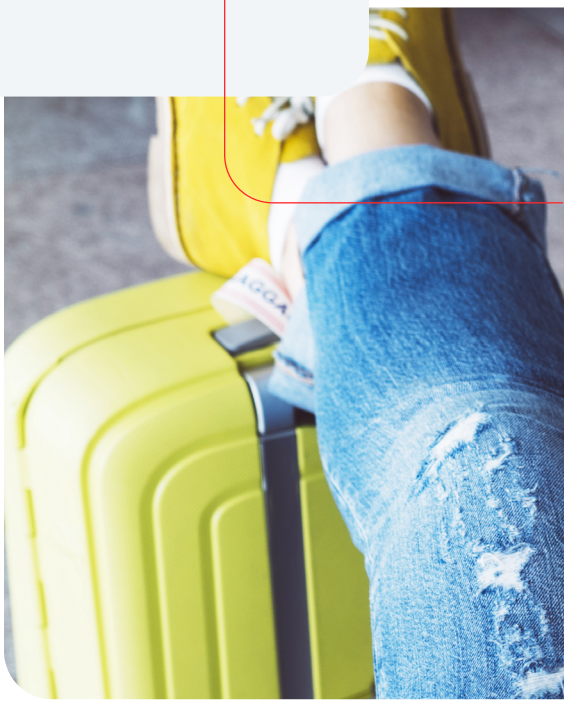
Signal Sciences
Now part of fastly

CASE STUDY

Fastly + Maritz

Maritz Achieves a Security Win with an Easy-to-Manage Next-Gen WAF



Challenge

Several business units within Maritz accept credit card information and therefore must report annually on PCI DSS compliance. To enhance the Maritz' security posture in support of PCI DSS requirement 6.6, the team implemented a web application firewall as an additional layer of security to the Maritz-hosted PCI environment.

Maritz is a holding company, whose businesses provide market and customer research; customer loyalty, sales incentives and employee rewards and recognition programs; and meeting, event and travel incentive services to Fortune 500 companies and beyond. With so many different business units and applications accompanied by different technology stacks, the team needed to find a single product to deploy across current and future hosting environments, whether physical or virtual, on-premises or cloud. With previous experience using an open source that required extensive manual effort to operate, Maritz was looking for ease of use, including automated blocking and simple deployment.

> *"For the Maritz WAF Project, the team objective was to implement an additional layer of security for web applications without a negative impact (performance issue) to the production environment. The rollout of Signal Sciences was very simple and successful, with no issues encountered during test or production deployments, which made for an easy win."*

Andy Wolfe
Technical Architect at Maritz

Solution

After initially deploying Signal Sciences to 5% of its corporate application footprint, the rollout was so successful that they're expanding to cover 90% of total applications across multiple business units.

Simple deployment accelerates adoption across teams and tech stacks

The project team's objective was to implement an additional layer of security without impacting legitimate traffic or performance, or changing complicated firewall rules that alter traffic between the network edge and web servers the way other security tools can. Signal Sciences' simple agent and module software deployed directly to the web server didn't require changing traffic flow, and the monitoring team confirmed load times and performance didn't spike.

Maritz ingests Signal Sciences agent status via API in their SIEM to ensure agents are up to date and arefunctioning properly. Signal Sciences dashboards easily show what IPs have been flagged and identified as malicious for a given reason — details which have given teams confidence and opened the door for deeper security discussions.

Signal Sciences' web server deployment provides support for varied infrastructure used by different business units. Technical Project Manager Lynette Ormsby explained,"The team gained confidence to continue rolling out more broadly earlier than expected after seeing how the tool did not require weeks or months of effort to deploy. The expedited timeline was accepted organizationally due to the benefits of the additional layer of security within our environment." Signal Sciences will now be a corporatewide offering with an opt-in model, allowing Maritz to achieve broader coverage than originally projected — up to 90% of its corporate applications.

Savings across the board: No dedicated FTEs required

One of the big selling points for Maritz was that Signal Sciences didn't require spinning up a new team to manage the product. Operationally, Signal Sciences fits in with their existing Security Operations Center (SOC) and new standard operating procedures. Although difficult to estimate overall time and costs saved due to the varied nature of unpredictable web traffic, Maritz can say with confidence that they're now able to automatically block certain attack patterns thatmight have taken a weekend to investigate and mitigate manually prior to Signal Sciences. The SOC can now see and investigate malicious activity quickly, determine the risk level and decide which teams to pull in.

Development and operational benefits include visibility and virtual patching

Signal Sciences has provided visibility at the application layer, which has helped the infrastructure services group at Maritz to have more meaningful conversations with engineers about the security of their application. "It's one thing for a developer to read hypotheticals on what OWASP attacks are, and another for them to see a command injection attack in production in real-time and say 'Hey that's my site, and we can block it,'" said Andy Wolfe, Technical Architect. Signal Sciences' automatic traffic categories also provide application engineers with insight into "anomalies," many of which can be cleaned up with minimal effort (such as robot files or favorite icons).

Signal Sciences' virtual patching capability has provided the team with insights into common vulnerabilities exposure (CVEs). Using Signal Sciences Power Rules to enable specific blocking based on pre-configured signatures, the team is able to block these malicious attempts and buy time to fix the underlying vulnerability. As Signal Sciences continues to build out its CVE library, this will become even more valuable and time-saving.

Maritz

"Thankfully, no one has to coordinate WAF rule sets with every change or deploy to the application. We anticipated a cost of adding 2 FTEs with a traditional signature-based WAF, but we didn't have to do it with Signal Sciences"

Andy Wolfe,
Technical Architect at Maritz

Any App

Infrastructure support

kubernetes IBM Cloud Google Cloud aws Pivotal

And more →

Web Server and Language Support

NGINX Microsoft IIS APACHE

And more →

Gateways and Proxies

section.io Kong

Any Attack Type

OWASP Top 10

Application DoS

Brute force attacks

Account abuse and misuse

Request rate limiting

Account takeover attacks

Bad bots

Virtual patching

Any DevOps Toolchain

slack HipChat

DATADOG VictorOps

pagerduty splunk>

elastic ArcSight

Radar

Generic webhooks

Any custom tools via a full RESTful/ JSON API