

Top 5 reasons why a modern WAF is critical in higher education

Your institution's reputation takes decades to build, but can be seriously damaged in an instant by a security incident. A modern Web Application Firewall (WAF) is vital component of your cyber program to keep web applications secure – an important protective layer that helps shape public perception of educational institutions.

Top 5 reasons to deploy a modern WAF in higher education

1	Protect sensitive student and research data	Universities store vast amounts of personal information, including student records, financial aid data, health information, and valuable research. A WAF helps prevent data breaches through SQL injection, cross-site scripting, and other application-level attacks targeting these sensitive assets.
2	Defend against targeted attacks on academia	Universities are increasingly targeted by sophisticated threat actors, including state-sponsored groups seeking research data. A WAF provides specialized protection against advanced persistent threats specifically targeting academic institutions.
3	Secure diverse, decentralized IT environments	University networks are uniquely challenging to secure due to their decentralized nature across departments, research labs, and administrative offices. A WAF provides consistent security across these varied environments without requiring standardization of underlying systems.
4	Keep intellectual property confidential	Universities produce valuable intellectual property through research that attracts sophisticated attackers. A WAF helps protect research data, patent information, and proprietary methodologies from theft through web application vulnerabilities.
5	Comply with industry regulations	Universities must comply with regulations like FERPA, HIPAA (for medical schools), PCI DSS (for payment processing), and CMMC (for government research). A WAF helps maintain compliance by preventing unauthorized access to regulated data through application vulnerabilities.

Why universities choose Cloudflare WAF over the competition

The higher education community selects Cloudflare WAF because it effectively uses threat intelligence and machine learning powered by platform intelligence from the Cloudflare connectivity cloud to stop the newest threats, including zero-days, OWASP Top 10 threats, account takeover attempts, malware file uploads, and many more.



Block common attacks like XSS & SQL injection

Cloudflare uses core OWASP Top 10 rules to block the most widespread layer 7 attacks.



Stop credential stuffing attacks

Cloudflare prevents, detects and blocks the use of stolen or exposed user login credentials.



Detect malware in uploaded files

Cloudflare scans files as they are uploaded to protect your sites from harmful content.

What our customers are saying

"With the Cloudflare platform, we're getting very high-powered, very technical [application security] detection and protections that take little to no effort to deploy — that's especially important for our organizations that already struggle with limited resources."

Deputy Director and Interim State CISO
State of Arizona

Cloudflare named a Leader in "The Forrester Wave™: Web Application Firewall Solutions, Q1 2025" report



Cloudflare has been recognized as a Leader in ["The Forrester Wave™: Web Application Firewall Solutions, Q1 2025"](#) report. Cloudflare received the highest score in the current offering category.

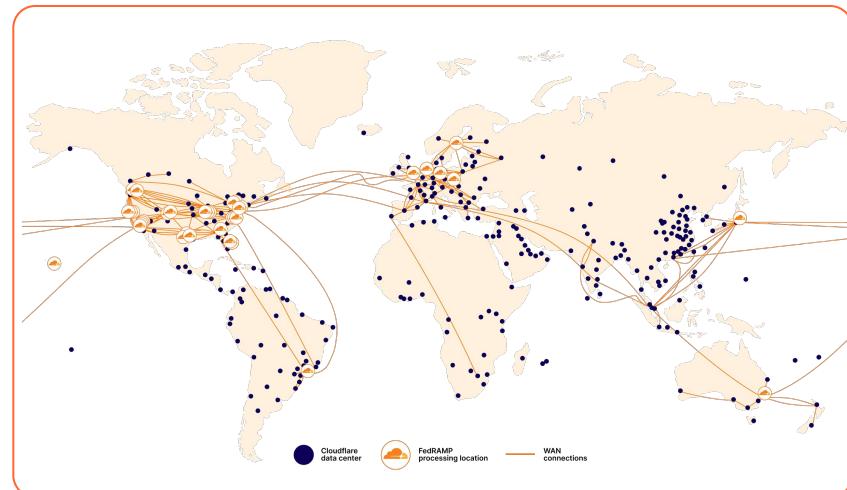
Cloudflare views this recognition as validation of our platform approach to security, aligned to user workflows and built to deliver broad-based mitigations. Cloudflare's WAF, as part of our integrated Application Security solution, provides organizations with DevOps-friendly, comprehensive application protections enhanced by machine learning and threat intelligence.

According to the report, "Cloudflare is a strong option for customers that want to manage an easy-to-use, unified web application protection platform that will continue to innovate."

The Cloudflare advantage over any other approach

One global cloud network unlike any other

Only Cloudflare offers an intelligent, global cloud network built from the ground up for security, speed, and reliability.



32

FedRAMP processing locations across 11 metro areas and growing

335+

cities in 125+ countries to serve data locally

227B

cyber threats blocked each day

20%

of all websites are protected by Cloudflare

~50 ms

from 95% of the world's Internet-connected population

150+

AI inference locations powered by GPUs

FedRAMP Moderate authorized and committed to High



Innovation everywhere

Our [unique approach](#) to authorization ensures every innovation is available everywhere – including FedRAMP processing locations



Continuous investment

We're [expanding our FedRAMP locations](#) both within the US and internationally to strengthen security and performance around the globe



Agility always

We're deploying tomorrow's requirements today, like [post-quantum cryptography](#), to secure your mission today – and tomorrow



Next stop: FedRAMP High

We [announced our intent](#) to pursue FedRAMP High as part of our long-term commitment to the federal government

Universal Advantages

As the world's first connectivity cloud, Cloudflare delivers differentiated capabilities that have earned the trust of millions of customers around the globe.

Significant Cost Savings

- Vendor consolidation
- CapEx offload
- Administration

Threat Intelligence

- Extensive visibility
- Threat models
- Intercepted attacks

Data Localization

- Data restriction
- Compliance
- End user privacy

Simplicity and Ease of Use

- Dashboard
- Integrations
- Automation

How can we help you secure your web applications?

Learn more about [Cloudflare for Education](#), or [contact us](#) today.

1 888 99 FLARE | cloudflare.com/public-sector