the student populations are taking advantage of the new threat surface outside of the core network created by online education. These endpoints are typically connected to the network via VPN or to online SaaS-based services. Because of this, the main focus area for any security strategy should be firewalls and VPNs where online learning has shifted student and teacher access. Furthermore, attackers are not only increasing their frequency, but they are also creating smaller, more intricate and complex attacks, so they are harder to detect by volumetric alerts in cloud scrubbing centers. According to the NETSCOUT Cyber Threat Horizon, only about 12% of all attacks clocked in above 1 Gbps during the first 3 months of this year.



## Mitigation

Because of the size and type of DDoS attacks that an educational institution may encounter, combined with the complexity of each institution's network, there are a variety of mitigation strategies and security postures that may be warranted. However, the need for on-premise protection as a first step against DDoS and cyberattacks is no longer optional in today's climate. Years ago, an educational institution could hope that they would not be attacked. Today, with the newly increased threat surface, it really comes down to when, not if it will happen.

On-premise protection is needed because application layer, or small sized attacks will slip by upstream protection by design. Likewise, TCP Flood or VPN and firewall targeted attacks can also slip by upstream protection. The threat to educational institutions is further amplified by the potential for compromised hosts within the network, ready to communicate with known Command & Control (C2C) infrastructures on the internet for further exploitation with malware.

Furthermore, due to the creation of new attack vectors (threat actors exploited or weaponized seven new reflection/amplification DDoS attack vectors within the last seven months); the number of attack vectors being used in a single attack (31 attack vectors deployed in a single attack); and what's known as a dynamic DDoS attack, which changes vectors based on the defense that is presented, on-premises protection, with its inherent attack management agility, local control and efficiency, is a priority.

NETSCOUT's Arbor Edge Defense (AED) is a stateless packet processing appliance (physical or virtual) that resides on-premise, in front of stateful infrastructure including firewalls and VPN concentrators to protect them from every type of DDoS attack (volumetric, state exhaustion, and application layer). It is an in-line device dedicated to, and customized for, your specific environment. AED protects the availability of your network and service infrastructure by detecting and reacting to attacks in real-time and without the need for traffic redirection. AED can manage volumetric DDoS attacks up to the capacity of your internet circuit.

AED can also detect and block IOC communication from hosts inside of your network to known malicious command and control centers on the internet. AED can decrypt encrypted traffic, on-premise, and inspect it for embedded attacks. Plus, AED's Cloud Signaling feature intelligently integrates with your cloud DDoS mitigation service or Arbor Cloud to automatically trigger upstream mitigations when an attack threatens to overwhelm your inbound internet circuit.

Additionally, many networks in today's interconnected world suffer from overexposure to attack and sometimes malicious traffic, even if they are not the target of that traffic. This increase in excessive and unnecessary traffic traversing the network edge can hurt the performance of devices designed to accomplish other critical tasks. This is particularly true of stateful devices in the security stack including IDS/IPS, WAFs, and most importantly Firewalls. DDoS attacks on Firewalls are the #1 cause of network outages today. This increased load on firewalls and other devices in the security stack leads to expensive capacity upgrades to maintain optimum performance levels in those devices. For more information: https://www.netscout.com/resources/quick-looks/protecting-firewall-capacity-with-netscout-arbor-edge-defense-aed

And finally, AED is continuously updated with NETSCOUT's own ATLAS® Threat Intelligence Feed enabling protection from the latest inbound and outbound threats.

Industry experts agree that a multi-layered DDoS defense strategy is the best practice to mitigate developing attacks of any size. For education institutions in the current landscape, it is a priority to protect the network at the edge first and then work toward augmenting that effort with additional layers of security outward as attacks evolve. With NETSCOUT Arbors 20+ years of innovation and improvement on the hybrid DDoS Defense approach, we can help you reach those goals while also attaining the lowest possible TCO.

## Summary

Educational institutions at all levels will have to come to terms with DDoS and cyberattacks in todays world that may never return to 90%+ in-person learning. Even if it does, both a student and teacher's reliance upon cloud-based technology, applications and services from the classroom or home will make education a high value target for attacks. Fortunately, there are powerful solutions to assist them in protecting their vital applications and services so teachers and students can be productive. Given the trends of the past year, starting with an on-premise security presence with NETSCOUT AED that complements your ISP protection is the smart first step. The good news is that no matter who your ISP may be, there is already a good chance they are using NETSCOUT technology for their DDoS mitigation service. And if you do not currently have Cloud based protection, we can provide that too with Arbor Cloud. The time to act is now to protect your students and teachers from the damage and disruptions of DDoS and cyberattacks.

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