威胁检测服务

产品介绍

文档版本 11

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 什么是威胁检测服务

威胁检测服务（Managed Threat Detection，简称MTD），通过接入目标区域中您在华为云操作所涉及到的IAM日志、DNS日志、CTS日志、OBS日志、VPC日志，持续实时检测日志中访问者的IP或域名是否存在潜在的恶意活动和未经授权行为并进行告警。

此服务集成了AI智能引擎、威胁情报、规则基线三种检测方式，智能检测来自多个云服务（包含IAM服务、DNS服务、CTS服务、OBS服务、VPC服务）日志数据中的访问行为，去发现是否存在潜在威胁，对可能存在威胁的访问行为生成告警信息，输出告警结果。您可通过告警描述对告警信息进行核查、处理，在未造成信息泄露等重大损失之前，及时对潜在威胁进行处理，对服务安全进行升级加固，从而保护您的账户安全、保障服务稳定运行。

说明

威胁检测服务即将下线，下线公告请参见**华为云产品威胁检测服务MTD下线通知**。

威胁检测服务的能力将由**安全云脑 SecMaster**服务提供。为了避免影响您的业务，建议您尽快提交工单协助您将业务切换至安全云脑，以更好地为您提供业务支持。

各 Region 支持的检测类型

各Region支持的检测类型如**表1-1**所示。

表 1-1 各 Region 支持的检测类型

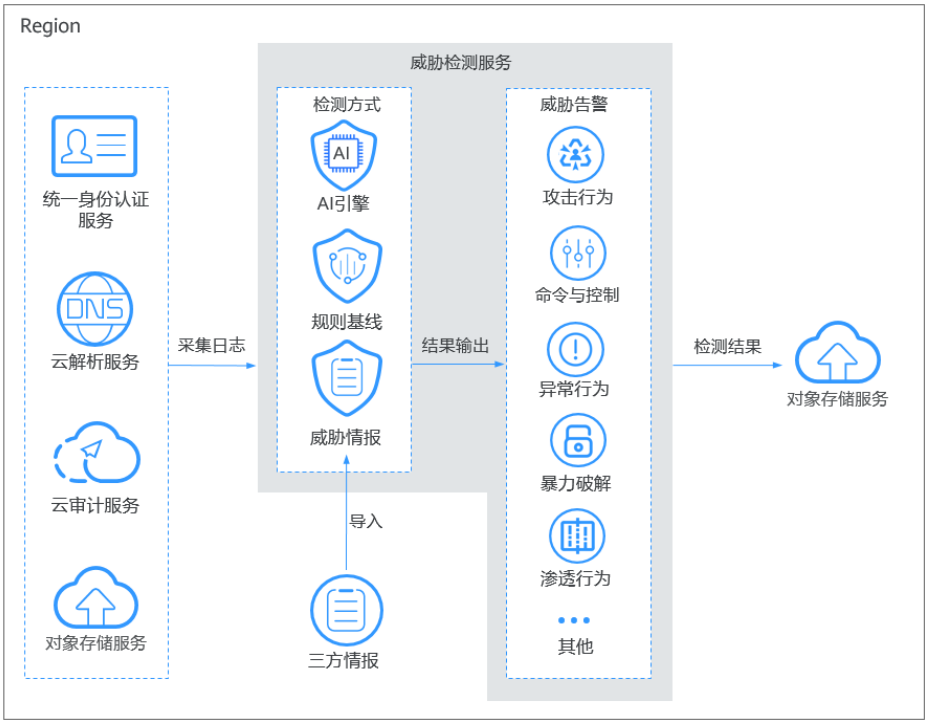
名称	IAM检测	DNS检测	CTS检测	OBS检测	VPC检测
华南-广州	√	√	√	√	√
华东-上海一	√	√	√	-	√
华北-北京四	√	√	√	√	-

检测原理

威胁检测服务通过采集统一身份认证（IAM）、云解析服务（DNS）、云审计服务（CTS）、对象存储服务（OBS）、虚拟私有云（VPC）的日志，利用AI智能引擎、威

胁情报、规则基线模型，持续监控暴力破解、恶意攻击、渗透、挖矿攻击等恶意活动和未经授权行为，识别云服务日志中的潜在威胁，并对检测出的威胁告警进行统计。威胁检测服务的检测原理如图1-1所示。

