安全云脑

产品介绍

文档版本 05

发布日期 2024-02-29

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 什么是安全云脑

安全云脑（SecMaster）是华为云原生的新一代安全运营中心，集华为云多年安全经验，基于云原生安全，提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力，可以鸟瞰整个云上安全，精简云安全配置、云防护策略的设置与维护，提前预防风险，同时，可以让威胁检测和响应更智能、更快速，帮助您实现一体化、自动化安全运营管理，满足您的安全需求。

为什么选择安全云脑

- 一键安全合规：一键生成遵从报告，华为积累的全球安全合规经验服务化，帮助用户快速实现云上业务安全/隐私保护遵从。
- 一屏全面感知：采集各类安全服务的告警事件，并进行大数据关联、检索、排序，全面评估安全运营态势，支持大屏展示安全运营动态。
- 一云全局分析：结合华为云积累的每日数亿威胁情报定位威胁，多维关联分析，消除无效告警、识别潜在高级威胁。
- 一体全程处置：服务内置多种处理剧本，实现99%以上的安全事件分钟级自动化响应。

更多安全云脑产品优势请参见**产品优势**。

2 产品优势

见微知著的指标脉络与态势呈现

您可以通过安全态势即时查看大屏、定期订阅安全运营报告，了解安全运营核心关注指标。

云原生的资产盘点与风险预防

云上资产自动盘点，云安全配置自动检查，支持定位到资产，指导并辅助自动加固，帮助您告别黑资产、错配置的焦虑。同时避免传统的外挂式安全方案引入的隐式通道或安全设备漏洞。

智能高效的威胁检测与响应处置

专注于快速找到真正的威胁。通过每天对数十亿安全日志进行分析，利用华为云安全运营团队多年沉淀经验，内置模型和研判剧本来降低合法事件的干扰。通过威胁及资产画像，与威胁告警环环关联，还原整个攻击链，配置自动化处置剧本进行响应，简化操作、提升安全性，提升了处理告警和事件的效率。

灵活的环境集成与作战协同

可通过配置连接到所有安全服务，进行数据对接或者联动操作；也可以定义您自己的模型、研判/处置剧本，以最佳适配您的安全需求。通过工作空间，还可以实现大型组织协同作战、MSSP（Managed Security Service Provider）托管等。

3 应用场景

云安全的理念是“三分建设，七分运营”，安全云脑的应用场景即是占了七分的安全运营。主要有以下几个应用场景：

日常安全运营

日常过程中，基于安全运营中关注的要素，对各个安全目标，执行各安全运营流程剧本，从而发现并消减风险，并对流程进行持续改进，避免风险再次发生。

重大保障

重大节日、假日、活动、会议期间，进行高强度7*24的安全保障，侧重于防攻击，保障业务可用性不因安全攻击受影响。

防护演练

国家机关单位、地方政府、企业组织的攻防演练中，进行高强度的安全防守保障，侧重于防入侵，保障不因入侵失分被问责（通报、批评等）。

安全评估

重大保障及防护演练前，信息全面的脆弱性盘点，包括白盒方式的基线评估、黑盒方式的攻击面、攻击路径探测。

4 产品功能

安全云脑基于云原生安全，提供全面的日志采集、安全治理、智能分析、态势感知、编排响应等快速闭环的安全信息和事件管理能力，助您守护云上安全。

提供有**总览**、**工作空间管理**、**安全治理**、**安全态势**、**资产管理**、**风险预防**、**威胁运营**、**安全编排**、**数据采集**、**数据集成**功能。

总览

总览呈现云上整体安全评估状况，并联动其他云安全服务，集中展示云上安全。

表 4-1 安全概览功能介绍

功能模块	功能详情
安全评分	根据不同版本的威胁检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况。 评估得分越低，即风险值越大，则整体资产安全隐患越大。
安全监控	集中呈现未处理的威胁告警、漏洞和合规检查的风险数目，支持快速查看威胁告警、漏洞和合规风险详情。
安全趋势	呈现最近7天整体资产安全健康得分的趋势图。

工作空间管理

工作空间属于安全云脑顶层工作台，单个工作空间可绑定普通项目、企业项目和Region，可支撑不同场景下的工作空间运营模式。

表 4-2 工作空间功能说明

功能模块	功能详情
工作空间	• 空间管理： 单个工作空间可绑定普通项目、Region，可支撑不同场景下的工作空间运营模式。 • 空间托管： – 工作空间数据委托：单租所有工作空间按照租户实际运营汇聚到某一个工作空间做集中安全运营，跨租汇聚安全运营。 – 工作空间委托：跨账号安全运营，可实现工作空间委托集中安全运营查看统一资产风险、告警和事件等。

