VMware Carbon Black Cloud Container

Full lifecycle container security at the speed of DevOps

AT A GLANCE

Balance business agility and speed to market without compromising security. VMware empowers organizations to secure the complete lifecycle of Kubernetes applications, detect and fix vulnerabilities and misconfigurations before deployment, meet compliance standards, and achieve simple, secure multi-cloud and hybrid cloud Kubernetes environments at scale.

USE CASES

- Secure containers and Kubernetes applications
- Increase visibility into Kubernetes environments
- Scan for container image vulnerabilities
- Ensure security compliance, governance and enforcement
- Kubernetes security posture management

BENEFITS FOR SECURITY TEAMS

- Gain complete visibility into the security posture of Kubernetes
- Enable prioritized vulnerability reporting
- Easily define and customize security policies
- Address vulnerabilities and misconfigurations at build
- Enable speed of delivery without compromising security

BENEFITS FOR DEVOPS TEAMS

- Easily deploy and set up products
- Seamlessly integrate into the CI/CD pipeline and existing processes
- Address vulnerabilities and misconfigurations at build
- Enable speed of delivery without compromising security

Containers and Kubernetes enable organizations to deliver applications fast, but it can't be at the expense of security. Development organizations are actively moving to cloud native applications, containers and platforms such as Kubernetes, and security teams must keep pace with modern application development practices. In contrast, DevOps teams live in a rapid response world tied to a continuous integration and continuous delivery (CI/CD) cycle that can be impeded by security. So, how do you incorporate modern security into your build, deploy and operate lifecycle?

Organizations moving to Kubernetes need to provide visibility for security teams, and set guardrails for development teams through configuration and compliance policies to avoid vulnerabilities and misconfigurations. These policies ensure steady governance and minimal disruption to DevOps workflows, and protect the complete development and deployment cycle without impacting business agility and speed to market.

VMware Carbon Black Cloud Container™ enables enterprise-grade container security at the speed of DevOps by providing continuous visibility, security and compliance for containerized applications from development to production—in any on-premises or public cloud environment. This solution provides security teams with visibility and the ability to enforce compliance while integrating seamlessly into existing DevOps processes to avoid adding operational complexity. With VMware, organizations can reduce risk, maintain compliance, and simplify security for Kubernetes environments at scale.

Complete visibility into Kubernetes security posture

VMware Carbon Black Container provides the visibility and control that DevOps and security teams need to secure Kubernetes clusters and the applications deployed on them. It delivers instant visibility into all workloads with the ability to enforce compliance, security and governance from a single dashboard. This single pane of glass gives complete visibility into the security posture across Kubernetes clusters and namespaces, including:

- Visibility into Kubernetes clusters and workload inventory
- A combined view of all vulnerabilities, misconfigurations and rules violations
- Workload configuration risk reporting and governance
- A consolidated risk score aggregated for all workload attributes to prioritize remediation

With VMware, application security and DevOps teams gain full visibility into Kubernetes environments to proactively harden workloads, and better identify and reduce the risks posed by vulnerabilities and misconfigurations.

FEATURES

- Security posture dashboard
- Container image scanning
- Compliance policy automation
- Prioritized risk assessment
- Governance and enforcement
- CI/CD integration
- Integration with Harbor registry

PLATFORM SUPPORT

- Upstream Kubernetes
- VMware Tanzu™ Kubernetes Grid™
- Red Hat OpenShift
- Amazon Elastic Kubernetes Service (EKS)
- Google Kubernetes Engine (GKE)
- Azure Kubernetes Service (AKS)

For information on additional platforms supported, please reach out to a VMware representative.

TECHNICAL REQUIREMENTS

- Connection to VMware Carbon Black Cloud™
- Admin privilege on your Kubernetes clusters

FOR MORE INFORMATION OR TO PURCHASE VMWARE PRODUCTS

Call 877-4-VMWARE (outside North America, +1-650-427-5000), visit *vmware.com/products*, or search online for an authorized reseller. For detailed product specifications and system requirements, please refer to the product documentation.

INTRINSIC SECURITY

At VMware, we take an intrinsic approach to delivering security—building it into the infrastructure everywhere workloads are deployed. Through this unique approach, we can eliminate the trade-off between security and operational simplicity by providing a single source of truth for security, infrastructure and development teams to accelerate response to critical vulnerabilities and attacks, while reducing friction.

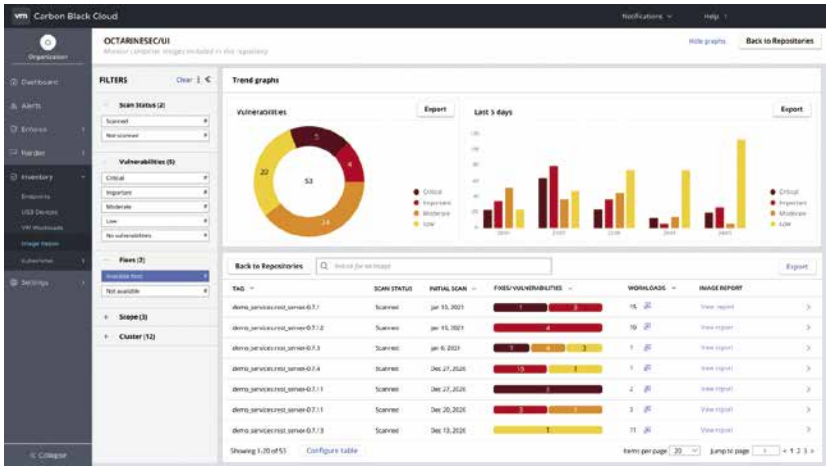

FIGURE 1: Prioritized vulnerability reporting in the security posture dashboard.

Secure the complete lifecycle of Kubernetes applications

Carbon Black Cloud Container integrates into the developer lifecycle to analyze and control application risks before they are deployed into production. This purpose-built solution automates DevSecOps, delivering continuous cloud native security and compliance for the full lifecycle of Kubernetes workloads:

- Integrate with the CI/CD pipeline for seamless guardrails
- Scan container images for vulnerabilities at build
- Create and enforce content-based security policies quickly and easily with simple policy management
- Customize and automate security policies and controls to harden the desired state and avoid configuration drift
- Enable reporting and enforcement of security posture across all workloads deployed in Kubernetes clusters

VMware achieves this goal with a simple, no-friction deployment process and a user-friendly platform that covers any Kubernetes cluster on any public cloud or on-premises deployment.

Simplify operations for security and DevOps teams

The agility and flexibility that Kubernetes and its configuration-as-code approach provide should not be a trade-off for security. At the same time, security can't be a roadblock to faster production deployments that drive business. Organizations need a solution that keeps their apps safe within their existing pipeline.

With VMware, security is maintained without slowing down developers and operators. Our solution empowers cross-functional teams to secure the complete lifecycle of Kubernetes applications, detect and fix vulnerabilities and misconfigurations before production deployment, meet compliance standards, and achieve simple, secure multi-cloud and hybrid cloud Kubernetes environments at scale.