Tencent Container Security Service

Product Introduction

Product Documentation

Contents

Product Introduction
Overview

Last updated：2024-01-23 15:35:06

TCSS Overview

TCSS provides rich security features such as container asset management, image security, and runtime intrusion detection. It safeguards containers through their entire lifecycle from image generation and storage to runtime and helps you set up a container security protection system.

Why TCSS

A variety of risks are involved throughout the lifecycle of a container, including:
Runtime environment security risks, such as vulnerabilities in OS components, unnecessary ports opened due to improper configuration, improper user access permissions, and shared OS kernel.
Image security risks, such as vulnerabilities in the image, malware, key in plaintext, improper image configuration, and use of non-trusted images.
Container security risks, such as vulnerabilities in the application, embedded viruses and trojans, and improper container resource configuration.
TCSS can safeguard containers against the above risks throughout their lifecycle.

Features

Asset management

TCSS leverages the automatic asset inventory feature to visualize key assets, such as containers, images, image repositories, and servers.

Image security

TCSS scans images and image repositories for vulnerabilities, trojans, viruses, sensitive information, and more.

Runtime security

TCSS identifies hacker attacks adaptively, monitors and protects container runtime security in real time, and utilizes diversified security features, including container escape, process blocklist/allowlist, and file access control.

Security baseline

TCSS supports CIS Benchmarks for containers, images, servers, and other container environment configurations, displays multidimensional baseline compliance of container assets, and helps set up baseline configurations in the container running environment.

Cluster security

TCSS supports scanning clusters for vulnerabilities and configuration risks automatically or manually and aggregates the data of risky clusters in the business environment and risks in each cluster.

Additional Services

To fix environment consistency issues during user development, testing, and Ops and offer a container-centered, highly scalable, and high-performance container management service based on native Kubernetes, see Tencent Kubernetes Engine.
To create dedicated instances in multiple regions around the world to pull container images nearby faster at lower bandwidth costs, see Tencent Container Registry.

Strengths

Last updated：2024-01-23 15:35:06

Lightweight deployment, high performance, and low RAM consumption

TCSS offers server and container security protection capabilities, and supports simple installation and lightweight deployment. In addition, it strictly limits resource usage by the agent. When it is overloaded, it is automatically downgraded to ensure normal system running; when it is normally loaded, the usage is low.

Full-lifecycle container security protection

To address the risks involved throughout the container lifecycle, TCSS provides rich security features such as container asset management, image security, and runtime intrusion detection. It safeguards containers throughout their entire lifecycle from image generation and storage to runtime and helps you set up a container security protection system.

Visual security operations analysis capabilities

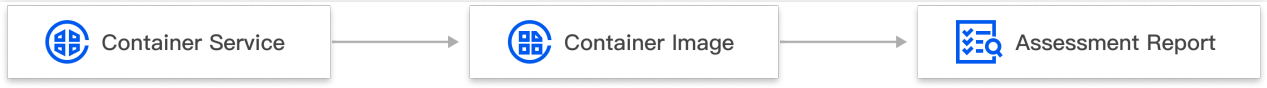
TCSS is constantly empowered by diversified operations features such as security alarm viewing and responding to visualize security, improve the operations capabilities, and simplify Ops.

Use Cases

Last updated：2024-01-23 15:35:06

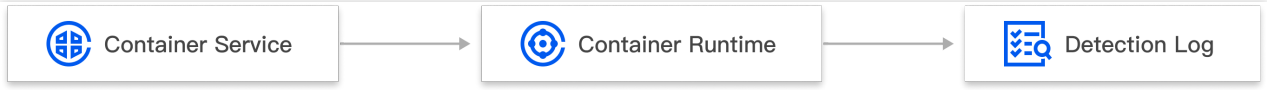
Container image protection

Images are vulnerable to application vulnerabilities, viruses, trojans, and sensitive information leakage. TCSS supports thorough image checks throughout the lifecycle from build and shipping to running. It can detect security risks to images and control image running. It also allows you to customize rules to protect images.



