SaaS Provider Upgrades Security to Reblaze Running Natively on AWS

Zoom Analytics (zoomanalytics.co) is a marketing and personalization platform which serves customers in numerous industries. It provides a wide variety of capabilities, allowing its customers to "give the right message to the right visitor at the right time"; customers can change the look of their sites, change the offers that are made, target specific site visitors with custom offers, and more.

Due to the capabilities that it provides, Zoom Analytics processes not only its own traffic, but also the traffic of its customers. In this situation, robust GDPR-compliant web security is mandatory. But recently, executives realized that their security measures were not enough.

Customer Requests Penetration Test

"We started working with a customer that wanted us to do a penetration test," explained Lilach Yashar, the VP R&D of Zoom Analytics. "Up to that point, we had relied on extensive security measures built into our platform. When they gave us the pen test report, we saw that we needed to do things differently, and we decided to start looking for a WAF solution that could meet our unique requirements. We had already known that we needed to do this, but the pen test was the trigger."

Seeking a New Web Security Solution

Company executives researched security platforms, and considered different solutions. Along with the usual requirements—securing the OWASP Top 10 vulnerabilities, blocking DDoS attacks, identifying and blocking malicious bots, and so on—Zoom Analytics had some unusual criteria.

Ms. Yashar said, "We wanted dynamic rules. This is very important to us. We also needed some specific capabilities which the pen test report showed us.

"Zoom Analytics has a special situation for web security. Along with the traffic that comes to our website, we also process the traffic for our customers. Our customers put our code on their websites, and all the traffic for their sites goes to our servers. Plus, we have our own API, and we also have an API for our customers' users."

Along with its complex security requirements, Zoom Analytics had other needs as

CASE STUDY

ZOOM ANALYTICS

INDUSTRY

SaaS

CHALLENGES

- Satisfying stringent security requirements with a GDPR-compliant, ISO 27001 certified next-generation WAF solution.
- Selecting a security solution that is robust, flexible, and scalable enough to process not only Zoom Analytics' traffic, but also the traffic of its customers, including full API protection.
- Deploying and configuring the solution to run natively and inexpensively on AWS.
- Upgrading its security posture with dynamic rulesets, full visibility into incoming traffic, comprehensive logs, and more.

SOLUTION

Reblaze was deployed to run in a Virtual Private Cloud under Zoom Analytics' AWS account.

RESULTS

- Reblaze now blocks hostile traffic for both Zoom Analytics and its customers.
- Executives now have access to real-time traffic data, full logs, immediate support, advanced bot mitigation, and other capabilities they did not have before.

well. “We also wanted better visibility into our traffic—to see more clearly what is going on.

“Regulatory compliance was also very important. We’re GDPR compliant, so we must work only with companies that are compliant as well. If a solution wasn’t GDPR compliant, we wouldn’t even evaluate it. Also, we have ISO 27001, so we wanted an ISO-certified solution.”

“Even though we could work with a company that didn’t have ISO, it’s a best practice and that’s what we prefer.”

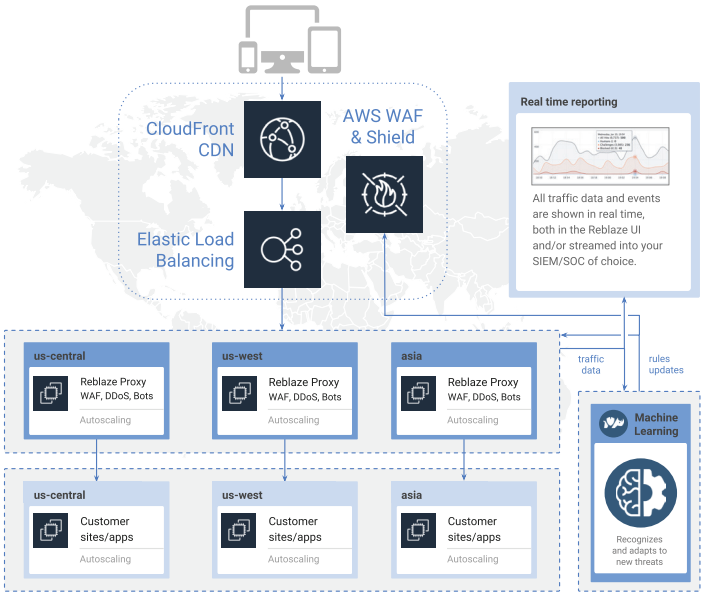
During its evaluation, Zoom Analytics tested several solutions. At the end of this process, the company chose Reblaze.

Reblaze and AWS

The Reblaze web security platform is fully integrated with Amazon Web Services. It provides comprehensive, effective web security for AWS, automating its inherent security capabilities and adding many more. This was an attractive feature for Zoom Analytics, but the flexibility of Reblaze’s architecture created a brief hiccup in the initial rollout.

Ms. Yashar explained, “At first, we used Reblaze outside our VPC [Virtual Private Cloud]. It looked like the easiest solution—I didn’t have to change anything within my Amazon configuration. So it seemed like a simple choice.

“However, having Reblaze outside our VPC meant that we had to pay for the traffic flow between Reblaze and us. We soon realized that we needed to move Reblaze into our VPC, and so we changed it over. We had really good support from the Reblaze team during this time.”



Reblaze runs natively on AWS. Running within the customer’s VPC is usually the optimal configuration.

Reblaze in Daily Use

What has Zoom Analytics experienced since deploying Reblaze? Ms. Yashar said, “Dynamic rules are very useful to us, as we expected. We’re also using Reblaze’s bot identification capabilities for our own interface.

“There are many parts of the system which are important to us, but for me the logs are especially useful. I find myself using them frequently. When I see something that looks suspicious to me—maybe a lead that came in over email or something—then I’ll want to see who did this. I’ll look in the logs and look up the time range when I saw the lead come in. I’ll find the IP address and put it in a blacklist. Later I can track down what the specific problem was. Usually it’s something like a web user trying to abuse a coupon code from one of our customers, or some similar malicious activity.”

Reblaze in a Nutshell

When asked to choose the best part of Reblaze, Ms. Yashar replied: “Quote me on this: they have a great support team. This is very important to us.

“For example, we had updated to a new version of our software, and I changed an API call. But I forgot to change the dynamic rule. Some of our customers said that they couldn’t save their campaigns. Immediately, I called one of the Reblaze support guys, and he fixed it for me right away.

“Another example: When I first deployed Reblaze into a configuration that didn’t work for us, their support led me step-by-step over the phone, and helped me set up a different configuration that was much more complex. I didn’t know how to do it in Amazon, and so they didn’t just send me a tutorial—they led me through it.

“To summarize my experience with Reblaze, they are very professional. They know the job, and whenever something happens, they respond very quickly. If there’s ever a crisis, I know I’m in good hands.”

About Reblaze

Reblaze (**www.reblaze.com**) is a comprehensive, cloud-based, **PCI DSS Certified GDPR compliant** protective shield for your web assets. Core technologies include: Next-Gen WAF/IPS, Multilayer DoS/DDoS protection, Scraping Prevention, High-level ACL, Advanced Human Detection & Bot Management, Advanced Management Console, and Real-time Traffic Analysis. Added value services include Layer 7 Load Balancing, Global Secured CDN, and a complete DNS solution. Contact: **hello@reblaze.com**. Int’l: +972 (73) 200-5200. U.S./Canada office: **(408) 907-7712**.