VMware Carbon Black Container Essentials

Automate DevSecOps to achieve full lifecycle container security at the speed of business

At a glance

Balance business agility and speed to market without compromising security. 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

- Securing containers and Kubernetes applications
- Kubernetes Security Posture Management (KSPM)
- Container image scanning
- Container image hardening
- Increase visibility into Kubernetes environments
- Ensure security compliance, governance and enforcement

Key benefits for DevOps teams

- Fast and easy deployment and setup
- Seamlessly integrate into the CI/CD pipeline and existing processes
- Address vulnerabilities and misconfigurations at build
- Enable speed of delivery without compromising security
- Complete visibility into application connectivity and configuration

Containers and Kubernetes enable organizations to deliver applications faster than ever, but they can't be deployed at the expense of security. Adversaries can use APIs to compromise clusters and access sensitive data from these workloads, either on premises or in the cloud. Security needs to be seamlessly integrated at each layer throughout the development lifecycle to effectively protect against attacks. When it comes to building modern applications, security is a team sport and cannot be an afterthought.

To address this growing threat, coupled with the increased complexity of modern environments, security requires a multilayered approach that spans the full application lifecycle. A unified security strategy from development to production is critical for detecting vulnerabilities and misconfigurations early in application development to minimize the attack surface for the growing threats that containers pose to organizations. By starting with the build phase, DevOps and Security teams can create workloads that are secure by design. These teams need the visibility into their workloads in the runtime layer to secure Kubernetes clusters and the applications deployed on them.

VMware Carbon Black Container™ Essentials 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 powerful solution provides DevOps and Security teams with detailed visibility, context and the ability to enforce compliance while integrating seamlessly into the existing application build and deploy processes to simplify operations. With VMware, organizations of all sizes can reduce risk, maintain compliance, and simplify security for Kubernetes environments at scale.

Key benefits for security teams

- Gain complete visibility into the security posture of Kubernetes
- Enable prioritized vulnerability reporting
- Easily define and customize security policies
- Enable developers to address vulnerabilities and misconfigurations at build
- Enable speed of delivery without compromising security
- Connect image vulnerabilities to specific running workloads

Features

- Security posture dashboard
- Continuous container image scanning
- Compliance policy automation
- Prebuilt, customizable policy templates, including CIS benchmarks
- Risk-prioritized assessment of vulnerabilities and misconfigurations
- Security policy 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.

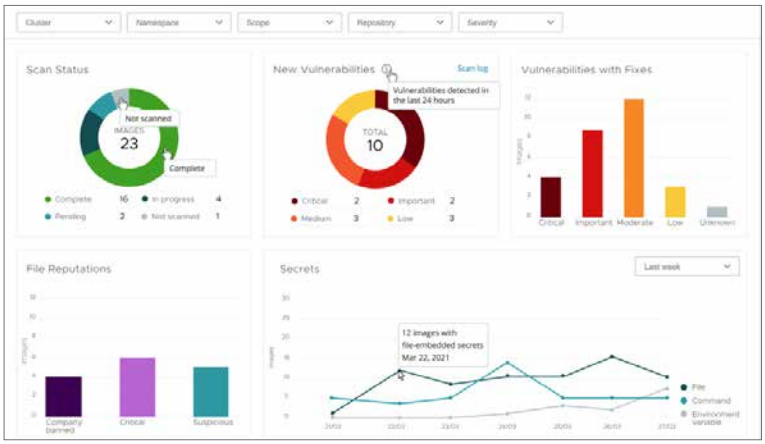

Figure 1: Continuous scanning of container images

Continuously scan container images throughout the development lifecycle

Scanning container images for vulnerability and misconfiguration is one of the best ways to reduce risk and exploitability. Due to the ephemeral and distributed nature of containers, images need to be scanned before they are deployed to successfully identify and reduce risk. While it is critical to scan these images throughout the Continuous Integration/Continuous Deployment (CI/CD) pipeline, monitoring the image posture in a dynamic environment like Kubernetes by continuously scanning running images is just as important.

Any image vulnerabilities or misconfigurations in a container image must be detected before that image is deployed, or those vulnerabilities will be more widespread across the environment. With VMware Carbon Black Container, DevOps teams can scan images throughout the development lifecycle within the CI/CD pipeline, before deployment and in production. This crucial visibility allows DevOps and Security teams to ensure only approved images that meet your organization's compliance and security standards are being deployed in production.

By automating runtime image scanning, organizations can easily detect zero-day vulnerabilities to ensure continuous security and compliance—without disrupting business agility. Only VMware Carbon Black Container provides robust risk prioritization that combines vulnerabilities and misconfigurations in a single dashboard to allow DevOps teams to focus on the most exploitable and critical risks and close security gaps quickly. Security teams can enforce security standards and compliance by restricting container deployments to prevent running unauthorized workloads. They can also configure minimum security standards and compliance requirements to align with security frameworks, such as Security Technical Implementation Guides (STIG) or Security Technical Implementation Guides (CIS), along with Kubernetes best practices. These policies can be automated, making proper configuration easier than ever. Leveraging prebuilt compliance templates, organizations can further customize to their specific environment and needs.

