态势感知

产品介绍

文档版本 36

发布日期 2022-10-26

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。

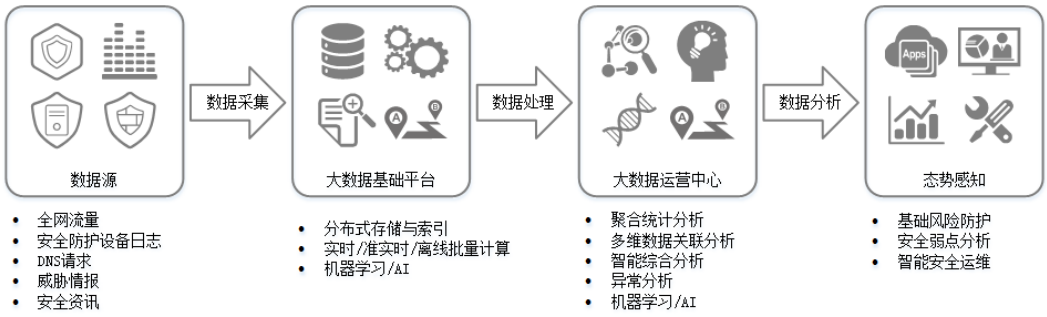
目 录

1 什么是态势感知?

态势感知（Situation Awareness，SA）是华为云安全管理与态势分析平台。能够检测出8大类的云上安全风险，包括DDoS攻击、暴力破解、Web攻击、后门木马、僵尸主机、异常行为、漏洞攻击、命令与控制等。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，为用户呈现出全局安全攻击态势。

工作原理

态势感知通过采集全网流量数据和安全防护设备日志信息，并利用大数据安全分析平台进行处理和分析，态势感知检测出威胁告警，同时将企业主机安全、Web应用防火墙和DDoS流量清洗等安全服务上报的告警数据进行汇合，实时为用户呈现完整的全网攻击态势，进而为安全事件的处置决策提供依据。



2 产品功能

态势感知提供安全概览、资源管理、业务分析、综合大屏、威胁告警、漏洞管理、基线检查、检测结果、安全报告、日志管理、产品集成等全局安全态势集中管理功能。具体说明如表2-1所示。

表 2-1 态势感知功能总览

功能	功能描述	参考链接
安全概览	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。 • 安全评分：根据版本威胁检测能力，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。 • 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。 • 威胁检测：集中呈现最近7天检测到的告警数量及类型。	安全概览
业务分析	关联HSS、WAF、DBSS服务，全面展示云上资产的安全状态和存在的安全风险。	业务分析
综合大屏	利用AI技术将海量云安全数据的分析并分类，通过综合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。	综合大屏
资源管理	同步资源信息，集中呈现资源整体安全状况。	资源管理

功能	功能描述	参考链接
威胁告警	实时监控云上威胁攻击，提供告警通知和监控，记录近180天告警事件详情，分析威胁攻击情况，并针对典型威胁事件预置策略实施防御手段。 ● 告警列表：列表呈现威胁告警事件统计信息，支持查看告警事件和受威胁资产详情，并支持导出全部告警事件。 ● 威胁分析：支持从“攻击源”或“被攻击资产”查询威胁攻击，统计威胁攻击次数或资产被攻击次数。 ● 告警监控：自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。 ● 通知告警：自定义威胁告警通知，支持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。	威胁告警
漏洞管理	通过实时获取业界热点安全漏洞讯息，同步主机漏洞扫描和网站漏洞扫描结果，全面掌握云上资产漏洞风险状况，并提供相应漏洞修复建议。	漏洞管理
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。	基线检查
检测结果	通过集成安全防护产品，接入安全产品检测数据，管理全部检测结果。	检测结果
分析报告	为统计全局安全攻击态势，通过开启安全报告，态势感知以邮件形式向指定的收件人发送安全报告，反映阶段性安全概况、安全风险趋势。	分析报告
日志管理	通过授权OBS服务存储态势感知日志，帮助用户轻松应对安全日志存储、导出场景，满足日志存储180天及集中审计的要求。	日志管理
安全产品集成	通过集成安全防护产品，接入安全产品检测数据，管理检测结果的数据来源。同时，支持查看传输数据量，管理数据上报健康状态。	安全产品集成

