Trend Cloud One™ – Container Security

Continuous protection for your container images and registries, automated within your CI/CD pipeline

Cloud-first application development strategies are becoming more prevalent amongst companies looking to improve the speed of deployment and cohesive application ecosystems. However, today's organizations find it hard to manage traditional security solutions with those required by DevOps teams and business units, as they operate with different resources and priorities. On top of that, microservices architecture approaches to application development are changing how organizations transition to cloud, container, and serverless platforms.

According to IT analyst and research firm, **ESG**, the number of organizations committed to or interested in a hybrid cloud strategy has increased from 81% to 93% since 2017. Furthermore, as this cloud-first strategy progresses, **Gartner** estimates that "90% of global organizations will be running containerized applications in production by 2026—up from 40% in 2021. Additionally, **Help Net Security** reports that 60% of respondents said Kubernetes was their preferred or only way to deploy new production applications , with 43% of all workloads already in K8s today .

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). To break down silos and build synergy between IT security and DevOps, 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.

Trend Cloud One™ – Container Security* delivers container image and registry security, container admission control policy, and container runtime protection. Designed for your developer and security operations teams, Container Security image and registry scanning enables earlier and faster detection of malware, secrets/keys, compliance violations, and vulnerabilities, including those found in open-source code dependencies. In addition, our Trend Cloud One™ solution gives you the ability to detect threats in package manager installed and directly installed apps by using Trend Micro industry-leading security. Container Security also enables your developers to embed best-in-class open-source vulnerability detection by Snyk for early detection and mitigation of vulnerabilities in open-source code dependencies.

With our container admission control, policy-only images with valid credentials and those that meet defined policies will be deployed. Using integration directly with Kubernetes open policy agent, Container Security can define the policy that either allows or blocks the image from running. This is based on a defined criterion, 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.

Container Security runtime protection gives your IT team an additional layer of defense. This SaaS solution for cloud-native security provides you with alerts and indicators of attacks (IoA) across running containerized applications. While runtime protection is deployed within the cluster, for all containerized applications within each node, a model of expected behavior is built via Learning Mode.

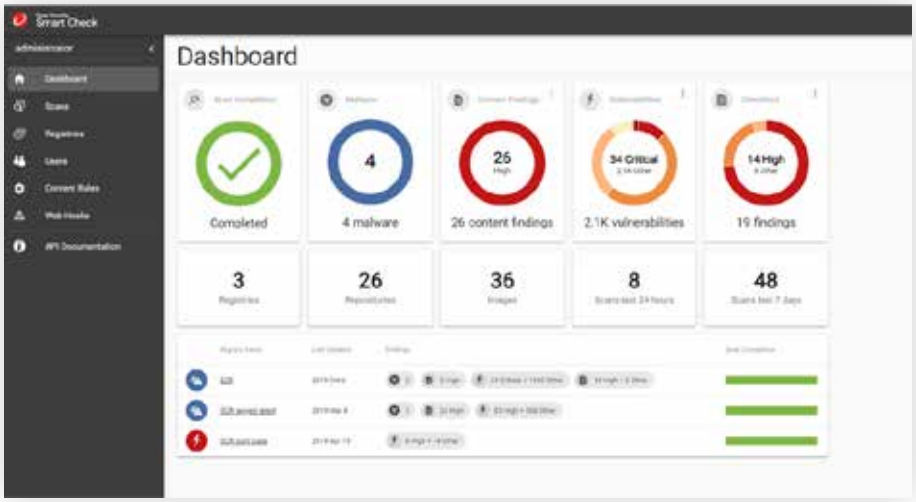
End-to-end scanning optimized for DevOps

Container Security helps DevOps teams deploy security with immediate and continuous protection, from the build pipeline to runtime. Optimized for leading container platforms including AKS, EKS, and GKS, Container Security can be seamlessly integrated into your existing toolchain. You get complete automated product functionality via a comprehensive catalog of APIs that are purpose-built to integrate into your CI/CD pipeline. Application architects and developers are given the ability to bake security-as-code into build pipelines for container image and registry scanning. 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.

Modern cloud-native protection

Our 15 global research centers, 450 internal researchers, coupled with non-intrusive security in the CI/CD pipeline empowers your IT teams to find issues earlier reduce disruption of development schedules and workflows. Container Security allows your security engineers to meet compliance requirements without impacting productivity by delivering policy compliance scanning with customizable polices. Your teams are also given runtime visibility so they can discover attempts to run disallowed commands or access files without permissions. Along with dashboard visibility, notifications and detailed log history allows for easy reporting and auditing.

Container Security container image and registry security



Container Security admission control policy

Key Advantages

Prevent exploits from build to runtime

Thanks to Trend's industry-leading protection, Container Security provides image scanning to detect threats present in directly installed apps and apps that were installed via a package manager. The proprietary Snyk open-source vulnerability database offers early detection and mitigation of vulnerabilities in open-source code dependencies.

