尚付容器安全管理系统

技术白皮书

杭州默安科技有限公司

浙江省杭州市余杭区文一西路 1378 号杭州师范大学科技园 E 幢 10 层

0571-5789 0067

www.moresec.cn

默安科技

企业信赖的安全伙伴

文档说明

文档负责人	冯河清	文档版本编号	V1.0.0
起草人	冯河清	文档起草日期	2021.05
复审人		复审日期	

版本控制

版本号	版本日期	创建/修订人	说明
1.0.0	2021-05	冯河清	创建
1.0.1	20201-09	冯河清	更新

版本申明

目录

1.概述

1.1 背景

在全球数字化转型浪潮席卷之下，云原生应用、容器技术被广泛接受和使用，容器环境的部署越来越常见，并逐渐成为包装、交付和部署新型应用的主流方式。以可移植、可扩展的开源平台 Kubernetes 为例，可实现跨主机集群自动执行应用程序容器的部署、扩展和操作，目前在容器编排市场占据了主导地位。

然而 Kubernetes 也面临着诸多安全挑战，例如 Kubernetes 本身仅提供少数原生安全功能，这使得保护 Kubernetes 带来众多困难，但并不意味着企业可以忽视 Kubernetes 安全。通过集成扩展 Kubernetes 原生安全控制措施，并将安全能力左移至 CI/CD 阶段，利用 Kubernetes 中相同的声明性方法执行策略，对集群资源、网络流量、合规性、微隔离、准入策略的分析、配置，为容器整个生命周期实现更完备的安全性提供自动化、可扩展的解决方案，保护基于 Kubernetes 的工作负载的安全。

1.2 现状

1.2.1 镜像与镜像仓库安全问题突出

镜像是容器技术的最基本的概念，镜像扫描是发现容器漏洞风险最基础的办法，即使是在 Docker Hub 下载的官方镜像中也经常包含大量的漏洞，同时加上开发人员在使用大量开源框架时候会将镜像漏洞问题进一步放大。对于企业来说，现有的安全人员对 devops 流程中的镜像缺少管控能力，镜像漏洞的发现、补丁信息采集、测试等面临着各种困难，甚至补丁本身就有可能成为新的漏洞。

组织在实际生产环境中使用容器官方镜像仓库，但镜像的质量参差不齐，无法保证，一些攻击者可能将含有后门、病毒等恶意漏洞的镜像上传至官方镜像库，可能存在较大的安全风险，基础镜像的安全与容器云环境的安全性有紧密关系。

1.2.2 容器网络通信缺少限制

集群中的容器在部署中需要实现相互通信以便交换彼此的数据，部分容器还需要将应用连接到互联网向公众提供相关应用服务。如果容器遭到恶意攻击，攻击者在集群环境中横向

移动的能力与该容器和其他容器通信的范围直接相关。当需要用户在庞大的容器环境中仅手动来配置此类策略，那么将带来巨大的人工成本。此外由于 Kubernetes 各类环境下的网络活动会不断波动，因此除能够感知集群中网络流量的细微差别外，还需要使用网络接口来创建不同的网络微隔离规则，防止来自网络上的威胁攻击。

