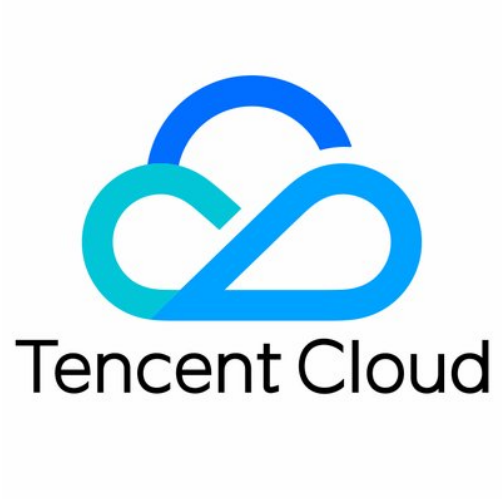
容器安全服务

产品简介

产品文档



文档目录

产品简介
产品概述

最近更新时间：2024-01-23 15:35:06

什么是容器安全服务

容器安全服务（Tencent Container Security Service, TCSS）提供容器资产管理、镜像安全及运行时入侵检测等安全服务，保障容器从镜像生成、存储到运行时的全生命周期安全，帮助企业构建容器安全防护体系。

为什么需要容器安全服务

在容器的生命周期中，会遇到各种风险，包括：

- 运行环境安全风险，例如，操作系统组件存在漏洞、配置不当导致暴露不必要的端口、用户访问权限不当、共享操作系统内核等风险。
- 镜像安全风险，例如，镜像存在漏洞、恶意软件、明文密钥、镜像配置不当或使用非信任镜像等风险。
- 容器安全风险，例如，容器内应用存在漏洞、被植入木马病毒，容器资源配置不当等风险。

使用容器安全服务可对上述风险进行防范，保障容器的生命周期安全。

产品功能

资产管理

容器安全服务提供自动化资产清点功能，支持清点容器、镜像、镜像仓库、主机等关键资产信息，帮助企业实现资产可视化。

镜像安全

容器安全服务可针对镜像、镜像仓库提供一键检测功能，支持对漏洞、木马病毒及敏感信息等多维度安全扫描。

运行时安全

容器安全服务支持自适应识别黑客攻击，实时监控和防护容器运行时安全，提供容器逃逸、进程黑白名单、文件访问控制等安全功能。

安全基线

容器安全服务支持 CIS Benchmark 标准检查，可对容器、镜像、主机等容器环境配置进行安全标准检查，多维度展现容器资产的基线合规情况并帮助建立容器运行环境下的基线配置。

集群安全

容器安全服务支持通过自动检查或手动检查的方式扫描集群存在的漏洞和配置风险，并对业务环境中存在风险的集群及每个集群存在的风险数据进行汇总。

相关服务

- 如需解决用户开发、测试及运维过程的环境一致性问题，基于原生 kubernetes 提供以容器为核心的、高度可扩展的高性能容器管理服务，请参见 容器服务产品文档 。
- 如需同时在全球多个地域创建独享实例，以实现容器镜像的就近拉取，降低拉取时间，节约带宽成本，请参见 容器镜像服务产品文档 。

产品优势

最近更新时间：2024-01-23 15:35:06

轻量级部署，高性能低占用

容器安全服务采用超融合架构，具备主机安全与容器安全防护能力，支持简易安装，轻量部署。同时容器安全服务严格限制 Agent 资源占用，负载过高时主动降级保证系统正常运行，正常负载时消耗较低。

容器全生命周期的安全防护

在容器生命周期会遇到各种风险，容器安全服务提供容器资产管理、镜像安全及运行时入侵检测等安全服务，保障容器从镜像生成、存储到运行时的全生命周期安全，帮助企业构建容器安全防护体系。

可视化的安全运营分析能力

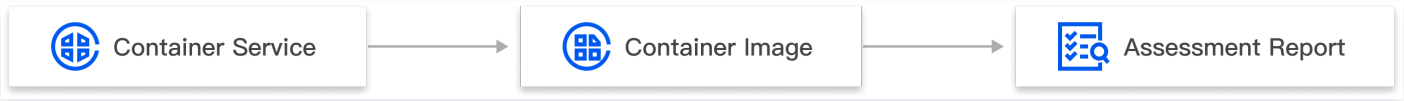
容器安全服务通过安全告警查看和响应处理等运营功能，不断为产品赋能，达到安全可视化，帮助企业提高运营能力，降低运维难度。

