

Carbonetes Launches Comprehensive Cloud Native Container Security Service

Provides Full Suite of Container Analyzers to Secure DevOps/GitOps Inside Your Preferred CI/CD Tool

HOUSTON, TX, UNITED STATES, May 6, 2021 /EINPresswire.com/ -- [Carbonetes](https://www.einpresswire.com/2021/05/06/carbonetes-comprehensive-container-security-service/) delivers all the tools developers need to analyze the security of their containers in a single unified service. Backed by a policy engine and remediation recommendations, Carbonetes accelerates development, while ensuring security and policy compliance.

Centralized software development is a thing of the past. Kubernetes and containers have enabled microservices that evolve independent of each other at high velocity. Offshoring, Covid-19, and remote collaboration tools have accelerated this trend. Security has not kept pace with these trends. Distributed and independent development cycles have made security compliance a nightmare.

“

Carbonetes provides one-click analysis of all aspects of your containerized code, then evaluates those results against your security policy; Carbonetes does it all.”

Mike Hogan, CEO, Carbonetes

development.

Carbonetes wins the hearts and minds of developers by helping them identify and resolve all



container security issues faster. Instead of the traditional trade-off between code security and development efficiency, Carbonetes delivers both. “Carbonetes provides one-click analysis of all aspects of your containerized code, then evaluates those results against your security policy,” said Mike Hogan, Founder & CEO of Carbonetes, “you no longer have to piece together expensive on-premise security applications and multiple policies; Carbonetes does it all.”

Carbonetes Container Analyzers:

- Infrastructure as Code (IaC): Evaluate your IaC for best practices and minimize your attack surface.
- Software Composition Analyzer: Analyzes open-source tools for dependencies and vulnerabilities.
- License Analyzer: Creates a list of licenses associated with each open-source tool in the container.
- Configuration Analyzer: Identifies risks in container configuration, such as privilege, root access, scaling constraints, memory utilization, and more.
- Secrets Analyzer: Identifies sensitive data in the container that could be compromised, such as passwords, AWS keys, credentials, and more.
- Multi-Engine Vulnerability Analyzer: Provides best of class vulnerability analysis with threat levels, CVE details, and the location in code along with suggested fixes.
- Bill of Materials Analyzer: Analyze all of the layers and artifacts of your containers looking for outdated and insecure applications and libraries.

While developers love a single integrated security solution, they really don't want to learn yet another tool, even one as elegant and efficient as Carbonetes. The company addresses this demand by delivering the full developer experience inside leading CI/CD tools such as Jenkins, TeamCity, CloudBees, Azure Pipelines, Drone, CircleCI, Bitbucket Pipelines, and GitLab Pipelines.

Carbonetes also appeals to security professionals with a full-spectrum policy engine designed for distributed compliance. Security teams can define, test, tune, and enforce their security policies, or industry standard policies like CIS and NIST, uniformly across all the above analyzers.

Carbonetes fits squarely in the realm of developer-centric shift-left container security. However, we are not oblivious to the industry trend of blending developer security and run-time security. Whether you practice GitOps, DevOps, or DevSecOps, there is a recognition that run-time and build-time fit together like chocolate and peanut butter. While IaC is one area of integration, shift-left tools gain considerable insight from run-time usage patterns when prioritizing threat levels. Run-time tools also benefit from continuous scanning to protect against stale images, outdated policies, and new vulnerabilities. The company is already addressing this challenge with run-time integrations like its plug-in for Mirantis Lens. By combining Lens and Carbonetes, your operations team gains visibility into the security of their containers in production, ensuring end-to-end security.

"We built Lens as a Kubernetes IDE - the one place that developers and platform engineers can access everything they need to be successful building and running cloud-native applications. With this new addition to our rapidly growing library of extensions, Lens puts the power of Carbonetes at the fingertips of developers and platform engineers, at the exact moment they need it and without interrupting their workflow," said Miska Kaipainen, Senior Director of Engineering, Mirantis.

By now, you are surely asking yourself: "This sounds amazing, how can I start using Carbonetes right now?" Carbonetes is available through [AWS Marketplace](#) and it offers a 30-day free trial. After the free trial, the service costs \$40 per developer on the monthly plan and \$32 on the annual plan.

Carbonetes delivers answers to some of the most concerning questions:

- Am my Infrastructure as Code (IaC) exposing an unnecessary attack surface?
- Am I using outdated and insecure libraries and apps?
- Do I have vulnerabilities in my code that hackers can exploit?
- Are my containers exposing secrets like passwords and AWS keys?
- Am I subject to open-source licenses that could jeopardize the company's intellectual property?
- Do I have newly discovered vulnerabilities in my Kubernetes cluster?
- What code, libraries and artifacts are in my images, and are they outdated?
- Are my containers compliant with my company's current security policy?

They say that a person is judged on the company they keep. Carbonetes' advisory board is stacked with security industry visionaries including, Mike Viscuso (VC, Founder & former CTO of Carbon Black), Tom Barsi (VP Business Development Palo Alto Networks), Anthony Bettini (CTO White Hat Security, Tech Editor of Hacking Exposed), Jeremy Carlson (OEM Sales Kaspersky), and Brendan Hogan (Strategy & Business Development VMWare).

About Carbonetes:

Carbonetes was founded to solve the shift-left security challenges in a microservices world. If you want faster development, distributed security compliance, and the development and security teams to not only be on speaking terms, but to be friends, then Carbonetes is for you. Try it for free at <https://aws.amazon.com/marketplace/pp/B08C6P4PFZ>

Mike Hogan
Carbonetes Inc.
+1 650-683-0394

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/540424633>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2021 IPD Group, Inc. All Right Reserved.