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 optimized for DevOps

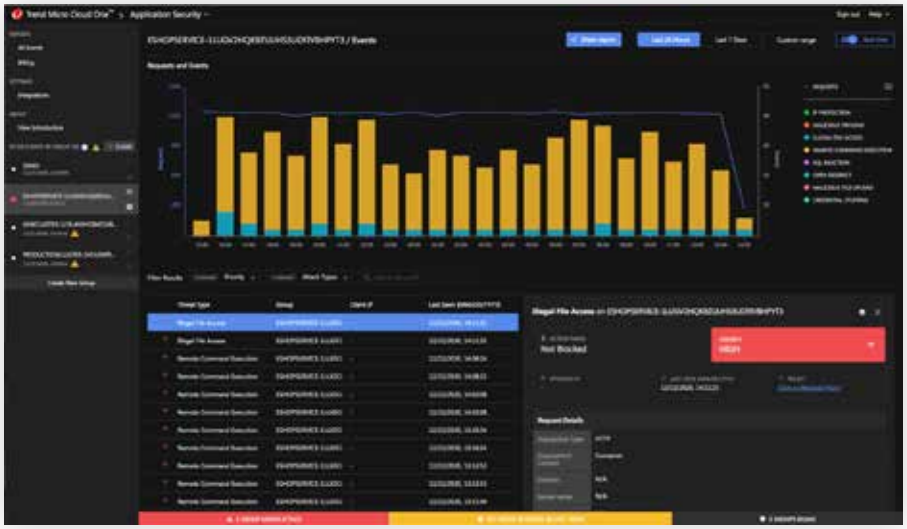
Container Security allows your application architects and developers to bake security-as-code into their build pipeline for container image and registry scanning. Implementing effective security earlier in the software-build pipeline helps to achieve consistent results faster in your development cycle and reduces manual security steps and application downtime.

Full lifecycle container protection

In addition to Container Security, Trend Cloud One™ – Workload Security provides host-based protection for your container hosts and integrates at the operating system level. This is done with real time anti-malware scanning against malicious files and intrusion prevention services to protect against remote exploits of software vulnerabilities. In addition, Workload Security can be configured for optimal inspection of network traffic, including east-west inter-container traffic.

Using both Container Security and Workload Security together will ensure the complete security of your container environments.

Container Security container runtime protection



Container Security capabilities

1. Continuous and automated container image scanning

What we look for:

Container image security scans and unpacks each layer and performs detailed scans on your content. 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**
- **Secrets, such as private keys and passwords**
- **Policy compliance**
- **Open-source vulnerabilities via Snyk**

What you can do:

Continuous scanning can be introduced in two ways. The first is through the CI/CD build pipeline, prior to the container being pushed into the registry. The second is by continuously scanning the registry for new malware and vulnerabilities in ready-to-use images. This ensures your images are secured from the first build and remain protected from future unknown threats. Container Security is registry agnostic across multiple cloud providers, including ECR, ACR, and GCR. As a bonus, you can also utilize Container Security APIs to invoke scans through your build pipeline and make decisions through image assertion and container image signing services, based on scan results.

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. Automate management tasks and policy via code, as part of a CI/CD pipeline**

3. Container runtime protection

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

- **Deployment within the cluster for all containerized applications within each node**
- **Greater visibility into attempts to run disallowed commands or attempts to illegally access files**
- **A model of expected behavior via Learning Mode along with the ability to switch to full block mode when you are ready to go to production.**

4. Console management and access control

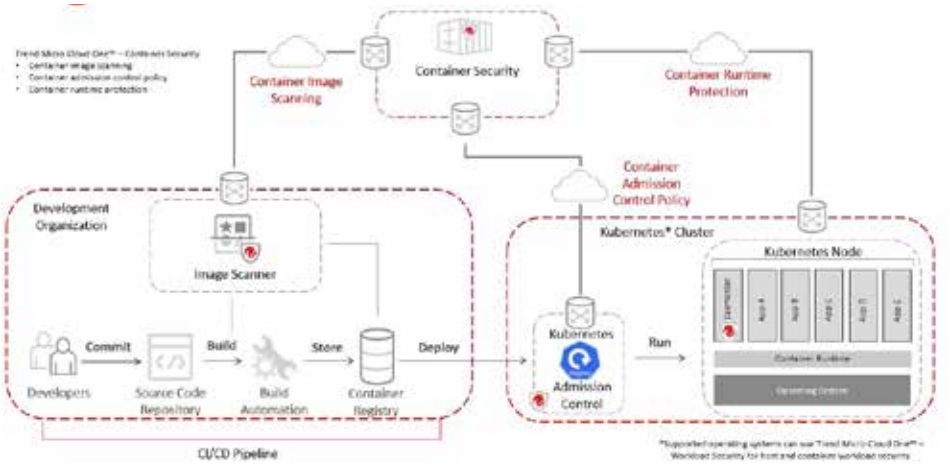
Container Security provides an extensive graphical user interface (GUI) management console. This includes a scan coverage dashboard, scan results, and scan target (view) configuration, as well as user and view management for role-based access control (RBAC). This GUI shows you:

