华为乾坤解决方案

产品文档

文档版本 01

发布日期 2023-10-30

华为技术有限公司

商标声明

HUAWEI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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 等保合规解决方案

1.1 方案概述

1.1.1 趋势和挑战

等保是等级保护的简称，2017年《中华人民共和国网络安全法》的实施，标志着等级保护2.0的正式启动，网络安全法明确“国家实行网络安全等级保护制度”、“国家对一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。当前企业等保2.0建设主要面临如下挑战。

- 为了满足等保2.0建设需求，企业采用传统方案时需要购买防火墙、IPS、日志审计、漏扫等多种安全设备，造成安全投资成本大幅提升，而现实情况是，大部分企业客户的安全预算往往比较有限，导致无法满足等保2.0要求。
- 即使企业进行了高昂的网络安全投资，但当前安全设备的防护策略是静态的，威胁特征变化后，需要人工重新配置防护策略，且安全设备从不同的维度进行安全防护，各自单点防御，缺乏全局统筹分析，难以准确识别威胁并进行全局防御，无法满足等保2.0对主动防护、动态防御、整体防御、精准防御的相关要求。
- 采用传统方案时，需要专业的运维人员才能较好的发挥安全设备的防护能力，但我国网络安全从业人员十分紧缺，且专业安全人才的人力成本过高，这就造成了大部分企业安全运维缺失、面对安全事件束手无策的局面。
- 企业存在多个分支机构时，网络覆盖面大、业务系统种类多，因漏洞导致的安全事件频发，企业已有安全措施很难达到等保2.0要求的风险漏洞管理要求。
- 随着企业业务场景不断变化，业务系统种类也不断增多，且使用人员身份复杂，导致日志收集、分析、管理困难，无法应对日益增加的海量日志数据。
- 传统终端安全产品忽视攻击路径分析，无法对威胁事件进行事后溯源，企业不能感知威胁事件发生的原因和过程。因此无法根据威胁发生原因制定对应的防御策略，不能从根本上阻断威胁。

1.1.2 方案简介

华为乾坤面向等保2.0推出的等保合规解决方案采用云边一体创新架构，打造简单高效、安全可靠的云化安全解决方案。如图1-1所示，等保合规解决方案由部署在华为公有云上的云服务和部署在客户网络边界的天关/防火墙构成。

图 1-1 产品架构图

表 1-1 主要服务/模块介绍

部署位置	设备/模块名称	功能介绍
云端	边界防护与响应服务	边界防护与响应服务包括智能分析和处置、安全专家服务两大核心能力，其采用智能大数据分析技术对安全日志进行智能分析和处置，同时安全专家深入分析威胁并结合自身经验准确识别复杂威胁并快速响应。

部署位置	设备/模块名称	功能介绍
	漏洞扫描服务	漏洞扫描服务是一种针对客户内部资产提供的在线漏洞检测服务。该服务从风险管理角度出发，基于AI算法，结合资产的漏洞扫描结果、资产面临的威胁事件、威胁信息等，整体评估出风险值，帮助客户全面了解资产存在的风险。
	云日志审计服务	云日志审计服务是一站式日志数据云端统一管理平台，主要致力于提供事后溯源取证的安全能力。通过对日志数据的全面解析、管理，对各种安全威胁和异常行为事件进行溯源取证，为管理人员提供全局的视角，确保客户业务的不间断运营安全。
	终端防护与响应服务	终端防护与响应服务是针对企业本地终端进行风险检测和处置，防止终端感染和威胁在内网传播的一种服务。它采用云、端协同架构，由云端和安装在终端侧的华为乾坤EDR Agent（后文简称为EDR Agent）软件组成。
企业边界	天关/防火墙	天关/防火墙与云端协同工作，其功能如下： ● 作为安全防御节点，既对进出流量进行反病毒、IPS等深度安全检测，为租户本地网络提供边界防护，同时向边界防护与响应服务提供日志，并执行边界防护与响应服务下发的防护策略。 ● 作为漏洞扫描服务与企业内部网络的通信桥梁。在执行漏洞扫描任务前，云端会在云端服务和天关/防火墙之间建立VPN隧道，以便云端服务能扫描到企业内部资产。 ● 作为云日志审计服务与企业内部网络的通信桥梁，用户资产的日志数据通过其上传到云端。