安全治理

安全治理为您提供安全治理模板与合规策略扫描服务，将安全遵从包内的法规标准条款转化成检查项。

表 4-3 安全治理功能说明

功能模块	功能详情
安全治理	• 提供安全遵从包 华为开放的安全治理模板，包含法规标准条款原文、扫描策略、自评估检查项以及华为专家的改进建议，覆盖PCI DSS、ISO27701、ISO27001、隐私等法规标准。用户可以订阅、取消订阅安全遵从包，查看合规评估与治理结果。 • 合规策略扫描 Policy as Code，将安全遵从包内的法规标准条款代码化，周期性、自动化扫描云上资产的合规情况，可视化看板呈现风险，提供华为专家改进建议。 • 自评估检查项 将安全遵从包内的法规标准条款转化成检查项，租户可根据检查项完成自身业务的合规评估，查看历史评估结果，进行证据上传和下载，根据华为专家改进建议进行治理。 • 合规结果可视 可视化呈现合规评估结果与安全治理情况，包括租户订阅的法规、标准条款遵从概况，各安全遵从包状态，各策略扫描概况。 **说明** 使用安全治理功能前，需先**提交工单**申请开通使用权限。

安全态势

支持通过安全态势即时查看大屏、定期订阅安全运营报告，了解安全运营核心关注指标。

表 4-4 安全态势功能介绍

功能模块		功能详情
态势总览	安全评分	根据不同版本的威胁检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况。 评估得分越低，即风险值越大，则整体资产安全隐患越大。
	安全监控	集中呈现未处理的威胁告警、漏洞和合规检查的风险数目，支持快速查看威胁告警、漏洞和合规风险详情。
	安全趋势	呈现最近7天整体资产安全健康得分的趋势图。
安全大屏		利用AI技术将海量云安全数据的分析并分类，通过安全大屏将数据可视化展示，集中呈现云上实时动态，云上关键风险一目了然，掌握云上安全态势更简单，更直观，更高效。
安全报告		通过创建分析报告，及时掌握资产的安全状况数据。
任务中心		集中呈现当前需要进行处理的任务。

资产管理

安全云脑支持对云上资产全面自动盘点，也可灵活纳管云外各种资产，点清所有资产，并呈现资产实时安全状态。

表 4-5 资产管理功能说明

功能模块	功能详情
资产管理	同步所有资源的安全状态统计信息，支持查看资源的名称、所属服务、安全状况等，帮助您快速定位安全风险问题。

风险预防

风险预防提供基线检查和漏洞管理功能，帮助您的云安全配置达到等保、ISO、PCI等各类权威安全标准和华为云安全最佳实践标准；知晓全局的漏洞分布。

功能模块	功能详情
基线检查	通过执行云服务基线扫描，检查基线配置风险状态，告警提示存在安全隐患的配置，并提供基线加固建议。
漏洞管理	通过自动同步华为云主机安全服务（Host Security Service，HSS）漏洞扫描数据，分类呈现漏洞扫描详情，支持查看漏洞详情，并提供相应漏洞修复建议。
应急漏洞公告	针对业界披露的热点安全漏洞，支持每5分钟抓取一次安全漏洞讯息，获取最新应急漏洞公告详情。
策略管理	支持统一管理防线策略和应急策略。

威胁运营

威胁运营提供丰富的威胁检测模型，帮助您从海量的安全日志中，发现威胁、生成告警；同时，提供丰富的安全响应剧本，帮助您对告警进行自动研判、处置，并对安全防线和安全配置自动加固。

表 4-6 威胁运营功能介绍

功能模块		功能详情
事件管理		集中呈现事件详情，支持人工转事件、自动化转事件。
告警管理		提供统一的数据类管理（安全运营对象），内置华为云告警标准。通过集成各云服务告警，包含HSS、WAF、DDoS等，集中呈现告警信息。
情报管理		提供统一的数据类管理（安全运营对象），内置华为云威胁情报指标库标准。支持接入各云服务情报，同时也可以基于告警和事件自定义规则提取指标。
智能建模		支持构建告警模型。
安全分析	查询与分析	• 检索分析：支持数据的快捷检索分析，支持安全调查场景安全数据的快速筛留、筛除等操作，快速定位关键数据。 • 筛选统计：支持数据字段快速分析统计，并基于分析结果进行数据的快速筛选；时序数据支持默认时间分区统计，快速识别数据量的变化趋势，支持基于时间分区的快速筛选；支持分析、统计、排序等丰富统计分析函数，支撑快速构建安全分析模型。 • 可视化：支持数据可视化分析，直观反映业务结构性和趋势性特征，并基于此构建自定义分析报告和分析指标。
	数据监控	支持数据流量端到端的监控管理。
	数据消费	• 提供数据消费和生产的流式通信接口，提供数据管道集成SDK，支持租户利用SDK进行系统集成，支持客户自定义数据的生产和消费。 • 提供Logstash开源采集软件插件，支持利用开源生态进行数据消费和生产。

