VMware Carbon Black Container

Frequently Asked Questions

Features and Support

Q: What are the key capabilities of VMware Carbon Black Container?

A: The key capabilities are listed below:

- Container Image Scanning
  - Provide visibility into all containers running in production and ensure they have been scanned to enforce security policies. Restrict registries and repositories allowed in production, prioritize vulnerabilities by severity, and ensure only approved images are deployed to production.
- Security Posture Dashboard
  - Provides a single pane of glass for complete visibility into your security posture across k8s clusters and namespaces, including visibility into rules violations and configurations. View a consolidated risk score for both vulnerabilities and misconfigurations.
- Prioritized Risk Assessment
  - Prioritize the most severe risks to your Kubernetes environment with the ability to detect and prevent vulnerabilities before containers are deployed by scanning Kubernetes manifests at continuous integration (CI/CD), and on Kubernetes clusters.
- CI/CD Pipeline Integration
  - Integrate into the developer lifecycle to analyze and control application risks before they are deployed into production. Scan containers and Kubernetes configuration files early in the build/deploy lifecycle, so vulnerabilities and misconfiguration can be addressed faster. Automate DevSecOps to deliver continuous cloud-native security and compliance for the full lifecycle of Kubernetes workloads.
- Governance & Enforcement
  - Ensure the integrity of your Kubernetes configurations through control and visibility of workloads that are deployed to your clusters. Customized policies enforce secure configuration by blocking or alerting on exceptions.
-
- Compliance Policy Automation
  - Shift-left into the development cycle to detect and prevent vulnerabilities at build. Create automated policies to enforce secure configuration and ensure compliance with organizational requirements and industry standards such as CIS benchmarking.
- Custom Queries
  - Gain deep visibility into workload security posture and governance to ensure compliance, with the ability to freely explore Kubernetes workload configuration via customized queries.
- Network Connectivity Mapping
  - Understand the application architecture, the connectivity between different workloads, and how they consume services with an egress connection from an external source outside of the cluster.
- Runtime Image Cluster Scanning
  - Scan for vulnerabilities to ensure container images used in any running workload are up to date and detect vulnerabilities.
- Integrated Alerts Dashboard
  - Consolidate events and alerts to a single dashboard to enable faster investigation and correlation of events from both host and container layers.
- Kubernetes Visibility Mapping
  - Get visibility to workload vulnerabilities, misconfigurations, and policy violations with risk scores to better mitigate the risk
- Anomaly Detection
  - Understand what normal network behavior looks like and identify malicious network activity with alerts.
- Egress and Ingress Security
  - Secure egress connections to private and public destinations. Identify malicious egress connections with IP reputation.
- Threat Detection
  - Scan open ports for vulnerabilities to quickly detect and uncover lateral attacks and attacks in progress

Q: Is Carbon Black Container only relevant for Kubernetes (K8s) environments?

A: Carbon Black Container Security can scan images for vulnerability regardless of what orchestration system you are using. The Image scanner (cbctl) is designed to integrate with the CI/CD pipelines to help support the Shift Left security expected from solutions in this space.

Kubernetes is the only container orchestration platform that we currently support. The Carbon Black Cloud will provide security for a variety of workload types including virtualized systems (vSphere), containers (K8's), and classic server systems. Our Container Security offering specifically adds support for securing Kubernetes workloads across on-premises, private and public cloud environments.

Q: What features are offered in each bundle?

A: The Container Essentials Bundle includes the following features:

- Container Image Scanning
- Security Posture Dashboard
- Compliance Policy Automation
- Prioritized Risk Assessment
- Governance Control & Enforcement
- CI/CD Integration
- Topology Map
- Cluster Image Scanning

The Container Advanced Bundle includes everything from Container Essentials in addition to the following features:

- Integrated Alerts
- Threat Detection
- Ingress & Egress Security
- Workload Anomaly Detection

Q: Which vendors/technologies are supported in public and private clouds?

A: Our solution supports Kubernetes (open-source version on cloud or on-prem), PKS/Tanzu, GKE (Google K8s Engine), Open-Shift (RedHat), AKS (Azure K8s Service), Amazon EKS.

Installation

Q: What are the pre-requisites for installation?

A: Before installing, you must meet the following criteria:

1. Kubernetes Security DevOps or Super Admin role assigned to you on the Carbon Black Cloud console.
2. Administrator privilege on your Kubernetes clusters
3. Kubernetes clusters have an admission control plugin with ValidatingAdmissionWebhook enabled.
4. Kubernetes clusters can be controlled using the Kubernetes command-line tool kubectl.
5. The Kubernetes cluster nodes can access the URL of the CBC environment for https requests on port 443. The URL is the CBC environment you are working with.
6. The Kubernetes cluster nodes can access the Event Stream URL for gRPC traffic on port 443.
7. The Kubernetes cluster nodes can pull container images from the Docker hub registry.

Resources

Q: Where can I find technical documentation and demos for our container security offering?

A: Technical Documentation can be found on TechZone:

- TechZone – Carbon Black Container Path

Q: Where can I find updated release notes?

A: Updated release notes can be found using this link: Release Notes

Q: Where can I go for additional resources and to learn more about containers?

A: For more on VMware Carbon Black Container, check out the Container FAQ page in TechZone. To learn more about containers, Kubernetes, and cloud-native applications, we recommend KubeAcademy.