AKAMAI CUSTOMER STORY

# Tokyo Medical and Dental University

TMDU improves its security posture with Secure Internet Access Enterprise

## Akamai helps university significantly reduce internal and external security alerts

When an organization undertakes a major network transformation project, securing the infrastructure and protecting users in the new environment needs careful consideration. This is precisely the situation that the IT Development Section at Tokyo Medical and Dental University (TMDU) faced after upgrading its network in 2017. This team is responsible for operating and managing the network covering the Yushima, Surugadai, and Kounodai campuses. They also manage the guest Wi-Fi in shared spaces throughout the university and oversee more than 6,000 users.

Initially, the team determined that deploying unified threat management appliances with firewall, URL filtering, and email filtering capabilities would provide the level of protection required in this new environment.

## The limitations of firewall-based protection

Despite the upgrade to the university's security architecture, the team saw a dramatic increase in the volume of targeted malicious emails that reached users' in-boxes.

"As well as the usual phishing emails asking people to change their ID and password, or pretending to be from a delivery service, we started seeing targeted emails that looked as though they came from the university's IT support team," says Kazuya Sato, Director of the Administrative Division of the Institute of Information Technology and Division Head of the IT Development Section.

Most of these emails contained URLs that redirected recipients to phishing sites, resulting in multiple firewall alerts. In addition, reports of suspicious emails came flooding in each day from students and staff. The IT team was responding  to and investigating hundreds of security alerts each month.

TMDU
TOKYO MEDICAL AND DENTAL UNIVERSITY

**Tokyo Medical and Dental University**
Tokyo, Japan
www.tmd.ac.jp

**Industry**
Public Sector

**Solution**
Secure Internet Access Enterprise

**Key impacts**

- Improved overall security posture and complemented existing security solutions with additional layer of protection
- Reduced internal and external security alerts
- Proactively identified and blocked targeted phishing attacks

"We used to think we could just block malicious IP addresses with the firewall. But targeted emails aren't that simple anymore. These days, the IP addresses of the embedded URLs change dynamically," says Kozo Takase, Professor and Division Head of the Division of Information Infrastructure and Security at TMDU. "And when the IP address changed, we could lose protection. In other words, there was a significant risk that the threat would get past the firewall. What's more, we weren't able to get a firm idea of how frequently this was happening."

The IT Development Section felt that the existing security measures had gaps, so they embarked on a project to add an additional layer of protection. While researching possible solutions, the team learned of a security approach that inspected recursive DNS queries — using DNS as a security control point.

"Since the firewall couldn't stop these malicious transactions, we thought it made sense to go one step earlier in the kill chain and block it at the DNS level. The logic checked out, but the question remained as to whether it would actually work effectively, so the only way to find out was to try it," says Takase.

In addition, using DNS as a control point would allow the university to inspect and control HTTPS web traffic without the complexities of decrypting that traffic in their firewalls.

## Proving effectiveness with a proof of concept

The IT Development Section evaluated a number of available solutions, including Akamai Secure Internet Access Enterprise. As the team was considering its options, Akamai informed them that the university could try the service with a free proof of concept (POC).

"When we first heard about Secure Internet Access Enterprise, it was a bit of a black box situation for us. We weren't sure what was involved. We didn't want to just blindly implement something we weren't 100% sure about, so we felt we needed proof of its effectiveness first," says Sato.

## The POC detects thousands of threats

As soon as Secure Internet Access Enterprise was activated, it highlighted a multitude of malicious DNS requests being made from the university's network.

"We were seeing thousands of malicious requests every day," explains Masanori Nasu, Technical Specialist in the IT Development Section. "I was taken aback, to be honest. We were expecting tens, or maybe hundreds at most."

The team was initially skeptical about the volume of malicious requests being flagged, but after investigating the requested domains, it became clear that the majority were in fact phishing sites or malware drop sites.

The IT Development Section was convinced of Secure Internet Access Enterprise's reliability and decided to broadly deploy it right away. "We could sense risk was heading our way, so there was no debate about whether we should adopt Secure Internet Access Enterprise. It was more a question of when, rather than if," says Takase.

> “
>
> We used to have to check if we had received an external alert about once every hour, even after leaving the office. But there's no need to do that anymore.
>
> **Masanori Nasu**
>
> Technical Specialist, Tokyo Medical and Dental University

## The results

After fully adopting Secure Internet Access Enterprise, malicious traffic that the firewall had been unable to identify was detected and securely blocked. And by stopping the threats at the DNS level, the number of threat alerts from the firewall decreased dramatically — down to just a few per month.

What's more, prior to deploying Secure Internet Access Enterprise, the university received numerous threat warnings from external institutions about malicious traffic exiting its network. After activating Secure Internet Access Enterprise, months went by with no warnings at all. "We used to have to check if we had received an external alert about once every hour, even after leaving the office. But there's no need to do that anymore. Our primary goal has been achieved, and we're very happy with that," says Nasu.

And while there had been some concern about switching the university's DNS traffic over to Secure Internet Access Enterprise, the transition was seamless because of the scale, capacity, and resilience of the Akamai Intelligent Edge Platform.

Secure Internet Access Enterprise was also cost effective for TMDU as Akamai offers a special license for universities. "We managed to gain approval thanks to the POC, which showcased Secure Internet Access Enterprise's effectiveness at blocking threats and heightening security," says Sato.

"There are a lot of universities with environments similar to ours — they just haven't realized [their risk exposure] yet. Adopting Secure Internet Access Enterprise is quick and easy. It can be done by simply changing your recursive DNS over to Akamai, with no other changes needed. There are very few aspects of Secure Internet Access Enterprise that overlapped with security measures we already had in place, so I really think other universities should consider Secure Internet Access Enterprise," says Takase.

TMDU
TOKYO MEDICAL AND DENTAL UNIVERSITY

TMDU was founded in October 1928 as the Tokyo National School of Dentistry. After merging the studies of medicine and dentistry at Yushima Shoheizaka, a hallowed site of learning, the institution became Japan's only university with a graduate school of both medical and dental sciences. It pursues cutting-edge medical practice and cultivates professionals with knowledge and humanity. The university aims to rear compassionate and scientifically-minded doctors, dentists, nurses, medical scientists, dental hygienists, and dental technicians. It strives to cultivate preeminent medical staff and researchers, and to widely contribute to people and society, while building a research and education system in the field of medicine and life sciences. http://www.tmd.ac.jp/