安全编排

安全编排支持剧本管理、流程管理、数据类管理（安全实体对象）和资产连接管理等。同时，可以自定义剧本和流程等。

通过安全编排可以对安全响应剧本进行拖拽式的灵活编排，动态适配您的业务需求。也可以对安全运营的对象、交互的页面进行灵活扩展和定义。

表 4-7 安全编排功能介绍

功能模块	功能详情
运营对象	集中对数据类、数据类类型、分类映射等运营对象进行管理。
剧本编排	支持对剧本、流程、资产连接、实例的全生命周期管理。
页面布局	提供安全可视化低代码开发平台，基于此平台可自定义安全分析报告、告警管理、事件管理、漏洞管理、基线管理、威胁情报指标库管理等页面布局。
插件管理	支持将安全编排流程中使用的插件进行统一管理。

数据采集

通过多种方式采集各类日志数据。采集后，可以快速实现历史数据分析比对、数据关联分析、以及未知威胁发现等相关分析。

表 4-8 数据采集功能说明

功能模块	功能详情
数据采集	使用Logstash通过多种方式采集各类日志数据。采集后，可以快速实现历史数据分析比对、数据关联分析、以及未知威胁发现等相关分析。

数据集成

通过集成云原生安全产品，进行联动操作或数据对接。集成后，可以检索并分析所有收集到的日志。

表 4-9 数据集成功能说明

功能模块	功能详情
数据集成	云内置采集系统，支持一键集成存储、管理与监管、安全等多种华为云云产品的日志数据。集成后，可以检索并分析所有收集到的日志。

5 服务版本差异

安全云脑提供基础版、标准版和专业版三个版本，不同版本有不同功能使用范围，详细功能差异请参见**版本功能差异**。如需了解各个功能的详细介绍，请参见**产品功能**。

版本说明

安全云脑各个版本的相关说明如**表5-1**所示。

表 5-1 版本说明

版本	计费模式	版本说明
基础版	包周期（免费）	了解安全态势。
标准版	包周期	• 满足安全态势及等保合规运营要求。 • 提供有**安全大屏**、**智能分析**、**安全编排**增值功能。
专业版	• 按需 • 包周期	• 满足企业日常运营、合规检查等要求。 • 提供有**安全大屏**、**智能分析**、**安全编排**增值功能。

版本功能差异

安全云脑各个版本的功能差异如下表所示，请您根据业务需求选择对应的服务版本：

表 5-2 不同版本功能差异

服务功能	功能模块	功能概述	基础版	标准版	专业版
总览		呈现云上整体安全评估状况，并联动其他云安全服务，集中展示云上安全。	√	√	√

服务功能	功能模块	功能概述	基础版	标准版	专业版
工作空间		● 空间管理：安全云脑顶层工作台，单个工作空间可绑定普通项目、企业项目和Region，可支撑不同场景下的工作空间运营模式。 ● 空间托管： – 工作空间数据委托：单租所有工作空间按照租户实际运营汇聚到某一个工作空间做集中安全运营，跨租汇聚安全运营。 – 工作空间委托：跨账号安全运营，可实现工作空间委托集中安全运营查看统一资产风险、告警和事件等。	√	√	√
安全治理①		提供安全治理模板与合规策略扫描服务，将安全遵从包内的法规标准条款转化成检查项。	×	×	√
安全态势	态势总览	● 安全评分：集中呈现资产安全风险评分和风险等级分布，同时展示当前风险防御能力。 ● 安全监控：实时展示安全监控统计数据。 ● 安全趋势：展示近7天内您的整体资产安全健康得分的趋势。	√	√	√
	安全大屏②	集中展示云上资产综合安全态势，动态呈现资产风险状况。	×	√	√
	安全报告	通过创建分析报告，及时掌握资产的安全状况数据。	×	×	√
	任务中心	集中呈现当前需要进行处理的任务。	×	√	√
资产管理		同步资源信息，集中呈现资源整体安全状况。	×	√	√
风险预防	基线检查	通过执行云服务基线扫描，检查基线配置风险状态，告警提示存在安全隐患的配置，并提供基线加固建议。	×	√(仅支持基线检查，不支持查看检查结果详情)	√

