VMware Carbon Black Container Advanced

Enterprise-grade Kubernetes security

At a glance

Increase visibility for security teams into containerized workloads at runtime, adding enforcement options for EDR, NDE and UEBA to containers.

Use cases

- Securing containers and Kubernetes applications
- Increase visibility into Kubernetes environments
- Container image vulnerability scanning at runtime
- Build behavior models for applications to identify and alert on anomalies

Key benefits for security teams

- Secure egress connections to private and public destinations
- Identify malicious egress connections with IP reputation
- Use machine learning and AI to build network behavior model for workloads
- Identify malicious network activity
- Consolidate events and alerts into a single dashboard
- Gain visibility into Kubernetes clusters, networking flow and application architecture

Containers and Kubernetes have become synonymous with the modern apps transformation as organizations increasingly adopt hybrid, multi-cloud architectures and break down legacy monolithic applications into distributed microservices. However, this transformation brings new development paradigms that have significant security implications. The container attack surface has grown in orders of magnitude relative to virtualized applications, providing many more points of entry for attackers who have already taken notice of the paradigm shift and new software ecosystem.

The complexity of Kubernetes environments combined with the ephemeral nature of containers and frequent use of open source components requires a multilayered security approach that addresses each layer (hypervisor/public cloud, Linux/Windows OS, Kubernetes and containers) and integrates seamlessly throughout the entire application lifecycle from development to production.

VMware Carbon Black Container™ brings VMware's deep knowledge and expertise in workloads and security to Kubernetes to help organizations reduce risk, maintain compliance, and achieve simple, secure Kubernetes environments at scale. With a fast and easy deployment process, this user-friendly solution provides immediate visibility and control that Security teams need to secure Kubernetes clusters and the applications deployed on them. Security teams gain instant visibility into all Kubernetes workloads, with the ability to enforce compliance, security, and governance from a single dashboard. With VMware, organizations can implement comprehensive built-in security for a holistic DevSecOps approach—from workloads and pipeline to the infrastructure they run on.

Runtime security for containers

The most important goal of container runtime security is to eliminate noise and alert on real and active events, or use tools to block them immediately without affecting the application and user experience. Effective runtime security for containers must address runtime image scanning and threat detection to understand overall security posture and manage risk. As a result, the ability to enforce compliance and security governance becomes easier. For example, correlation between the Kubernetes node and the container's events are crucial to better understanding overall security posture and mitigate risk. With VMware Carbon Black Container, security teams can reduce false positives and achieve accurate network anomaly detection and response to manage risk without impacting business agility.

Key benefits for DevOps teams

- Gain visibility into application connectivity with in-cluster network visibility map
- Risk-prioritized vulnerability assessment of container images at runtime
- Understand misconfiguration of secret management in Kubernetes

Features

- Runtime image and cluster scanning
- Network visibility map
- Ingress and egress security
- Workload anomaly detection
- Integrated alerts for workloads and containers
- Threat detection
- Customizable egress groups

Platform support

- Kubernetes platforms:
  - VMware Tanzu™
  - Amazon Elastic Kubernetes Service (EKS)
  - Microsoft Azure Kubernetes Service (AKS)
  - Google Kubernetes Engine (GKE)
  - Red Hat® OpenShift®
  - SUSE
  - Upstream
  - Rancher
  - VMware Tanzu™ Kubernetes Grid™
- Linux OS:
  - Linux kernel — 4.8 +
- Cloud Network interface (CNI):
  - Antrea, Calico, Flannel, Canal, Wave, Cilium, VMware NSX NCP

If you have additional platforms, we likely support them! Please reach out to a VMware Representative for more information.

Integrated alert dashboard

Workload security is more than just securing containers and virtual machines; for example, a security risk caused by the combination of events that occurred in both the container layer and the host layer. Integrated alerts consolidate these events into a single dashboard to allow better investigation and correlation of different types of events for different types of objects.