Technical requirements

- Connection to VMware Carbon Black
- Admin privilege on your Kubernetes clusters
- Cluster nodes can access dashboard.confer.net for https requests on port 443 (or alternate option port 50051)

VMware security

At VMware, we are taking 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.

Gain complete visibility into Kubernetes security posture

Organizations adopting 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 deployment lifecycle without impacting business agility and speed to market. 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.

The Security Posture Dashboard provides a single pane of glass with complete visibility into security posture across Kubernetes clusters or applications, 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
- Visibility and governance into developer activity on Kubernetes

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. Organizations can use the image repository to take inventory of the risks associated with an image, and directly align that vulnerability with a running workload.

Secure the complete lifecycle of Kubernetes applications

VMware Carbon Black 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 workloads running in Kubernetes:

- Integrate with the CI/CD pipeline for seamless guardrails
- Scan container images for vulnerabilities at build and runtime
- 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 Carbon Black achieves this goal with a simple, no-friction deployment process and a user-friendly platform that protects any Kubernetes cluster on any public cloud or on-premises deployment.

Secure modern apps with network runtime visibility

The dynamic nature of cloud native environments is what makes them so powerful, but it comes at a cost to security. DevOps and Security teams often lack visibility into workloads that are running in a given cluster, and the connectivity to and from those workloads.

To simplify this process, the network visibility map allows you to view these workload connections in a single map of the application architecture. The network visibility map provides detailed information and context to better understand the application architecture and network traffic behavior. Tracking the application's internal and external traffic by customizing group-to-group internal or external IPs can help gain the control required in such a chaotic environment.

To get a clean view of an application, filters allow the connectivity of the map to remove unnecessary "noise" such as system namespaces. You can also use similar filters to better understand what connection is encrypted or not encrypted to gain full visibility into your application traffic posture. The goal of the networking map is to give teams a better understanding of the connectivity and configuration of applications installed in the cluster.

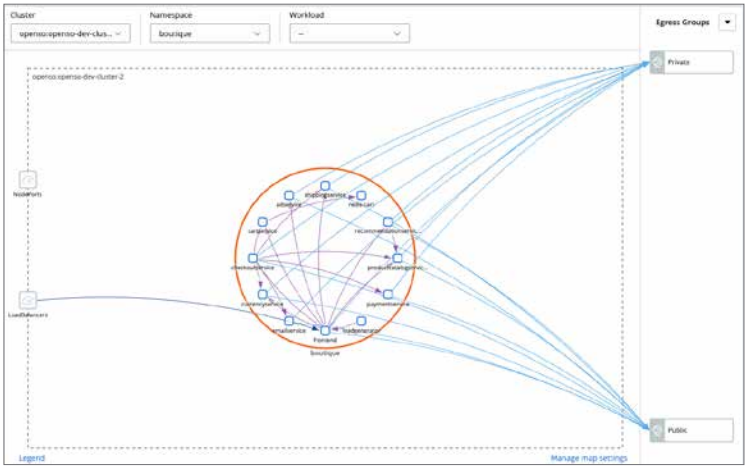

Figure 2: Workload connectivity in the Network Map.

Learn more

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.

Automate runtime cluster scanning

While CI/CD integration and a "shift-left" approach is an effective strategy, continuously monitoring security posture in production is required. Cluster scanning provides the same level of visibility as scanning applications developed in CI/CD to third-party and infrastructure-level components. It is critical to ensure container images used in any running workload are up to date and can detect vulnerabilities.

Runtime cluster scanning ensures all running images are scanned for misconfigurations and vulnerabilities to better evaluate overall risk; for example, confirming the configuration and manifest that is applied still aligns with the policy, identifying vulnerable misconfigurations, and ensuring the cluster itself doesn't have any clear text secrets or malicious containers running. This enables DevOps and Security teams to understand the level of security in the run state, and to make changes to the pipeline if necessary to better secure workloads.

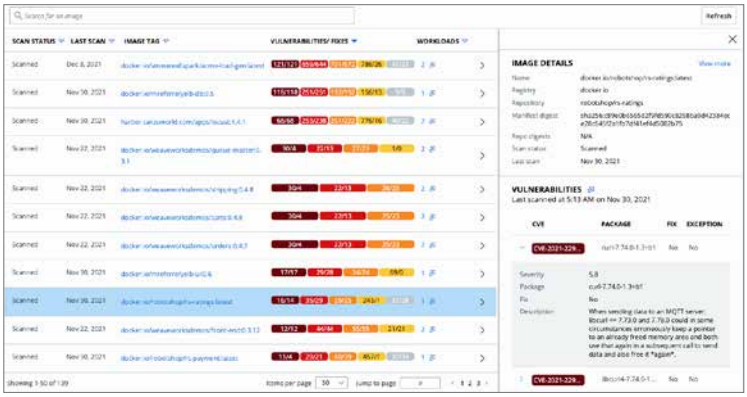

Figure 3: Scanned images in a running cluster.

Simplify operations for DevOps and Security 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. VMware Carbon Black Container empowers cross-functional teams to secure the complete lifecycle of Kubernetes applications, detect and fix vulnerabilities and misconfigurations early in the development lifecycle, meet compliance standards, and achieve simple, secure multi-cloud and hybrid cloud Kubernetes environments at scale.