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. Additionally, microservices architectures are presenting new layers of security complexity. Organizations are adopting a cloud-first approach to application design, and are focusing on container and serverless platforms. This approach expands the attack surface through loosely coupled services that are developed, deployed, and maintained independently.

ESG, an analyst firm, recently conducted a survey that outlined a “cloud-first policy”, which indicated that 39 percent of the companies surveyed deploy new applications using public cloud services—unless there is a compelling case to deploy using on-premises resources.

With production workloads shifting to cloud-native platforms and DevOps teams adopting security best practices across their build pipelines and cloud-native applications, security solutions need to be designed to succeed across environments (physical, virtual, cloud, containers, and serverless). This provides synergy between IT security and DevOps practices. It also promotes tool consolidation and collaboration of security and compliance requirements, without interfering in continuous implementation/continuous delivery (CI/CD) development cycles.

Trend Micro Cloud One™ - Container Image Security delivers automated build pipeline and registry image scanning with detection for malware, vulnerabilities, secrets, and policy compliance. Designed for developers, it adapts to their surroundings by protecting images earlier in the CI/CD pipeline. Container Image Security allows DevOps teams to continuously deliver production-ready applications and meet the needs of the business—without impacting build cycles.

### Key Advantages

**Prevent exploits prior to runtime**
- Protect against malware, vulnerabilities, and secrets with build-time and registry scanning of container images. Ensure threats are detected before applications are deployed.

**Protection optimized for DevOps**
- Implement frictionless security early in the CI/CD workflow with security as code and automated protection that won’t slow down your DevOps processes.

**Full life cycle container protection**
Continuous scanning optimized for DevOps

Container Image Security helps DevOps teams adopt frictionless security with immediate, continuous scanning for threats, vulnerabilities, secrets, and compliance. Container Image Security also provides dashboard visibility, notifications, and scanning logs for compliance assistance. Optimized for leading container platforms, Container Image Security can be seamlessly integrated into your existing toolchain.

Automate processes with APIs

Container Image Security provides complete automated product functionality using a comprehensive catalog of application programming interfaces (APIs), purposely built to integrate into your CI/CD pipeline. Container Image Security allows application architects and developers to bake security as code into applications prior to runtime. Implementing effective security earlier in the software build pipeline helps to achieve consistent results earlier in the development cycle and reduces manual security steps by automatically scanning images against new vulnerabilities and malware.

Smart protection

Container Image Security reduces disruption of development schedules and workflows with unmatched research and detection of threats, as well as non-intrusive security for the CI/CD pipeline. Container Image Security eliminates the complexity and volume of threats with detection of vulnerabilities, secrets, and zero-day malware using Trend Micro™ Smart Protection Network™.

Compliance-ready protection

Container Image Security allows security engineers to meet compliance requirements without impacting productivity and interfering in the CI/CD pipeline. What’s more, it delivers policy compliance scanning, with customizable policies to meet compliance and governance needs. Container Image Security also offers detailed log history, allowing for easy reporting and auditing.
CONTAINER IMAGE SECURITY CAPABILITIES

Advanced image scanning
When scanning, Container Image Security unpacks each layer of the image and performs detailed scans on the content. Ensure issues are fixed early on and filter out false positives by correlating patch layers with packages that are vulnerable in the same image. Container Image Security will scan images for:

- Malware detection
- Vulnerability assessment
- Secrets, such as private keys and passwords
- Policy compliance

Continuous protection
Container Image Security scans can be invoked when images are first built and will continually scan in the registry for new malware and vulnerabilities. This ensures your golden images are secured from the first build and remain protected from future threats. What's more, you can scan your images across multiple cloud environments from a single Container Image Security deployment.

Automated pipeline security
The full functionality of Container Image Security is available via APIs for fully-automated integration with your CI/CD pipeline.

- Add registries and target repositories with tags for scanning
- Automatically initiate subsequent image re-scans to check against new vulnerabilities when updates are received
- Invoke scans at any stage of the pipeline using the Container Image Security API
- Ensure that only clean images proceed through the pipeline and block bad images using image assertion
- Derive results from Container Image Security, via Webhook, to accommodate specific automated workflows. For example, a Docker® image signing service could be written to sign and promote images based on scan results

Enforce compliance
Container Image Security provides advanced compliance scanning, with customizable policies to ensure you meet both internal and external requirements. Container Image Security's scan logs support business and audit needs with detailed scan history and results.

Console management and access control
Container Image Security provides an extensive graphical user interface (GUI) management console that 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).

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

Scanned image details
Container Image Security provides DevOps with security details and output, allowing for immediate response to any issues.

- List of image layers that have been scanned
- Malware flag, including file name and location
- Content findings, including secrets or indicators of compromise (IOCs)
- Vulnerability details, including:
  - The number of common vulnerabilities and exposures (CVEs) by L/M/H CVSS rating
  - Layer and package information for each CVE
  - CVE and link to CVE file
  - Fix/patch version

World-class threat feed
Container Image Security receives up-to-date threat feeds from both private Trend Micro sources and public sources for scanning performance.

- Provided by Trend Micro via the Trend Micro™ Smart Protection Network™ infrastructure for malware detection
- Machine learning algorithms to detect zero-day threats
WORKLOAD SECURITY COMPLEMENTS CONTAINER IMAGE SECURITY BY PROVIDING LEADING CONTAINER HOST PROTECTION OF THE OPERATING SYSTEM

Protection across the container life cycle

Complementing Container Image 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.

CONTAINER IMAGE SECURITY ARCHITECTURE

Installation

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

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

DEPLOYMENT AND INTEGRATION

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

It scans your container images and your preferred registry, such as Docker. All Container Image Security operations are available through a documented collection of APIs to simplify integration into your CI/CD pipeline. Its APIs can be invoked automatically by your CI/CD system to start scans when an image is pushed to a private Docker registry, for example. Scan results are also available through the API.

The Container Image Security API includes a Webhook facility that allows CI/CD components to register. This allows you to receive notifications of scan events, such as "scan completed", giving you the ability to automate workflows.

System requirements:

- Kubernetes 1.8.7 or higher
- Helm/Tiller 2.8.1 or higher
- Docker 17.06 or higher
- OpenShift 3.11.82

Supported registries

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

- Amazon Elastic Container Registry
- Azure Container Registry
- Docker Trusted Registry
- Google Container Registry
- Harbor
- JFrog Artifactory
- Nexus
- Red Hat Quay

For more information visit trendmicro.com/containerimagesecurity
BUILD SECURE. SHIP FAST. RUN ANYWHERE.

Kubernetes and Docker: Container Image 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, such as Docker, and orchestration tools, like Kubernetes’ files and processes, ensuring full protection across the container life cycle.

Amazon Web Services™ (AWS): Container Image 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 Image 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.


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

VMware Cloud™: Workload Security’s 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 Image Security is part of Trend Micro Cloud One™, a security services platform for cloud builders, which also includes:

- Trend Micro Cloud One™ – Workload Security: Runtime protection for workloads (virtual, physical, cloud, and containers)
- Trend Micro Cloud One™ – Application Security: Security for serverless functions, APIs, and applications
- Trend Micro Cloud One™ – Network Security: Cloud network layer IPS security
- Trend Micro Cloud One™ – Conformity: Cloud security and compliance posture management