华为乾坤

更多文档

文档版本	01
发布日期	2023-03-31

华为技术有限公司

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 规格清单

1.1 边界防护与响应

表 1-1 规格清单

一级分类	二级分类	规格名称	规格描述
管理	安全态势大屏	资产失陷态势	资产失陷态势，包括：失陷主机趋势、失陷主机分布、失陷事件阻断率、最新失陷事件、top失陷主机、top失陷类型、top失陷事件。
		基础安全事件态势	基础安全事件态势，包括：攻击位置、威胁判定平均时长、阻断率、top攻击类型展示，最近威胁事件，专项事件数量。
		外部攻击源态势	外部攻击源态势，包括：外部攻击源趋势、攻击源分布、外部攻击阻断率、最新外部攻击、top攻击源、攻击资产、攻击类型。
	定期安全报告	定期安全报告	按周、按月为用户提供安全服务报告，安全服务报告将以邮件形式发送至用户订阅邮箱。通过安全服务报告，客户可清晰了解以下信息： 1. 安全服务概况。 2. 威胁防护次数及趋势。 3. 失陷主机数量及详情。 4. 外部攻击源数量及趋势。 5. 恶意文件数量及趋势。 支持应用访问行为统计，支持基于源IP、时间和应用分布等维度的统计，按周月提供统计分析报表 1. 支持历史安全报告的查看和预览功能。 2. 支持报告下载。

一级分类	二级分类	规格名称	规格描述
	安全域管理	安全域状态管理	1. 支持安全域状态监测，检查安全域物理连线是否接反。 2. 支持针对安全域设置信任标签。
	MSSP	MSSP代维	可在用户运维平台对安全服务建立委托关系，给指定被委托方建立不同操作权限角色（管理员、审计员等）的代维委托。委托建立后，被委托方可查看、处置安全威胁事件。
		MSSP安全大屏	支持针对MSSP管辖的租户进行安全大屏呈现。
		MSSP工单流转	支持租户的工单流转到MSSP进行分析和处置。
防护	天关/防火墙威胁防护	恶意软件防护	支持多级防护技术，支持多种恶意代码载体类型检测，实时更新病毒库，覆盖流行高危恶意软件。注：1U款型支持500万病毒库，桌面型款型支持300万病毒库。
		僵木蠕防护	支持基于僵尸网络拓扑分析技术的精准角色识别，支持500+僵尸网络识别，支持1000+蠕虫和木马识别。
		业务感知	支持识别6000+应用，支持主流应用协议全覆盖。
		WEB分类	支持Web分类库超1.2亿，对访问行为进行管理，防范恶意网站对企业网络的侵害。
		入侵防御	支持基于漏洞与行为分析的攻击检测技术，支持上下文语义还原的防躲避技术，最大支持12000+特征库，支持自动更新 。1U款型支持12000特征库，桌面型款型支持5000特征库 支持僵尸网络检测及应用服务器防护 。
响应	手动封禁	手动封禁	可以通过检测到的外部攻击源事件，进行手动封禁攻击源的操作。
	威胁自动阻断	外部攻击源自动阻断	支持对外部高危攻击源精准识别，自动下发黑名单，阻拦其后续的攻击行为。
		恶意域名自动阻断	支持基于DNS过滤实现恶意域名自动阻断，拦截用户网络内主机对恶意域名的访问行为。
	紧急安全通知	短信通知	支持短信紧急安全通知，针对威胁事件发送紧急通知，及时指导进行响应。
		邮件通知	支持邮件紧急安全通知，针对威胁事件发送紧急通知，及时指导进行响应。
		告警模板	对于需要发送给用户的紧急告警，提供对应的告警模板自定义能力。

一级分类	二级分类	规格名称	规格描述
	黑白名单功能	域名黑名单	支持配置域名黑名单，拦截用户网络内主机对恶意域名的访问行为。
		设备黑名单	1. 支持设备黑名单设置能力，快速阻断威胁攻击源。 2. 支持设备历史黑名单的查看。 3. 支持一键清除。
		设备保护网段	支持设备保护网段联动能力，保护已知业务，防止黑名单误阻断。
		租户全局白名单	支持租户全局白名单设置能力，保护已知业务，防止黑名单误阻断。
		设备白名单	支持设备白名单设置能力，保护已知业务，加入设备白名单的地址不会再进行内容安全检测。
分析	专项事件分析	失陷主机	支持按失陷主机维度自动聚合，基于失陷主机进行快速分析和处置。
		外部攻击源	1. 支持按外部攻击源维度自动聚合，基于外部攻击源进行快速分析和处置。 2. 支持外部攻击源导出能力。
		恶意文件	支持按恶意文件维度自动聚合，基于恶意文件进行快速分析和处置

2 License 介绍

2.1 必读须知

华为乾坤各服务或解决方案均支持线下购买。部分支持线上购买。

- 线上购买是指由客户自己在华为云商店上购买。线上购买后，华为乾坤后台会自动开通服务，随后可以正常使用。
- 线下购买是指由华为产品经理或渠道商工程师在SCT配置器上购买。线下购买后，需要客户根据License授权ID等信息，手动在华为乾坤上开通。

本文主要介绍的License信息，主要与线下购买有关。

2.2 License 概念

- **License**：许可证，是供应商与客户对所销售/购买的产品（这里特指软件版本）使用范围、期限等进行授权/被授权的一种合约形式，通过License，客户获得供应商所承诺的相应服务。物理形式表现为License授权证书和License文件。
- **License授权证书**

  也叫License证书，记录License的产品名、授权ID（以前叫LAC（License Authorization Code））、客户名称和有效期等，作为拥有华为产品License的证明。License授权证书为PDF文件格式，可从ESDP下载打印，合同发货采用电子件替代纸面件。

  只有商用License才有License授权证书。
- **ESDP（Electronic Software Delivery Platform）**

  华为销售的License文件发放管理系统，主要功能是根据订单或申请信息产生、发放License Key，并对License信息进行管理。

  ESDP Web网址：**https://app.huawei.com/sdp/svrportal.html**。
- **ESN（Equipment Serial Number）**

  设备序列号，唯一标识设备的字符串，是用来保证将License授权给指定设备的关键，又称“设备指纹”。
- **LAC（License Authorization Code）**

License授权码，又叫Entitlement ID，是由ESDP产生，用于客户身份验证。用户登录ESDP WEB，输入LAC和ESN等信息以激活License文件。华为公司将LAC定义成License授权证书的必要组成部分。

2.3 License 控制项

线下购买边界防护与响应服务的License控制项介绍，如表2-1所示。

表 2-1 License 控制项介绍

服务/方案名称	License控制项		使用说明
边界防护与响应服务 **说明** License跟随设备购买。不同的设备款型对应的License控制项不同。	Eudemon1000E-T1	License控制项类别如下： • 边界防护服务标准版 • 威胁防护库升级服务	云端激活（服务开通），未激活功能不可用。