1.1.3 客户价值

按需订阅

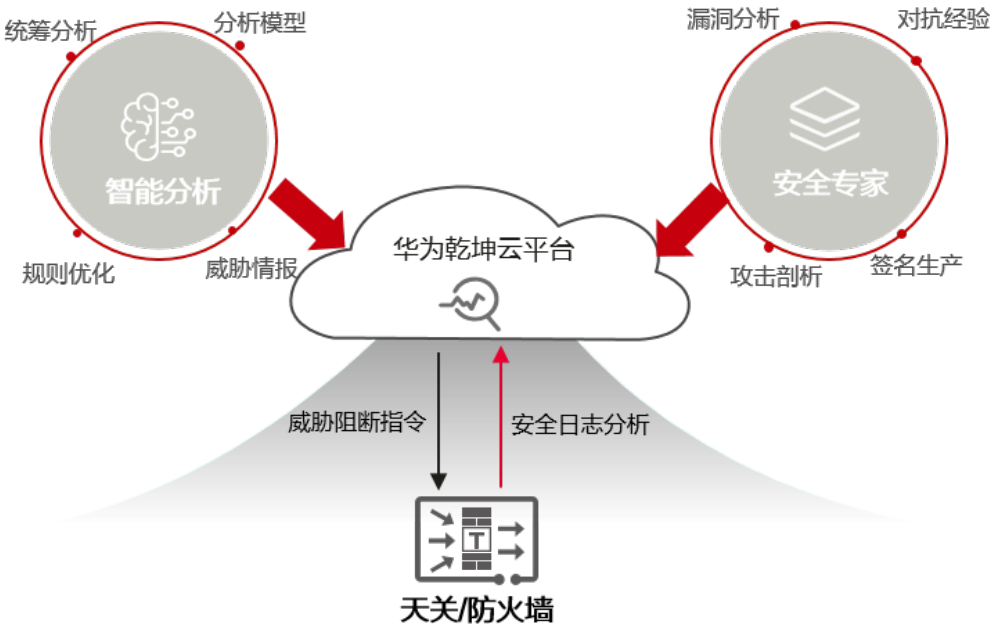
华为乾坤提供的等保合规解决方案当前包括边界防护与响应服务、漏洞扫描服务、云日志审计服务、终端防护与响应服务等多种服务，并且支持安全能力快速扩展，以满足等保标准不断变化的需求。

企业根据实际需求订阅后，即可开通云端和本地天关/防火墙的安全能力，只需少量的安全投资，即可替代部署在本地的防火墙、IPS、漏扫、日志审计等多种传统安全产品。

提升实效

如图1-2所示，华为乾坤通过云端的“智能分析+安全专家”快速提升防护实效，满足等保2.0对主动防护、动态防御、整体防御、精准防御的相关要求。

图 1-2 提升实效



智能分析

云端对天关/防火墙提供的日志文件进行智能分析和响应。

- 全局统筹分析：对日志文件进行全局关联分析，降噪处理，精准识别有效异常事件。
- 丰富的自动化分析模型：基于主机失陷模型、告警自动确认模型、误报模型、威胁情报关联分析模型、历史复用等模型全面提升自动化分析效率。
- 全面的威胁情报库：基于华为安全能力中心、未然实验室信息收集，本地天关/防火墙有效分析结果等多种途径汇总威胁情报库，全面提升分析准确率。
- 威胁信息全局共享：威胁信息全局共享，威胁信息一处检出，所有企业全局快速免疫。
- 规则快速迭代优化：基于安全误报事件，云端将快速实现检测规则优化，实时更新天关/防火墙的检测防护能力，不断提升防护效果。

安全专家

云端专家深入攻防对抗过程，整合安全能力，快速准确识别复杂攻击。

- 专家现网攻防对抗经验固化到云端，不断增强云端安全能力。
- 最新漏洞分析、新型攻击方法剖析、云端智能签名生产，快速应对新型攻击。
- 专家针对发现的每一条安全告警进行统一分析，运用云端各种安全能力，解决最新“疑难杂症”。

