Deep Security Solutions for Web Applications in Higher Education

Scale and precision for your institution’s growing list of web applications
The expansion of online learning and operations

2020 completely changed the way higher education institutions run. Everything from teaching students to running operations to conducting research were affected by the necessity to support remote work. Higher education institutions are learning that was just the beginning: now they must address securing apps and access.

Many universities first allowed access to school IT systems and applications via virtual private network (VPN) connections. This was a quick way to get users back into the university systems, but VPNs require distribution, installation, and maintenance of VPN clients and an upgrade to VPN infrastructure. With so many active connections, the systems slowed down considerably.

Universities also saw a drastic rise in potential attack surfaces and opportunities for cyber-attacks. Devices continue to evolve as the underlying application components evolve and changes occur with every software update. With each person using multiple devices (laptop, phones, tables, etc.) at any given time to access the university, the VPN system experiences further strain, and the chances of threats rise exponentially. How is a small university security team to keep up?

And, the threats are more and more advanced. The Open Web Application Security Project (OWASP) Top 10 represent the most critical web application security threats, including injection, broken authentication, and sensitive data exposure, but there are other threats, risks, and vulnerabilities beyond that scope. Breaches can happen fast—87% take place in just minutes—and most go undiscovered for months or more.

In this eBook, learn how pivoting to cloud-based applications secured by web application firewall, or WAF-as-a-Service (WAFaaS):

- enables rapid growth
- saves time, money, and resources
- protects the institution’s network, students, faculty, staff, and researchers.

6. Ibid.
Universities have specific use cases for protecting their increasing web apps

With the onset of precautions from the pandemic at the beginning of 2020, and a swift shift to online learning, there was a clear need for tools to keep operations and learning going. The three main user groups for the university's systems are students, faculty/staff, and researchers. There were different challenges for each group.

For students, accessing classes was challenge number one.

- Accessing information systems in the school's environment, such as the library, needs a little more finesse to connect with. Deploying web applications in the cloud leverages the cloud infrastructure and avoids straining the university network causing slow-downs or unavailability. For students, keeping a second layer of security with multi-factor authentication (MFA) has helped applications and devices stay that much more secure.

Faculty and staff need access to all the systems they had while working on campus.

- Faculty and staff manage a large amount of personal identification information (PII). Applications such as enterprise resource planning (ERP), payroll and budget systems, and compliance reporting are some of the vital systems that must be accessed and protected. Further, these systems may previously have been secured with the assumption they would be accessed only from within the university’s infrastructure.

Research teams need a higher amount of compute and storage capacity.

- VPN wasn’t the best choice for all the users the university supports, especially for research teams. Research projects can have large amounts of highly sensitive data to manage and protect. These datasets and existing applications may have been built assuming robust connections within the university network infrastructure.

- Outside parties and nation-states stealing research is very common, so protection from outside forces is paramount. A web application firewall (WAF) system protects the data and allows for easier access on the Amazon Web Services (AWS) Cloud.

Getting these user groups access to the university was priority number one. But this needed to happen quickly, and production of web-based tools built with readily available open-source and COTS (commercial off the shelf) components were the best tools to meet that need for a rapid shift.
Challenges of rapid web development

The rapid development of web apps brought other challenges. As independent groups within the university accelerate the deployment of new code using DevOps methodologies, security teams can struggle to keep up and must keep pace with potential attack surfaces that are changing and evolving more rapidly than ever before.

Many apps are developed using a distributed responsibility, with several constituent organizations involved. Security teams need to have visibility and enforce a consistent security posture as apps are created. Even if all the different apps have security controls in place, they could potentially be different, creating a management nightmare and a nearly impossible situation for the security team to get a full picture of how secure each application is. Any lag in deployment and some organizations may not want to wait. They may choose to launch their apps eschewing security best practices. This creates the possibility of unsecured apps and exposed information.

The net learning: the process for onboarding and launching applications has to be easy to manage for both the owner of the application and the security team.

An East Coast university enabled security for many applications with FortiWeb Cloud on AWS

If the effort and process to stand up a security function is too cumbersome, teams will try to work around you, rather than with you.

An East Coast university wanted its security team to provide an easy service to its users. With dozens of departments responsible for different kinds of work, they all needed a standardized security control in front of the web apps they were creating.

The IT department didn’t have control of the apps, but was still required to supply a layer of security. The security team used delegated administrative roles to assign an owner in each department to care for each app. If there is an issue, a person who understands the application could go in and set exceptions. Then, the security team didn’t have to be the responsible single point of contact for all the work. With many applications being launched, it would be nearly impossible for them to understand all requirements and details for the different applications.

Now, teams wanting to deploy an application don’t have to go through a laborious process to get approval from IT and wait for WAF infrastructure to be deployed. They can simply request the security team to provision the application in FortiWeb Cloud, removing barriers that slow down or stall application deployments.