服务功能	功能模块	功能概述	基础版	标准版	专业版
	漏洞管理	通过自动同步HSS漏洞扫描数据，分类呈现漏洞扫描详情，支持查看漏洞详情，并提供相应漏洞修复建议。	×	×	√
	应急漏洞公告	集中呈现业界披露的热点安全漏洞，全面掌握资产漏洞风险。	√	√	√
	策略管理	支持统一管理防线策略和应急策略。	×	√	√
威胁运营	事件管理	集中呈现安全威胁事件。	×	√	√
	告警管理	提供统一的安全告警管理，内置华为云告警标准。通过集成各云服务告警，集中呈现告警信息。	×	√	√
	情报管理	提供统一的安全威胁情报指标管理，内置华为云威胁情报指标库标准。支持接入各云服务情报，同时也可以基于告警和事件自定义规则提取指标。	×	×	√
	智能建模	支持构建告警模型。	×	√	√
	安全分析②	支持对数据进行查询分析、消费、监控、投递。	×	√	√
安全编排	运营对象	集中对数据类、数据类类型、分类映射等进行管理。	×	√	√
	剧本编排②	支持对剧本、流程、资产连接、实例的全生命周期管理。	×	√	√
	页面布局	提供安全可视化低代码开发平台，基于此平台可自定义安全分析报告、告警管理、事件管理、漏洞管理、基线管理、威胁情报指标库管理等页面布局。	×	√	√
	插件管理	支持将安全编排流程中使用的插件进行统一管理。	×	×	√
数据采集		使用Logstash通过多种方式采集各类日志数据。采集后，可以快速实现历史数据分析比对、数据关联分析、以及未知威胁发现等相关分析。	×	√	√
数据集成		通过集成生态安全产品，进行联动操作或数据对接。集成后，可以检索并分析所有收集到的日志。	×	√（仅支持集成云服务告警）	√

服务功能	功能模块	功能概述	基础版	标准版	专业版
目录定制		支持查看已有目录及更换布局等操作。	×	√	√

说明

不同版本支持功能差别，标识符号说明如下：

- ×：代表不支持该功能。
- √：代表支持该功能。
- ①：使用安全治理功能前，需先**提交工单**申请开通使用权限。
- ②：代表标准版、专业版支持该功能，但需额外购买增值包功能，如安全大屏、安全分析、剧本编排功能。

6 约束与限制

安全云脑约束与限制如下所示：

表 6-1 约束与限制

模块	约束与限制
计费	● 基础版不支持购买增值包，如需使用增值包功能，请升级为标准版或专业版。 ● 增值包不支持单独使用。 – 如果需要购买增值包，请先购买标准版或专业版。 – 如果退订了按需计费的专业版，系统将自动一并退订增值包。 – 如果退订了包周期计费的标准版或专业版，需手动一并退订增值包。
工作空间	● 付费版本安全云脑：单账号单Region内最多创建5个工作空间。 ● 免费版本安全云脑：单账号单Region内最多创建1个工作空间。 ● 工作空间永久删除：永久删除的workspace立即删除，不能进行恢复。 ● 空间托管： – 单账号单Region内最多创建1个空间托管视图。 – 单/跨账号单Region空间托管视图（包含的纳管工作空间数）中的工作空间数 ≤ 100个。 – 跨账号跨Region空间托管视图（包含的纳管工作空间数）中的工作空间数 ≤ 10个。 – 单账号创建账号委托 ≤ 10个。 ● 暂不支持在同一个浏览器的多个窗口进入不同的工作空间进行操作。
数据空间/管道	● 单账号单Region单Workspace最多创建5个数据空间。 ● 单账号单Region单数据空间最多创建20个数据管道。