3 应用场景

资产风险管理

云上业务众多，云上资产日益庞大，以及云资产的变化频繁，大大增加了云上安全风险。

态势感知集中呈现云上所有资产安全状况，实时监控云上业务整体安全，让服务器中的漏洞、威胁和攻击情况一目了然，保障所有资产的安全，帮助企业轻松应对资产安全风险。

威胁事件告警

面对云上各类安全威胁，以及不断涌出的新型威胁类型，态势感知通过汇集全网流量数据和安全防护设备日志信息，能够实时检测和监控云上安全风险，实时呈现告警事件的统计信息，并可对各种威胁事件进行汇聚统计。

此外，针对常见的暴力破解、Web攻击、后门木马、僵尸主机威胁事件，可预制的安全防护策略有效防御威胁风险，提升运维效率。

漏洞风险通报

随着企业业务的不断上云，为避免漏洞被成功利用，需尽可能多的找出并修复漏洞。

态势感知通过采集云上应急安全通告，能够实时披露新发现的漏洞，通报突发安全漏洞事件和预警潜在漏洞；同时通过集成漏洞扫描结果，能够定期进行漏洞扫描，集中管理主机漏洞和网站漏洞，对系统、软件和网站进行检测，检测出系统、软件和网站存在的漏洞，针对检测到的漏洞提供修复建议。

集中的云上漏洞管理，快速帮助用户识别关键风险，发现攻击者可能感兴趣的资产，帮助用户快速弥补安全短板。

风险配置管理

支持检测云服务关键配置项，通过执行扫描任务，检查云服务基线配置风险状态，分类呈现云服务配置检测结果，告警提示存在安全隐患的配置，并提供相应配置加固建议和帮助指导。

4 服务版本差异

目前态势感知提供基础版、标准版和专业版三个版本，不同版本有不同功能使用范围，详细功能介绍请参见**产品功能**。

- **基础版**免费使用，仅需登录SA管理控制台，即可免费体验基础版功能。
  基础版提供检测部分威胁风险，呈现一定云上资产安全态势。
- **标准版**仅支持包周期计费模式。购买标准版后，呈现一定云上资产安全态势。提供安全检测、威胁分析等功能，满足企业安全运营要求。
- **专业版**可选择包周期和按需计费模式。购买专业版后，呈现全局安全态势，通过动态安全检测和威胁分析，并提供安全加固建议。
- **综合大屏**可选择包周期和按需计费模式。为充分呈现云上安全态势，建议您在购买态势感知专业版后，再开通综合大屏功能。

版本功能差异

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。
- √+：代表支持该功能，但需额外购买功能或服务。

表 4-1 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
安全概览	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	实时呈现展示待处理威胁告警、待修复漏洞、基线异常问题的安全监控统计数据。	√	√	√

服务功能	功能模块	功能概述	基础版	标准版	专业版
	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。	√	√	√
	威胁检测	集中呈现最近7天检测到的告警数量及类型。	√	√	√
资源管理	资源安全状况	同步资源信息，集中呈现资源整体安全状况。	×	√	√
业务分析	专项分析	关联HSS、WAF、DBSS安全防护服务，全面展示主机、应用、数据库的安全状态和存在的安全风险。	√+	√+	√+
综合大屏	综合态势感知	大屏集中展示云上资产综合安全态势，动态呈现资产风险状况。	×	×	√+
	主机安全态势	大屏集中呈现华为云主机安全态势，动态呈现主机安全状况。	×	×	√+
威胁告警	告警列表	集中呈现威胁告警事件统计信息，导出告警事件。	√	√	√
		通过将告警忽略、标记为线下处理，标识告警事件。	×	√	√
	威胁分析	根据“攻击源”的IP查询被攻击的资产信息，亦可根据“被攻击的资产”的IP查询威胁攻击来源信息。	×	√	√
	告警监控	通过设置监控的威胁名单，以及设置关注的告警条件，自定义呈现关注的威胁告警。	×	×	√
	通知告警	通过自定义威胁告警通知，及时了解威胁风险。	×	√	√
漏洞管理	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。	√	√	√
	主机漏洞	集中呈现主机漏洞扫描结果信息，并提供相应修复建议。	×	√	√
	网站漏洞	集中呈现网站漏洞扫描结果信息，并提供相应修复建议。	×	×	√
基线检查	云服务基线	通过一键扫描云服务基线，分类呈现云服务配置项检测结果信息。	×	√	√
		通过一键扫描云服务基线，分类呈现云服务配置项检测结果信息。支持查看检测结果详情，并提供相应修复建议。	×	×	√

