Online learning is here to stay, and it’s imperative for education technology companies to make sure their platforms are secure. Here’s how the right technology partner can help.
Overview

As the world moved online at the start of the global pandemic, education technology (or edtech) platforms had to adapt fast, to not only deliver consistent user experiences across multiple devices — regardless of geography or connection speeds — but also scale quickly, with about 93% of households using some form of online learning.

With the help of modern content delivery networks (CDNs), forward-thinking edtech companies were able to scale their online experiences fast. But there's another area the right CDN can help edtech companies with, and it's one that K–12 IT leaders said is top of mind, according to The State of Ed Tech Leadership in 2020 — security.

Education ranks third in the top targets of security breaches, making up 13% of all data breaches.*

* https://www.1rti.com/the-importance-of-information-security-in-education/
Security threats facing edtech companies

The education industry is attractive to cyber criminals because of the volume of data most companies hold, including financial data, alumni databases, supplier details, research data, etc. for both students and staff. In a recent attack, hackers attempted to extort a university system by threatening to sell stolen information including social security numbers and bank account information. In general, ransomware attacks against higher education institutions are up 100% year over year, with an average ransom of $447,000.

A lack of funding and technology personnel have left the education sector with security gaps like unsecured networks, unchecked BYOD by staff and students, and outdated APIs, gateways, and connections for accessing accounts, learning portals, SaaS applications, and school systems. Now, with massive online learning, these gaps can be even more damaging, and schools are quickly realizing that they need the knowledge and updated technology infrastructure to continue virtual learning securely.

Successful educational technology breaches have included:

- **Account takeovers**: Hackers can take over accounts of teachers and students to obtain financial info, send phishing emails to other contacts, and gain access to more accounts and information.

- **Data loss**: Hackers can destroy school records once they have access. They’ve also been known to redirect contractor payments to dummy accounts that the hackers control and use employee information to steal tax returns. On a personal level, students, staff, and parents can face identity theft, a problem that can take years to resolve.

- **Classroom and learning disruption**: Whether students are unable to access online lessons or teachers are unable to prepare and present online lessons, the disruption to the classroom and learning opportunities is a significant problem.

- **Extortion**: Ransomware attacks have resulted in financial losses on already strapped districts

Most attacks are directed at the application layer (layer 7) and happen through public-facing apps and APIs. Luckily, the right content delivery partner can help prevent these attacks as edtech companies move through their digital transformation.

The Center for Digital Education says these are the major cybersecurity challenges facing higher education:

- Phishing
- User Education (Cybersecurity Awareness)
- Cloud Security
- High-Profile Information Security Strategy
- Next-Generation Security Technology Planning
- Identity and Access Management
- Governance Over Data Security
- Unsecure Personal Devices
# Mitigating threats with a CDN

As digital transformation occurs in education, schools and online education platforms need cybersecurity processes and technology that actively evolve with the “new normal.” Implementing vulnerability management, patching procedures, multi-factor authentication, and anti-virus software, as well as disabling scripting environments and macros are all solid techniques to stay protected. Administrators must be proactive in creating a security plan that informs teachers, administrators, employees, and students/users of their platforms and sites.

When it comes to working with technology partners to ensure security, there are a few key considerations for administrators as well. They should:

- **Employ a next-gen web application firewall (WAF)** to provide app and API protection everywhere. If an origin is constantly bombarded with a lot of requests, it affects the health and performance of a site in the long-term. However, not all WAFs are created equal, and with limited resources, admins should look for a solution that doesn’t need a full-time employee for WAF tuning or block legitimate traffic with false positives.

- **Employ real-time log data** as part of your observability pipeline to be used for 24/7 monitoring of abnormal behavior, alerting you to threats including account takeover. Ensure that security policies can be updated in real time to address threats and vulnerabilities.

- **Employ a CDN with built-in security** across its network to protect their origin from unnecessary hits and malicious traffic. Modern CDNs provide protection against sophisticated DDoS attacks without sacrificing performance for protection by leveraging their entire network as a scrubbing center.

- **Use transport layer security (TLS) encryption** to secure information that travels between their origin and end user to ensure that information the user supplies (usernames, passwords, financial information, the names of web pages visited, etc.) cannot be read, modified, or destroyed by any third parties. Modern CDNs can reduce the round trip times and the total performance costs of TLS handshakes with TLS termination located closer to students.
THE FASTLY SOLUTION

It’s not just about ensuring you’re delivering a fast, always-on experience. Protecting privacy is crucial to the brand, reputation, and user experience of institutions and edtech platforms, and the right technology provider can help.

In addition to improving performance and reducing bandwidth costs, Fastly secures connections and authenticates at the edge to help block malicious traffic and keep student data safe. Explore how we can help you exceed user expectations and student needs by delivering high-performance, secure learning experiences at scale.