

Global Payment Provider Defeats Hourly Attacks with Reblaze's Cloud Web Security Solution

It's difficult to imagine a more attractive industry for cybercrime than financial companies.

With millions of users worldwide, Payoneer (www.Payoneer.com) accepts and transfers funds among 200 countries and territories, in 150 local currencies. The platform allows businesses and professionals to pay and get paid globally, conducting international financial transactions as easily as they do local ones.

Payoneer has quickly achieved international prominence. Thousands of corporations now rely upon the platform for payment processing, including Amazon, Airbnb, Upwork, Shutterstock, and Google.

A well-known global financial platform, processing millions of transactions every hour and handling large amounts of funds, which by its nature must be accessible to users all over the world, including regions with high levels of cybercrime—you might expect such a company to attract more than its fair share of hacking attempts.

Yaron Weiss, VP of IT operations at Payoneer, said the company gets attacked on an hourly basis. "Preventing attacks and web security are a core part of our business."

When Mr. Weiss first joined Payoneer, he wanted a platform built on best practices. He considered several popular solutions, including the Reblaze cloud-based web security platform, and benchmarked them all. He explained:

"I considered multiple factors: price, features, support level, and more. Ultimately, I chose Reblaze."

When asked what specific factor convinced him to go with Reblaze over the other solutions, he said, "The entire package." But he especially liked Reblaze's advanced bot recognition, traffic transparency, platform independence, convenience, and automation.

Advanced Bot Recognition

Bots make up a large portion of modern web traffic. Although a few (such as search

CASE STUDY



INDUSTRY

Financial: Payment Processing

CHALLENGES

- Protecting a high-profile target that's very attractive to attackers, with high perceived value for successful breaches and DDoS extortion.
- Defeating frequent attacks.
- Maintaining availability for users in 200 nations.
- Scrubbing high traffic volumes without noticeable increases in latency, for all global users regardless of their geographical location.

SOLUTION

Payoneer adopted Reblaze for comprehensive, cloud-based web security. The selection was based on platform features such as advanced bot recognition, full traffic transparency, platform independence, convenience, automation, and more.

RESULTS

Payoneer is still the target of frequent attacks, but hostile traffic is now filtered in the cloud before it reaches Payoneer's networks.

engine spiders) are benign, many are malicious. Harmful bots include those used for pen testing, data scraping and content theft, DDoS assaults, and more.

Most web attacks involve bots in one way or another. Accurate bot identification is crucial for robust web security today.

However, modern bots have grown quite sophisticated. Some can mimic human visitors very well. As a result, many web security solutions have difficulty distinguishing them from actual human users.

Mr. Weiss found it appealing that Reblaze is a leader in accurate bot identification. "Reblaze has very good algorithms to identify bots—to identify human actions versus bot actions."

Full Traffic Transparency

Few web security solutions provide complete transparency into the traffic they process. Some only describe the requests that were blocked. Others provide even less information than that. Obviously, this makes it very difficult to fully understand what is going on within a site.

Mr. Weiss appreciated how Reblaze displays complete information, including full details (headers and payload) of every request.

"I like that Reblaze's solution shows me everything in real time, and also in the log files. I can see all the traffic, not just the blocked requests, but everything. This is one of the most important features for me."

Platform Independence

Many cloud solutions run on self-owned cloud infrastructure. As such, they're less performant and scalable than industry leaders such as Google Cloud Platform, Microsoft Azure, and AWS, and they tend to lag behind technologically.

Conversely, Reblaze runs on all of the leading cloud platforms. This means that Reblaze can always leverage the latest cloud technologies, and scales easily. In addition, as Mr. Weiss said, "It has been very useful to us that we can move from one cloud to another: Amazon to Google and vice versa.

"Also, this has allowed us to deploy our cloud web security very close to our data centers around the world." As a result, Reblaze can provide robust protection with near-zero latency.

Convenience and Automation

Many web security solutions require ongoing administration and maintenance by their users. Not so with Reblaze, which is managed remotely by Reblaze's team of security experts. However, users still have the ability to see what is going on with their deployment, and make adjustments if desired.

Mr. Weiss commented, "I like a lot that it's a managed service. I don't have to waste manpower on configuring and maintaining the platform. But it's very important that I can also do it myself. There are other managed solutions in the market. But they're either managed or self-run. I like the combination, so that I can both manage it myself, and have the site managed by Reblaze.

"Another important thing is that I can automate almost everything, using the Reblaze API. I have a lot of automation. Whenever I launch a new application in Payoneer, which happens once or twice a week, I'm able to automate the process of creating the site and configuring the profiles."

Another attractive benefit is that Reblaze is provided as month-to-month SaaS, with no contractual obligations. Clients are free to cancel their accounts at any time.

"I liked a lot that there was no contract. And there still isn't."

"It saves me money."

Mr. Weiss has found that Reblaze works very well for Payoneer. And there's minimal effort required from his staff. "The Reblaze platform handles everything for us. When DDoS attacks occur, there's automatic scale-up of bandwidth and other resources for the attack. Also, I don't have to hire an on-site person to manage the WAF. That's very important."

Despite the web attacks that target Payoneer, the company is able to operate securely online. "Reblaze saves me downtime. It saves me money."

He also appreciates the level of support he receives. As he said:

"The truth is, I feel that I'm working with a partner. Whenever we have a problem, I approach them with the issue. They stand with us 24/7."

About Reblaze

Reblaze 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. More info: www.reblaze.com. Contact: hello@reblaze.com. International: +972 (73) 200-5200. U.S./Canada office: Reblaze Technologies, 3031 Tisch Way, 110 Plaza West, San Jose CA 95128. (408) 907-7712.