服务功能	功能模块	功能概述	基础版	标准版	专业版
检测结果	全部结果	集中呈现安全产品的检测结果，可导出结果、标识结果等。	√	√	√
安全报告	分析报告	默认自动创建一个周报和月报，仅可生成两期报告。	×	×	√
		通过创建报告，定向发送报告内容。可管理历史报告和报告列表。	×	×	√
产品集成	安全产品集成	通过集成安全产品，接入安全产品检测结果，管理检测结果的数据来源。	√	√	√
日志管理	日志管理	通过授权OBS存储SA日志，满足日志审计和容灾需求。	×	×	√

5 基本概念

本节介绍态势感知相关概念。

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。对于态势感知来讲，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。

主机漏洞

主机漏洞是通过版本对比检测，检测出的系统和软件（例如：Apache、MySQL等）存在的漏洞，帮助用户识别出存在的风险。

网站漏洞

网站漏洞是通过网络进行爬虫，智能对比漏洞特征检测出的web漏洞。态势感知具有OWASP TOP10和WASC的漏洞检测能力，支持扫描22种类型以上的漏洞，扫描规则云端自动更新，全网生效，及时涵盖最新爆发的漏洞及支持HTTPS扫描。

云服务基线

云服务基线是应用在公有云场景下，帮助用户检测云产品上存在的风险配置项，并提供修复建议。目前提供“安全上云合规检查1.0”、“等保2.0三级要求”、“护网检查”等方面的检查。

攻击类型

- DDoS攻击

  分布式拒绝服务（Distributed Denial of Service，简称DDoS）攻击是指攻击者使用网络上多个被攻陷的电脑作为攻击机器，向特定的目标发动DoS攻击。DoS（Denial of Service）攻击也称洪水攻击，是一种网络攻击手法，其目的在于使目

标电脑的网络或系统资源耗尽，服务暂时中断或停止，导致合法用户不能够访问正常网络服务的行为。

- 暴力破解

  暴力破解法是一种密码分析方法，基本原理是在一定条件范围内对所有可能结果进行逐一验证，直到找出符合条件的结果为止。攻击者通常使用暴力破解的方式猜测远程登录的用户名和密码，一旦破解成功，即可实施攻击和控制。

- Web攻击

  Web攻击是针对用户上网行为或网站服务器等设备进行攻击的行为。常见的Web攻击方式包括SQL注入攻击、跨站脚本攻击、跨站请求伪造攻击等。

- 后门木马

  后门木马又称特洛伊木马（Trojan Horse），是一种后门程序。后门木马具有很高的伪装性，通常表现为一个正常的应用程序或文件，以获得广泛的传播和目标用户的信任。当目标用户执行后门木马程序后，攻击者即可对用户的主机进行破坏或盗取敏感数据，如各种账户、密码、保密文件等。在黑客进行的各种攻击行为中，后门木马基本上都起到了先导作用，为进一步的攻击打下基础。

- 僵尸主机

  僵尸主机亦称傀儡机，是由攻击者通过木马蠕虫感染的主机，大量僵尸主机可以组成僵尸网络（Botnet）。攻击者通过控制信道向僵尸网络内的大量僵尸主机下达指令，令其发送伪造包或垃圾数据包，使攻击目标瘫痪并“拒绝服务”，这就是常见的DDoS攻击。此外，随着虚拟货币（如比特币）价值的持续增长，以及挖矿成本的逐渐增高，攻击者也开始利用僵尸主机进行挖矿和牟利。

- 异常行为

  异常行为主要指在主机中发生了一些不应当出现的事件。例如，某用户在非正常时间成功登录了系统，一些文件目录发生了计划外的变更，进程出现了非正常的行为等。这些异常的行为事件很多是有恶意程序在背后作乱。所以在发生这类异常行为时，应当引起重视。态势感知中的异常行为数据主要来源于主机安全服务。

- 漏洞攻击

  漏洞是指计算机系统安全方面的缺陷，可导致系统或应用数据遭受保密性、完整性、可用性等方面的威胁。攻击者利用漏洞获取计算机权限、盗取敏感数据、破坏软硬件系统等行为均可称为漏洞攻击。

