Trend Vision One™ – Container Security

Simplify container security with advanced image scanning, policy-based admission control, and runtime protection, detection, and response

Modern application development strategies are becoming more prevalent among companies looking to increase the speed that new capabilities and features are delivered, driving additional customer value. However, with the endless benefits of cloud-native application development come with a major risk: lack of security and fragmented tooling. Today's organizations are challenged to meet the objectives of both security teams and application teams, as they operate with different resources and priorities. On top of that, microservice-based architectures are changing how organizations transition to cloud, container, and serverless platforms, requiring an integrated platform approach to cloud security.

With the technology's many benefits, containers have become mainstream. According to the Cloud Native Computing Foundation (CNCF), **88% of organizations are using containers today**, and the majority are running them in production. Container environments have also become quite diverse, with many organizations running containers on-premises and in the cloud, and Kubernetes has emerged as the de facto aid to assist with orchestration and streamline operations.

Security teams are facing new challenges

With production workloads shifting to cloud-native platforms and DevOps teams adopting security best practices across their build pipelines and runtime deployments, security solutions need to be designed to succeed across hybrid- and multi-cloud environments (physical, virtual, cloud, containers, and serverless). With security teams absorbing more cloud security responsibilities, you need trusted security controls in place from build-time to runtime. This promotes tool consolidation and collaboration of security and compliance requirements without interfering in continuous integration/continuous delivery (CI/CD) development cycles.

Introducing Trend Vision One™ – Container Security

Delivering container image security, container admission control policy, and container runtime protection, detection, and response. Container Security enables earlier and faster detection of malware, vulnerabilities, and compliance violations. Your security operations and application teams are able to address and remediate issues before they can be exploited in production, decreasing cost and complexity.

Define policies once and manage container risk

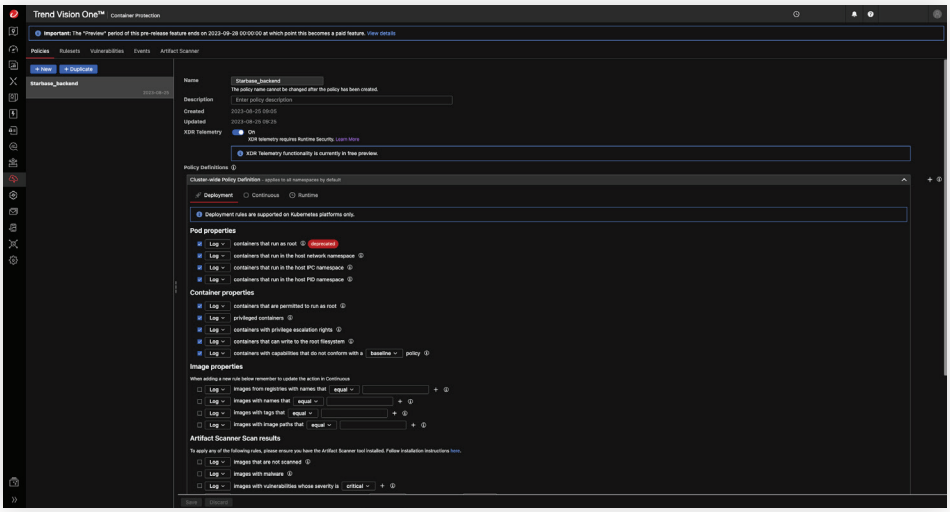
Select and define policies so that only the most secure Kubernetes container are deployed with container admission control. Integrating directly with Kubernetes, Container Security can define the policy that either allows or blocks the image from running. This is based on preferences you've defined once, including whether it is a privileged container or whether it has been scanned for malware and vulnerabilities. This gives your security team control over the containers that are allowed to run in their environment.

Runtime protection gives your security team an additional layer of defense. This provides you with alerts and indicators of attacks (IoA) across running containerized applications with insights aligned to the MITRE ATT&CK framework. Get visibility of risks in running containers, discover attempts to run disallowed commands or illegally access files, and detect and respond to suspicious activity with extended detection and response (XDR) capabilities.

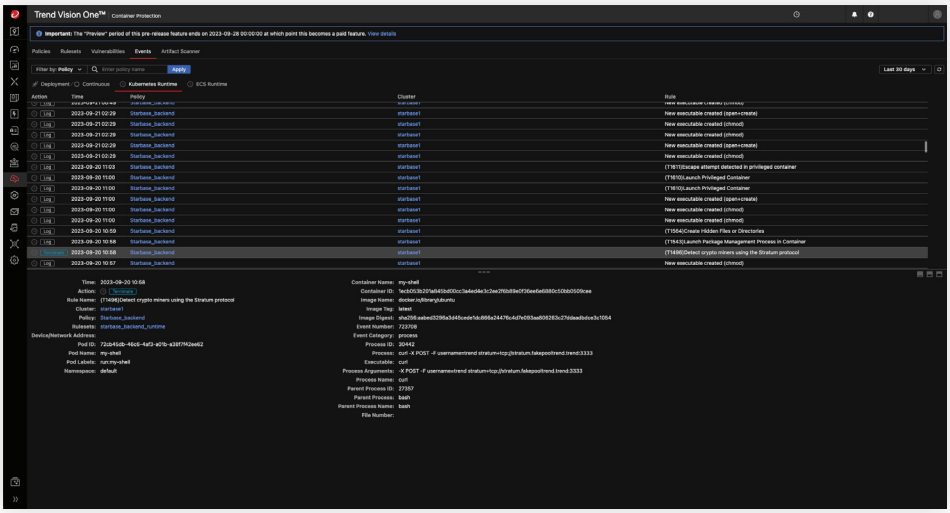
End-to-end container protection

Container Security helps DevOps teams deploy security with immediate and continuous protection, from the build pipeline to runtime. With support for leading container platforms including Amazon EKS, Amazon ECS, AWS Fargate, Azure AKE, and Google GKE, Container Security can be seamlessly integrated across your existing CI/CD toolchains and container environments. Implementing effective security earlier in the software build-pipeline helps to achieve consistent results faster in the development cycle and reduces manual security steps and application downtime. In addition, runtime protection, detection, and response shields running containers from evolving threats and allows for the investigation of activities across layers. Simplify resource management with a clear and organized overview of your Kubernetes clusters' inventory.

