

# Defending Educational Institutions Against High-Volume DDoS Attacks

DDoS attacks on educational institutions can have wide and significant impacts, from disrupting the availability of online educational resources such as virtual classrooms and online exams, to interrupting university research activities. It is critical for educational institutions, from K-12 to colleges and universities, to have effective solutions in place to stop these attacks quickly and minimize their impacts. The most effective protection against dynamic multi-vector layer 3-7 attacks is a multi-layer hybrid solution comprising both on-prem and global cloud-based protection.

## Threat

DDoS attacks in general have increased in both number and complexity in recent years. In the first half of 2023, NETSCOUT® observed a staggering total of ~7.9 million DDoS attacks, representing a 31 percent increase year over year. Attacks on educational institutions in particular have gained in frequency and effectiveness, with adversaries often employing automated attack generators.

NETSCOUT's DDoS Threat Intelligence Report for the first half of 2023 reported:

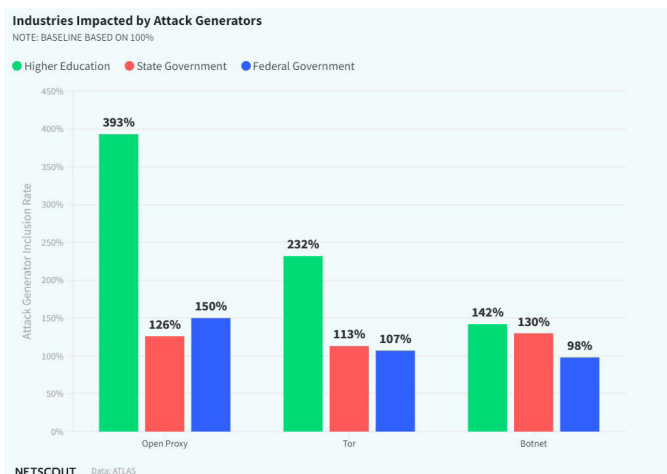
- Higher Education was the top industry vertical targeted by attack generators.
- Open proxies were consistently leveraged in HTTP/S application-layer DDoS attacks primarily directed toward the higher education and national government sectors.
- Botnets, open proxies, and Tor nodes display disproportionately high rates of activity in security events targeting institutions of higher education.

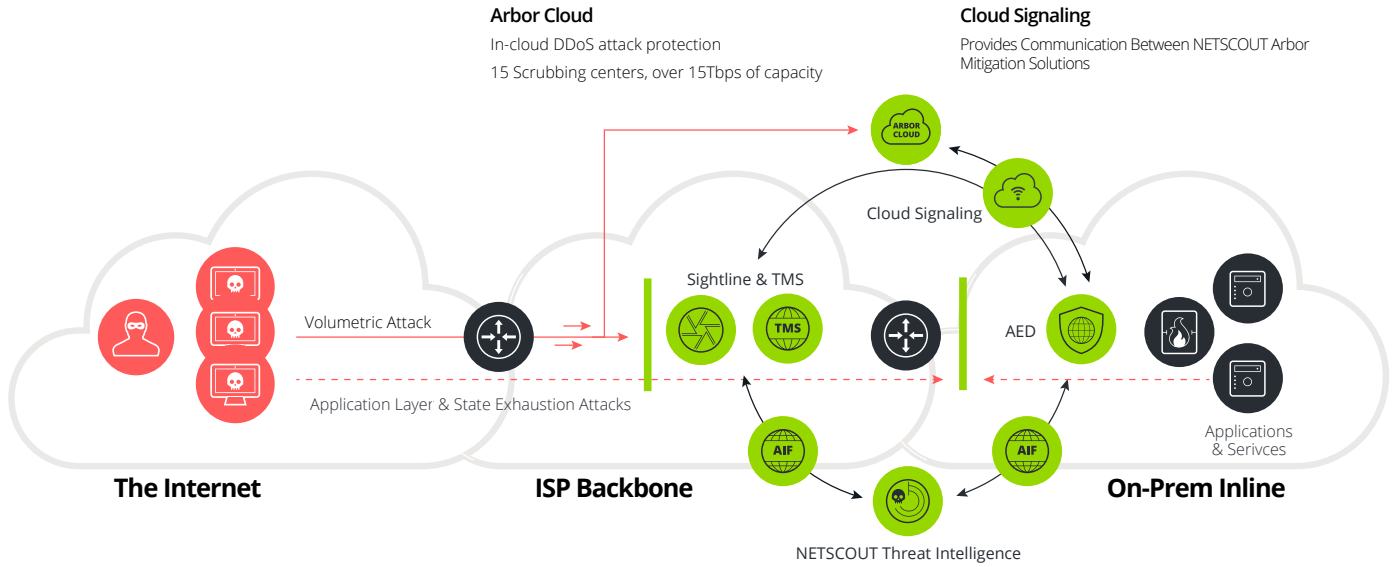
For university research facilities, the frequent transfers of large volumes of data require high bandwidth availability 7x24. This provides an attractive target for attackers. Online course delivery systems are also frequently attacked, and downtime for these systems can be highly impactful to both students and faculty.

