Signal Sciences

Defending Apps in AWS with Signal Sciences

BENEFITS

- Reliable, automated blocking of attacks
- DevOps focused protection
- Platform agnostic with unified management
- Coverage against all threats

Deploying applications in cloud environments provides organizations with greater business agility, data availability, and cost savings. Yet security remains a primary concern: 73%[1] of organizations with cloud-native applications say they lack actionable, fine-grain, real-time insights into threats and ongoing attacks.

Amazon Web Services WAF: A Legacy Approach

Deploying Amazon Web Services Web Application Firewall (AWS WAF) to monitor and protect applications on AWS might seem like a simple option. In reality, it's based on a legacy approach where the WAF is deployed at the edge, making it impossible to see what's getting through to the origin or how the application is behaving. AWS WAF suffers from several deficiencies.

- **High maintenance cost:** AWS WAF requires you to configure web ACLs, then apply rules for each. Rules are costly to write and maintain, and don't show request details when triggered. Few ever make it to blocking mode. AWS WAF becomes increasingly burdensome to manage as instances are difficult to stand up as applications and services scale.
- **Constant configuring and tuning of rules:** Preventing SQLi and XSS attacks requires ongoing rule set tuning on a per web ACL basis.
- **No unified management across multi and hybrid cloud:** Cloud or DevOps teams must configure Amazon CloudWatch to surface AWS WAF metrics on a per web ACL basis. And if not all your properties run on AWS, you won't have a unified view of the security of your non-AWS applications and services.
- **Limited protection against application abuse:** AWS WAF lacks the ability to monitor and protect against application abuse and misuse.
- **Integrations with DevOps tools are not widely supported:** Because AWS WAF lacks DevOps toolchain integrations, visibility into security data is limited. APIs, if available, are hard to parse and consume.

1 The State of Cloud Native Security 2018 - Co-Authored by Capsule8, Signal Sciences, Duo Security

Signal Sciences Secures Any App Against Any Attack

With Signal Sciences next-gen WAF, cloud and DevOps teams can easily secure their applications, APIs, and microservices running in AWS. Our easy-to-install software supports any application without noticeably impacting performance. It protects against any attack, and integrates with any DevOps toolchain products for cross-team visibility.

Customers who chose our next-gen WAF solution over AWS WAF

bambora

Bambora provides flexible software solutions that allow businesses to accept online payments. Customer data flows into AWS via Bambora's API for payment processing. Originally using a CDN WAF that was costing them too much operationally, Bambora transitioned to AWS Shield for volumetric DDoS protection and Signal Sciences for application layer visibility and protection.

Bambora wanted a flexible solution that went beyond OWASP injection attacks. Signal Sciences delivered, providing defense capabilities against attacks like credential stuffing and abuses of business logic (e.g., sensitive or high-risk transactions). Bambora found that AWS WAF, like other legacy WAF solutions, was limited in scope and would have been costly to manage. Signal Sciences is scalable and enables Bambora to monitor and protect against application-specific risk and abuse in real time.

DOORDASH

DoorDash is a last-mile logistics platform that connects customers with their favorite local and national businesses in more than 1,200 cities across the United States and Canada. Experiencing rapid growth with accompanying high traffic volumes, their security team tried a homebrew combination of Splunk and AWS WAF as a means to block attacks while allowing legitimate traffic through.

When their staff realized that AWS WAF would require significant rules maintenance as customer traffic scaled, they decided to switch. Signal Sciences deployed in minutes, and offered superior visibility, detection and blocking capabilities with no false positives. DoorDash now fortifies their security posture with Power Rules to block bots, business logic attacks using signals that include the traffic source, and APIs to integrate with custom tooling.

commonbond

As a provider of student loan refinancing with an online application process, security is paramount to CommonBond. As an AWS customer, they considered AWS WAF, but they preferred the modern approach of Signal Sciences.

CommonBond deployed Signal Sciences in their Kubernetes environment. The solution has proven to be both effective and extremely easy to manage. Being a very lean team, a solution that worked "out of the box" was a huge win. Anticipating future growth both in users and application footprint, CommonBond values the flexible deployment methods and DevOps toolchain integrations that will allow them to protect their applications however and wherever deployed, now and in the future.