1.2.3 合规性挑战

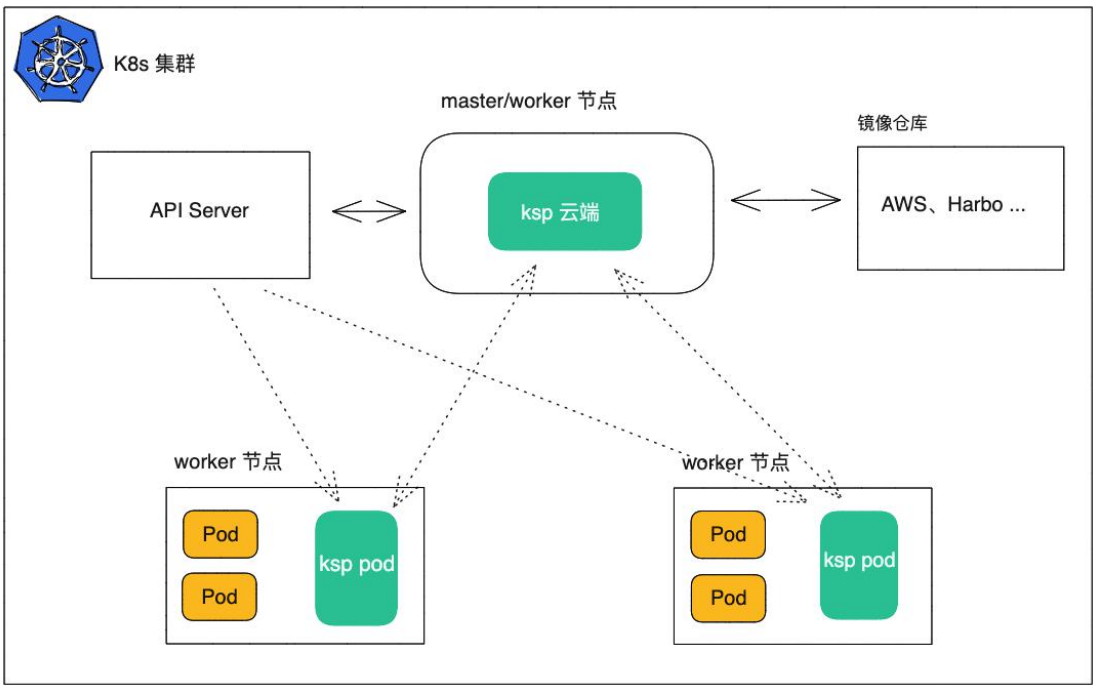
云原生环境需要实施定期的审查策略来扫描 Kubernetes 集群的资源及其配置，确保其符合行业标准和最佳实践。同时容器化应用程序的分布式和动态特性意味着在实现合规性监控和审核自动化时，才能大规模运行。同时需要支持用户可以编写符合自身实际情况的的合规性检查条目以满足特定行业的合规性规则或要部署具有通用审核策略无法解决的安全需求的自定义业务应用。

1.2.4 默认安全配置无法满足实际情况

Kubernetes 旨在加快应用程序部署并简化管理和操作，Kubernetes 是一个复杂的系统，一个集群由许多不同的部分组成。为了保持集群的整体完整性，需要对每一个组件进行安全保护。Pod 安全策略依据定义只能利用于 pods，例如应用 Linux 内核性能，应用主机命名空间、网络、端口或文件系统等等。但其余 Kubernetes 资源的安全问题并未得到解决，如 Ingresses、Deployments、Services 等。需要一个通用引擎策略来统一，例如 OPA，可以将策略指定为代码和简单的 API，减轻软件决策的负担，在微服务、Kubernetes、CI/CD、API 网关中来实施安全策略。

2.产品概述

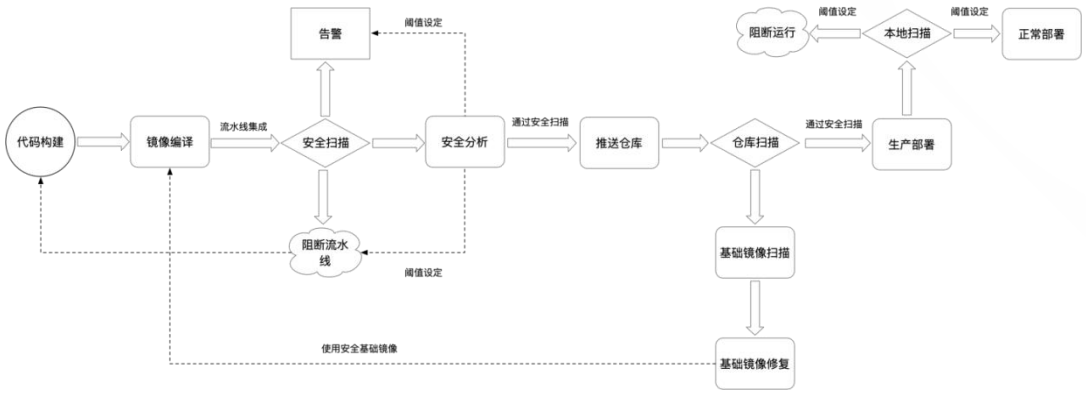
2.2 产品功能架构



2.1 产品介绍

尚付容器安全管理系统能力覆盖容器生命周期中的三个关键阶段，即：容器构建时的镜像安全、容器部署时基线检查以及运行时的入侵检测和防御。为容器安全提供全天候监测与保护，构建基于云原生的容器安全防护。