模块	约束与限制
安全报告	单账号单workspace内，最多可创建10个安全报告（包含日报、周报和月报）。
告警模型	● 单账号单Region单workspace最多创建100个告警模型。 ● 一个告警模型的运行时间间隔须 ≥ 5分钟，查询数据的时间范围 ≤ 14天。
查询分析	● 单次查询分析最多支持返回500条结果。 ● 一个数据管道内最多创建50个快速查询，即最多可以将50个查询分析条件保存为快速查询。 ● 单次查询结果大于50000条时，准确率可能会下降。请通过缩短查询的时间范围、添加查询限制条件等方法减少查询结果的数量。 ● 使用聚合查询（例如group by语句）聚合多个字段时，第二个字段默认分桶数量为10，如果超出会有数据丢失的情况，将导致查询结果不准确。
事件/告警/情报/漏洞	● 单账号单Workspace内，每天最多新增告警/事件/情报/漏洞100个。 ● 单账号单Workspace内，每天最多可以告警转事件100个。
剧本	● 单账号单workspace内，单剧本调度频率时间 ≥ 5分钟。
剧本和流程实例	单账号单workspace内一天内的重试次数限制如下： ● 手动重试：流程实例最大重试次数100次。重试之后，等剧本执行完毕之后才允许再次重试。 ● API接口重试：流程实例最大重试次数100次。重试之后，等剧本执行完毕之后才允许再次重试。
分类&映射	● 单账号单workspace内，分类&映射模板 ≤ 50个。 ● 单账号单workspace内，分类和映射的映射关系规格为1:100。 ● 单账号单workspace内，最多可新增分类&映射100个。

7 安全

7.1 责任共担

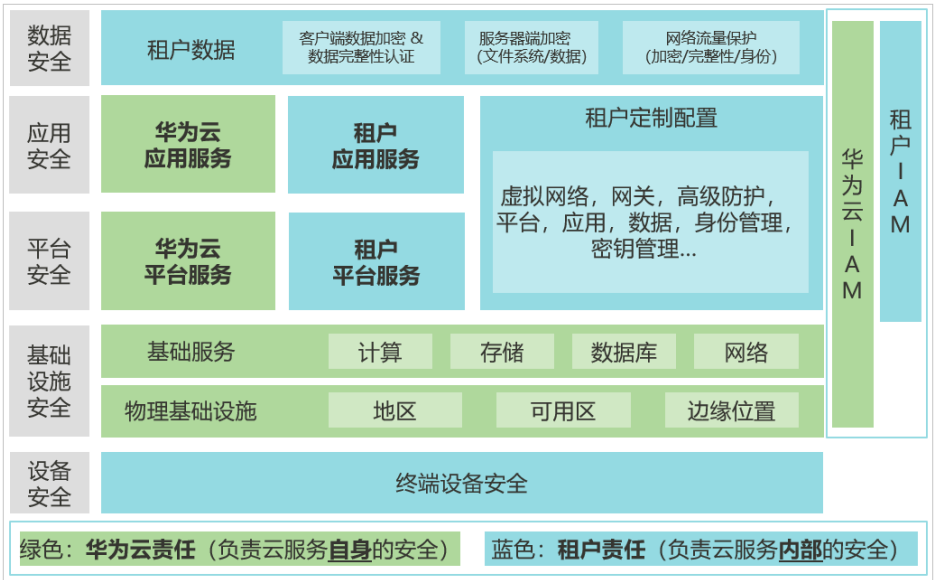
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图7-1所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 7-1 华为云安全责任共担模型



7.2 身份认证与访问控制

SecMaster对接了统一身份认证服务（Identity and Access Management，IAM）服务。SecMaster租户身份认证与访问控制通过IAM权限控制。

统一身份认证（Identity and Access Management，简称IAM）是华为云提供权限管理的基础服务，可以帮助SecMaster服务安全地控制访问权限。通过IAM，可以将用户加入到一个用户组中，并用策略来控制他们对SecMasterr资源的访问范围。SecMaster权限可以通过细粒度定义允许和拒绝的访问操作，以此实现SecMaster资源的权限访问控制。

7.3 数据保护技术

SecMaster通过多种数据保护手段和特性，保证通过SecMaster的数据安全可靠。

表 7-1 SecMaster 的数据保护手段和特性

数据保护手段	简要说明
静态数据保护	SecMaster通过敏感数据加密保证用户流量中敏感数据的安全性。
传输中的数据保护	微服务间数据传输进行加密，防止数据在传输过程中泄露或被篡改。用户的配置数据传输采用安全协议HTTPS，防止数据被窃取。
数据完整性校验	1. SecMaster接入云服务告警、漏洞和基线等时，有数据完整性校验。 2. SecMaster核心数据面进程启动时，配置数据执行可靠事件模式确保数据完整性（网络抖动、延迟、配置数据重发&重试等场景）。

数据保护手段	简要说明
数据隔离机制	租户区与管理面隔离，租户的所有操作权限隔离，不同租户间的策略、日志等数据隔离。
数据销毁机制	考虑到残留数据导致的信息泄露问题，华为云根据客户等级设定了不同的保留期时长，保留期到期仍未续订或充值，存储在云服务中的数据将被删除，云服务资源将被释放。SecMaster对云服务自动感知并在保留期到期后释放资源。