- **Content sources: A list of configured registries that are being scanned/monitored**
- **Active scans: The status of any scan in progress**
- **Protection coverage: The portion of the total images in a target registry that have been scanned**
- **Scan alarms: Results that include detections of malware, vulnerabilities, and secrets**

World-class threat feed

Receive up-to-date threat feeds from both private Trend sources and public sources for scanning performance, this allows you to:

- **Detect malware via the Trend Micro™ Smart Protection Network™ infrastructure.**
- **Discover zero-day threats detected by machine learning algorithms.**



Container Security admission control policy

Installation

Container Security is supported on the Kubernetes platform within a Kubernetes cluster.

- **Public:** https://github.com/deep-security/smartcheck-helm

Container Security users are given access to a shell script and a suite of Kubernetes resources in the Container Security GitHub repository. The images that comprise the application are available in Docker Hub.

Protection across the container lifecycle

Complementing Container Security image scanning capabilities, Workload Security provides advanced protection for runtime containers, with real-time malware protection, container vulnerability shielding, container traffic inspection, as well as protection for your container host, Kubernetes layers, and more.

System requirements:

- Kubernetes 1.14.0 or greater on a Kubernetes Certified platform (or equivalent). See www.cncf.io/certification/software-conformance/
- Helm/Tiller 2.14.1 or greater
- Google Chrome™ browser to access the container image scanning administrator console.

Supported registries

Container Security allows catalog listing and scanning in any registry that supports the Docker V2 API.

- Amazon Elastic Container Registry (ECR)
- Microsoft Azure Container Registry (ACR)
- Docker Trusted Registry (DTR)
- Google Container Registry (GCR)
- VMware Harbor
- JFrog Artifactory
- Sonatype Nexus
- Red Hat Quay Container Registry

For more information visit trendmicro.com/en_ca/ business/products/hybrid-cloud/cloud-one-container-image-security.html

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 Cloud One – Container Security Documentation page for more information on how to get started, use cases, and more.

Build Secure. Ship Fast. Run Anywhere.

Ready on:

Kubernetes and Docker: Container Security deploys as a helm chart for easy installation within a Kubernetes cluster and provides advanced build-time, as well as registry image scanning for malware, vulnerabilities, secrets, and policy compliance. Workload Security will provide additional protection for containers at runtime, as well as monitor for changes in container platforms, orchestration tools, files, and processes, ensuring full protection across your container lifecycle

Amazon Web Services (AWS): Container Security deploys to Amazon Elastic Container Service for Kubernetes (EKS) for container image scanning, and with the addition of Workload Security, you get runtime container and Amazon Machine Image (AMI) workload protection across your AWS environment.

Microsoft Azure: Container Security deploys to Azure Kubernetes Service (AKS) for container image scanning, with additional runtime container and Azure virtual machine (VM) protection available through Workload Security.

Google Cloud™: Deploy Container Security to your Google Kubernetes Engine (GKE) for build pipeline image scanning, with additional runtime container and VM instance protection available through Workload Security. Deploy Container Security in GKE to provision scanning across multiple cloud environments.

Red Hat OpenShift: Container Security can be deployed into your OpenShift environments and secure your applications with advanced scanning during the software build pipeline. Runtime containers can be secured through Container Security (on supported hosts) to ensure full lifecycle container protection.

VMware Cloud™: Workload Security strong integration across VMware services ensures consistent protection across your virtual and cloud-based workloads, including containers, with broad platform and kernel support, automated policy management, and hypervisor-based security.

Container Security is part of Trend Cloud One, a security services platform for cloud builders, which also includes:

- **Trend Micro™ Cloud Sentry:** Visibility of the threats in your AWS environment with quick, actionable insights in the context of your application
- **Trend Cloud One™ – Application Security:** Security for serverless functions, APIs, and applications
- **Trend Cloud One™ – Conformity:** Cloud security and compliance posture management
- **Trend Cloud One™ – Endpoint Security:** Protection, detection, and response across
- endpoints, servers, and cloud workloads
- **Trend Cloud One™ – File Storage Security:** Security for cloud file and object storage services
- **Trend Cloud One™ – Network Security:** Cloud network layer IPS security
- **Trend Cloud One™ - Open Source Security by Snyk:** Visibility and monitoring of open source vulnerabilities and license risks
- **Trend Cloud One™ – Workload Security:** Runtime protection for workloads (virtual, physical, cloud, and containers)

*Trend's container security offering integrates with Snyk in Trend Cloud One - Container Security.

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