图 1-1 检测原理



2 功能特性

基于 AI 智能引擎的威胁检测

威胁检测服务在基于威胁情报和规则基线检测的基础之上，融入了AI智能检测引擎。通过弹性画像模型、无监督学习模型、有监督学习模型实现对风险口令、凭证泄露、Token利用、异常委托、异地登录、未知威胁、暴力破解七大IAM高危场景进行智能检测。通过SVM、随机森林、神经网络等算法实现对隧道域名、DGA域名以及异常行为的智能检测。

AI引擎检测保持模型对真实数据的学习，保证数据对模型的反复验证和人工审查，精准制定预过滤和后处理逻辑，结合先验知识，模型达成零误报。同时，以阶段性检测结果为输入，通过模型重训练和依赖文件定期更新持续优化模型，提升模型告警准确率。

实时检测，缩短风险处理周期

威胁检测服务采用实时获取统一身份认证（IAM）、云解析服务（DNS）、云审计服务（CTS）、对象存储服务（OBS）、虚拟私有云（VPC）的日志数据进行持续不断的检测，威胁检测服务在第一时间发现潜在威胁告警，您可在第一时间进行核查、处理，缩短潜在威胁的风险周期，大程度降低风险损失。

威胁告警按严重等级划分

威胁检测服务对检测到的告警结果通过告警的严重性等级（致命、高危、中危、低危、提示）进行统计，对告警结果进行详细的等级划分，帮助您确定威胁告警内容的响应等级，通过告警描述能及时对告警做出判断进行优先级处理。

告警信息支持转储满足合规要求

MTD检测到的告警结果默认存储最近30天数据，为满足等保合规要求，您可将MTD告警结果转存至OBS，实现数据的更长时间存储。

名单库管理策略

您可自定义上传和添加情报/白名单到OBS桶，异步同步到威胁检测服务，上传后检测服务将优先关联检测名单库中的IP和域名，及时发现（情报）/忽略（白名单）名单库中IP/域名地址的活动，降低检测响应时间，减轻服务运行负载。

3 产品优势

基于 AI 智能引擎的 IAM 异常行为检测

威胁检测服务在基于威胁情报和规则基线检测的基础之上，融入了AI智能检测引擎。通过弹性画像模型、无监督模型、有监督模型实现对风险口令、凭证泄露、Token利用、异常委托、异地登录、未知威胁、暴力破解七大IAM高危场景实现了异常行为的智能检测。

挖掘数据特性，创新算法架构

在算法方面，分析DNS域名格式特点，创新的结合BERT思想构造三通道CNN模型，相比传统直接将域名输入到神经网络的方法具有更好的检测效果，在业界内较先采用。

多模型协同检测，准确识别威胁

威胁检测服务除威胁情报和规则基线检测外，还提供4类基于AI智能引擎的算法能力：IAM异常检测、DGA检测、DNS挖矿木马检测、DNS可疑域名检测。针对不同检测目标，利用有监督、无监督深度神经网络、马尔科夫等算法训练7种AI模型，结合特征规则、分布统计以及外部输入的威胁情报，综合构建检测系统，有效提升威胁分析效率和准确性。

智能化威胁响应

MTD可以通过联动态势感知服务（SA）对接消息通知服务（SMN），在发现威胁的情况下，迅速通过短信或邮件的方式直接触达用户，高效率完成从威胁检测发现到告知安全运维人员的响应闭环。

黑/白名单汇集

可将MTD服务或其它所有服务历史发现的情报通过纯文本（Plaintext）格式添加到威胁检测服务中，也可将白名单添加到威胁检测服务，实现自定义威胁检测的范围，威胁检测服务会忽略白名单中IP地址的活动并对情报中IP地址的活动生成告警结果。

跨服务联动响应

- 为满足等保合规要求，支持将检测结果存储至对象存储服务（OBS）。
- 支持将检测结果向上同步至态势感知（SA）形成可视化运营，作为SA的重要能力输入，进行后续关联的安全运营动作。