简化运维

网络安全实效的达成离不开专业人员的运维，华为乾坤通过“智能分析+安全专家”降低本地运维难度，同时租户可以多维度快速感知安全态势。

- 智能分析：利用智能分析能力提升自动运维效率，自动拦截攻击，响应效率由小时级提升到分钟级。

- 安全专家：云端共享安全专家资源7*24小时在线服务，解决复杂网络安全问题。
- 安全态势感知：按周、月提供安全报告，全面掌握网络安全态势；重要事件邮件短信告警，及时感知紧急安全事件，并指导用户及时安全处置；登录华为乾坤APP随时查看安全态势、防护状态、安全报表，针对安全事件及时执行封禁动作。

四合一全面漏扫

- 云端提炼多种场景化模板，支持按需选择模板进行更具针对性的扫描。
- 支持系统漏洞扫描、WEB漏洞扫描、数据库扫描、弱密码扫描，四合一全面检测资产脆弱性。

日志一体化管控

华为乾坤集日志接收、存储、解析、查询合规于一体，可以快速实现网络设备、安全设备、Windows/Linux操作系统、中间件等资产的日志审计，全面满足各个行业及组织的等保2.0要求。同时针对复杂格式日志，提供统一日志解析规则，提高企业的日志管理能力。能够快速方便的实现存储的分钟级快速扩容，确保业务不中断。

终端威胁感知全，检测快，判定准，处置优

- 轻量级软件EDR Agent部署在租户端侧，全面覆盖安全日志采集点，能够实时感知终端上的异常行为。当其与云端网络断连后，仍可提供主动防御能力，进行有效防护
- EDR Agent内置防病毒引擎和行为检测引擎，根据全攻击路径检测规则，对终端上的文件和目录进行毫秒级检测，快速判定威胁。针对勒索病毒，EDR Agent采用诱饵捕获技术，在病毒入侵初期即可精准识别风险，向云端及时上报异常事件。终端防护与响应服务实时同步威胁信息，检出新威胁后及时更新威胁特征库，增强对全网的安全防护能力。
- 基于海量数据库和智能检测算法，云端能够检出常规签名无法检测到的恶意样本，发现多种WAF（Web Application Firewall，网站应用程式防火墙）绕过手段，对抗未知和变种威胁。
- 终端防护与响应服务可联动边界防护与响应服务，进行威胁分析和封禁外部攻击源，为租户提供最优阻断方案，全方位抵御安全风险。云端采用智能化技术，当攻击发生时，可自动挖掘同一攻击链上所有威胁事件，提供一键快速处置方式。