- 命令与控制

  域名生成算法（Domain Generation Algorithm，简称DGA）是一种利用随机字符生成命令与控制（Command and Control，简称C&C）域名的技术，常被用于逃避域名黑名单功能的检测。

  攻击者利用DGA生产恶意域名后，选择部分域名进行注册并指向C&C服务器。当受害者运行恶意程序后，主机将通过恶意域名连接至C&C服务器，攻击者即可远程操控主机。

6 SA 权限管理

如果您需要对华为云上购买的态势感知（Situation Awareness，SA）资源，给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，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，您希望他们拥有态势感知（Situation Awareness，SA）的使用权限，但是不希望他们拥有删除SA数据等高危操作的权限，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SA，但是不允许删除SA数据的权限策略，控制他们对SA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SA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》**。

SA 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。

SA部署时不区分物理区域，为全局级服务。授权时，在全局级服务中设置权限，访问SA时，不需要切换区域。

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SA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。SA支持的授权项请参见**权限及授权项**。

如表6-1所示，包括了SA的所有系统权限。

表 6-1 SA 系统权限

策略名称	描述	类别	依赖关系
SA FullAccess	态势感知的所有权限。	系统策略	无
SA ReadOnlyAccess	态势感知只读权限，拥有该权限的用户仅能查看态势感知数据，不具备态势感知配置权限。	系统策略	无

说明

目前，“SA FullAccess”或“SA ReadOnlyAccess”权限需要配合“Tenant Guest”权限才能使用。具体说明如下：

- 配置SA所有权限：“SA FullAccess”和“Tenant Guest”权限。

  其中，如果需要使用SA的**资源管理**和**基线检查**功能需要配置以下权限：

  - **资源管理**：“SA FullAccess”和“Tenant Administrator”权限，详细操作请参见**配置相关功能所需的权限**。
  - **基线检查**：“SA FullAccess”、“Tenant Administrator”和IAM相关权限，详细操作请参见**配置相关功能所需的权限**。
- 配置SA只读权限：“SA ReadOnlyAccess”和“Tenant Guest”权限。

如表6-2列出了SA常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 6-2 常用操作与系统权限的关系

操作	SA FullAccess	SA ReadOnlyAccess
获取告警列表	√	√
获取威胁分析结果	√	√
获取主机列表	√	√
查看综合态势感知大屏	√	√
查看主机安全态势大屏	√	√
查看安全概览	√	√
查看安全概览	√	√
配置告警设置	√	x
查看告警设置	√	√
获取全局态势信息	√	√
获取订阅主题	√	x

操作	SA FullAccess	SA ReadOnlyAccess
获取云服务基线检查结果	√	√
设置云服务基线扫描	√	x

相关介绍

- IAM产品介绍
- 创建用户组、用户并授予SA权限
- SA自定义策略
- SA权限及授权项

SA FullAccess 策略内容

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "sa:*:*"
         ],
         "Effect": "Allow"
      }
   ]
}
```

SA ReadOnlyAccess 策略内容

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "sa:cssb:get",
            "sa:service:get",
            "sa:subscribe:get",
            "sa:subscribe:getList",
            "sa:threatevent:getAnalyze",
            "sa:threatevent:getAsset",
            "sa:threatevent:getDashboard",
            "sa:threatevent:getHostscreen",
            "sa:threatevent:getList",
            "sa:threatevent:getOverview",
            "sa:threatevent:getSafety"
         ],
         "Effect": "Allow"
      }
   ]
}
```

7 与其他云服务的关系

本小节主要介绍态势感知与其他云服务之间的关系。

与安全服务的关系

态势感知从**主机安全服务**（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**态势感知与其他安全服务之间的关系与区别**。

与 ECS 的关系

态势感知为**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 IAM 的关系

统一身份认证服务（Identity and Access Management，IAM）为态势感知提供用户身份鉴权、IAM用户权限设置等权限管理服务，更多详细说明请参见**SA权限管理**。

与 CTS 的关系

云审计服务（Cloud Trace Service，CTS），为SA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SA相关操作事件，方便用户日后的查询、审计和回溯。

与 OBS 的关系

通过对象存储服务（Object Storage Service，OBS），您可以将SA日志存储至OBS桶中，确保日志不丢失，实现数据持久化，更多详细说明请参见**SA日志管理**。