4 应用场景

检测全局服务日志数据

威胁检测服务接入全量的统一身份认证（IAM）、云解析服务（DNS）、云审计服务（CTS）、对象存储服务（OBS）、虚拟私有云（VPC）的日志数据，利用AI智能引擎、威胁情报、规则基线模型一站式检测，持续监控暴力破解、恶意攻击、渗透、挖矿攻击等恶意活动和未经授权行为，识别云服务日志中的潜在威胁，对检测出的威胁告警信息进行统计展示。

识别分布式暴破攻击

威胁检测服务在业内领先引用AI智能引擎进行检测，提高检测的效率及标准，将潜在威胁纳入检测范围。

针对IAM重点保护对象，融入了AI智能检测引擎。通过弹性画像模型、无监督模型、有监督模型实现对风险口令、凭证泄露、Token利用、异常委托、异地登录、未知威胁、暴力破解七大IAM高危场景实现了异常行为的智能检测。可有效对化整为零低频次的分布式暴破攻击行为进行成功捕获。

捕获僵尸网络木马

威胁检测服务创新的结合BERT思想将DNS分成Bigram、Segment、Position三个Channel，构造三通道CNN模型，对已知/未知DGA和隧道域名、扫描行为、挖矿行为进行检测。模型可对Linux.Ngioweb僵尸网络、SystemdMiner挖矿木马、WatchBog挖矿木马、BadRabbit勒索病毒进行有效检测、捕获。

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，MTD可以通过联动态势感知服务（SA）对接消息通知服务（SMN），在发现威胁的情况下，迅速通过短信或邮件的方式直接触达用户，高效率完成从威胁检测发现到告知安全运维人员的响应闭环。

MTD满足识别弱口令、暴力破解、恶意攻击、渗透、挖矿攻击等40余种类型的威胁，满足云上安全威胁分析检测需求。

协同服务

MTD为了更准确、更全面的检测分析，支持与态势感知hub联动，将检测结果向上同步至态势感知（SA），统一界面呈现和未来的演进SOAR处理，形成可视化运营，进行

后续关联的安全运营动作。同时，支持通过联动态势感知（SA）对接消息通知服务（SMN），推送邮件、短信。

数据联动

威胁检测服务支持导入第三方STIX，CSV格式威胁情报及可信IP列表至OBS，异步同步到威胁检测服务，上传后检测服务将优先关联检测名单库中的IP和域名，及时发现（情报）/忽略（白名单）名单库中IP/域名地址的活动，减少检测响应时间，减轻服务运行负载；同时支持将检测结果存储至对象存储服务（OBS），满足等保合规要求。

5 相关概念

检测器

检测器是一个区域（Region）实体，当您在某个区域（Region）启用威胁检测服务时，将在该区域（Region）生成一个检测器，威胁检测服务的所有检测结果都与检测器关联。

数据源

数据源是指威胁检测服务分析、处理的各类服务日志。为了检测各种未经授权的恶意活动，威胁检测服务会获取您授权开启检测的服务（包含IAM、DNS、CTS、OBS、VPC）的日志数据，这些日志数据就是威胁检测服务的数据源。

6 计费说明

威胁检测服务提供包周期（包年/包月）计费模式，使用越久越便宜。

计费项

威胁检测服务根据您购买的服务规格、使用时长和超出服务规格的检测量进行计费。

表 6-1 计费项信息

计费项	计费说明
服务规格（必选）	按购买的服务规格：入门包、初级包、基础包、高级包计费。
叠加包	按实际检测量超出您所购买的服务规格部分计费。 **注意** 无需主动购买。在您的购买时长内，若某月实际检测量超出您所购买的服务规格，系统将根据实际检测量自动购买对应的叠加包，自动按需计费。
购买时长（必选）	提供包月和包年的购买模式。

计费模式

提供包周期（包年/包月）计费模式，使用越久越便宜。包周期计费将按照订单的购买周期进行结算。

续费

为了避免历史告警数据等相关资源被删除，建议您及时续费。服务到期后未续费，MTD将根据您的使用情况按需收费。

如需续费，请在管理控制台续费管理页面进行续费操作。详细操作请参考**手动续费**。

到期与欠费

- 到期

服务到期后，如果您没有按时续费，华为云将提供一定的资源保留期，保留期结束后，您的相关资源会被自动删除，且不能再找回资源，也不能再续费。关于保留期时长等信息请参考**资源停止服务或逾期释放说明**。

说明

如果您所购买的服务规格到期，且未进行续购，MTD将根据您的使用情况按需计费。

- 欠费

  如果存在月检测量超出您所购买的服务规格的情况，检测量“叠加包”的按需购买可能会导致您的账号欠费。

  欠费后，您可以在管理控制台费用中心查询欠费详情。为了相关资源不受影响，请您及时充值，详细操作请参考**欠费还款**。

相关问题

购买MTD服务后，关闭所有日志数据源开关是否会计费?

