Trend Micro™

DEEP SECURITY™ SMART CHECK – CONTAINER IMAGE SECURITY

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

Traditional security for development teams has been functionally separated, with different tools for different departments operated by different resources. However, this monolithic approach is changing rapidly as organizations look to transition development operations to cloud and container platforms.

Security solutions need to be designed to succeed across environments (physical, virtual, cloud, and containers). This provides synergy between IT security and DevOps practices to help with tool consolidation and collaboration of security and compliance requirements without interfering in continuous implementation/continuous deployment (CI/CD) development cycles.

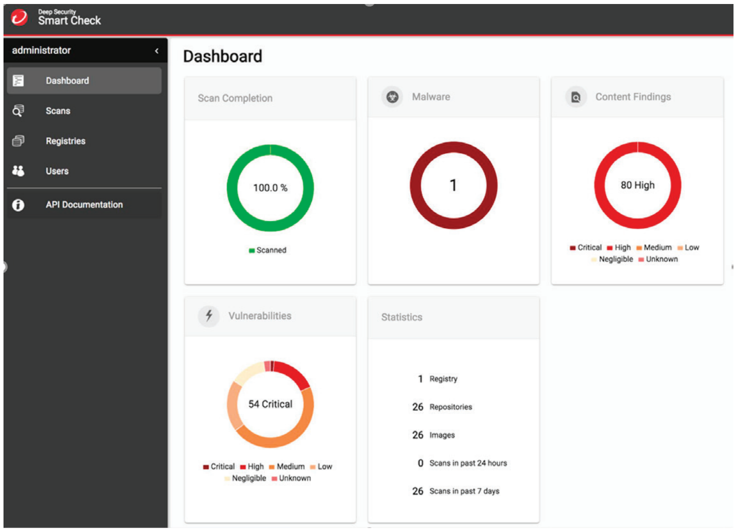
Trend Micro™ Deep Security™ Smart Check – Container Image Security delivers automated build-time and registry-image scanning with detection for malware, vulnerabilities, secrets, and policy compliance. This is designed to secure images earlier in the CI/CD pipeline without negatively impacting the ability for DevOps teams to continuously deliver production-ready applications and meet the needs of the business.

Continuous scanning optimized for DevOps

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

Automate processes with APIs

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



1 Registry
26 Repositories
26 Images
0 Scans in past 24 hours
26 Scans in past 7 days

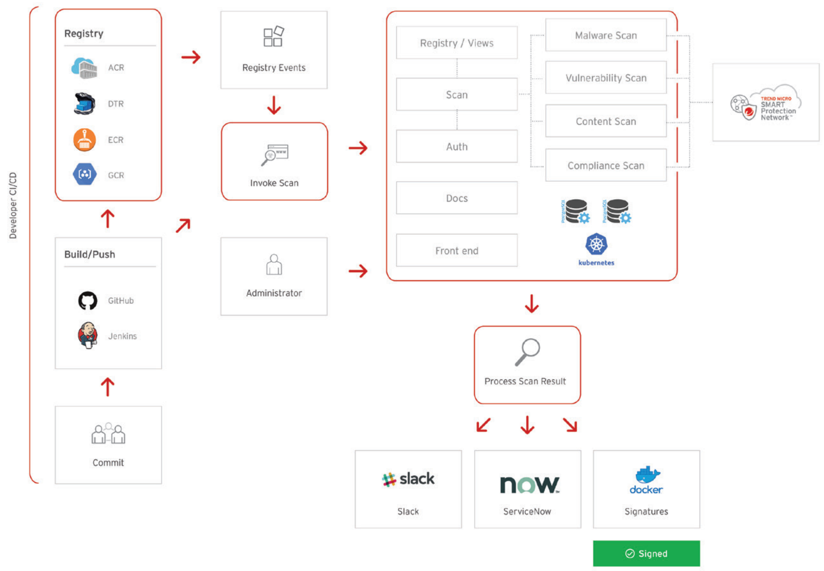
Smart protection

Smart Check – Container Image Security reduces disruption of development schedules and workflows with unmatched research and detection of threats, along with non-intrusive security for the CI/CD pipeline. Smart Check – 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

Smart Check – Container Image Security allows security engineers to meet compliance requirements without impacting productivity and interfering in the CI/CD pipeline. It delivers policy compliance scanning, with customizable policies to meet compliance and governance needs. Its detailed log history allows for easy reporting and auditing.

SMART CHECK – CONTAINER IMAGE SECURITY ARCHITECTURE



Key Advantages

Prevent exploits prior to runtime

Protect against malware, vulnerabilities, and secrets with build-time and registry scanning of Docker® 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

Trend Micro provides leading runtime protection, complementing Smart Check – Container Image Security for full life cycle container security.

SMART CHECK – CONTAINER IMAGE SECURITY CAPABILITIES

Advanced image scanning

When scanning, Smart Check – 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. Smart Check – Container Image Security will scan images for:

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

Continuous protection

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. Scan your images across multiple cloud environments from a single Smart Check – Container Image Security deployment.

