Reblaze

Web Application and API Security

coinberry

Crypto Trading Platform Gets Customized and Fully Managed Web Security on AWS

Coinberry (coinberry.com) is a crypto trading platform in Canada. As a large financial platform that has exceeded $1 billion in trading volume in a prominent market, it is a conspicuous target for attackers.

"Security is a number-one concern for any large site," said Coinberry DevOps engineer Ishan Patel. "Up until last year, we were using AWS WAF and AWS Shield. But we had some DDoS incidents, and I realized that we were paying for something that we didn't have control over."

Visibility and Customization

"AWS Shield protects against DDoS, and AWS WAF protects against some other attacks. But they have limited customization, with very few options," Mr. Patel said. "And you cannot have direct access to the traffic logs. You have to send the logs to an S3 bucket, and then get them from there. Even though there are some queries available, it's still a headache, and it's not ideal. We had very limited visibility."

He continued, "Whenever an incident happens, the AWS dashboard only shows its time and duration, and what it blocked. It has very limited information. So we'd have to go back into the logs and track those things down, which isn't easy. And even when we upgraded, the problems remained."

At this point, Coinberry decided to seek a different security solution. A partner recommended Reblaze: a cloud-native WAAP platform that's fully integrated with AWS.

(next page, please)

Industry

FinTech (crypto trading)

Challenges

- Defending a prominent target with a high perceived value for attackers
- Gaining full visibility for security incidents
- Customizing security policies to protect AWS workloads

Solution

Reblaze was deployed on AWS to provide WAAP (Web Application and API Protection) for Coinberry.

Results

- Internet attacks are blocked automatically, including threat categories not addressed by AWS WAF or AWS Shield.
- Security policies are highly customizable.
- Coinberry personnel have full traffic visibility in real time.
- Security updates are deployed immediately and automatically.
- The Coinberry team now enjoys "worry-free" web security.

Comprehensive Web Security for AWS

Mr. Patel explained, "We found that the Reblaze solution was less expensive, it has more options for customization, and it has a good dashboard." It also provides security technologies that AWS WAF and AWS Shield do not, such as biometric human/bot identification, advanced rate limiting, flow control, account takeover prevention, and more. "It looked good to us, so we decided to switch."

Since deploying Reblaze, Coinberry now has full control over incoming traffic. Mr. Patel said, "It already came with good rules and signatures, and we can customize it even further—much more than AWS."

Reblaze's traffic transparency is a key feature for Coinberry; the dashboard shows full details of all incoming traffic in real time, with the ability to drill down into specific time periods, all the way down to individual requests. Mr. Patel explained, "The dashboard is the most useful thing for me, where I can see day-to-day activities. The second most useful thing is the weekly reports. We can just walk through the reports and see if there were any flags or unusual activities."

The Fully Managed Experience

As a fully managed platform, Reblaze is maintained remotely by a team of security experts. As new web threats arise, countermeasures are deployed immediately, so that every customer has up-to-date protection. But the overall experience is much more than this.

Mr. Patel explained, "There have been attacks where we didn't even know about them until Reblaze informed us. The support team would say something like, 'There is a DDoS from these IPs, we've already blocked it. If you want to see it in the logs, here is a query string.'

"At other times, Reblaze has come to us and said, 'OK, there was an incident and we need to modify the rules to protect you guys.' It's nice to have someone who looks after you pro-actively like that."

When asked to summarize his experience with Reblaze, Mr. Patel thought for a moment, and then answered: "Worry-free."

"**The support is really good.** Whenever we have a high-priority issue, we always get a response in a timely manner. I can even message them on Slack and get a reply at any time."

"**If I have any questions, I can quickly raise a support ticket and they'll explain to me what is going on. I feel that there's always someone standing behind us, ready to help us.**"

"For us, security is a number-one concern. With Reblaze, we feel safe and confident."

Ishan Patel, DevOps engineer

Reblaze: Web Application and API Protection (WAAP)

Core technologies include:	Added value services include:	Contact:
Next-Gen WAF/IPS, Multilayer DDoS Protection, Precise ACL, API Security, ATO Prevention, Scraping Prevention, Advanced Human Detection and Bot Management, Unified Management Console, and Real-Time Traffic Analysis.	Mobile/Native Client SDK, Layer 7 Load Balancing, Global Secured CDN, and a complete DNS solution.	contactus@reblaze.com Int'l: +972 (73) 200-5200 U.S./Canada office: (408) 907-7712 www.reblaze.com