1.1.4 应用场景

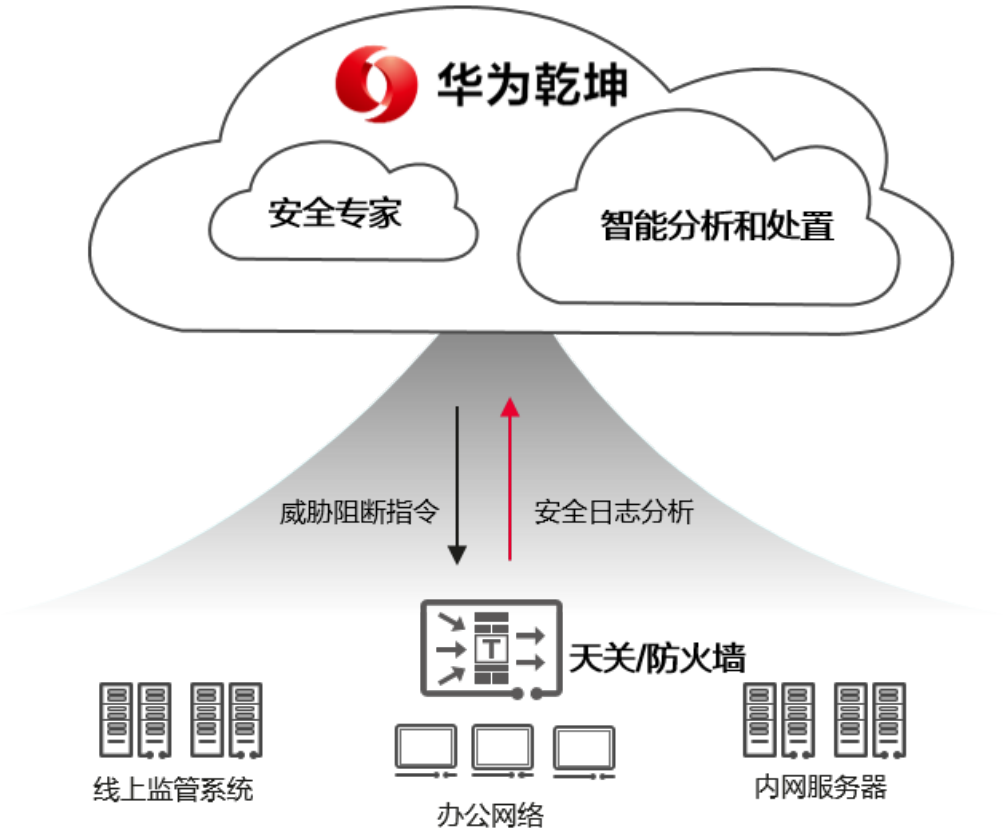
在政府、医疗、教育等行业，上级行政主管部门要求下级单位按照等保2.0要求完成安全建设，但下级单位由于技术能力储备不足、安全预算有限等问题较难实现完善的网络安全建设，安全防护效果不理想，同时上级主管部门无法有效管理网络安全要求是否落到实处，也无法督促下级单位针对不满足项及时进行整改。

此类型单位安全建设的主要诉求包括：

- 下级单位在安全预算有限的前提下，完成等保2.0安全建设以满足上级主管部门的网络安全要求。
- 完成等保2.0网络安全建设后，部署的安全产品能够准确识别威胁并及时处置，提升企业整体安全防护效果。
- 上级主管部门能够对下级单位进行有效管理，对不满足项可以及时督促整改。

采用如**图1-3**所示的等保合规解决方案即可满足上述诉求。

图 1-3 行业安全管理建设场景



采用华为乾坤的等保合规解决方案可以实现：

- 只需少量的投资，即可购买云服务安全能力并获得安全专家服务和智能处置能力。
- 借助云端对威胁事件进行统一分析，统一响应及时阻断，同时借助云端专家解决疑难问题，提升防护效果，弥补下级单位技术能力储备不足的问题。
- 云端向下级单位发送安全告警和邮件报告的同时，也向上级主管部门发送全局安全检测报告，全面展示下级单位的安全状况，安全事件处置是否及时等，实现对下级单位的有效管理、及时督促。

1.1.5 关键特性

边界防护与响应服务

表 1-2 边界防护与响应服务功能描述

功能	描述
自动化分析	云端基于分析模型对安全日志进行分析判定，并根据判定结果执行不同的处置。租户可依靠云端的自动化分析能力提升防护响应速度。 自动化分析以后，可以有如下几种处置方式： ● 事件命中误报模型，则此事件状态变更为误报。 ● 事件命中告警自动确认模型、威胁分析等模型，则自动化分析将请求安全响应执行相应的处置。 ● 在自动化分析的基础上，安全专家进一步分析处置事件。
安全响应	提供安全事件的响应闭环能力，主要包括下发黑名单、发送告警两种安全响应动作，租户可利用云端的安全响应能力有效提高安全事件的闭环效率。 针对以下场景提供下发黑名单、发送告警两种安全响应动作： ● 自动化分析判定后可以自动处置的事件，自动化分析将请求安全响应下发黑名单或发送告警。 ● 自动化分析判定后需要安全专家处置的事件，安全专家分析后可通过Portal页面的事件管理菜单人工下发黑名单或发送告警。 ● 租户在租户门户中下发黑名单。
云端专家精准分析	云端专家整合安全能力，快速准确识别复杂威胁： ● 现网对抗经验固化到云端，不断增强云端安全能力。 ● 最新漏洞分析、云端智能签名生产，快速应对新型威胁。 ● 专家针对发现的每一条安全告警进行统一分析，运用云端各种安全能力，解决最新“疑难杂症”。
资产暴露面风险监测	采用流量实时分析技术与云端探测相结合的方式，对暴露面进行精确识别和活跃度持续跟踪，快速感知暴露面风险，做到一目了然且有据可查。
极致体验	● 定期安全报告：定期自动生成周报、月报，并通过邮件发送至用户邮箱。 ● 事件紧急通知：通过短信、邮件两种方式通知用户。 ● 安全态势大屏：提供全局的攻击防御大屏展示。