同时，SecMaster服务充分尊重用户隐私，遵循法律法规，不会采集和存储任何用户隐私数据。更多隐私数据使用和保护问题，请参考**隐私政策声明**。

7.4 审计与日志

- 审计

  云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

  用户开通云审计服务并创建和配置追踪器后，CTS可记录SecMaster的管理事件和数据事件用于审计。

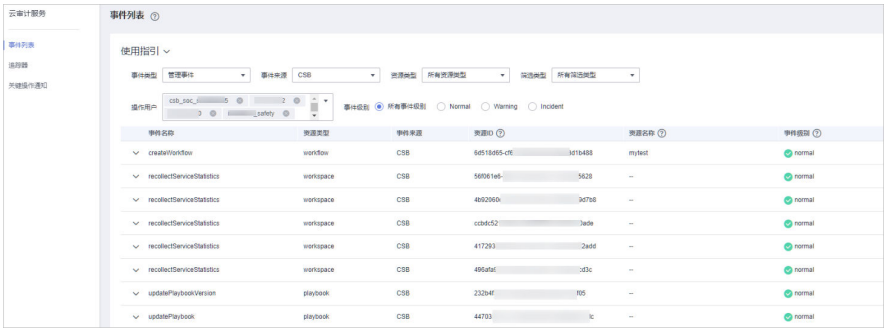
  CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

- 日志
  - 查询

    出于分析或审计等目的，用户开启了云审计服务后，系统开始记录SecMaster资源的操作。云审计服务管理控制台保存最近7天的操作记录。

    关于SecMaster云审计日志的查看，如**图7-2**所示。

    图 7-2 查询日志

7.5 服务韧性

华为云SecMaster当前主要部署在国内，已部署数据中心都处于正常运营状态，无一闲置。数据中心互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。为了减小由硬件故障、自然灾害或其他灾难带来的服务中断，华为云SecMaster提供灾难恢复计划。

当发生故障时，SecMaster的五级可靠性架构支持不同层级的可靠性，因此具有更高的可用性、容错性和可扩展性。

华为云SecMaster当前主要部署在国内，并在多个分区部署，同时SecMaster的所有管理面、引擎等组件均采用主备或集群方式部署。

7.6 监控安全风险

SecMaster已对接云监控服务（Cloud Eye，CES），可以通过管理控制台，查看SecMaster的相关运行指标，及时了解SecMaster运行状况。CES服务是华为云为用户提供一个针对各种云上资源的立体化监控平台，用户通过云监控服务可以全面了解云上的资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。

SecMaster自身作为云上安全运营作战平台，可以接入其他云服务的安全告警，按照告警类型和等级统一维度呈现，可以准确实时监控云上威胁攻击、检测您资产中的安全告警事件；定义威胁告警通知，设置每日定时告警通知和实时告警通知，通过接收消息通知及时了解威胁风险。定义监控的威胁名单、告警类型、告警级别等，选择性呈现关注的威胁告警。帮助用户及时了解安全状况，从而起到预警作用。

CES的详细介绍和开通配置方法，请参见**CES快速入门**。

表 7-2 监控

事件来源	事件名称	事件级别	事件说明	处理建议	事件影响
SYS.SecMaster	独享引擎创建失败	重要	一般是由于底层资源不足等原因导致。	提交工单让运维在后台协调资源再重试。	无法创建独享引擎
SYS.SecMaster	独享引擎运行异常	紧急	一般是由于流量过大或者恶意流程，插件导致。	1. 排查流程，插件执行是否占用资源过多。 2. 查看实例监控，短期内是否实例数量暴增。	无法执行实例
SYS.SecMaster	剧本实例执行失败	一般	一般是由于剧本，流程配置出错导致。	通过实例监控查看失败原因，修改剧本，流程配置。	无
SYS.SecMaster	剧本实例突增	一般	一般是由于剧本，流程配置出错导致。	通过实例监控查看突增原因，修改剧本，流程配置。	无
SYS.SecMaster	日志消息突增	重要	上游服务产生大量日志，导致消息快速增加。	需要排查上游服务业务是否正常。	无
SYS.SecMaster	日志消息突减	重要	上游服务产生日志突然变小。	需要排查上游业务是否正常	无

告警监控相关内容详细操作请参见：

- **漏洞管理**
- **基线检查**
- **安全报告**

7.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 7-3 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 7-4 资源中心