2.3 产品检测流程示意

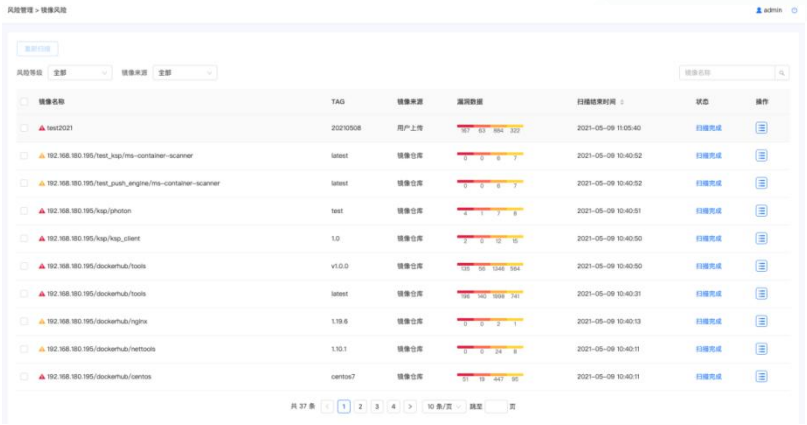


3.产品功能

3.1 镜像防护

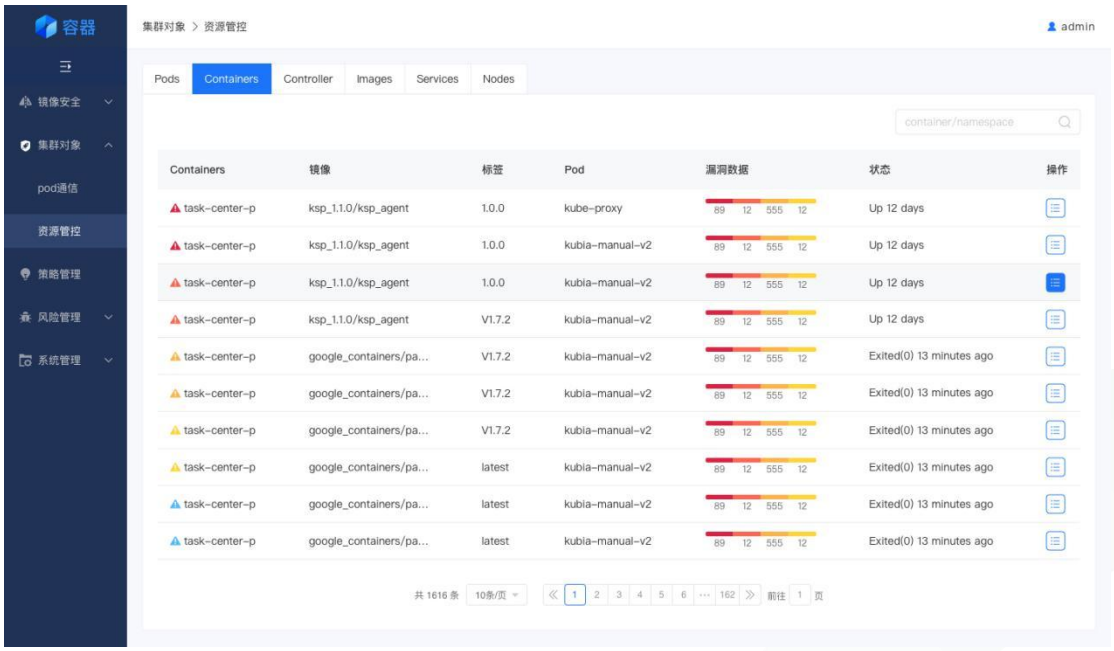
从构建镜像到部署到运行，尚付容器安全管理系统通过对镜像的安全扫描，发现、追踪与镜像相关的风险威胁、第三方组件许可证信息、镜像分层信息等，帮助客户解决 Docker 镜像文件风险发现难、补丁信息缺少的问题，给用户提供一个安全、纯净的镜像文件。此外尚付容器安全管理系统支持对公共或私有仓库内的容器镜像进行漏洞扫描，并支持 webhook 消息通知机制，对有更新的容器镜像重新进行自动扫描。

