Trend Micro™

DEEP SECURITY™ SMART CHECK

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. This has led to organizational reviews on how to best secure new approaches to business application development while maintaining the integrity and confidence in the organization's overall server security posture.

Today's security administrators require acute awareness of cyber threats in order to protect the types of environments and platforms being used within an organization. As the speed of business changes, cybersecurity is shifting to the left and development teams are now being tasked with identifying and protecting against threats not only at run time but prior to deployment as well.

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

Deep Security™ Smart Check delivers automated continuous image scanning with both vulnerability assessment and malware detection, image assertion, and access control. This is designed to secure images earlier in the CI/CD (Continuous Implementation/Continuous Delivery) 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

Deep Security Smart Check helps DevOps teams adopt frictionless security with immediate, continuous threat and vulnerability scanning, dashboard visibility, notifications, and scanning logs for compliance assistance. Smart Check is optimized for leading container platforms with Docker API 2.0 support such, as Docker Trusted Registry, Amazon Elastic Container Registry, Azure Container Registry, and Google Container Registry, and is integrated with leading SIEMs and orchestration tools like Jenkins, Kubernetes, SumoLogic, Splunk, and more.

Reduce manual processes with APIs for automated image scanning protection

Deep Security Smart Check provides complete automated product functionality using a comprehensive catalog of APIs purposely built to be integrated into your CI/CD pipeline. Smart Check allows application architects and developers to bake security-as-code into applications prior to run-time, effectively shifting security to the left to achieve consistent results earlier in the build cycle, while reducing manual security steps by automatically scanning images against new vulnerabilities and malware.

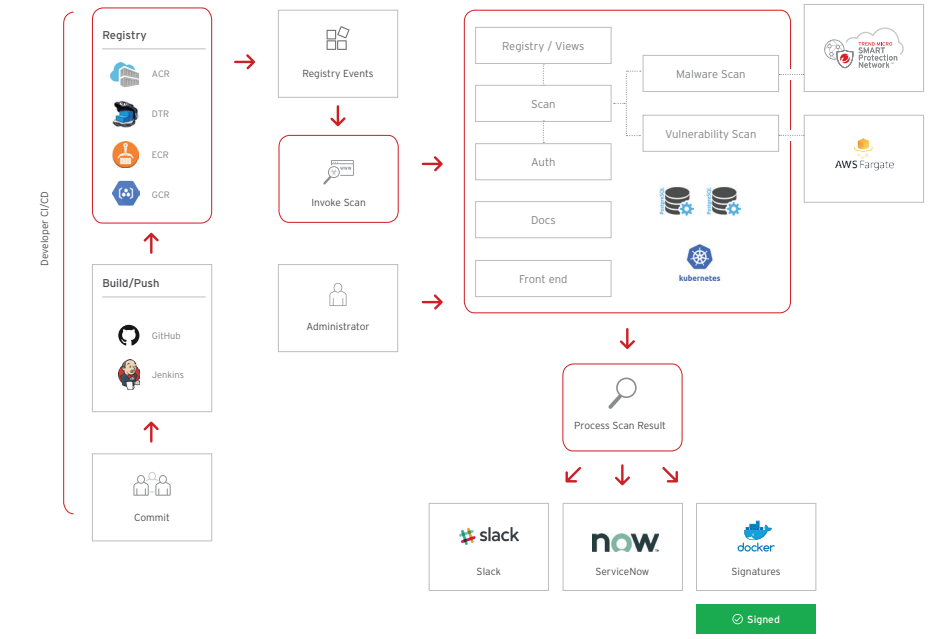
Smart protection

Deep Security Smart Check 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 eliminates the complexity and volume of threats with vulnerability assessment and zero-day machine learning malware detection using Trend Micro's global Smart Protection Network.

Compliance-ready protection

Deep Security Smart Check allows security engineers to meet compliance requirements without impacting productivity and interfering in the CI/CD pipeline. Smart Check delivers critical vulnerability assessment and malware detection capability for assurance across environments. This helps simplify audit reporting with log history in order to help address compliance and governance requests.

