C A R B O N E T E S

E V A L U A T I O N  G U I D E

Cloud-Native Container Security Done Right

20+ GUIDE

POWERED BY AWS
Hello!

Introduction

Our goal with this Evaluation Guide is to provide you with an overview of Carbonetes features and how you can get the most value from it. We use videos since it gives you a visual hands-on step-by-step introduction to the process.
**Overview**

Kubernetes enables applications to be broken down into large collections of microservices that can evolve independently, resulting in a dramatic acceleration of product development and evolution. However, these microservices, and their respective APIs, result in an exponential expansion of the attack surfaces of the application. Kubernetes has security features to mitigate this, but nothing is perfect. The age-old truism applies: “An ounce of prevention is worth a pound of cure.” Carbonetes enables developers to analyze their code across a variety of criteria to ensure that the code is as secure as possible prior to being deployed in a Kubernetes cluster.

To further complicate things, Covid-19, Work-from-Home, and offshoring have resulted in a dramatic increase in distributed development. This creates additional challenges for security who must have distributed tools for enforcing policy compliance in a distributed model. In fact, the most efficient way to distribute this compliance function is to embed it right into the CI/CD tools your developers are using. This is what Carbonetes provides.

In summary, Carbonetes enables developers to analyze their containers for vulnerabilities, dependencies, secrets, open-source license types, and a complete bill of materials. It then evaluates the resulting data against your policy, resulting in a go, warn, or stop result. Carbonetes then helps developers remediate their repositories to get compliant, prior to deploying into Kubernetes. There is quite a bit more detail, as described below, but this overview should help put Carbonetes’ functions below into context of the problems they solve.
START-UP WIZARD

We’ve created a Start-up Wizard that makes it fast and easy to get your service set-up and derive the maximum value from it. It also walks you through some of the core capabilities. Click image above or here to open the video.

COMPLETE ANALYSIS

With a single click, you can analyze your containers for vulnerabilities, SCA, open-source license types, secrets, and bill of materials (contents of your repositories). Click the image or here to open the video or you can follow the step by step guide below.
**SINGLE ANALYZER**

Maybe you’ve fixed an issue that was found in the Complete Analysis and now you want to verify that fix. Instead of running a complete analysis again, you can run a Single Analyzer. Click image or here to open the video.

**RESOLVING A SECURITY THREAT**

We can view the analysis results using the image overview found on the complete analysis. It provides a report of all of the threats found in the most recent scan of each repository. It also described the fixes for those CVEs that have fixes available. Click image above or here to open the video.
One of the first things that needs to be set up is your registries, so you can start pulling images. Carbonetes growing list of supported registries includes: AWS ECR, Google Container Registry, Azure Container Registry, Docker Private Registry, Quay, and Docker Trusted Registry. The target registry must be accessible via the Internet. Support for on-premise container registries will be released soon. Once your registries have been verified and added, Carbonetes will read the information of the images present on the registries. Click image above or here to open the video.

We often find that pods in production are filled with older and less secure versions of open source applications, libraries and more. One of the best ways to improve your security posture is to use the most current versions of code, because they have been patched against the most recent threats. Click image or here to open the video.
USING SEARCH & FILTERS ON ANALYSIS RESULTS

You’ve analyzed your containers and you have a collection of results, how do you focus on the most important issues? One way is to use search and filters against those results. While search is self-explanatory, Carbonetes offers two types of filters:
1. Filter by Exclusion: The results of the scan provide a collection of tags indicating information found. In this case it shows all of the tags found in the repositories. If you click on the (X) of a tag it will remove that tag and it will remove the repositories in the result set that have this tag.
2. Filter by Inclusion: Clicking on the checkboxes will only include those repositories that have the checked items. If all boxes are unchecked, it includes all. Click image above or here to open the video.

CREATING, EDITING, & TESTING POLICY BUNDLES

Policies are used by the security teams to enforce compliance in a distributed and automated fashion. Click image or here to open the video.
Creating Environments

If you want to use different security policies for different purposes, you can create Environments. For example, you might want a more lenient policy in the development phase, in order to avoid over scanning, but you probably want a license policy as early as possible so the developer doesn't spend a lot of time working with a tool that has an unacceptable open source license. Environments enable you to have specialized policies for different purposes. Click image or here to open the video.

Creating Roles & Their Rights

You might want to define what type of permissions you give your users and teams. You can have different roles with different permissions. A Policy Editor for example, is only allowed to update policies while a Team Manager can only update teams. These roles are fully customizable depending on your needs. Click image above or here to open the video.
Assigning Roles to Users

Roles-Based Access Control (RBAC) is enabled in Carbonetes by defining the various roles and their respective rights, and then assigning those roles to individuals. This video demonstrates how that is done using Carbonetes. Click image above or here to open the video.

Scheduling Scans

When you want Carbonetes to do automated complete analysis to your registries or images. You can choose the time, frequency and type. These types can be of an incremental scan or a full scan. With incremental scans, a complete analysis will only trigger if there are updates to the images. A full scan on the other hand, will do complete analysis even if there are no changes on the image. Click image or here to open the video.
USING JIRA WITH CARBONETES

Jira can be integrated with your Carbonetes account to easily generate tickets based on the vulnerabilities found on your images. You could also view all the generated tickets that are related to your personal images and monitor progress of those tickets. Click image above or here to open the video.

USING INTEGRATIONS

Connect your repositories, JIRA and Slack channel. We also support Github, Gitlab and Bitbucket for versioning. Add your credentials and import the repositories in Carbonetes. These imported repositories can be analyzed on software composition analysis. Click image or here to open the video.
**DASHBOARD & ACTIONABLE ITEMS**

Daily report at a glance. The dashboard is a series of charts and metrics that give you an overview of the files and images you scanned, so you can quickly check the health of your containers. On top of that is the list of actionable items, which need your attention and help you to sort through the noise and get your work done quickly. Click image or here to open the video.

---

**MARKETPLACE**

Carbonetes can be found on the AWS Marketplace. We offer a 30 day trial for each new user and after that, licenses can be purchased from the marketplace and the purchases will be automatically reflected on Carbonetes. Click image above or here to open the video.
In order to provide the most comprehensive analysis, Carbonetes uses multiple vulnerability engines and feeds. It combines the vulnerabilities from these engines, removes duplicates and then normalizes the threat levels based on your settings. Set up how you want to view your vulnerabilities and detect secrets. Prioritize vulnerabilities by their severity (high or low) or which engine’s severity to use. When a vulnerability is detected by multiple engines, Carbonetes will check your settings and select the appropriate threat level. Click image above or here to open the video.

User Management

Invite and add new users. Carbonetes will send an email inviting those users to use the app. Click image or here to open the video.
RUN-TIME SECURITY VISUALIZATION USING LENS

Lens is an open-source tool from Mirantis that provides visibility into your running Kubernetes clusters. The Carbonetes plugin enables you to see the security details for each pod in your cluster, including the scanning history, policy history and also to scan the images in selected pods against current CVEs and your current policy. This provides you with continuous scanning to avoid stale images which can expose various attack surfaces. Click image above or here to open the video.

TEAM MANAGEMENT

Create and assign teams to users. Teams can have different roles that add up to the user’s current role. Teams can also be assigned specific registries they are allowed to access. Click image or here to open the video.
Carbonetes provides plugin integrations such as Jenkins, Drone, TeamCity, CircleCI, Azure, Bitbucket, GitLab. The plugins are designed to scan your images and provide detailed information on vulnerabilities, software compositions, secrets and licenses.
The most comprehensive Container Application Security Testing Solution on the Market.

www.carbonetes.com