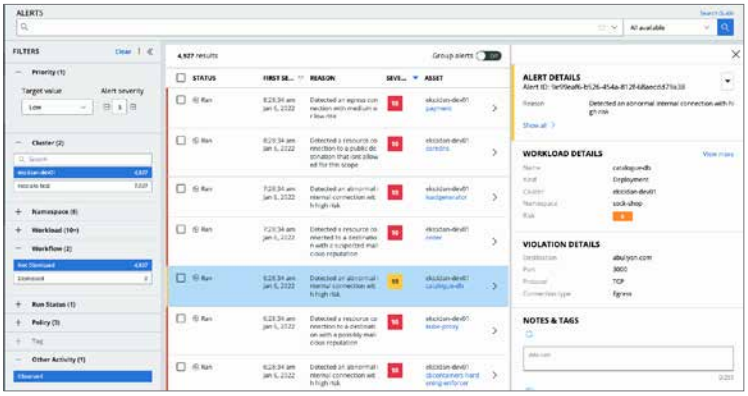

Figure 1: The integrated alert dashboard allows security teams to correlate between hardening, runtime and vulnerability scanning data

Workload anomaly detection

Cloud native architecture is declarative, and by leveraging network visibility and ingress and egress management, we can create a model for how applications should run and connect. VMware Carbon Black Container uses machine learning and AI to build a network behavior model for workloads to send an alert if the behavior is deviating from that model. The workload anomaly detection model is for ingress, egress and internal connections.

Threat detection

Threat detection is especially critical for stopping lateral attacks—where an attacker gains initial access into your network environment and leverages that access to get deeper into your network and workloads. One of the best ways to stop this type of attack is by identifying scans of open ports, which is crucial to uncovering an attack in progress. If an attacker tries to exploit a vulnerability to find the next lateral move, the internal port scan and egress port scan will raise an alert.

Technical requirements

- Connection to the VMware Carbon Black Cloud™
- Admin privilege on your Kubernetes clusters
- Root privilege POD running on every node (daemonset)
- 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.

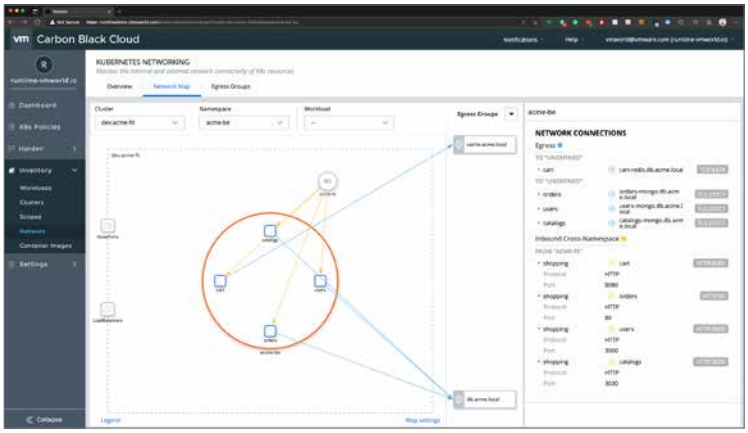

Figure 2: Network visibility map showing ingress and egress connections with detailed context.

Ingress and egress security

The ingress is the entry point for any connection to the Kubernetes cluster. The service that will be exposed externally will, in most cases, be either the load balancer or ingress controller. Most organizations will leverage their current infrastructure to divert traffic to this service, and eventually to the application behind it. VMware Carbon Black Container ingress identification provides visibility into the external source that is reaching out to the Kubernetes service to know if it is malicious or not.

Egress management is even more important than ingress. If there is malicious code inside a cluster, it will use egress since this is the primary exit point for Kubernetes services inside the cluster. By managing the egress groups and checking for the destination IP/DNS against known IP reputations, risk scoring is added to the connection and can alert on other rogue IPs. For security teams, egress control easily provides detection of data being exfiltrated out of the cluster.

Item No: 1265124aq-ds-cb-cld-cnt-adv-uslet 3/22