针对于类似于 Jenkins 的 CI 工具，平台提供相应插件进行配置，可在 CI 过程中扫描所采用的镜像，让开发人员在每次运行构建时都能看到漏洞状态，而无需运行单独的工具或使用不同的界面。安全团队可以通过设置相应阻断策范风险略来防。



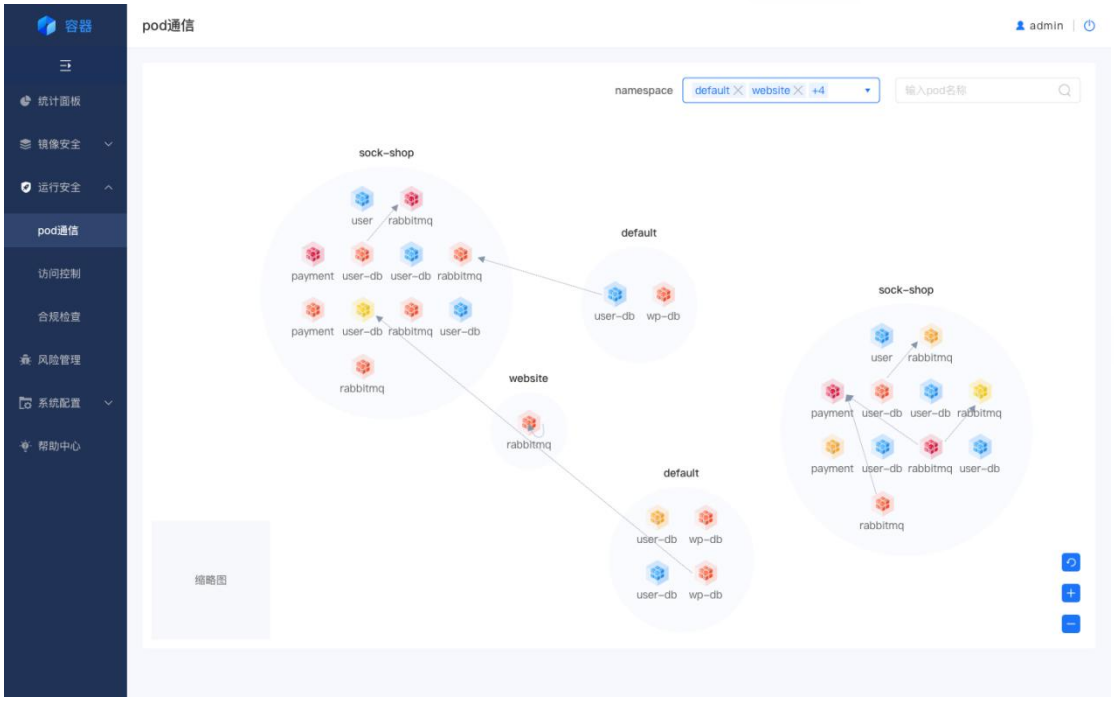
3.3 集群资产管理

Kubernetes 对容器 Pod 进行编排，组织出多种不同类型的资产，尚付容器安全管理系统通过 Kubernetes 环境中各类资产识别，包括但不限于：container、image、node、service、controller 等基础资产信息，展示所有容器相关资产的统计数据和风险状态，自动对各类资产信息进行同步，并实时监控资产信息的变化。



