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 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