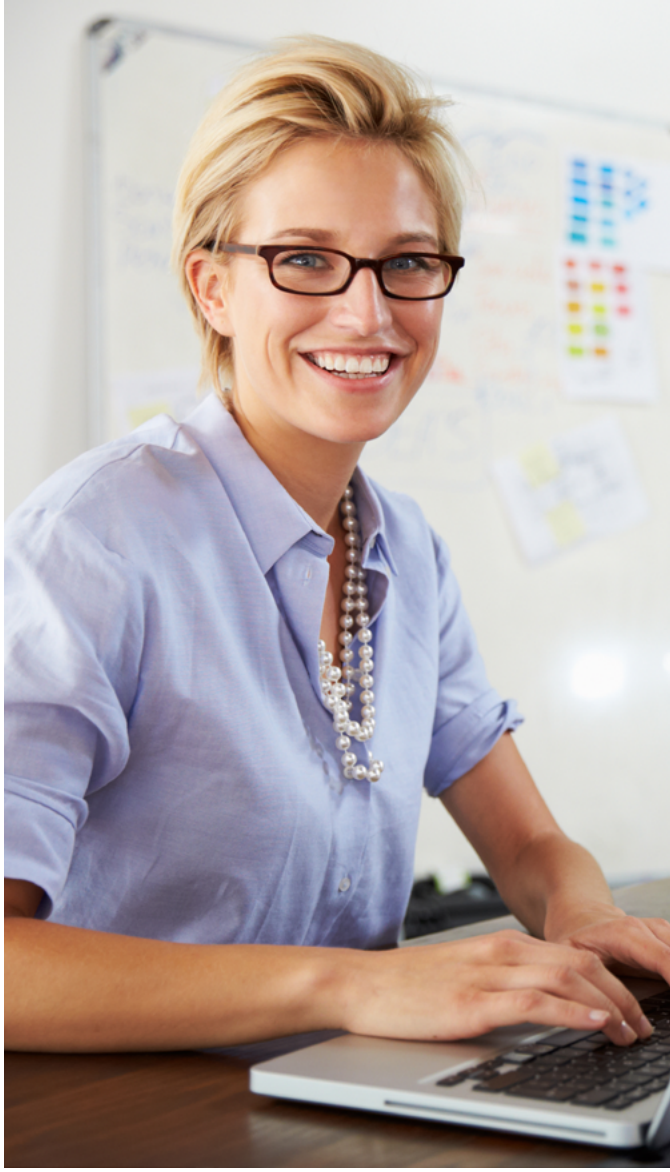
Signal Sciences

Autoscaling Production Application Security in Betterment's CI/CD Pipeline



CHALLENGE

Betterment needed a solution to help protect customer PII and financial assets that could automatically scale and block attacks, without requiring ongoing signature tuning or impacting performance.

Betterment is an online financial advisor with more than $14 billion in assets under management. To support a user base of over 380,000 customers who access its online platform, the company spins up numerous web servers daily through its continuous integration and deployment (CI/CD) pipeline. Knowing if, when, and how their user accounts might be under attack is key to keeping them secure. Prior to implementing Signal Sciences, Betterment's Engineering and Security teams' biggest concern (based on previous experience with legacy WAFs) was the signal-to-noise ratio. It was critical that a WAF could automatically scale and accurately block attacks without increasing support call volume or creating more work for Engineering or Security.

"The high signal-to-noise ratio was key in our selection of Signal Sciences. IT enables the Security team to understand and track malicious activity against our applications keeping our customers safe. After its deployment and configuration there have been zero false positives. This has reduced the workload on Security while also providing a very friendly user experience. It also allows the team to configure and modify rules addressing new attack vectors and payloads in an ever evolving threat landscape, to help mitigate business risk."

Anson Gomes, Lead Security Engineer

SOLUTION

Since adopting Signal Sciences, Betterment's Security team has seen its workload reduced by automating deployment and updates, and by getting quick access to informed insights without compromising performance.

Auto-scalable Web Defense

To provision Signal Sciences, Betterment's Operations team wrote a simple Ansible playbook so that any new application instance will automatically have Signal Sciences modules and agents installed as a part of its CI/CD pipeline. "We haven't had to touch it for install or update," said Betterment's Lead Security Engineer, Anson Gomes. As a former security consultant, Gomes had previously tested legacy WAFs that didn't scale natively, and required new deployment of a WAF instance for every app server, which drove up costs and complexities that they didn't have time to manage.

Better Coverage While Maintaining Site SLAs

Betterment's team was impressed with Signal Sciences' robust security coverage out of the box that can block malicious requests. The fact that Signal Sciences doesn't impact performance and availability of the application or increase Betterment's attack surface are additional benefits. With easy-to-use dashboards that provide visibility, any vulnerabilities detected are clearly surfaced and reported to the respective team, who remediate them in a timely manner.

Signal Sciences added visibility for the Operations team as well. The dashboards showed the results after a standard scan that uncovered some unknown services and misconfigurations that they used to tune their alerting system and fix application behavior.

Customizable Power Rules Help Ensure Security and Compliance

In addition to the turn-key detections that auto-block malicious traffic, Betterment uses Power Rules to help prevent attacks against their unique application logic to keep financial data safe. For example, they're able to define, monitor, and block abuse against their APIs by restricting access based on point of origin. Account takeover (ATO) protection Power Rules that are configurable with easy-to-use drop-down menus in the dashboard have also been leveraged to help prevent user account compromise.

> "It works straight out of the box, scales automatically, and does a great job at providing visibility while securing the application."
>
> **Anson Gomes,** Lead Security Engineer