The Standard Achievement Test (SAT) is going online for US students by mid-2024, providing a prime new target for DDoS attacks against K-12 institutions. (<https://blog.collegeboard.org/international-students-college-board-answers-your-questions-about-digital-sat>).

One notable attack occurred in May 2023, when Greece's Education Ministry said it was targeted in an attack described as the most extensive in the country's history. The attack aimed at disabling a nationwide high school examination platform. It said the DDoS attacks aimed at overwhelming the platform occurred over multiple days and involved computers from 114 countries, causing outages and delays in high school exams (<https://apnews.com/article/cyberattack-cybercrime-greece-school-highschool-ddos-9258842dbd84d67430cf5eb39999f93d>).

What's more, with today's readily available DDoS-For-Hire services, virtually anyone can launch an attack on the institution of their choice for just a few dollars.





**Arbor Cloud**  
In-cloud DDoS attack protection  
15 Scrubbing centers, over 15Tbps of capacity

**Cloud Signaling**  
Provides Communication Between NETSCOUT Arbor Mitigation Solutions

**Sightline and TMS**  
Automated detection, Out of Band, surgical mitigation (up to 400G); Can be 100% Virtual  
Used by many MSSPs for in-cloud DDoS protection services.

**NETSCOUT Threat Intelligence**  
Global Visibility and Threat Intelligence  
ATLAS Intelligence Feed (AIF) arms products with latest, global, actionable, threat intelligence.

**Arbor Edge Defense (AED)**  
Always-on, protection (up to 200G); from inbound and outbound threats (i.e. DDoS attacks and IoCs).  
Cloud Signaling upstream for large attacks.

## A Real-World Example of the Risk

A regional educational co-op in the U.S. with many locations and two different ISPs for redundancy came under a series of DDoS attacks that disrupted online learning for several days. They quickly determined they needed a better solution to protect their network, consolidate costs and bring everything under a single umbrella for operational efficiency.

They reached out and received emergency provisioning from Arbor Cloud, and the attack was mitigated within minutes. Once the situation stabilized, they switched their focus to deploying a complete and permanent solution for monitoring attacks across several sites, mitigating fast enough to avoid downtime, and aligning on a single solution provider.

## Solution

The educational co-op deployed NETSCOUT's Arbor Sightline for enhanced network visibility and threat detection and provisioned an Arbor Cloud service for on-demand mitigation. They placed 17 different subnets under the protection services of Arbor Cloud. The solution is fully integrated so that attacks can be detected and automatically re-directed to Arbor Cloud for mitigation without customer intervention.

Sightline monitors all traffic going to all sites. When it detects an attack, it signals to Arbor Cloud. Within minutes, traffic for the subnet under attack from around the world is re-directed to Arbor Cloud's 15 global scrubbing centers for mitigation. The clean traffic is then returned to the customer over two GRE tunnels for load balancing and redundancy.

Since the Arbor solution was deployed, several attacks have occurred, but online resources have remained available. They are seeing on average two attacks per month ranging from 2 hours to 9 days in duration. These attacks have included UDP amplification/reflection, botnet zombie attacks, and DNS query floods. In all cases, the attacks were detected by Sightline, re-routed to Arbor Cloud, and mitigated within a few minutes. Arbor Cloud can stop attacks from around the world and as close as possible to the sources so attack traffic doesn't even reach the customer's ISPs.

The Arbor Cloud Security Operations Center (SOC) worked with the co-op to create a custom configuration for DDoS protection. The SOC provides frequent service reviews to maintain consistency across all subnets and assets under protection and keep the configuration updated with the latest recommendations.

The co-op is now well prepared for online SAT testing expected to begin in the Spring of 2024.

**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](http://www.netscout.com/company/contact-us)