Container escape attack detection

Containers are poorly isolated, and attackers can utilize sensitive path mounting and vulnerabilities to escape to the host, which directly affects the confidentiality, integrity, and availability of the underlying infrastructure. TCSS supports detecting a variety of escapes, such as:
Escape caused by the container running in privileged mode.
Container escape caused by dangerous mounting (mounting of the Docker socket and proc file system of the host).
Privilege escalation caused by the switch from a general account to a root account during the container process.
Capability privilege escalation during the container process.
Mount file namespace isolation broken during the container process.
Blocklist limits broken by seccomp syscall during the container process.
Modification of a host file not mounted to the container during the process (such as CVE-2019-5736).



Features and Versions

Last updated：2024-01-23 15:35:06

Main features available in different editions are as compared below:

Category	Subcategory	Description	Pro	Value-Added Feature
Security overview	Security overview	This feature displays asset (container, image, and server) information, the number of security incidents to be handled, new trends of runtime security incidents, as well as new risk trends and details of local images in real time in visual graphs and charts.	Supported	-
Asset center	Asset management	This feature automatically collects the basic information of assets such as containers, images, servers, processes, ports, applications, web services, running applications, and database applications.	Supported	-
Security enhancement	Vulnerability detection	This feature allows quick detection of vulnerabilities in the container environment to facilitate vulnerability emergency response and vulnerability operations. Vulnerabilities are categorized into two types based on the actual handling and response type: system vulnerabilities and web application vulnerabilities.It quickly filters vulnerabilities based on the urgency of their impact on the assets and their priorities. For example, it can display only vulnerabilities that affect the container, vulnerabilities that	Supported	-

			affect the latest image version, high-priority vulnerabilities, high-risk and extreme vulnerabilities, and remote EXP. In addition, it associates the data of assets affected by vulnerabilities such as local images, repository images, and containers.		
	Image risk management	Local image	This feature can scan local images quickly or on a scheduled basis to get the basic image asset information and image security risk details. It aggregates the total number of risky images, security vulnerabilities, viruses, trojans, and sensitive information in the business environment.	-	Supported
		Repository image	This feature can scan repository images quickly or on a scheduled basis to get the basic image asset information and image security risk details. It aggregates the total number of risky images, security vulnerabilities, viruses, trojans, and sensitive information in the business environment.	-	Supported
	Cluster risk management	Cluster check	This feature supports automatic and manual checks to get the basic information and configuration and vulnerability risks of cluster assets, and aggregates the data of risky clusters in the business environment and risks in each cluster. Two cluster check modes are available: general mode and proactive mode. The general mode is the default mode, which doesn't	Supported	-

			change or affect the cluster status. It is a conventional check method. The proactive mode leverages known vulnerabilities for penetration or exploitation and may change the cluster status, which means it should be enabled with caution in certain scenarios.		
		Risk analysis	This feature organizes risky cluster nodes by extreme, high, medium, and low risk levels and displays the number of affected clusters and nodes by check item.	Supported	-
	Baseline management		This feature uses CIS Benchmarks to check the security baselines of Docker and Kubernetes and collects the proportion of compliant containers in the business environment as well as the number of extreme-risk, high-risk, medium-risk, and low-risk check items. The baseline check result contains the baseline check item, type, baseline standard, severity, check result, and check item details. Check objects include containers, images, servers, and Kubernetes.	Supported	-
Intrusion protection	Runtime security	Container escape	This feature detects sensitive path mounting in the container, privileged containers, privilege escalation events, escape vulnerability exploitation, Docker API access escape, sensitive file tampering escape, and escape with the cgroup mechanism in real time.	Supported	-