应用场景

最近更新时间：2024-01-23 15:35:06

容器镜像防护

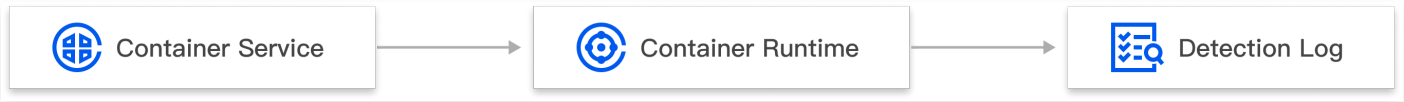
镜像存在应用漏洞、木马病毒及敏感信息泄露等多种安全问题， 容器安全服务支持 BUILD（构建）、SHIP（分发）、RUN（运行）全生命周期的镜像深度检查，可发现镜像存在的安全风险，并对镜像进行运行控制。容器安全服务允许用户自定义规则，实现对镜像的防护。



容器逃逸攻击检测

容器隔离性较弱，攻击者可利用敏感挂载和漏洞实现逃逸到宿主机的行为。逃逸问题直接影响承载容器底层基础设施的保密性、完整性和可用性。容器安全支持检测各类容器逃逸行为，例如：

- Privileged 特权模式运行容器引起的逃逸。
- 危险挂载导致的容器逃逸（挂载 Docker Socket、挂载宿主机 procfs）。
- 容器内进程从普通账号切换到 root 账号导致的提权。
- 容器内进程 capability 提权。
- 容器内进程突破 mount file namespace 隔离。
- 容器内进程突破 seccomp syscall 黑名单调用限制。
- 容器内进程修改未挂载进容器的宿主机文件（如 CVE-2019-5736）。



功能介绍与版本对比

最近更新时间：2024-01-23 15:35:06

不同版本提供的主要功能对比如下表所示：

分类	类别		详细描述	专业版	增值功能
安全概览	安全概览		以可视化的图形、图表等方式实时展示资产信息（容器、镜像、主机）、待处理安全事件数量、运行时安全事件新增趋势、本地镜像新增风险趋势及详情。	支持	-
资产中心	资产管理		支持自动化统计容器、镜像、主机、进程端口、应用 Web 资产、运行应用、数据库应用等资产基本信息。	支持	-
安全加固	漏洞管理		漏洞管理模块支持对容器环境中的漏洞开展一键检测，为漏洞应急响应及漏洞运营场景提供更好体验。根据实际处理及漏洞响应类型，将漏洞划分为两类，分别是：系统漏洞、Web 应用漏洞。支持按影响资产紧急度和关注紧急度快速筛选漏洞，例如仅展示影响容器的漏洞、仅展示影响最新版本的镜像、重点关注、高危及严重、远程 EXP 等。同时关联漏洞影响的本地镜像、仓库镜像、容器等资产数据。	支持	-
	镜像风险管理	本地镜像	• 支持定时扫描、一键扫描本地镜像获取镜像资产基本信息及镜像安全风险详情。 • 支持对业务环境存在风险的镜像总数、安全漏洞、木马病毒、敏感信息进行汇总。	-	支持
		仓库镜像	• 支持定时扫描、一键扫描仓库镜像获取镜像资产基本信息及镜像安全风险详情。 • 支持对业务环境存在风险的镜像总数、安全漏洞、木马病毒、敏感信息进行汇总。	-	支持
	集群风险	集群检	支持自动检查、手动检查获取集群资产	支持	-

	管理	查	基本信息及其存在的配置和漏洞风险，并对业务环境中存在风险的集群及每个集群存在的风险数据进行汇总；集群检查模式包括正常模式和主动模式。 • 正常模式为默认模式，该模式不会改变和影响集群状态，是一种常规检查方式。 • 主动模式会主动利用已知漏洞进行渗透或执行利用，**可能改变集群状态，请在特定场景下谨慎开启使用。**		
		风险分析	支持按严重、高危、中危、低危对存在风险的集群节点进行统计，并按检查项对受影响的集群数、受影响的节点数进行统计。	支持	-
	基线管理		• 支持 CIS Benchmark 基线检查标准，检测 Docker 及 kubernetes 安全基线，并对业务环境中合规容器占比、严重检查项、高危检查项、中危检查项、低危检查项进行统计。 • 基线检测结果包括基线检测项、类型、基线标准、威胁等级、检测结果、检测项详情等，检测对象包括容器、镜像、主机和 kubernetes。	支持	-
入侵防御	运行时安全	容器逃逸	• 支持实时检测容器内存在的敏感路径挂载、特权容器、提权事件、逃逸漏洞利用、访问 Docker API 接口逃逸、篡改敏感文件逃逸、利用 cgroup 机制逃逸等行为，并自定义开启/关闭检测规则。 • 支持按风险容器、程序提权、容器逃逸等对告警事件进行分类，明确区分存在风险的容器和容器逃逸行为。 • 告警信息包括：逃逸事件类型、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID、节点名称、POD 名称等，同时告警详情提供事件描述、解决方案、进程信息、父进程信息、祖先进程信息等详情。	支持	-