Deep Security Smart Check Architecture



Key Advantages

Prevent exploits prior to runtime

Protect against vulnerabilities and malware with pre-runtime scanning of Docker images. Ensure threats are detected before applications are deployed.

Expedite deployments with image assertion

Provide development engineers with RESTful APIs and the ability to automatically push images that meet security requirements to production for faster business cycles.

Complements Deep Security runtime protection

Deep Security provides leading host protection along with Docker container protection, complimented by Deep Security Smart Check for image/container protection.

SMART CHECK CAPABILITIES

Multiple scanning techniques

DevOps teams are delivering software releases with greater reliability and performance. Ensuring that containers are not vulnerable must be implemented early in the build cycle prior to runtime.

- Malware detection
- Vulnerability assessment
- Use results to fix issues before the images are scheduled into the orchestration environment (e.g.: Kubernetes)
- Prevent the execution of malicious code and the deployment of vulnerable software

Automating operations

The full functionality of Smart Check 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
- Results can be delivered from Smart Check 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 – this type of service is considered a customer integration because it requires intimate knowledge of a customer's operating environment (it must have access to image signing keys or orchestrator admission controllers)

Scan console dashboard for management and visibility

Smart Check provides an extensive GUI management console that includes a scan coverage dashboard, scan results, scan target (view) configuration, along with user and view management.

- Content Sources - Shows a list of configured registries which are being scanned/monitored
- Active Scans - Shows the status of any scans in progress
- Protection Coverage - Shows what portion of total images in a target registry that has been scanned
- Scan Alarms - Shows results that include detections of malware and/or vulnerabilities

Scanned image details

Smart Check provides DevOps with security details and output, allowing for immediate response to any issues that may disrupt the build cycle or impact deployment.

- List of Image layers that have been scanned
- Malware flag, including file name and location
- Vulnerability details including
  - The number of CVEs by L/M/H CVSS rating
  - Layer and package information for each CVE
  - CVE and link to CVE file
  - Fix/Patch version

Threat feeds to protect against vulnerabilities

Smart Check 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™ (SPN) infrastructure for malware detection
- Machine learning algorithms to detect zero-day threats

Risk and compliance assistance

Configure Smart Check to retain scan history logs for a period of time that suites your business and audit needs. Smart Check reporting provides security architects with peace of mind and response to image vulnerability health checks.

- Scan type
- Date/Time/Duration
- Results

Key Business Issues

Secure the migration of traditional applications

Move from monolithic to microservice-orientated architecture with security baked into the continuous integration pipeline through automation, allowing consistent results and fewer manual security steps. Additionally, Deep Security for containers protects against key host-based threats and vulnerability exploitation that can occur between containers and their shared kernel at the host level. This includes key capabilities such as Intrusion Prevention, Application Control, Integrity Monitoring, and Behavioral Analysis to secure against vulnerabilities.

