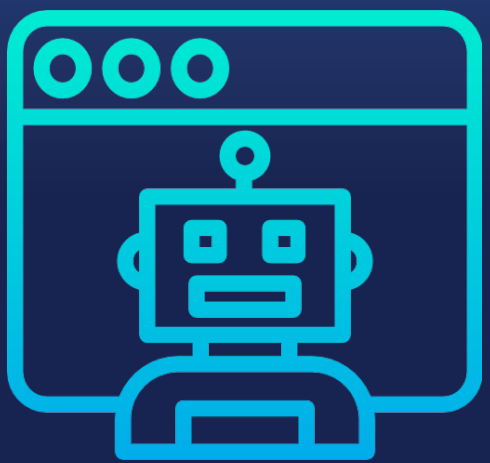

# Advanced Protection from sophisticated bots

## Overview

Digitalisation and the thrive to enhance transparency in education has pushed universities to adopt cloud solutions for their data. One of our clients, i.e. an International University based out of the USA was also facing a similar transformation in their system. Earlier, the website was made on premise and had faced various AI bot attacks, blocking various portals and disrupted operations for a whole week. From then onwards, the IT team was always asked to stay on-guard and had to work even overtime during peak times like admissions and examinations. This also peaked their security development costs. No sooner did they realize the dire need of a single and automated solution that could mitigate continuous bot attacks and could combat other malicious attacks as well. It was after all, a matter of their rapport as well.

## The Challenges that they experienced

The on premise solution that they had wasn't actually able to handle large data loads that was coming during peak times and ultimately was a sign that it needed something robust and fast to run smoothly. The advanced attacks they had faced also couldn't be controlled well with the existing solution. Also, the IT teams were just overtaxing themselves with no efficient security outputs.

One of the bot attacks had hacked their websites during admissions and the management had to face the hardships of the disrupted website that lasted for days. Later on, it was found that it was a BotKit attack. The management declared the need of some external help and contacted Prophaze.

After a detailed meeting, Prophaze team could get insights into various incidents the university had faced. Since, Prophaze facilitates equal protection to K8s, cloud, and on premise, it could provide a fully integrated solution that is designed on a massive platform.

## How Prophaze could help?

Prophaze Bot protection Solution is fighting against other ML based malicious bots and it blocks targeted and automated attacks against web APIs and applications from sophisticated bots that penetrate corporate defenses.

Prophaze will send a reset to the bot connection on a regular basis and re-route the traffic and fake the bots in an infinite closed loop, once it detects any bot activity. This helps to reduce the time, skill and cost needed.

Prophaze WAF is easily deployed On-Premises on AWS, Google Cloud, and Microsoft Azure also have several advantages including flexibility, cost-effectiveness, scalability, accessibility and many others. The easy-to-configure dashboard is very user-friendly and customizable and the deployment took just a few minutes. Also, customers can review their domain health check status in real time with help of infographic representations.

Prophaze On-prem WAFs are usually placed close to the application, therefore can proactively block threats with the help of IP reputation and also using threat intelligence. Prophaze protects the organisations from such attacks with the help of their advanced security research activities.