CodeWave

aws partner network

Serverless DevSecOps
Case Study

Executive Summary

Flotiq is a producer of a headless CMS with the same name. Being highly aware of the responsibility behind storing their customer data, Flotiq wanted to address security issues as soon as they arose - ideally before the product ends up being available to the public.

Flotiq approached CodeWave with a challenge of producing automated CI/CD pipeline parts, which would automate security scans and reporting. At the same time, they hit the limit of their current infrastructure and sought solutions, which wouldn't require buying new servers.

The Challenge

Data security

Flotiq team treats security considerations very seriously. For that reason, they wanted to ensure their product is not vulnerable to common attack patterns.

Dependency based attacks

Team needs to constantly keep an eye on all libraries, their versions and vulnerabilities to avoid security holes.

Infrastructure limitations

Flotiq's servers are already utilized for hosting, deployments and existing automated processes. The new solution should not impact existing infrastructure and keep cost at minimum.

Why AWS

In this scenario, serverless solutions and an on-demand pricing model is a great solution for Flotiq team. It is hosted completely outside of their infrastructure, impacting it as little as possible. What's even more important, considering the Lambda free tier, it is possible to achieve a solution which is almost free in terms of computing power.

FLOTIQ

About Flotiq

Flotiq is an upcoming Headless CMS based on an innovative approach to data and website management.

> "CodeWave approached our problem very professionally and designed a great solution, which costs us next to nothing."
>
> Flotiq Team

Why CodeWave

Flotiq approached CodeWave after receiving a recommendation from a previous CodeWave customer. Initially, they didn't know what is possible when using AWS. CodeWave team had the required knowledge of AWS products, pricing models and architecting cloud-native solutions to address almost all of the Flotiq's concerns.

The Solution

The final solution is a set of four Lambda functions, each performing a different type of automated scan. Those scans make use of popular tools for OWASP static code scan, OWASP dynamic security scan, Code quality check and website performance assessment thanks to PageSpeed Insights API. The last two scans were extracted from the existing pipeline jobs, to address resource usage and building time problems on the existing, dedicated server. Additionally, there is a pair of lambda functions performing final report conversion to a format digestible by customers self-hosted GitLab instance. GitLab access key is stored as an SSM parameter, encrypted by AWS managed KMS keys.

Because some of the scans can take up to 10 minutes, there is a Lamba function, which sends information about the results to the Flotiq developers through their RocketChat. When one of the scan function fails, it sends the event to an SNS topic. The topic passes messages to both messaging lambda and to a function responsible for writing failure report to the S3.

The scans are incorporated into existing CI/CD pipeline for the GitLab project, and each function and conversion needs to be called separately via API Gateway in the respective pipeline job. Since the execution of Lambdas could take a few minutes, and it was required that the existing pipeline is not delayed in deploying the staging environment, CodeWave decided to use an asynchronous model. Each API call goes through the scheduling function, which schedules asynchronous function, depending on the endpoint of the request, and returns the S3 signed URL, at which result will be available after the scheduled function completes. Finally, GitLab worker downloads the report and displays it in the web application (e.g. next to the merge request). The results of SonarQube quality scan are sent directly to the SonarQube server, which reports to GitLab via the dedicated plugin.

Access to the lambda functions is protected via API Gateway with the use of API Keys. To address customers cost-awareness, CodeWave team applied S3 bucket life-cycle policies to the results bucket, to reduce the costs of storage for the reports, which in most cases will be accessed only once.

To deploy Lambda functions CodeWave used the Serverless Framework and Terraform to manage policies and S3 buckets. It provides a convenient way of deploying Lambda functions, as well as separating them into staging or production environments if needed. It also manages the creation of API Gateway.

> "CodeWave managed to address our need for automated security scan and they reduced the workload on our existing infrastructure..
>
> Flotiq Team
>
> "

> "The results exceeded our expectations. CodeWave produced a solution, which costs us virtually nothing.
>
> Flotiq Team
>
> "

Results and Benefits

Currently, Flotiq team launches between 40 and 60 staging deployments monthly. This translates to a few hundred AWS Lambda Requests and a few thousand Lambda GB-Seconds. Both of those values are well within the Lambda free tier making the required compute power entirely free of charge.

Generated reports are small XML files (usually less than 1 MB each), with a summary of detected faults. Most of them are generated only once and downloaded only during deployment. This, again, fits into free tier usage of Amazon S3. Once Free tier expires, the final costs will be below $1/mo, especially after applying life-cycle policies.

This not only addresses Flotiq cost considerations but also makes space for extending security and quality scans to other projects, or to all of the existing environments, including the ephemeral environments produced solely for merge request review.

Thanks to the usage of the Serverless Framework, solution deployment is quick and easy, which allows regular updates for scanning rules.

Because some parts of the pipeline were running on the on-premise system, by extracting them, CodeWave managed to reduce system maximum load during deployment by 5-7%.

The same solution deployed in a classical model, on the on-premise server, would require a purchase of separate server instance due to overloaded existing infrastructure. This alone saved Flotiq around $1000 of infrastructure upgrade fees.

CodeWave

aws partner network

Future of Flotiq automatic deployment pipeline

Currently, Flotiq team considers extending the scope of the security scan pipelines to each ephemeral environment, built for feature branch reviews. This will allow developers to act on the scan results quicker, reducing the risk of deploying faulty code to the production environment. If this will prove successful, the production deployment will be protected by security scan results, allowing production deployment only when security reports are “green”.

Considering current costs and Lambda pricing model, in case of extending scans to all branches, the TCO will most likely be lower than $20/mo.

Benefits

Scalable solution

The proposed solution is ready to accept requests for many more projects, making it possible for the customer to grow

Avoided costs

Thanks to serverless nature of the solution, Flotiq team doesn’t have to provision additional servers to satisfy their

Low TCO

The Total Cost of Ownership is reduced to a minimum thanks to the on-demand pricing model and generous AWS

Omni-cloud solution

The use of the Serverless Framework allows the customer to deploy the scanning solution to any AWS region, or even to

About CodeWave

CodeWave is a Select Consulting Partner, with departments specialized in highly available web applications, content management systems, devops support and machine learning.

Since 2008 we empower our clients with technical expertise needed to operate always-on web applications. We build long term relationships with our clients.

amazon web services | Partner Network

CONSULTING PARTNER