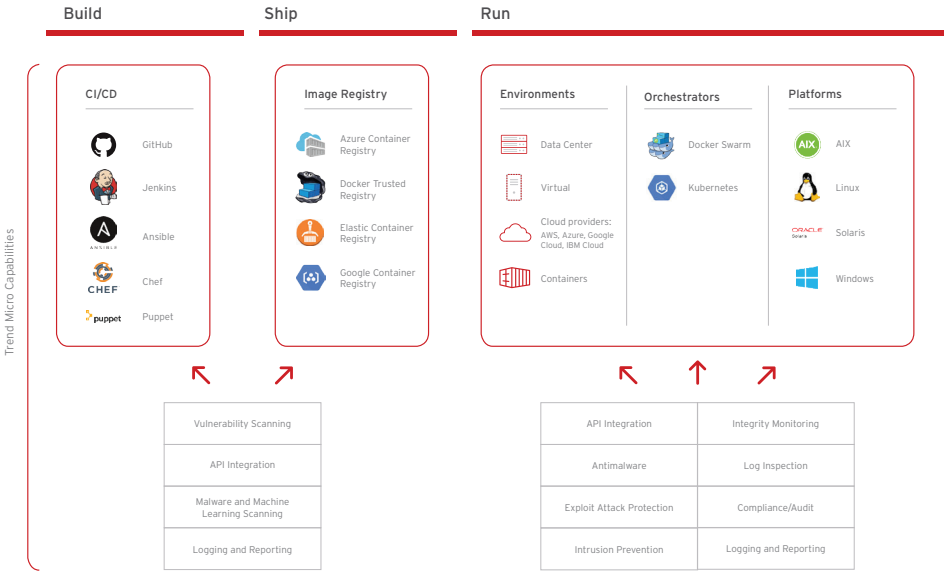
Continuous integration protection

Implement security early in the CI/CD workflow process where image vulnerabilities are less likely to impact production and business reputation, and can be identified, tracked, and mitigated automatically, without relying on manual interaction.

Compliance

Help meet compliance requirements with critical vulnerability assessment and malware detection capabilities early in the build cycle of a container for assurance across environments.

DEEP SECURITY COMPLIMENTS DEEP SECURITY SMART CHECK BY PROVIDING LEADING HOST PROTECTION OF THE OS



SMART CHECK SECURITY ARCHITECTURE

Installation

Deep Security Smart Check is supported on the Kubernetes platform within a Kubernetes cluster.

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

Smart Check 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.

Role Based Access Control (RBAC)

Various stakeholders need different levels of access to Smart Check based on their roles. Smart Check administrators can configure authorized users or groups of users and assign roles accordingly.

Supported registries

Smart Check supports the scanning of Docker images in any registry that supports the Docker Registry V2 API. Integration logic triggers a scan based on the event model of the registry. Support is available for Docker Trusted Registry, Amazon Elastic Container Registry, Azure Container Registry and Google Container Registry.

Scanning services

When Smart Check receives a scan request it pulls the specified image, unpacks each layer and performs malware and vulnerability scans on the content. The detection engines leverage Trend Micro's strengths in malware pattern matching and vulnerability detection through their malware scanning engine. Smart Check also scans for vulnerabilities of the OS and continually scans for new CVEs.

Deployment and Integration

Deep Security Smart Check provides a valuable step in your continuous integration (CI) or continuous delivery (CD) pipeline.

Deep Security Smart Check scans Docker images in any registry that implements the Docker Registry API. All Deep Security Smart Check operations are available through a documented collection of APIs to simplify integration into your CI/CD pipeline. Deep Security Smart Check 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 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.

Deep Security Smart Check includes an administrator console that provides:

- a dashboard (system-wide summary of scan information, including metrics)
- view summary (including scan results and metrics for the view)
- user management
- registry and view configuration
- access to scan results
- scan history

SYSTEM REQUIREMENTS

Deep Security Smart Check requires:

Kubernetes 1.8.7 or higher

Helm/Tiller 2.8.1 or higher

Docker 17.06 or higher

Supported registries

Deep Security Smart Check supports the scanning of Docker images in any registry that supports the Docker Registry V2 API.

Included Registries:

- Docker Trusted Registry (DTR)
- Amazon Elastic Container Registry (ECR)
- Azure Container Registry
- Google Container Registry (GCR)

To integrate Deep Security Smart Check into your CI/CD pipeline, you can write integration logic to trigger scanning based on the event model of your registry. For example, Google Container Registry uses a pub/sub model to publish events about registry activity, and Docker Trusted Registry uses a Webhook model.

KEY CERTIFICATIONS AND ALLIANCES

- Amazon Advanced Technology Partner
- HP Business Partnership
- Microsoft Application Protection Program
- Microsoft Certified Partnership
- Oracle Partnership

Securing Your Connected World

For more information visit trendmicro.com/smartcheck