7.8 安全编排

SecMaster的安全编排功能可以针对云上安全事件提供安全编排剧本，实现安全事件的高效、自动化响应处置。其主要功能如下：

- 剧本管理：内置自动响应的剧本，支持按需定义扩展。

  编写剧本的过程就是将安全运营流程和规程转换为剧本，并在剧本中将各种应用编排到一起的过程，也是将人读安全运营流程转换为机读工作流的过程。
- 流程管理：绘制流程图响应剧本触发。
- 资产管理：支持对关键资产、安全资产等进行统一管理呈现。
- 实例管理：支持对运行的实例进行监控管理及记录查看。
- 安全事件自动化响应：对需要处理的安全事件（incidence）以及可疑事件，通过安全编排实现自动化处置及事件调查。

安全编排设置方法请参见**安全编排**。

8 SecMaster 权限管理

如果您需要对华为云上购买的安全云脑（SecMaster）资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并使用策略来控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有安全云脑（SecMaster）的使用权限，但是不希望他们拥有删除SecMaster等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用SecMaster，但是不允许删除SecMaster的权限策略，控制他们对SecMaster资源的使用范围。

如果账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用SecMaster的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账户中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

SecMaster 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

SecMaster部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问SecMaster时，需要先切换至授权区域。

权限根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对SecMaster服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。

如表8-1所示，包括了SecMaster的所有系统权限。

表 8-1 SecMaster 系统权限

系统角色/策略名称	描述	类别	依赖关系
SecMaster FullAccess	安全云脑的所有权限。	系统策略	无
SecMaster ReadOnlyAccess	安全云脑只读权限，拥有该权限的用户仅能查看安全云脑数据，不具备安全云脑配置权限。	系统策略	无

SecMaster FullAccess 策略内容

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "secmaster:*:*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "vpc:vpcs:list",
        "vpc:subnets:get",
        "vpcep:endpoints:*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "obs:bucket:ListBucketVersions"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "iam:permissions:checkRoleForAgencyOnDomain",
        "iam:permissions:checkRoleForAgencyOnProject",
        "iam:permissions:checkRoleForAgency",
        "iam:permissions:grantRoleToAgency",
        "iam:permissions:grantRoleToAgencyOnDomain",
        "iam:permissions:grantRoleToAgencyOnProject",
        "iam:policies:*",
        "iam:agencies:*",
        "iam:roles:*",
        "iam:users:listUsers",
        "iam:tokens:assume"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "organizations:organizations:get",
        "organizations:delegatedAdministrators:list",
        "organizations:roots:list",
        "organizations:ous:list",
        "organizations:accounts:list"
      ],
      "Effect": "Allow"
```

```
    },
    {
      "Action": [
        "ecs:cloudServers:list"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "sts:agencies:assume"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "lts:log*:list*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

SecMaster ReadOnlyAccess 策略内容

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "secmaster:*:get*",
        "secmaster:*:list*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "vpc:vpcs:list",
        "vpc:subnets:get",
        "vpcep:endpoints:get",
        "vpcep:endpoints:list"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "obs:bucket:ListBucketVersions"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "iam:permissions:checkRoleForAgencyOnDomain",
        "iam:permissions:checkRoleForAgencyOnProject",
        "iam:permissions:checkRoleForAgency",
        "iam:policies:get*",
        "iam:policies:list*",
        "iam:agencies:get*",
        "iam:agencies:list*",
        "iam:roles:get*",
        "iam:roles:list*",
        "iam:users:listUsers"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "organizations:organizations:get",
        "organizations:delegatedAdministrators:list",
        "organizations:roots:list",
```