		反弹 Shell	• 支持实时检测容器内存在的反弹 Shell 行为并产生告警，告警信息包括：进程名称、父进程名称、目标地址、进程路径、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID 等，同时告警详情提供风险描述、解决方案、进程、父进程和祖先进程详细信息。 • 支持用户对告警事件加白处理，或按目标地址（IP、端口）、连接进程和生效镜像范围自定义新增白名单。	支持	-
		文件查杀	• 支持实时检测容器运行时存在的木马病毒并产生告警，告警信息包括文件名称、文件路径、病毒名称、首次生成时间、最近生成时间、容器名称/ID、镜像名称/ID、容器状态等；同时告警详情提供恶意文件详情、事件详情、解决方案、进程、父进程、祖先进程等详细信息 • 支持实时监控、一键扫描和定时扫描容器内恶意文件；同时支持客户自定义开启自动隔离恶意文件开关。	支持	-
	高级防御	异常进程	• 支持实时检测容器内存在的进程异常启动行为并告警通知或拦截异常进程。告警信息包括：进程路径、命中规则、威胁等级、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID、动作执行结果等，同时告警详情提供风险描述、解决方案、进程、父进程和祖先进程详细信息。 • 异常进程检测系统策略至少包括代理软件、横向渗透、恶意命令、反弹 Shell、无文件程序执行、高危命令、敏感服务异常子进程启动等。 • 支持用户对告警事件加白处理，或按进程路径和生效镜像范围自定义新增进程放行规则。 • 支持用户自定义新增进程检测规则，配置内容包括规则名称、进程	支持	-

			路径、执行动作（拦截、告警、放行）和生效镜像范围。		
		文件篡改	• 支持实时检测容器内存在的文件异常访问行为并告警通知或拦截异常访问。告警信息包括：文件名称、进程路径、命中规则、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID、动作执行结果等。同时告警详情提供风险描述、解决方案、进程、父进程和祖先进程详细信息。 • 文件篡改系统策略至少包括篡改计划任务、篡改系统程序、篡改用户配置等规则。 • 支持用户对告警事件加白处理，或按进程路径、被访问文件路径和生效镜像范围自定义新增放行规则。 • 支持用户自定义新增访问控制规则，配置内容包括规则名称、进程路径、被访问文件路径、执行动作（拦截、告警、放行）和生效镜像范围。	支持	–
		高危系统调用	• 支持实时检测容器内存在的高危系统调用行为并产生告警，告警信息包括：进程路径、系统调用名称、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID、节点名称、POD 名称等，同时告警详情提供风险描述、解决方案、进程、父进程和祖先进程详细信息。 • 支持用户对告警事件加白处理，或按进程路径、系统调用名称和生效镜像范围自定义新增白名单。	支持	–
安全运营	日志分析		• 支持按时间、日志类型、日志内容等自定义检索容器 bash 日志、容器启动审计日志、kubernetes API 审计日志，并按检索结果展示日志趋势图。支持自定义日志的展示字段和隐藏字段，查看 json 格式日志，并支持导出日志。	支持	–

		• 日志配置：支持自定义配置容器 bash 日志、容器启动审计日志和 kubernetes API 审计日志是否开启日志审计，以及按照日志类型自定义节点是否开启审计。支持按百分比和存储天数清理日志。 • 日志投递：支持自定义配置 CKAFKA 和 CLS 日志投递功能。CKAFKA 日志投递支持按公网域名接入，客户可自定义选择投递的消息队列实例、接入的公网域名、每类日志投递的 Topic ID 和名称，以及是否开启投递；CLS 日志投递支持自定义日志投递的日志集和日志主题，以及是否开启投递。		
设置中心	告警设置	支持自定义对本地镜像（安全漏洞、木马病毒、敏感信息）、仓库镜像（安全漏洞、木马病毒、敏感信息）、运行时安全&高级防御（容器逃逸、反弹 Shell、文件查杀、异常进程、文件篡改）等告警进行通知，可配置内容包括告警状态、告警时间和告警项，接收渠道包括站内信、邮件、短信等。	支持	-