REPORT REPRINT

Fastly already seeing dividends from Signal Sciences acquisition

JANUARY 14 2021

By Daniel Kennedy, Craig Matsumoto

Last October, Fastly completed its $775m acquisition of Signal Sciences. Within two months, it noted several significant transactions that leverage the new combined offering, matching Fastly products with acquired Signal Science's web application firewall capabilities.

451 Research

S&P Global
Market Intelligence

Introduction

On October 1, 2020, Fastly completed its acquisition of Signal Sciences for $775m in cash and stocks. Within two months, it noted several significant transactions that leverage the new combined offering, matching Fastly products like delivery and TLS (Transport Layer Security) with the acquired Signal Sciences web application firewall (WAF) capabilities.

451 TAKE

The major content-delivery network (CDN) players, including Fastly, Akamai and Cloudflare, all have some version of a WAF offering in place. For Akamai, Kona Site Defender is built into its Intelligent Edge Platform. For Cloudflare, which has a security reputation rooted in its anti-DDoS (distributed denial of service) offerings, there is the CloudFlare WAF. Fastly has a cloud-based WAF that uses third-party rulesets and custom rules to inspect requests not served from cache. The acquisition of Signal Sciences, which brought with it an independent WAF platform with a reputation for being able to effectively run in blocking mode and had significant customer penetration without the benefit of being attached to an existing platform, was an interesting move. In essence, it added a WAF that could fly on its own into a CDN product suite and customer base.

Details

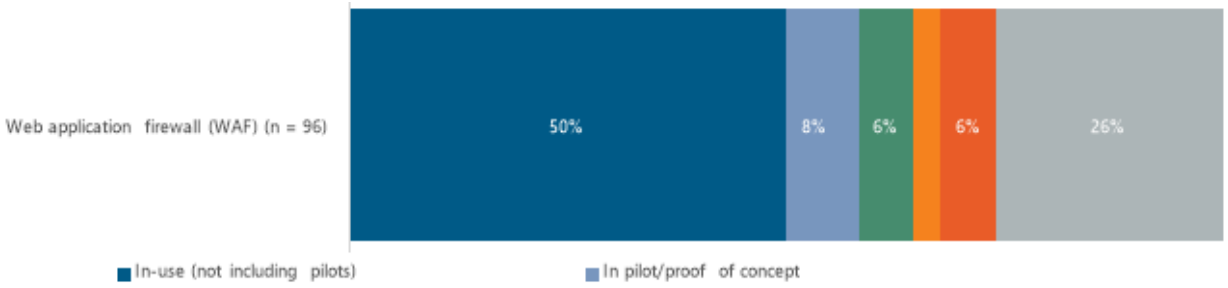
Part of the goal that led Fastly to Signal Sciences was to avoid attempting to stitch together a solution set for API security, bot detection and mitigation, application layer anti-DDoS, and related WAF functions. There was also a common developer-oriented focus between both companies, as well as some joint customers that stood to benefit from a more integrated set of product offerings. Finally, Signal Sciences executed on a vision to run security wherever the application is, and therefore had a number of different deployment options, including RASP, to support on-premises and the cloud with a common management dashboard. Fastly has adopted a similar vision, augmenting datacenter and the cloud with security at the edge, with the hope that an expanded security offering will increase take-up for Compute@Edge, Fastly's edge serverless compute environment.

There are situations where an attack type can be mitigated better with a combined offering. A straightforward example is DDoS, where a WAF can be helpful in dealing with a targeted layer 7 denial of service, but a CDN offering is better equipped to handle a network layer or volumetric DDoS.

In terms of integration, there is the practical, such as integrated onboarding (to expose Fastly customers to the acquired offerings) and integrating deployment such that Signal Sciences works within the Fastly Edge Cloud Platform. Then there is the larger task of developing an integrated defense, mapping Fastly's existing security capabilities and the Signal Sciences WAF capabilities together. Signal Sciences was already capable of taking in data from other customers (with the SigSci network) and using it toward a common defense across its customer network. Fastly's scale of traffic could improve this reach. Both product sides of the acquisition remain flexible when it comes to product delivery. Fastly had existing partnerships with bot-prevention players such as PerimeterX, DataDome and Shape Security (now part of F5), and will integrate with other partners where it serves customer needs. The Signal Sciences WAF similarly continues to be available outside of using parts of the Fastly platform.

The major CDNs are jockeying for position as edge cloud platforms. Security is a major part of that push, and API security has been a particular emphasis for some, including Akamai and Cloudflare. Signal Sciences will help Fastly on that front. Moreover, the startup's developer-minded heritage should not be overlooked. Fastly, like many of the largest CDN players, views its edge computing as a major evolution in that it lets developers customize the CDN's behavior. Security is an area where this could have immediate benefits – in areas such as WAF rules or the treatment of DDoS attacks. In that sense, Signal Sciences plays into Fastly's edge computing ambitions as well as its security plans.

Enterprise WAF Implementation Status and Plans



Source: 451 Research's Voice of the Enterprise: Information Security, Workloads & Key Projects 2020
Q: What is your organization's implementation status for the following information security technologies?