7 MTD 权限管理

如果您需要对华为云上购买的MTD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，并授权控制员工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，您希望这些员工拥有MTD的使用权限，但是不希望这些员工拥有删除MTD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MTD，但是不允许删除MTD的权限，控制员工对MTD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MTD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，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

MTD 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。

MTD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MTD时，需要先切换至授权区域。

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MTD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。

8 与其他云服务的关系

与统一身份认证服务的关系

统一身份认证（Identity and Access Management，简称IAM）为威胁检测服务提供了权限管理的功能。需要拥有MTD Administrator权限的用户才能使用MTD服务。如需开通该权限，请联系拥有Security Administrator权限的用户。威胁检测服务可以为IAM提供对日志数据中访客可能存在的恶意活动和未经授权行为进行检测。

与云审计服务的关系

云审计服务（Cloud Trace Service，简称CTS）记录了威胁检测服务相关的操作事件，方便用户日后的查询、审计和回溯。威胁检测服务可以为CTS提供对日志数据中访客可能存在的恶意活动和未经授权行为进行检测。

与虚拟私有云的关系

虚拟私有云（Virtual Private Cloud，简称VPC）是用户在华为云上申请的隔离的、私密的虚拟网络环境。经用户授权后，威胁检测服务可以为VPC的日志数据提供恶意活动和未经授权的行为检测服务。

与云解析服务的关系

云解析服务（Domain Name Service，简称DNS）提供DNS服务和DNS管理服务。威胁检测服务可以为DNS提供对日志数据中访客可能存在的恶意活动和未经授权行为进行检测。

与对象存储服务的关系

对象存储服务（Object Storage Service，简称OBS）提供海量、安全、高可靠、低成本的数据存储能力，可供用户存储任意类型和大小的数据。用户根据需要可开启数据转存，可将威胁检测结果存储至OBS，满足合规要求，详情请参见**同步检测结果**。

与消息通知服务的关系

消息通知服务（Simple Message Notification，简称SMN）提供消息通知功能。威胁检测服务开启通知设置后，如果检测到恶意活动和未经授权的行为，告警信息会通过用户设置的接收通知方式发送给用户。

9 与其他云服务的区别

MTD 与 SA 的区别

态势感知（Situation Awareness，简称SA）是华为云可视化威胁检测和分析的安全管理平台。着重呈现全局安全威胁攻击态势，统筹分析多服务威胁数据和云上安全威胁，帮助企业构建全局安全体系，呈现全局安全威胁攻击态势。

威胁检测服务（Managed Threat Detection，简称MTD）主要检测云服务日志侧的潜在威胁，利用服务自身的AI智能引擎、威胁情报和规则基线检测模型实现对各类云服务日志的威胁检测，满足对检测到的威胁进行告警，对告警结果进行统计和展示。

表 9-1 MTD 与 SA 主要区别

功能项	威胁检测服务（MTD）	态势感知（SA）
支持产品/服务	• 统一身份认证服务（IAM） • 云解析服务（DNS） • 云审计服务（CTS） • 虚拟私有云服务（VPC） • 对象存储服务（OBS）	• 主机安全服务（HSS） • Anti-DDoS流量清洗（Anti-DDOS） • Web应用防火墙（WAF） • 云堡垒机（CBH） • 容器安全服务（CGS） • 漏洞扫描服务（VSS）
检测/分析数据源	• 统一身份认证服务（IAM）全量日志 • 云解析服务（DNS）全量日志 • 云审计服务（CTS）全量日志 • 全局服务的虚拟私有云服务（VPC）全量日志 • 对象存储服务（OBS）全量日志	• 全网流量 • 安全防护设备日志 • DNS请求 • 威胁情报 • 安全资讯

