Signal Sciences

Sauce Labs Enhances Control Over Web Application Threats

CHALLENGE

Sauce Labs needed a single technology to protect its web applications distributed across a hybrid cloud environment with different application stacks.

Sauce Labs provides the world's largest continuous testing cloud for web and mobile applications. Recently named to the Deloitte Technology Fast 500 list for the fourth consecutive year, the company helps businesses ensure that their mobile applications and websites work flawlessly on every device, operating system and browser, so that they can deliver an impeccable digital experience to their users.

Knowing how critical web application security is to the fabric of the company's business, Senior Director of Product Security, John Kennedy, wanted to defend against potential attack vectors including click fraud and abuse of its free trial virtual machine offering.

"With Power Rules, Signal Sciences helped us take a big bite out of click fraud occurring on our site."

John Kennedy, Senior Director of Product Security

SOLUTION

Sauce Labs immediately gained intelligent blocking of web threats from Signal Sciences and used the visibility to identify unique application abuse, which they thwarted using Power Rules.

Clearer Insights with Signals

For applications running across different stacks and hybrid cloud environments, Signal Sciences provided unified visibility with clearer insights. Sauce Labs has extensive logging in place for all its resources, but the team didn't have the bandwidth to monitor logs for suspicious events. Signal Sciences applies descriptive signals to each request—such as "Malicious IP" and "TOR traffic"—enabling the team to see a picture of what is going on in real time. Better visibility into how Sauce Labs' resources are being used and misused helps the team know where to focus.

Geo-blocking with Power Rules to Limit Click Fraud

Sauce Labs was seeing unique application abuse in which malicious users would attempt to request free trials to get access to virtual machines. Kennedy's team was able to determine that the attackers were using disposable email domains coming from a certain range of IP addresses. Since the company doesn't do business in certain countries where the attacks originated, they configured a Power Rule to restrict access to specific pages based on geo-blocking and were thus able to curb abuse of their virtual machine service.

An Easy Sell to Other Teams

Kennedy expected initial questions from the TechOps team regarding Signal Sciences including, "What's security going to put in there, and is it going to screw up performance?" After reviewing Signal Sciences' architecture with the NGINX module and web server agent, both TechOps and Engineering were on board. Their support was due to the technology's simplicity compared with hardware appliance models that they had used in the past.

> "In our business, users need to run tests on our platform 24/7. Signal Sciences does intelligent blocking that doesn't interrupt user workflows or impact legitimate users from using our service."
>
> **John Kennedy**, Senior Director of Product Security at Sauce Labs