With a delegated admin reporting information back, FortiWeb Cloud provided a single place where the IT team can get full visibility across what was happening with all the applications from a security perspective—still allowing individual application owners to set policies. Further, the university applied a bandwidth-based pricing model, which allowed the security team to pass the security cost of maintaining each application back to the application owner’s budget.
How a WaaS helps ease quick growth for your web applications

The main priority for the university's security team is to secure mission-critical web applications and data. Web applications are a more efficient way for a school to communicate with and enable students, faculty and staff, and research teams. Web apps fuel productivity, whether it's schoolwork, record keeping and tracking, or housing and accessing research. Web apps also help your IT department, too.

By developing a web application, or moving a program to a cloud provider, universities no longer put strain on the system with increased VPN traffic.

Web apps can also enhance security and protection. Web apps can employ a two-factor authentication for added protection. This is important as users are logging in over public internet service providers, and users with multiple devices, however 2FA by itself is insufficient.

The attack surface of a modern web application isn't just the web interface. Modern applications may expose APIs to support today's highly interactive applications and to let a wide range of mobile devices consume information for use in mobile applications. WaaS provides protection for web applications as well as API interfaces. API abuses will become the most frequent attack vector by 2022.¹ Because APIs access underlying data, there is a vulnerability. Good defenses against this include looking for signature-based attacks, rate limiting, and managing API keys for service to service communications.

Since API interactions are more defined, you need the ability to validate input against XML schema (or JSON schema) and make sure that content that doesn't fit that definition never reaches your application. Validating input allows you to keep the security function and block malicious interaction before it reaches the application. This saves on resources and provides a higher level of protection than trying to accomplish it in the application.

With an effective WaaS you enable faster deployment, advanced security, and minimize disruption to the user experience.

¹ Maria Korolov, "What you need to know about the new OWASP API Security Top 10 list," CSO, November 14, 2019.
FortiWeb Cloud offers superior performance at the scale universities need

Designed for web applications that demand the highest level of protection, FortiWeb Cloud provides robust security that is simple to deploy, easy to manage, and cost effective. This is ideal for a university that needs to keep personally identifiable information (PII) secure, while also providing easy and reliable access to information and learning.

Strength in threat detection

FortiWeb Cloud offers advanced, web application firewalls (WAF). With the ability to control policies, your WAF protects the information on the application and prevents any unauthorized manipulation of the data on the app—especially important for research teams. It determines what traffic is safe and what traffic is malicious. It safeguards applications from vulnerability exploits, bots, malware uploads, distributed denial-of-service (DDoS) attacks, advanced persistent threats (APTs), and zero-day attacks.

Cost-effective deployment and faster updates

The service is subscription-based, so you pay for what you use, allowing most organizations to move their budget from a capital expenditure to an operational expenditure. It allows for delegated administration, acknowledging that application owners are in the best position to manage exceptions and permissions. They understand the application, its data, and its users.

DevOps teams benefit from the machine learning (ML) model for code testing, allowing new code to launch quicker while still blocking threats. It can monitor how the application is evolving, how it’s being used by users to further inform the ML model. It’s more accurate, reduces false-positives, and code is released faster.

Comprehensive visibility

You can deploy a consistent security posture across multiple applications, and automate security capabilities across existing web applications. FortiGuard Labs detect new exploits and potential threats and updates FortiWeb Cloud to be prepared for those threats.

Easy management

For non-security professionals, FortiWeb-Cloud comes with a setup wizard and a default configuration that can be easily modified to meet individual requirements. There are predefined templates for common open-source applications like WordPress and consumer-off-the-shelf (COTS) applications such as SharePoint.

Busy security teams and DevOps staff can access an intuitive real-time dashboard that allows them and other non-security professionals to quickly see and understand the security status of their web applications. Machine learning automatically adapts with your application and eliminates the need for manual tuning.
This new model for operating a higher education institution is likely not going away soon. Universities will need to create a system in which teaching can be done anywhere, anytime, on any platform. The long-term goal should be to move applications to a cloud-based environment, and that could be as simple as changing where the application is hosted.

With AWS infrastructure you don't have to build or manage it. Leveraging multiple AWS Regions provides strong availability, offers cost-effective data transfers, controls excessive latency, and provides a consistent compliance environment. Unlike VPN, the AWS Cloud environment allows for easier scaling, as departments are building applications faster and faster, and pay only for what you use; there is no costly hardware or software to maintain. Automated security tasks make it easier for your security team to work closely with DevOps teams to create and deploy code faster and more securely. FortiWeb Cloud runs inside the robust, serverless AWS infrastructure with a variety of protections. AWS has great controls for volume metrics attacks meant to overwhelm the infrastructure so FortiWeb Cloud can focus on logic based attacks. And detailed identity and access controls combined with continuous monitoring for near real-time security information ensures that students, faculty and staff, and research teams have the right access at all times.

FortiWeb Cloud provides the security for web applications and APIs within the AWS Well-Architected Framework. It provides content delivery network (CDN) capabilities at no additional cost. AWS AI/ML services help identify anomalies by monitoring how the application is being used. Within the AWS environment, FortiWeb Cloud ML identifies the potential for new threats and implements changes.

Protect your university's applications and users with the reliability of the AWS environment, and the security of an advanced WAF with FortiWeb Cloud.

Learn more about FortiWeb Cloud