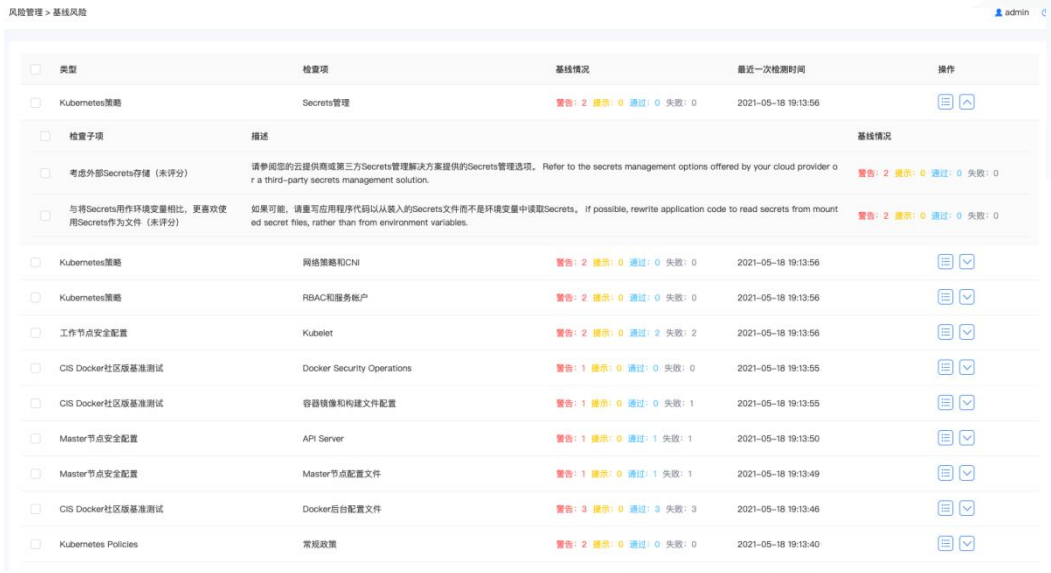
3.2 容器网络拓扑

尚付容器安全管理系统支持展示 kubernetes 集群中的网络访问。在企业云原生生态建设过程中，尚付容器安全管理系统通过利用宿主机系统内核引流机制，对容器资产之间或容器跟外部网络之间交互进行统计展示，帮助用户自动化构建集群容器资产相关信息，提供集群环境中各类资产的识别，包括 pod、image、namespace 等信息，并提供资产可视化能力，帮助用户梳理容器资产间的互访关系，发现非法访问。



