Signal Sciences

Microservices and API security for OFX's International Wire Transfer Business

CHALLENGE

OFX is an international financial transfer platform based in Sydney, Australia, that processes over $22 billion annually through its web application. Having recently completed a total migration to the cloud over a period of three years, OFX wanted to get visibility and protection against Open Web Application Security Project (OWASP) attacks and authentication abuse in its cloud-first microservices infrastructure.

Partners interact with the OFX platform via APIs that talk to microservices internal to the OFX network. Tasked to build the security program and team, Head of Digital Security Richard Lane wanted to ensure their microservices weren't implicitly trusting others and sought a product that would provide visibility there. He wanted a solution that would prove easy to install, use, and effectively block malicious traffic automatically — including logins — without hand holding or causing production incidents.

SOLUTION

Deploying Signal Sciences in their mid-tier environment with an agent on their web servers allowed OFX to "get into the guts of the application," as Lane explains. "Signal Sciences has provided a whole ton of visibility where we didn't have it before."

Engineering benefits without tradeoffs

Using Signal Sciences web server module plugins that communicate with lightweight agents, the security team and cloud architect were able to deploy easily without taxing the engineering team and gain deep application visibility. After installing the software in minutes, the security team used Signal Sciences to uncover application errors that they weren't expecting, including 5xx errors that allowed engineering teams to find and address root causes more efficiently and effectively.

In addition, the quality assurance team uses Signal Sciences monitoring via easy-to-consume dashboards as a part of their release protocols to catch any issues quickly. By seeing response anomaly patterns in Signal Sciences, they're able to ensure the applications' RESTful APIs are functioning as expected.

Authentication defense with Power Rules

OFX wanted visibility into the origin IP and behavior of user logins to detect suspicious actors and patterns. After configuring Signal Sciences Power Rules for successful and failed login attempts, they established a baseline for their normal authentication traffic. With a low risk tolerance and low traffic volume, OFX used Power Rules to create custom thresholds to alert and block malicious authentication traffic aggressively whenever it deviates from normal behavior, and they haven't experienced any false positives.

Penetration testing visibility and validation

Another Power Rules use case was to gain visibility for penetration testing to understand the breadth and range of testing, which also helped to validate Signal Sciences effectiveness during the initial evaluation. With toggles in Signal Sciences console UI to easily turn on or off detection against particular pen test sources, they confirmed Signal Sciences would have blocked the pen testers' attempts.

"When we published a full release to the OFX site, we didn't need to tune Signal Sciences at all. We were confident it would function effectively through that process, which it did without any ongoing maintenance or fiddling, which was the main issue we had with legacy WAFs."

Richard Lane, Head of Security at OFX