功能项	威胁检测服务（MTD）	态势感知（SA）
威胁检测	• 告警事件 支持基于AI智能引擎、威胁情报和规则基线合计40+类的告警示例类型。	• 告警事件 支持检测和呈现8大类告警事件，共200+种子告警类型。支持上报告警通知。 • 安全编排 支持一键实施预置的安全编排策略，加固资产安全。

MTD 暴力破解与 HSS 暴力破解的区别

主机安全服务（Host Security Service，简称HSS）是华为云提升主机整体安全性的服务。着重于全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，降低服务器面临的安全风险，保障主机整体安全。

威胁检测服务（Managed Threat Detection，简称MTD）在满足规则和情报检测基础之上，新增算法模型AI智能引擎，实现IAM异常检测、DGA检测、DNS隧道检测。针对IAM账号的爆破攻击，新增异常行为检测模型，实现账号分布式暴破攻击威胁的检测。

表 9-2 MTD 与 HSS 账号暴力破解的区别

功能项	威胁检测服务（MTD）	主机安全服务（HSS）
检测对象	• 您所使用服务的全量账户	• SSH账户 • RDP账户 • FTP账户 • SQL Server账户 • MySQL账户 • 其他服务账户
账户暴力攻击	• 支持导入威胁情报及白名单来自定义威胁检测的范围，威胁检测服务会忽略白名单中IP地址的活动，对发现与历史情报相似的IP或域名访问直接触发告警。 • 在IAM锁定时间窗口登录失败，或跨多个region登录、调用token直接触发告警。	• 如果30秒内，账户暴力破解次数达到5次及以上，HSS就会拦截该源IP，禁止其再次登录。 • 根据账户暴力破解告警详情，如“攻击源IP”、“攻击类型”和“拦截次数”，您能够快速识别出该源IP是否为可信IP，如果为可信IP，您可以通过手动解除拦截的方式，解除拦截的可信IP。

功能项	威胁检测服务（MTD）	主机安全服务（HSS）
账户异常登录	• 登录或获取token的成功率突变或总次数突增，触发威胁告警。 • IP首次尝试登录或获取token，触发威胁告警。 • IP异地登录，触发威胁告警。	• 检测主机异地登录行为并进行告警。 异地登录检测信息包括“登录源IP”、“登录时间”，攻击者尝试登录主机时使用的“用户名”和“云服务器名称”。 • 若在非常用登录地登录，则触发安全事件告警。 • 若账户暴力破解成功，登录到云主机，则触发安全事件告警。
异常行为	• 识别分布式暴破攻击 有效检测通过HTTP隧道使用随机公网IP对IAM账户进行连续攻击，每个攻击IP暴破次数在3次以内，化整为零的分布式攻击行为成功绕过传统监控。 • 检测账号AK/SK疑似泄露被利用的行为。 • 检测账号疑似被建立委托的行为。 • 检测Token疑似被恶意利用的行为。 • 检测账号疑似被口令破解的行为。	• 监控进程CPU使用异常。 • 检测进程对恶意IP的访问。 • 检测进程并发连接数异常等。

A 修订记录

发布日期	修改记录
2022-10-26	第十一次正式发布。 刷新**计费说明**章节，增加各版本包的计费模式说明。
2022-06-14	第十次正式发布。 新增**计费说明**章节。
2022-05-06	第九次正式发布。 刷新**产品优势**章节，新增智能化威胁响应相关描述，新增跨服务联动响应关于态势感知（SA）的描述。 刷新**应用场景**章节，新增威胁事件告警、协同服务相关描述。
2022-03-08	第八次正式发布。 修改**什么是威胁检测服务**。
2022-01-14	第七次正式发布。 增加检查VPC能力，优化内容描述。
2021-11-17	第六次正式发布。 增加细粒度授权，修改**MTD权限管理**。
2021-10-30	第五次正式发布。 增加检查OBS能力，优化内容描述。
2021-08-23	第四次正式发布。 修改新增支持的AI算法能力。
2021-07-10	第三次正式发布。 正式版本上线相关资料修改。
2021-05-17	第二次正式发布。 内容完善优化，新增与其他服务区别。
2021-01-20	第一次正式发布。