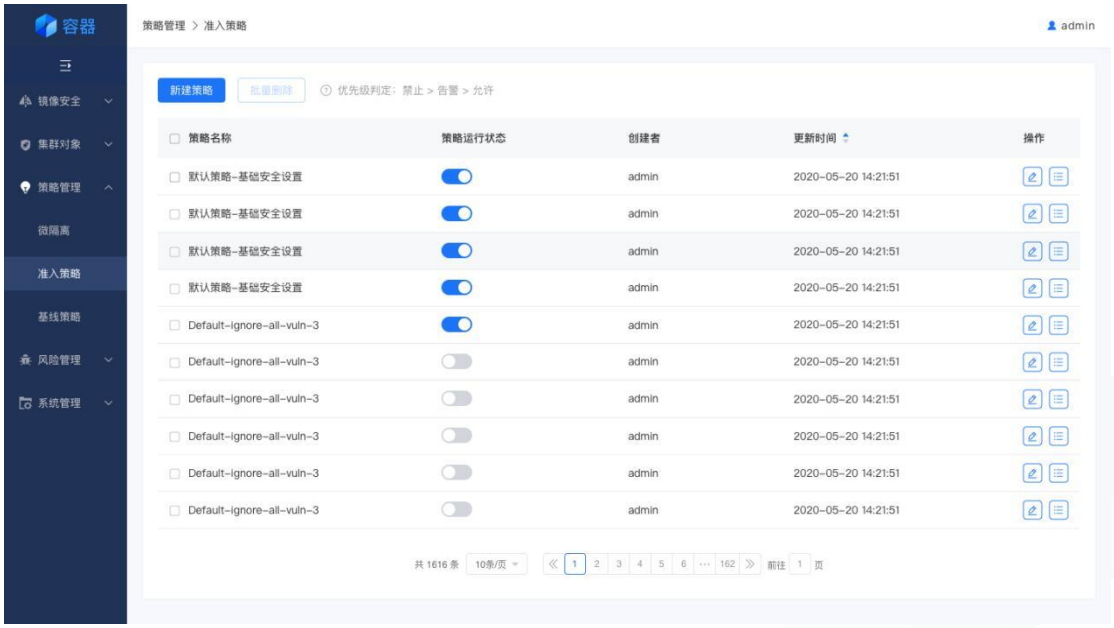
3.4 基线策略

尚付容器安全管理系统提供行业领先的合规性功能，确保遵守 docker、kubernetes 的 CIS 基线标准。平台通过构建基于 CIS Benchmark 的 docker、kubernetes 的基线检查安全配置策略，实现对集群中相关资源的基线检查，帮助用户完成自动化检测，并且提供完备的基线检查结果和代码级的修复建议。



