Signal Sciences

Chick-fil-A Protects Digital Transformation Assets with Automated Web App Security

CHALLENGE

Chick-fil-A needed a flexible and effective web application security solution to protect key assets of their digital transformation strategy, including consumer-facing mobile and web apps that improve customer satisfaction and drive revenue growth.

Chick-fil-A, Inc. operates 2,400 restaurants in the United States with combined annual revenues of over $10 billion. Mobile and web applications that allow customers to place food orders are critical to both improving customer satisfaction and Chick-fil-A's growth. But the incumbent legacy WAF that depends on pattern matching rulesets was not up to the task in a development lifecycle where distributed software design and deployments are the norm. This meant finding a future-ready Web Application Firewall that installs easily across distributed architecture and effectively prevents account takeover (ATO) attempts and other attacks on those public-facing apps in production.

> "The model of blocking based on pattern matching such as a specific SQL-injection string won't work for us in the future. Signal Sciences provides more context and visibility at the app layer and makes more precise blocking decisions to stop bad web requests."
>
> **Robert Davis,** Director of Cybersecurity

SOLUTION

Davis and his team chose Signal Sciences for both the ability to provide extensive context for web request blocking decisions and being easy to deploy. With a distributed agent model that protects code where it operates, Signal Sciences is also future ready for any infrastructure or architecture. Moreover, Chick-fil-A's application footprint will merge and become a hybrid of Amazon Web Services and managed data centers: Signal Sciences is ready to protect their web assets in such hybrid environments.

Davis found Signal Sciences ease of deployment, low maintenance overhead and built-in detection and blocking capabilities provided effective protection against web application attacks—all without impacting app performance or dedicating a full time staff member to maintain the solution.

Effective account takeover prevention without impacting app performance

The Signal Sciences agent instruments and observes Chick-fil-A's consumer-facing user authentication flows in their mobile and web apps. This provides Chick-fil-A's Engineering and Security teams the visibility necessary to stop account takeovers without impacting application performance—and without the rules maintenance and tuning legacy WAFs require.

Easy to deploy and use in any architecture—and at the network edge

Signal Sciences can deploy within any architecture and with our Power Rules feature provides Davis and his team the self-service ability to create advanced protections in addition to the default detection and blocking that stops account takeovers and other web layer attacks.

Signal Sciences runs on the web servers Chick-fil-A operates: Apache, NGINX, Tomcat, and IIS. Within AWS, they use Cloudfront CDN in front of their APIs and will put Signal Sciences at the network edge to inspect and decision on web requests before they reach application origin.

Future-ready Web Application Security for any environment

The distributed nature of Signal Sciences patented solution enabled Davis and his team to deploy the agent where production code operates and instrument and monitor web requests while providing superior inspection and decisioning. Currently, Chick-fil-A runs apps separately in AWS and data centers, but in the future they will deploy apps and APIs running across both environments—and Signal Sciences will protect those web layer assets in their hybrid environment.

> "Getting Signal Sciences up and running is quick and easy. It was literally a five minute process: with just a few Signal Sciences rules changes specific to our authentication flows, we were able to effectively block account takeover attempts in production."
>
> **Robert Davis,** Director of Cybersecurity