```
            "organizations:ous:list",
            "organizations:accounts:list"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "ecs:cloudServers:list"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "lts:log*:list*"
         ],
         "Effect": "Allow"
      }
   ]
}
```

9 与其他云服务的关系

本章节主要介绍安全云脑与其他云服务之间的关系。

与安全服务的关系

安全云脑从**主机安全**（Host Security Service，HSS）、**Web应用防火墙**（Web Application Firewall，WAF）、**Anti-DDoS流量清洗**（Anti-DDoS）等安全防护服务中获取必要的安全事件记录，进行大数据挖掘和机器学习，智能AI分析并识别出攻击和入侵，帮助用户了解攻击和入侵过程，并提供相关的防护措施建议。更多说明请参见**安全云脑与其他安全服务之间的关系与区别**。

与弹性云服务器的关系

安全云脑为**弹性云服务器**（Elastic Cloud Server，ECS）提供资产安全管理服务，结合HSS主机防护状态，全方位呈现当前ECS安全风险态势，并提供相应防护建议。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS），为SecMaster提供云服务资源的操作记录，记录内容包括从访问管理控制台发起的云服务资源操作请求以及每次请求的结果，供您查询、审计和回溯使用。

CTS记录SecMaster相关操作事件，方便用户日后的查询、审计和回溯。

与云监控服务的关系

云监控（Cloud Eye）为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。用户可以通过事件及时了解安全云脑的状况，并及时收到异常报警做出反应，保证业务顺畅运行。具体请参见《云监控服务用户指南》。

与标签管理服务的关系

标签管理服务（Tag Management Service，简称TMS）是一种快速便捷将标签集中管理的可视化服务，方便用户通过标签标识管理工作空间实例。

表 9-1 标签管理服务支持的 SecMaster 操作列表

操作名称	资源类型	事件名称
查询资源实例列表	Workspace	listResourceInstance
查询资源实例数量	Workspace	countResourceInstance
批量查询资源标签	Tag	batchTagResources
批量删除资源标签	Tag	batchUntagResources
查询项目标签	Tag	listProjectTag
更新标签值	Tag	updateTagValue
查询资源标签	Tag	listResourceTag

与企业管理的关系

企业中有多个项目，多个项目的资源需要分开结算，且分属不同人员进行管理。同时项目可以单独启动或停止，对其他项目没有影响。**企业管理**可以针对企业中的每个项目，分别建立企业项目，管理各自的资源，并且针对不同的企业项目，设置不同的人员进行管理。

安全云脑支持企业管理，您可以将安全云脑上的资源按照企业项目进行管理，并设置每个企业项目的用户权限。

10 基本概念

本节介绍安全云脑相关概念。

安全风险

安全风险是对资产安全状况的综合评估，反映了一段时间内资产遭受的安全风险。安全风险通常体现为一个量化的数值，便于用户理解目前资产的安全状况，数值大小并不代表资产的安全或危险，仅作为资产遭受攻击严重程度的参考。

威胁告警

广义的威胁告警是指由于自然因素、人为因素或软硬件本身的原因，对信息系统造成危害的事件，或对社会造成负面影响的威胁。对于安全云脑来讲，威胁告警泛指根据大数据分析检测出的，对用户资产产生威胁的安全事件。

工作空间

工作空间（Workspace）属于安全云脑顶层工作台，单个工作空间可绑定普通项目、企业项目和Region，可支撑不同场景下的工作空间运营模式。

数据空间

数据空间是进行数据分组、负载、流控单元。同一数据空间的数据共享同一载均衡策略。

数据管道

数据传输消息主题和存储索引组合为数据管道。

分类和映射

分类和映射是指对云服务告警进行类型匹配和字段映射。

安全编排

安全编排（Security Orchestration）是将企业和组织在安全运营过程中涉及的不同系统或者一个系统内部不同组件的安全功能通过可编程接口（API）封装后形成的安全能力（即应用）和人工检查点按照一定的逻辑关系组合到一起，以完成某个特定的安全运营过程和规程。

安全编排是将安全运营相关的工具/技术、流程和人员等各种能力整合到一起的一种协同工作方式。

生产者

是用来构建并传输数据到服务端的逻辑概念，负责把数据放入消息队列。

订阅器

用于订阅安全云脑管道消息，一个管道可由多个订阅器进行订阅，安全云脑通过订阅器进行消息分发。

消费者

是用来接收并处理数据的运行实体，负责通过订阅器把安全云脑管道中的消息进行消费并处理。

消息队列

是数据存储和传输的实际容器。

威胁检测模型

是一种被训练的AI智能识别算法模型。能针对特定威胁，自动化的完成数据汇聚、分析和报警，这种检测模式具备较好的泛化能力，防躲避能力强，可在不同业务系统中发挥同等效果，应对复杂的新型攻击。

A 修订记录

发布日期	修改记录
2024-02-29	第五次正式发布。 ● 更新**SecMaster权限管理**章节，更新安全云脑策略内容。 ● 更新**约束与限制**章节，补充工作空间、安全分析的约束与限制。 ● 更新**产品功能**章节内容，优化描述信息。
2023-08-10	第四次正式发布。 ● 更新**产品功能**章节内容，新增策略管理内容。 ● 更新**服务版本差异**章节内容，新增策略管理内容。 ● 计费说明章节内容合入计费说明手册。
2023-05-25	第三次正式发布。 ● 新增**产品功能**章节中数据采集内容。 ● 更新**“基本概念”**章节中描述信息。
2023-04-25	第二次正式发布。 ● 刷新“计费说明”章节内容，新增版本计费、升级等说明。 ● 刷新**服务版本差异**章节描述。
2023-02-28	第一次正式发布。