NETSCOUT

U.S. University Detects and Prevents DDoS Attacks with NETSCOUT Arbor Solution

OVERVIEW

The Challenge

- Planned technology upgrade, including cybersecurity and network solutions
- DDoS attack impacts university services on student move-in day
- IT needs quick solution deployment on existing infrastructure

The Solution

- Arbor Cloud™ for Enterprise
- Arbor SP
- Arbor Threat Mitigation System
- ATLAS® Intelligence Feed

The Results

- Multi-level DDoS protection with cloud and on-premises solution
- IT directly preventing DDoS application attacks with on-site Arbor solution elements
- 100G-compatible solution

Customer Profile

This historic U.S. university is known the world over for its long-standing commitment to academic excellence. The university's vast graduate and undergraduate programs have produced alumni who serve as leaders in international government, finance, industry, healthcare, science, and the arts.

A massive Information Technology (IT) commitment is needed to keep essential university services up and running, and this effort includes numerous departments delivering more than 200 business services to students and faculty. These IT services vary from infrastructure, unified communications and collaboration (UC&C), security and identity & access management (I&AM), research computing, professional services, and client computing oversight.

The Challenge

The university's IT team participates in an informal, regional collaborative, where their higher-education peers share knowledge regarding research & development, technology, or cybersecurity initiatives under consideration at their own institutions. The IT team knew they needed to refresh their technology baseline, and from these peer exchanges they gained a sense of how best to proceed with next-generation network, firewall, and cybersecurity solutions.

For those reasons, the IT team convened a series of roundtables and individual meetings with leading technology vendors to discuss how their respective solutions might interoperate in the university's environment.

Unfortunately, on their way home from one of these vendor meetings, the IT team learned the university had just experienced a volumetric DDoS attack that had consumed university bandwidth on a targeted service. With this DDoS attack coinciding with annual student "move-in" day, the IT team was turning to the cybersecurity vendor whose site they'd just left to discuss solutions that could quickly assist recovery efforts in the current university infrastructure, as well as prevent future DDoS attacks. Given the immediacy of this DDoS attack and their need to restore services quickly to returning to students, IT placed a premium on deploying a solution that could support its existing Cisco infrastructure, while also scaling to their 100G network environment.

Solution in Action

The IT team found both near-term relief from, and ongoing prevention of, DDoS attacks with NETSCOUT® Arbor quickly deploying a multi-layer solution that leveraged the university's existing infrastructure. The Arbor security solution protects against DDoS attacks that threaten availability, as well as advanced threats that could infiltrate the network. The university's DDoS Protection solution includes:

· **Arbor Cloud for Enterprise** – Provides integrated on-premise and Cloud-based mitigation for protection from the full spectrum of modern DDoS attacks. On-premise protection guards against state-exhausting attacks aimed at the security infrastructure of the enterprise. The Cloud-based global, multi-terabit, on-demand traffic scrubbing service defends against volumetric DDoS attacks that are too large to be mitigated on-premise.
· **Arbor SP** – Proactively detects network or service availability threats, quickly diagnosing and preventing misconfigurations, flash crowds, or malicious DDoS attack threats from impacting availability.
· **Arbor Threat Mitigation System (TMS)** – Automatically removes attack traffic without interrupting the flow of non-attack business traffic in the university's 100G network environment.
· **ATLAS Intelligence Feed (AIF)** – Provides policies and countermeasures that enable the university's IT team to quickly address attacks as part of an advanced threat or DDoS attack.

The Results

The university is better-safeguarding institutional assets (e.g., scientific research, student applications, financial and payment information, notification of admissions, issuance of grades, post-graduate work) by using the Arbor solution's capabilities to protect diverse resources from complex, blended DDoS attacks.

IT did not move ahead with solution selection without first consulting some of their peers at other institutions regarding their respective DDoS prevention solutions, with one informing them, "We have Arbor, we're fine, we use it everywhere."

As a result, the university is moving ahead with their plan to deploy best-of-breed vendor solutions as part of its technology refresh, with the Arbor approach offering integration with IT's preferred network and firewall choices.

The university is achieving increased collaboration among their Network Operations and Security Operations teams, with these IT resources using the Arbor solution as part of their everyday toolset.

The university is also taking control of addressing DDoS attacks at the local level with the Arbor solution, with the IT team taking advantage of their on-premises elements to address emerging threats without the need for vendor consultation.

The Arbor on-premises solution elements are particularly useful in addressing application attacks that Cloud-only vendor approaches would have difficulty detecting.

LEARN MORE

For more information about Arbor DDoS Protection solutions, please visit:

https://www.netscout.com/ddos-protection.

NETSCOUT®