Signal Sciences broadens deployment options with a cloud WAF

AUGUST 30 2019
By Daniel Kennedy

Signal Sciences continues a strategy of platform expansion of its next-gen WAF platform with the recent release of a hosted cloud WAF. The WAF has two parts, a server or application-side installation and a cloud engine that functions like a SaaS, evaluating data from various sources and pushing application-specific detections to the on-site installation.
Introduction
Signal Sciences continues a strategy of platform expansion of its next-generation web application firewall (WAF) platform with the recent release of a hosted cloud WAF. This new deployment option requires only a DNS change to enable for an application, does not require deployment of an agent, retains the full feature set of the existing WAF offering, and feeds into the same dashboard as its other deployment options. The latter is a key consideration in implementing application protection in modern enterprise IT architectures, which are increasingly hosting applications both on-premises and across one or multiple hosted clouds.

451 TAKE

‘Next generation’ is a common moniker in information security, extending from firewalls to endpoints, and is usually representative of both increased breadth or precision in security-issue detection and an attempt to market that a product is markedly different than its predecessors. Most next-generation WAF vendors highlight such increased precision largely over legacy signature-based approaches; Signal Sciences in particular notes that 95% of its customers are running in full blocking mode (automatically blocking bad requests to an application rather than just alerting on them, a key consideration for resource-constrained security and development teams). Actually blocking bad requests typically had a short shelf life in legacy WAF implementations, usually lasting until the first legitimate piece of traffic was blocked and blocking was turned off or minimized. The next-generation milestone extends beyond this, however, to characteristics that support modern application deployment, which typically means a variety of hosting options across varied hosting locations including on-premises and hosted cloud. These characteristics include a variety of deployment options for enabling the WAF across different applications, and operational management considerations across multiple architectures such as a common management dashboard or interface.

Context
A WAF is a type of protection for web applications, evaluating, for example, http requests and determining whether a request to the application is a legitimate one, or a request attempting to get the application to behave in unexpected ways, such as with application-directed attacks – e.g., SQL injection or cross-site scripting. According to our latest Voice of the Enterprise, Information Security: Key Projects survey, 55% of enterprises have a WAF in place. Much of the early growth for WAF deployments was aided by compliance requirements; notable among these was a payment card industry (PCI) requirement for securing web applications (PCI DSS Requirement 6.6) that said in essence that an enterprise handling credit card transactions could either install an application security testing capability (SAST or DAST, for example) or implement a WAF. While the intention was good, this led to many WAF installations motivated by checking off a compliance requirement versus a strategic risk-reduction choice as part of an application security program, many of which acknowledge the need for both some level of application security testing and application protection in production for the inevitable vulnerabilities that escape the testing process – application denial of service (DoS) attacks, known bad source IPs, bots, etc. Signal Sciences notes a number of competitive displacements of WAF solutions installed under these circumstances.
Company
Signal Sciences, headquartered in Culver City, California was founded in 2014. The founding team came from online marketplace Etsy and sought to develop and commercialize products for modern application environments after finding a lack of security offerings able to operate effectively at Etsy’s scale and pace of change. The company raised $35m in a C round in February, adding to a 2017 series B round of $15m, a 2016 series A of $9.7m and a seed round of $2m in 2014. The company employs 150, tripling the number reported in 2017, and protects roughly 25,000 applications. Customers are diverse from an industry vertical standpoint, and include Prezi, Chick-fil-A, OFX, DoorDash, Yelp, One Medical and Duo (Cisco).

Products
The Signal Sciences WAF product has two parts, a server or application-side installation and a cloud engine that functions like a SaaS, evaluating data from various sources and pushing application-specific detections to the on-site installation. One of those sources, Network Learning Exchange (NLX) provides a type of cloud network intelligence between customers of Signal Sciences’ platform, offering a feed of suspicious traffic characteristics based on observations made via other customers’ WAF installations.

Deployment options for the WAF in addition to the aforementioned cloud WAF, include classic installation points such as on a web server, load balancer or as a reverse proxy, but also a RASP-style option where the module is installed within the application, which supports Java, .NET, GO, Node.js and PHP applications. The WAF can also be installed in container environments, either in the container itself or as a sidecar.

A dashboard capable of taking information from different deployments shares information on OWASP-style injection attacks, scanner activity, unusual traffic sources including bad traffic as identified by the SigSci Network of other customers, and request anomalies. An operator can note both flagged IPs and those that have exceeded thresholds for a type of attack or activity, as well as IPs that have nearly approached those thresholds. Power Rules allow the WAF operator to define a set of input conditions (e.g., user agent, path, cookies), as well as thresholds alongside an action to take if those conditions are met, allowing customers to define custom rule sets and deal with custom application requirements, such as blocking excessive login requests.

The product supports integrations with popular DevOps tools including container management platforms (e.g., Kubernetes) and issue tracking or alerting (e.g., Jira, Slack). It also integrates with SIEM and analytics tools such as Splunk and Elastic, as well as other SOC tools such as Cisco Threat Response, and integrates with the major cloud offerings, such as Azure, AWS and Google Cloud.

Competition
WAFs were classically deployed as hardware networking devices, and F5 Networks, Fortinet, Imperva and Citrix featured as responses in 451’s VotE survey for WAFs that respondents are actively using. Add to that companies such as Barracuda, Radware and A10 Networks. Vendors such as Imperva (acquired Prevoy) and Rapid7 (acquired tCell) offer both WAF and RASP offerings similar to Signal Sciences. CDNs including Akamai and Cloudflare bundle WAF and anti-DDoS services. AWS WAF is also an option cited for cloud-hosted applications. The RASP space opens competition with additional vendors such as Contrast Security, Waratek, Micro Focus and Threat Stack (acquired Bluefyre).
## SWOT Analysis

### STRENGTHS
Legacy WAFs are somewhat difficult to scale quickly and weren’t originally built for a hybrid cloud environment, meaning there’s runway left for next-gen WAF offerings to continue to grow. Products such as Signal Sciences that offer many deployment options across multiple architectures (but one reporting dashboard and management interface) are well positioned to address these architectural shifts.

### WEAKNESSES
The WAF moniker has baggage. Application security in general is a weak area for many enterprise security teams in terms of on-site skill sets, yet is gaining in importance as infrastructure continues to abstract (invisible infrastructure) and attackers continue to focus their efforts there.

### OPPORTUNITIES
There are several WAF installations in place that are network-based and more suited to on-premises application installations. While that use case remains valid, solution sets that allow for a common management interface between on-premises apps and cloud-hosted ones provide one less dashboard for security operations to look at.

### THREATS
The AWS WAF in particular has seen a significant uptick in mentions in 451’s end-user research, and the cloud provider can limit competition on their hosted cloud offerings by introducing pricing pressure.