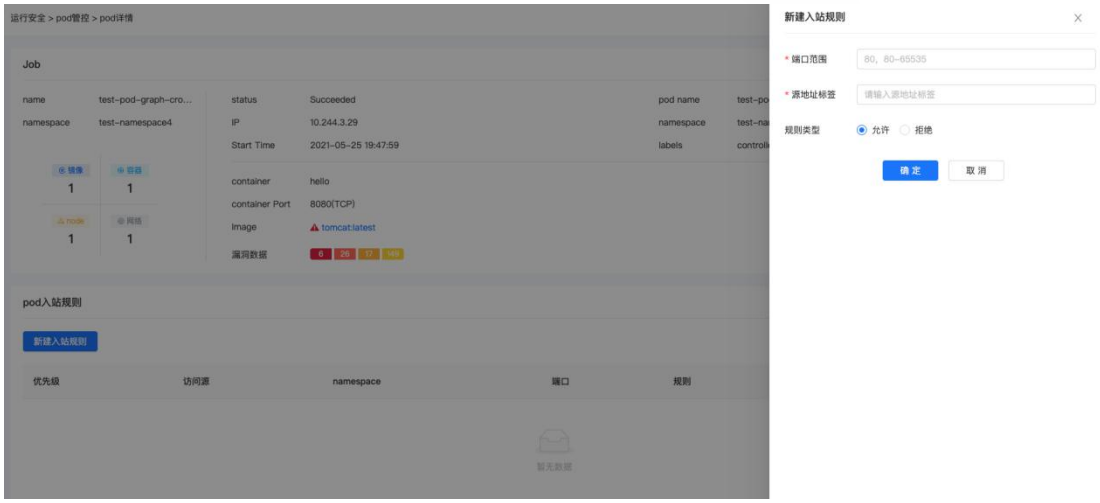
3.5 准入策略

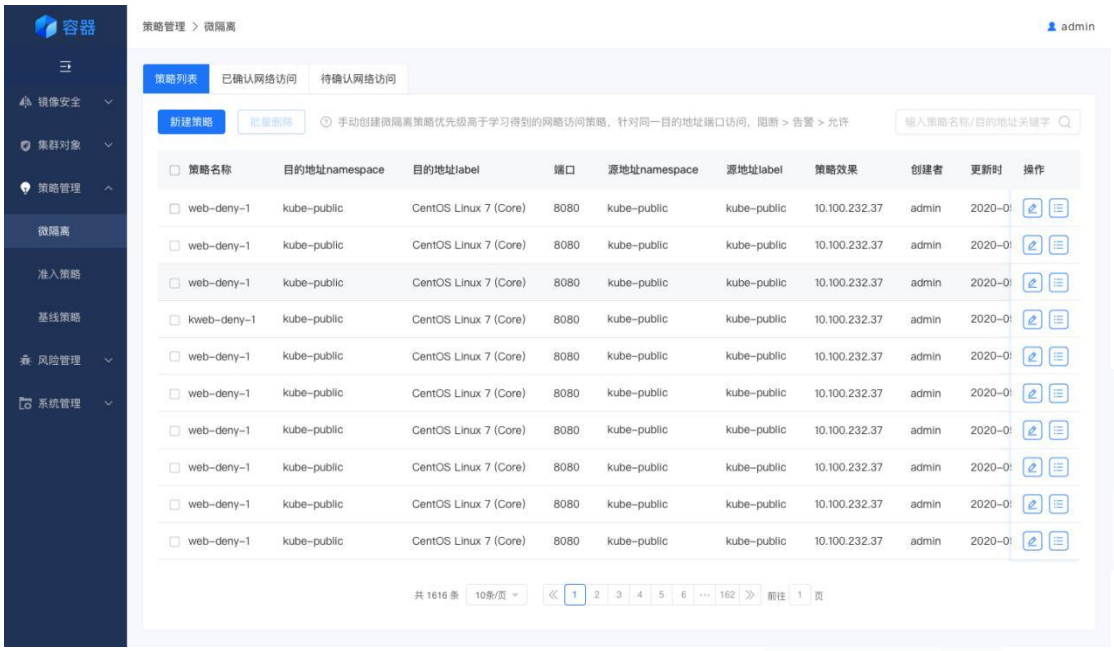
尚付容器安全管理系统确保符合准入的策略的资源进入到集群中。通过建立集群准入策略，在请求进入 API 服务器时，平台使用预设的准入策略规则进行验证。如果满足策略阻断的条件，则拒绝该请求，并通过 kubernetes API 服务器将错误的原因提供给请求该操作的用户。



3.6 微隔离策略

尚付容器安全管理系统提供全面的网络隔离策略保护集群中 Pod 通信安全。平台通过集成容器网络接口，利用 kubernetess 来执行网络策略，帮助用户对集群中容器网络访问关系完成学习建模，自动生成 Pod 网络访问关系图，查看所有允许、告警、阻断的网络活动。此外平台可以根据已完成学习的网络访问关系建立严格的网络隔离策略对集群中的 Pod 进行网络访问限制。





3.7 进程策略

尚付容器安全管理系统通过对集群中各容器内的进程进行学习，不断对。

4.产品优势

4.1 云原生架构

尚付容器安全管理系统采用 daemonset 方式部署运行，支持 kubernetes 编排部署，降低管理人员工作强度。可适应 kubernetes 的冗余机制，适应各种 CNI 环境，对业务无影响。

4.2 四层访问控制

尚付容器安全管理系统提供四层网络访问控制，它可自动学习应用程序的网络拓扑。在四层网络访问控制上，可以自动学习所有微服务之间的所有流量，并允许安全团队集中查看和阻断所有网络访问，同时自动阻止异常访问流量，无需手动创建和管理规则。

4.3 集群资源展示

攻击行为可能以各种各样的方式发生，保持 Kubernetes 各类服务和资源持续可见是十分重要的。尚付容器安全管理系统可以帮助安全团队实时了解集群中各类资源的状态。

4.4 运行时防护

Kubernetes 集群会随着节点的脱机或关闭而不断变化，应用的规模也会根据需求的转变而扩大或缩小。借助尚付容器安全管理系统可以帮助安全团队了解 Kubernetes 中部署的应用在不同条件下的行为。帮助用户有效地区分应用行为的正常变化和反映安全问题的应用行为变化。

4.5 Kubernetes 安全审核和合规性

尚付容器安全管理系统支持自上而下的 kubernetes 安全审核，可以检测集群中的节点是否通过 CIS 基线规则。用户可以通过自定义扫描对 kubernetes 集群的所有节点及其配置，确保其符合行业标准和最佳实践。

5.客户价值

尚付容器安全管理系统通过与 kubernetes 深度结合，对各类云环境的完美适配，完成对容器业务环境中的集群资源、网络访问、进程文件、操作权限等进行持续监控，及时发现容器资产的异常行为并进行阻断，对容器资产访问关系进行可视化，掌握业务环境中容器资产间的网络互访关系，帮助用户构建符合 kubernetes 容器业务环境的安全管理机制，实现容器业务环境中各类风险的管理与控制。