CLOUDFLARE

CASE STUDY

# Major U.S. state university ensures eLearning security and availability in partnership with Cloudflare

## Cloudflare's modern application services help the university focus on students' outcomes

### Background

With more than 21,000 students enrolled, a premier state university embraced eLearning more than 15 years ago. It began with a learning management system (LMS) deployment, used initially for online homework submissions. Since then, its role has expanded to distance learning, and today some courses are available exclusively online. Therefore, the system's continued uptime and performance continues to be a top priority.

### Challenge: Ensuring availability and security of eLearning platform

The university's Information Technology Services (ITS) team is proud of its history of adopting new technologies that enable student success, but they were also acutely aware of the risks: cyber attacks, traffic spikes, and operational problems that can cause disruption.

In 2010, ITS initially addressed the uptime and performance risks with appliance-based local load balancers – their best option back then. However, like many on-premises technologies, these boxes arrived with the burden of installing, managing, maintaining, patching, and updating them. For this small, 30-person team responsible for the university's entire technology infrastructure, it was costly and time-consuming to keep them running. Every update consumed about 30 hours of testing and deployment, and rollouts were only permitted during green zones in the middle of the night.

As the appliances approached their end-of-life, the ITS team seized the opportunity to modernize their entire approach – not simply replicating existing functionality. By adopting cloud-based solutions, they could radically improve security and availability of the eLearning platform while reducing costs and operational effort, freeing them to focus on the university's highest priorities.

### Key Results

- Eliminated 30+ hours of load balancer management per month
- Enhanced web application security with built-in Cloudflare Web Application Firewall (WAF)
- Improved application accessibility secured by Cloudflare Access

## Cloudflare load balancer improves efficiency and ease of use

As the ITS team evaluated cloud-based technologies, ease of use emerged as a critical factor. When they saw Cloudflare's intuitive management interface, they were impressed at how fast and easy configuration and administration became. It also enabled them to delegate app migration to application owners who never touched the old system.

ITS was also excited about how Cloudflare readily supports multi-cloud strategies, which enabled them to offer enhanced availability guarantees to the university. With Cloudflare, they can easily direct traffic wherever it needs to go. And in total system failure scenarios, they can seamlessly shift critical applications to warm stand-bys in the cloud.

## Protecting public-facing systems against cyber threats

The LMS is one of many public-facing applications at the university, and the security team updated its requirements to ensure that all traffic flows through a web application firewall (WAF) before reaching the load balancers (and applications). With the appliance-based load balancers, re-architecting to meet this requirement would have been a major challenge. Addressing this requirement became another top priority for ITS, and another key reason why they selected Cloudflare.

Cloudflare's global network provides ITS with private network load balancing capabilities to secure Internet traffic through WAF and then sends the traffic over secure tunnels to their infrastructure without re-architecting, essentially snapping easily into their existing environment.

Shortly thereafter, the Log4j application vulnerability was discovered, and put Cloudflare to the test. The vulnerability affected several of the university's applications and, if exploited, could allow attackers to steal credentials, data, and distribute malware. With Cloudflare, the university quickly wrote and deployed a custom rule to detect and block any potential exploits.

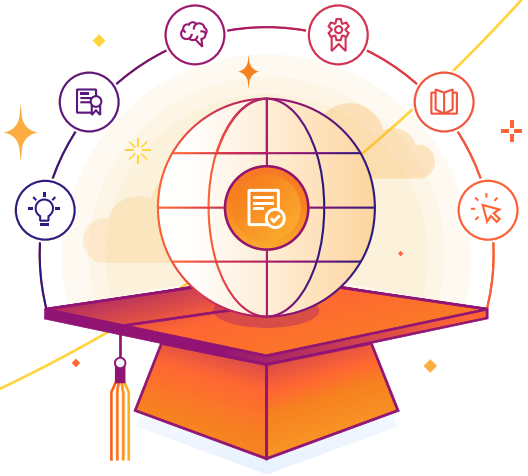
Then they learned that Cloudflare had already taken care of it, deploying that rule for all of its customers in about the same timeframe. ITS was delighted to learn that Cloudflare is always vigilant, detecting a wide range of attacks across its global network, and preventing them from reaching its customers.

## Supporting zero-trust initiatives and user experience

While the university's initial focus was on meeting its short-term requirements for a load balancer and WAF, it was also looking for an innovative approach that could support its future needs and improve its security and user experience. Cloudflare Access plays a central role in the university's Zero Trust security strategy and plans to streamline access to its applications and systems.

One example is an application used for residential maintenance requests. Historically, they managed access by requiring users to be on the university's network. However, students wanted to be able to place requests via their smartphones. With Cloudflare Access, the university could make the application accessible from anywhere, but perform authentication before students reached the application.

By working toward a Zero Trust security strategy, the university continues its history of proactively identifying and adopting solutions that provide next-generation security and user experience for students and educators.





REV:BDES-7215.2025APR15