

Carbonetes supports Breached.Me for an improved and secured container deployment



Breached.Me as a Software

People regularly check emails, unaware of the potential breaches in the background. Breached.Me is the first line of defense to prevent these potential threats to the users' data so they can focus on improving products and services without worrying about information leakage. Breached.Me will automatically detect these personal data menaces to warn and give users the heads up they need against hackers.

Container Concern

Numerous data breaches are handled by Breached.Me. Ironically, they are yet to employ any container security solutions to protect their images. Concerned that they might deploy images with outdated libraries and incompatible versions, they look for softwares to mitigate possible critical issues.

Jenkins Configuration

Breached.Me integrate the Jenkins Plugin from Carbonetes in their CI/CD. Carbonetes Serverless Container Scanning and Policy Compliance plugin automatically scans images before deploying to Kubernetes. Performing this configuration ensures a seamless and secure deployment.

Carbonetes as a Solution

Employing Carbonetes in their CI/CD, Breached.Me no longer require manual screening for potential breaches prior to deployment. They never worry about deploying vulnerable and inoperative images. It hastens their deployment cycle by eliminating a step they previously did manually. Carbonetes will also check their software bill of materials. This feature gives them awareness of which open-source software they are currently using.

Breached.Me secure container images using the AWS Elastic Container Registry. As a partner that also leverages AWS services, they trust Carbonetes for their container security. Any data they share, including all analysis results of their container images, are safely stored in Carbonetes' database using AWS RDS.

About Breached.Me



<https://breached.me/>

Confidential information could be traded or sold on the dark web hundreds of times. Breached.Me is a website that alerts users if hackers have breached their personal information. Data breach reporting requirements vary by industry; people often only hear about data breaches long after the breach has already happened.



"Carbonetes is a cloud-based container security scanner. No installation is required—less hassle in maintaining another development application. Carbonetes has a Jenkins plugin, which is part of our CI/CD pipeline. One key feature we love about Carbonetes is its scan scheduler. The fact that a scheduled scan has been set up, means we don't need to be concerned about the threat build-up in our images. It also has various integrations such as Jira, which helps us to log and track any vulnerability issues found in our images; Slack, BitBucket, and many more. Another good thing about Carbonetes is that it is always updated. That's why we don't need to worry about missing out on the latest vulnerabilities in our scan."

-Breached.Me

Why Carbonetes

It appears laborious to run numerous security tools to scan images for vulnerabilities. With Carbonetes, users will be able to accomplish that with ease. Anyone who wants to efficiently reduce the risk of security breaches and vulnerabilities on their containers should consider employing Carbonetes in their system.

Increased DevOps Productivity

Developers waste a lot of time running codes through multiple security tools to check individual aspects of their code: open-source licenses, dependencies, vulnerabilities, secrets, and more. Each tool has its workflow and learning curve that drains developer productivity. Many companies skip one or more of these tests because they slow down productivity. 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 powerful API for custom integrations enable Carbonetes to fit seamlessly and automate any Software Development Life Cycle workflow.

About Carbonetes

Carbonetes is currently the most comprehensive container security analysis in the market. It can be integrated seamlessly into your CI/CD pipeline so that you can automatically scan and evaluate your containers to ensure optimal security.

