Signal Sciences

DeNA: Centralizing Visibility While Reducing Operational Cost

CHALLENGE

Legacy WAFs provided high operational costs and response times, especially during critical traffic spikes.

DeNA is a Japanese corporation that focuses on digital portals, mobile games, and e-commerce platforms.

As the company continued to expand its offerings and provide great digital experiences for their customers, DeNA knew it needed to scale its web security posture to match. But their legacy hardware WAF was causing the team multiple issues and made it difficult to operate efficiently.

During traffic spikes, the legacy WAF's admin portal loaded slowly and prevented the team from addressing issues quickly. Additionally, it was impossible for the DeNA team to reroute customer page requests if their WAF was not performing correctly.

The legacy WAF performance, combined with the high price of scaling hardware investments, made it clear to DeNA that they needed a new solution that can perform under pressure.

> “Signal Sciences was more cost-efficient to scale.”
>
> **Yuki Shigeiwa**, General Manager, Cyber Security Dept.

SOLUTION

Signal Sciences provided DeNA scalable performance and centralized visibility that couldn't be provided by their legacy hardware WAF.

DeNA deployed Signal Sciences across five of its properties and saw performance improvements after an easy installation.

Reduced Operational and Capital Expenses

DeNA was able to reduce their operational expenses by using Signal Sciences. They no longer needed engineers dedicated to costly rules or policy tuning necessary for a traditional WAF. Additionally, Signal Sciences was more cost-efficient to scale with their business than their previous hardware WAF.

Attack Detection Based on Rich Web Request Context

The legacy WAF DeNA had in place based on static regex pattern-matching rules often let attacks pass through without this additional context, such as reconnaissance attacks. Signal Sciences provides a better, more innovative approach to detecting and blocking potential attacks. We leverage known-bad IP lists to compliment our proprietary SmartParse technology, to make fast, inline decisions to block malicious web requests. Additionally, Signal Sciences enriches decisioning with our Network Learning Exchange to further evaluate web requests' source IP reputation.

Deeper Visibility Across the Organization

With Signal Sciences, DeNA now has deeper organizational and attack visibility. Our dashboards provide a single source of truth for multiple teams and stakeholders throughout the business. Additionally, they now see new activity on their network that was previously unknown to them, such as traffic from the Tor network.

> "Signal Sciences provides a better, more innovative approach to detecting and blocking potential attacks."
>
> **Takayuki Yasunaga,** Cyber Security Engineer