Automated pipeline security

The full functionality of Smart Check – 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
- Subsequent image re-scans to check against new vulnerabilities are auto-initiated when updates are received
- Invoke scans at any stage of the pipeline using the Smart Check – Container Image Security API
- Ensure that only clean images proceed through the pipeline and block bad images using image assertion
- Results can be delivered from Smart Check – 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

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

Console management and access control

Smart Check – 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, along with 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 scans in progress
- Protection coverage: Shows what portion of the total images in a target registry have been scanned
- Scan alarms: Shows results that include detections of malware, vulnerabilities, and secrets

Scanned image details

Smart Check – Container Image Security provides DevOps with security details and output, allowing for immediate response to any issues.

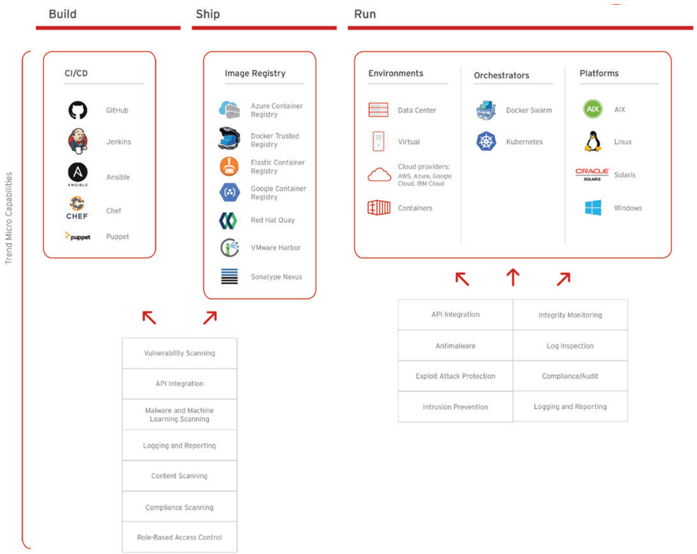
- List of image layers that have been scanned
- Malware flag, including file name and location
- Content findings, including secrets or indicators of compromise (IOCs)
- Vulnerability details, including:
  - The number of common vulnerabilities and exposures (CVEs) by L/M/H CVSS rating
  - Layer and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

World-class threat feed

Smart Check – 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 Smart Protection Network infrastructure for malware detection
- Machine learning algorithms to detect zero-day threats

TREND MICRO COMPLEMENTS SMART CHECK – CONTAINER IMAGE SECURITY BY PROVIDING LEADING HOST PROTECTION OF THE OPERATING SYSTEM



Protection across the container life cycle

Complementing Smart Check – Container Image Security's image scanning capabilities, Trend Micro provides advanced protection for runtime containers, with real-time malware protection, container vulnerability shielding, container traffic inspection, and more.

SMART CHECK – CONTAINER IMAGE SECURITY ARCHITECTURE

Installation

Smart Check – Container Image Security is supported on the Kubernetes platform, within a Kubernetes cluster.

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

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

Deployment and Integration

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

It scans Docker images in any registry that implements the Docker Registry API. All Smart Check – Container Image Security operations are available through a documented collection of APIs to simplify integration into your CI/CD pipeline. Trend Micro's APIs can be invoked automatically by your CI/CD system to start scans when an image is pushed to a Docker registry. Scan results are also available through the API.

The Smart Check – Container Image Security API includes a Webhook facility that allows CI/CD components to register in order to receive notifications of scan events, including "scan completed", allowing you to automate workflows.

Container Image Security includes an administrator console that provides:

- A dashboard (system-wide summary of scan information, including metrics)
- A view summary (including scan results and metrics for the view)
- User management
- Registry and view configuration
- Access to scan results
- Scan history

BUILD SECURE. SHIP FAST. RUN ANYWHERE.

Ready on:

Kubernetes and Docker: Smart Check - Container Image Security deploys as a helm chart for easy installation within a Kubernetes cluster, and provides advanced build-time and registry Docker image scanning for malware, vulnerabilities, secrets, and policy compliance. Trend Micro will provide additional protection for containers at runtime, as well as monitor for changes in Docker and Kubernetes files and processes, ensuring full protection across the container life cycle.

Amazon Web Services (AWS): Smart Check - Container Image Security deploys to Amazon Elastic Container Service for Kubernetes (EKS) for container image scanning, with additional runtime container and Amazon Machine Image (AMI) workload protection available through Trend Micro Cloud One™, a security services platform for cloud builders, for protection across your AWS environment.

Microsoft® Azure™: Smart Check - 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 Deep Security for full Azure protection.

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

Red Hat OpenShift: Smart Check - 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 Trend Micro Cloud One (on supported hosts) to ensure full life cycle container protection.

VMware Cloud™: The strong integration Trend Micro has across VMware® services ensures consistent protection across your virtual and cloud-based workloads, with broad platform and kernel support, automated policy management, and hypervisor-based security.

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

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

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

For more information visit
trendmicro.com/smartcheck

Smart Check - Container Image Security is part of the Trend Micro Hybrid Cloud Security solutions. Also included within our Hybrid Cloud Security is Trend Micro Cloud One™, consisting of:

- **Trend Micro Cloud One™ - Workload Security:** Runtime protection for workloads (virtual, physical, cloud, and containers)
- **Trend Micro Cloud One™ - File Storage Security:** Security for cloud file and object storage services
- **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

Securing Your Connected World

[DS02_DeepSecurity_SmartCheck_Container_Image_Security_200108US] trendmicro.com