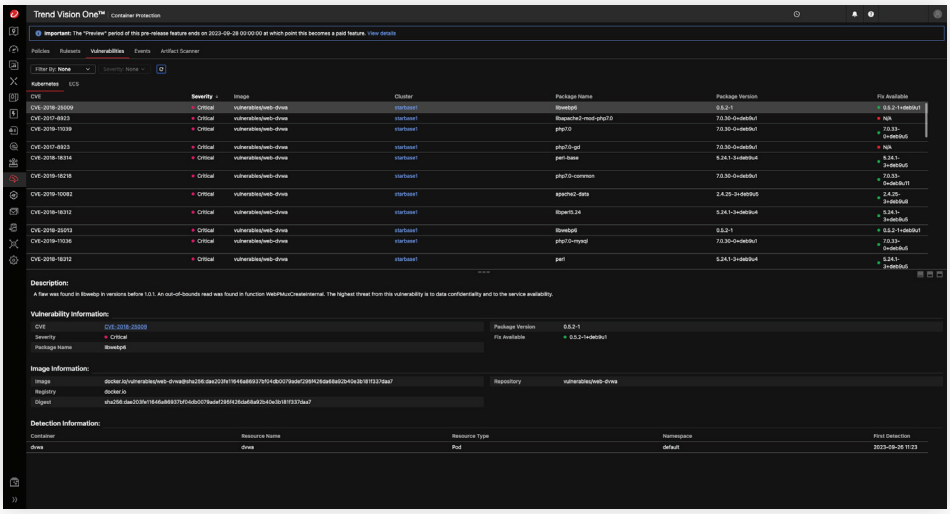
Admission control policy



Container runtime protection



Container vulnerability view



Proven Leadership

- A Leader in the Forrester New Wave™: Extended Detection and Response, Q4 2021
- Ranked #1 for Cloud Workload Security Market Share for the 6th consecutive year (2023)
- MITRE Engenuity ATT&CK (2023) - #1 in the protection category, with 100% detection of all critical attack steps.

Key Advantages

Address security issues before they can be exploited in production

Container Security provides image scanning to detect threats present in directly installed apps and apps that were installed via a package manager. Fix issues fast with actionable insights, enabling developers to remediate issues before deployment via their existing tools and workflows.

Ensure ongoing container security

Policy-based deployment control, through a native integration, ensures the Kubernetes deployments you run in your production environment are safe.

Container Security enables you to create policies that allow or block deployments based on a set rules that include pod and container security properties and the results of container image and registry scans. When an image is ready to be deployed with Kubernetes, the admission control webhook is triggered, which checks whether the image is safe to deploy and either allows or blocks it from running.

Protection with full visibility, detection, and response

Once deployed, protect containers with runtime protection for additional assurance. Discover and block suspicious activity, get visibility of vulnerable running containers and container drift, and detect, track, and investigate cross-layer threats or activities with XDR.

Learn more about host-based security. Visit the Trend Vision One™ – Workload Security webpage

Container Security capabilities

1. Continuous and automated container image scanning

What we look for:
Container Security generates and scans a software bill of materials based on the container image. This allows you to ensure issues are fixed early and filter out false positives by correlating patch layers with packages that are vulnerable in the same image. Container Security will scan images for:

- **Malware detection**
- **Vulnerability assessment**
- **Policy compliance**

Scan images in your CI/CD build pipeline, ensuring your images are secured from the first build and remain protected from future unknown threats.

2. Container admissions control policy

Using native Kubernetes integration, Container Security can define policies that ensure that only compliant containers run in production environments. Container Security admission control policies allow you to:

- **Build policies based on container image scanning and detection**
- **Only allow images that meet specific application or organization security policies to run in Kubernetes**
- **Define advanced policies—such as disallowing images set as privileged containers—or allow exceptions based on names or tags**

3. Container runtime protection

Runtime protection ensures containers running in your environment continue to be protected even after they've been deployed, giving you:

- **Kubernetes cluster inventory**
- **Visibility of vulnerable running containers**
- **Protection from attempts to run disallowed commands, illegally access files, container drift, and other suspicious activity**
- **Context to detect, track, and investigate cross-layer threats or activities with XDR**

System requirements:

- Kubernetes 1.14.0 or greater on a Kubernetes Certified platform (or equivalent).
- Helm 3.0.1 or greater

For more information visit trendmicro.com/container_security

Deployment and Integration

Container Security provides a valuable step in your CI/CD pipeline.

To perform policy-based deployment control, create a Kubernetes cluster (or open your existing Kubernetes cluster) and install the policy-based deployment controller. Next, create a policy that Container Security will enforce for the cluster. Finally, test the policy.

Visit the **Trend Vision One – Container Security Documentation** page for more information on how to get started, use cases, and more.

For more information, please visit **trendmicro.com**