

# Carbonetes supports Breached Me to Improve and secure Container deployment



## Breached Applications

Their product provides an added security for company and private individuals by notifying them when their credentials have been compromised. If they don't hear about it fast enough (or at all) then we (the users) blissfully carry on with zero knowledge except for the occasional news article about a breach...but did it really affect me, the consumer? Who knows..

## Breached Container Concern

Breached is dealing with some breach data and yet they have not using any container security tools to secure their own container images. They were worried that they are deploying images with outdated libraries, incompatible versions .

## Breached Me Applied Carbonetes on their Software Development Life Cycle

They use the Carbonetes Jenkins Plugin in their CI/CD. They set it up as a part of the steps their Jenkins job goes through each time they make a deployment. After an image has been built, They immediately scan it using the Carbonetes Serverless Container Scanning and Policy Compliance plugin before ultimately deploying it to Kubernetes.

## Carbonetes as a Solution

Since they use Carbonetes in their CI/CD, there is no longer a need for manual checking for potential breaches before deployment. They no longer have to worry about deploying an image that doesn't work, or is potentially vulnerable. It hastens their deployment cycle as it removes an extra step that they previously do manually. Carbonetes also check their software bill of materials including its licenses that they are using. This gives them awareness which current Open-source software they are using.

Breached Me Uses AWS Elastic Container Registry for Securing their container images. As a partner that also leverages AWS services they put trust in Carbonetes for their container security any data they shared with us and analysis result of their container images is safely stored in our database using AWS RDS.

## About Breached Me



<https://breached.me/>

**Breached.Me is a website that tells you if your information has been breached by hackers. Data breach reporting requirements vary by industry and often we only hear about data breaches long after the fact. In the meantime, our personal information could be traded or sold hundreds of times on the dark web.**



*“It is a Cloud-based container security scanner. No installation needed. Less hassle in maintaining another development tool/application. Carbonetes has Jenkins plugin that’s why it is part of our CI/CD pipeline. One key feature that we really love about in Carbonetes is, it has scan scheduler that helps our images to be come freshly scanned daily/nightly. It also has various integrations such as Jira, which helps us to log and track the Vulnerabilities found in our images; Slack, BitBucket and many more. And another good thing about Carbonetes is, it is always up to date that’s why we don’t need to worry about missing checking the latest vulnerabilities in our scan.”*

*-BreachMe*

## **Why Carbonetes**

The idea of running multiple security tools to scan images for vulnerabilities seems tedious. Carbonetes will allow users to just that with ease. Anyone who wants to mitigate the risk of security breaches and vulnerabilities on their containers in the most efficient way possible should consider using Carbonetes.

## **INCREASED DEVOPS PRODUCTIVITY**

Developers waste a lot of time running their code through various security tools to check individual aspects of their code: open source licenses, open source dependencies, vulnerabilities, secrets and more. Each of these tools has their own workflow and learning curve that drains developer productivity. Many companies skip one or more of these tests because they drag productivity to a crawl. Carbonetes unifies all container analysis into a single streamlined workflow that integrates into your existing product development workflow. This one-stop-shop approach to security significantly increases developer satisfaction and productivity.

## **INTEGRATION**

Packaged integrations with leading tools like Jenkins (CI/CD), Jira (Bug Tracking), top container registries, and a powerful API for custom integrations enables Carbonetes to seamlessly fit into, and automate, any SDLC workflow.

## **About Carbonetes**

Carbonetes is the most comprehensive container security analysis in the market. It can be integrated seamlessly into your CI/CD pipeline so that your containers are automatically scanned and evaluated to ensure their safety.

