Signal Sciences

BloomNation: Halting a Flood of Abusive Traffic

CHALLENGE

BloomNation is an online retailer delivering fresh flowers direct from local florists. Founded in 2011, the company serves customers in 5,000 cities and towns across the United States.

In late 2019, the company was listed on Built In LA's 50 Best Small Places to Work list, which boosted their national profile. But this also attracted malicious actors to their website at a much greater scale. BloomNation was experiencing a flood of abusive attack traffic, such as DDOS, SQLi, XSS, and credential stuffing, from malicious actors attempting to scan their web applications.

The impact on the organization was significant: engineers spent time away from building and deploying product features and focused instead on manually researching and blocking IP addresses to keep the website up. The influx of traffic also impacted the customer experience: page load times slowed and broke the site as attack requests increasingly hit their server instances.

Before Signal Sciences

- 90% CPU consumption
- Slow page loads and broken sites
- 3+ FTEs dedicated to attack mitigation

BloomNation needed tools to not only repel these attacks, but also give their engineering team the ability to rate limit traffic to quickly tag and identify traffic signals based on custom criteria.

> "The attacks turned our office into a war room and the headcount and resource cost to our team was significant. Without Signal Sciences I don't think we'd be able to keep the website up."

Ashlin Jones, Lead DevOps Engineer

SOLUTION

With Signal Sciences rate limiting features, BloomNation easily identifies malicious traffic and stops it from hitting their servers while reducing resource utilization and improving customer experience.

Immediate Reduction in Resource Load

At the peak of their attacks, BloomNation was dedicating three engineers to triaging web attacks a few days a week, but the company did not want to sustain that level of attention to manually identifying attack traffic sources. Signal Sciences tagging and filter features enabled BloomNation to categorize traffic through custom signals and freed them from manual operations related to identifying abusive web requests.

Improved Customer Experience

While BloomNation was able to block IPs from further attacking their applications, the initial requests were still hitting their servers. This caused considerable strain on their load balancers, which saw up to 90% CPU consumption. Signal Sciences rate limiting was able stop these requests, speed up page load times, and prevent sites from being unavailable for legitimate users. Operationally, Jones and team have not had to access their load balancer since implementing Signal Sciences.

Solution Outcomes

- **Zero load balancer maintenance**
- **High site availability**
- **0 FTEs dedicated to attack mitigation**

A Secure Path Forward

The BloomNation team had experienced malicious traffic spikes in the past, but their resources weren't prepared to scale so quickly. Signal Sciences tools and features gave Jones the ability to dive deeper into his architecture and plan out best practices as the company grows. Our next-gen WAF also provides BloomNation a forward-looking approach to application security.

BloomNation

> "Signal Sciences rate limiting has opened a new dimension into securing our application. It gave us a better understanding of this traffic and where it was coming from."

Ashlin Jones, Lead DevOps Engineer

Signal Sciences Platform Capabilities

Next-Gen WAF | Bot Protection | **Rate Limiting**

API Protection | RASP | DDoS Mitigation

Attack Types Blocked

XSS | DDoS | Abusive Traffic

Credential Stuffing | SQLi