			Detection rules can be enabled/disabled as needed. It categorizes alarm events into risky container, program privilege escalation, and container escape to identify risky containers and container escapes. Alarm information includes the escape event type, first generation time, last generation time, event count, container name/ID, image name/ID, server name, and Pod name. Alarm details include the event description, solution, and information of the process, parent process, and grandparent process.		
		Reverse shell	This feature detects reverse shells in the container in real time and generates alarms. Alarm information includes the process name, parent process name, destination address, process path, first generation time, last generation time, event count, container name/ID, and image name/ID. Alarm details include the risk description, solution, and information of the process, parent process, and grandparent process. It allows you to add alarm events to the allowlist or customize a new allowlist by destination address (IP and port), connection process, and affected images.	Supported	-
		Virus scanning	This feature detects viruses and trojans during container running in real time and generates alarms. Alarm	Supported	-

			information includes the filename, file path, virus name, first generation time, last generation time, container name/ID, image name/ID, and container status. Alarm details include the malicious file details, event details, solution, and information of the process, parent process, and grandparent process. It monitors in real time and scans for malicious files in the container quickly or on a scheduled basis, and allows you to enable automatic isolation of malicious files as needed.		
	Advanced defense	Abnormal process	This feature detects abnormal process startups in the container in real time and generates alarms or blocks them. Alarm information includes the process path, hit rule, severity, first generation time, last generation time, event count, container name/ID, image name/ID, and action execution result. Alarm details include the risk description, solution, and information of the process, parent process, and grandparent process. The preset policy for abnormal process detection covers at least proxy software, horizontal penetration, malicious commands, reverse shells, fileless program execution, high-risk commands, and abnormal subprocess startups in sensitive services.	Supported	-

			It allows you to add alarm events to the allowlist or customize new process allow rules by process path and affected images. It enables you to customize new process detection rules by configuring the rule name, process path, action (block, alarm, allow), and affected images.		
		File tampering	This feature detects abnormal file access behaviors in the container in real time and generates alarms or blocks them. Alarm information includes the filename, process path, hit rule, first generation time, last generation time, event count, container name/ID, image name/ID, and action execution result. Alarm details include the risk description, solution, and information of the process, parent process, and grandparent process. The preset policy for file tampering covers at least rules about tampering with scheduled tasks, system programs, and user configurations. It allows you to add alarm events to the allowlist or customize new allow rules by process path, accessed file path, and affected images. It enables you to customize new access control rules, with configurable content such as rule name, process path, accessed file path, action	Supported	-

			(block, alarm, allow), and affected images.		
		High-risk syscall	This feature detects high-risk syscalls in the container in real time and generates alarms. Alarm information includes the process path, syscall name, first generation time, last generation time, event count, container name/ID, image name/ID, server name, and Pod name. Alarm details include the risk description, solution, and information of the process, parent process, and grandparent process. It allows you to add alarm events to the allowlist or customize a new allowlist by process path, syscall name, and affected images.	Supported	-
Security operations	Log analysis		This feature allows you to search for container bash logs, container startup audit logs, and Kubernetes API audit logs by time, log type, and log content, and displays the log trend based on the search results. You can customize the displayed and hidden fields of logs, view logs in JSON format, and export logs. Log configuration: You can specify whether to enable audit for container bash logs, container startup audit logs, and Kubernetes API audit logs, and whether to enable audit for nodes by log type. You can clear logs by percentage and storage period. Log shipping: You can configure CKafka and CLS log shipping as needed. The	Supported	-

		CKafka log shipping feature can be connected by a public network domain name, and you can select the target message queue instance, public network domain name for connection, and the ID and name of the target topic for each type of log, and specify whether to enable shipping. For CLS log shipping, you can customize logsets and log topics and specify whether to enable shipping.		
Settings center	Alarm settings	This feature allows you to customize alarm notifications for local images (vulnerabilities, viruses, trojans, and sensitive information), repository images (vulnerabilities, viruses, trojans, and sensitive information), as well as runtime security and advanced defense (container escape, reverse shell, virus scanning, abnormal process, and file tampering) by configuring the alarm status, alarm time, alarm item, and receiving channel (Message Center, email, or SMS).	Supported	-