FinTech Provider Migrates to AWS, Upgrades Security for Web Applications and APIs

Pango (www.mypango.com) is a Mobile SmartCity Company, offering mobile payment services for parking, transit, and ride-hail, along with other services such as navigation & smart routing, road assistance, and insurance.

As a popular FinTech provider, Pango is a prominent target for attackers. Further, its products are offered not only via the web, but also through mobile and native apps. This creates a large number of potential attack surfaces that must be defended.

In 2018, Pango began a migration to AWS (Amazon Web Services). As part of that process, executives also decided to strengthen the company's web security.

Pango CTO Yaniv Kalo explained:

> "We were always under attack. We saw attempts at SQL injection, DDoS, brute force logins—there were attacks of every kind. As Pango grew, we knew we needed to take our security to the next level."

"When we decided to move our whole environment to Amazon—our development, staging, and production—we saw an opportunity to upgrade our security too."

Complex Challenges

For the migration and security upgrade to be successful, Pango had to solve multiple problems. The company's web security requirements are broad and complex; it needs to protect both web applications and mobile/native APIs.

Furthermore, the migration and security upgrade had to be done without harming production environments. Numerous products and services had to remain performant and secure during the migration.

Evaluating Security Solutions

Pango executives began by receiving quotes from multiple security vendors. Cloud security solutions have significant differences, such as:

- **Infrastructure.** Most cloud security solutions rely on self-owned infrastructure. This defeats much of the purpose of migrating to a public cloud platform such as AWS, since the security solutions will not have the resiliency and redundancy that AWS provides.

CASE STUDY

pango

INDUSTRY

FinTech mobile payment

CHALLENGES

- Migrating development, staging, and production to AWS while keeping numerous web applications secure and performant.
- Protecting a complex array of applications and APIs.

SOLUTION

Reblaze was deployed in a Virtual Private Cloud under Pango's AWS account before the migration began.

RESULTS

- Reblaze's report-only mode allowed Pango to train it for each web application and API before it was moved to AWS. The platform's granularity and flexibility allowed each one to be protected individually throughout Pango's sequential migration. Once fine-tuning was complete for an application, Reblaze went live for it.
- Today, Reblaze continues to block hostile traffic in the cloud before it reaches Pango's applications. Its comprehensive security includes a next-gen WAF, multi-layer DDoS protection, advanced bot management, and more.

- **Privacy.** Most solutions only offer shared cloud resources, which creates multi-tenancy vulnerabilities.
- **Effectiveness.** In order to detect bots, most web security solutions are still using legacy methods such as blacklists, rate limiting, reCAPTCHAs, and Javascript injection—all of which can be evaded by modern bots. Pango needed a solution which can effectively detect and block even the latest generation of bots.
- **Full API protection.** Many web security solutions have difficulty in securing APIs. See below for more on this.

Pango's choice

After performing its due diligence, Pango chose a security platform. As Mr. Kalo said, "We evaluated several solutions. Ultimately I was convinced that Reblaze was the best choice."

Reblaze runs natively on AWS. It is single-tenant, providing dedicated Virtual Private Clouds (VPCs) for every customer. It provides comprehensive web security, including a next-generation WAF, DDoS protection, full API protection, and human behavioral analysis & bot detection.

Migrating to AWS

Pango's migration was executed carefully. First, Reblaze was deployed in a VPC within AWS. (Reblaze can protect web applications and APIs whether they are on-premise, in cloud, or hybrid.) Thus, Reblaze was active throughout the migration.

The migration itself occurred in stages. Mr. Kalo explained, "We have many domains, integrations, and APIs. We took several months to move and turn on the various parts one at a time."

Pango took advantage of Reblaze's report-only mode. "In the beginning, we configured it to only monitor traffic, and not block anything. During the monitoring period we learned about our traffic and user behavior, and we fine-tuned Reblaze to eliminate false positives and false negatives—anything that could be harmful to production processes.

"Out of the box, Reblaze was already about 75-85 percent accurate. Then as it learned and built profiles for each application and API, and we were satisfied with its accuracy, it went live for each one."

As Reblaze went live for each application, it began to block attack traffic in the cloud, preventing it from reaching the protected web application or API. The platform proved useful in many ways, especially its dashboard which shows all incoming requests in real time. Mr. Kalo explained:

> "Reblaze's WAF revealed issues with our traffic that we hadn't known about. We saw requests that produced response codes in the 400s and 500s. Reblaze helped us to recover and fix these issues."

When asked if he had any final comments, Mr. Kalo said, "The Reblaze team have helped us a lot. Even when we were having production issues, they did great and helped us figure it out.

> "Every time we've had a problem or question, we have enjoyed working with Reblaze."

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**.

The Challenge of API Security

As mobile/native applications have proliferated, so have APIs. Detecting and blocking API abuse is a vital, and increasingly challenging, requirement for robust security.

Threat actors have more opportunities and less risk of detection. Some methods of threat recognition within web applications (e.g., browser environment analysis) do not apply to APIs. Further, each time new mobile/native apps or features go live, an API's attack surface expands.

Reblaze is at the forefront of API security. The platform provides a variety of advanced features, including a robust client-side SDK, automated schema ingestion and enforcement, reverse-engineering prevention, direct client authentication, deep payload inspection, and more.

The platform goes beyond rule-based enforcement. For each application and API it protects, Reblaze uses machine learning to build a sophisticated, comprehensive biometric profile of legitimate users. It learns and understands how legitimate users behave and interact with each application.

Every hostile user will, at some point, deviate from legitimate behavior. As soon as it does, Reblaze blocks it from further access.