漏洞扫描服务

表 1-3 漏洞扫描服务功能描述

功能	描述
漏洞扫描	漏洞扫描支持系统扫描、应用扫描等多种扫描类型，并为扫描出的漏洞提供修复建议。同时支持漏洞扫描报告下载。
资产发现	基于客户提供的IP网段，主动发现网段内的联网资产。经客户确认后，支持资产一键录入，提高资产梳理效率。
漏洞管理	以漏洞视角呈现每个漏洞的详细信息和关联资产。 ● **详细信息**包括漏洞名称、漏洞编号、漏洞优先级评级VPR和修复建议等。 漏洞优先级评级VPR（Vulnerability Priority Rating）用来表示漏洞修复优先级，是漏洞扫描服务基于漏洞利用代码成熟度、漏洞公布时长、产品的覆盖率、CVSS评分等多维度数据，通过机器学习算法计算的漏洞风险评分。分数越高，说明越需要优先修复。 ● **关联资产**能够帮助客户快速定位到风险资产，使漏洞修复更有针对性。
边界漏洞免疫（自动消减处置措施）	一般情况下，漏洞是通过在资产上安装补丁进行修复。当客户的实际环境无法满足安装补丁的条件，又希望降低被攻击风险时，可以利用天关/防火墙的入侵防御（IPS）能力，设置漏洞关联的IPS签名动作为“阻断”，通过在边界拦截异常流量，缓解漏洞被利用的风险。漏洞关联的IPS签名ID会被查询出来，显示在漏洞详情的界面中。 天关/防火墙侧的IPS签名动作一般有“告警”和“阻断”两种。 ● 如果签名动作为“阻断”，则表示天关/防火墙会阻断异常流量。漏洞被利用的风险低。 ● 如果签名动作为“告警”，则表示天关/防火墙只产生告警，不会阻断异常流量。漏洞可能会被利用。 天关/防火墙侧的IPS签名动作是根据长期运营数据统计结果进行设置的，请不要随意修改。如果一定要修改，请在右上角的帐号下，单击“我的工单”，提交工单寻求解决方法。 **说明** 使用本功能时，天关/防火墙需要联网，且可以自动升级特征库，以便保持特征库为最新版本。

云日志审计服务

表 1-4 云日志审计服务功能描述

功能	描述
日志采集/存储	● 支持接收不同类型资产（如服务器/终端、网络设备、安全设备、业务系统等）所产生的日志，将日志留存在云端，实现日志的集中管理和存储。 ● 支持解析多种格式及多种来源的日志，将其标准化。 ● 支持日志审计留存在云端，支持180天的日志留存时长。
日志查询	● 支持用户按需实时查询日志信息，查询条件包含时间、日志级别、日志类型、资产名称、源/目的IP地址和端口等。 ● 支持多关键字组合精确查询日志。
审计资产管理	● 支持增加多种类型的资产，如服务器、终端设备、网络设备、安全设备等，并对资产的等级进行标识，为客户判断是否需要进行日志审计提供参考信息。 ● 支持灵活管理需要审计的资产。
日志审计统计数据可视化	● 支持查看当前所有日志数量以及各日志级别的日志数量。 ● 支持按时间段查看日志容量使用趋势和日志数量趋势，如近7天、近一个月。 ● 支持查看当前审计的资产数量及类型。 ● 支持查看每天上报日志最多的TOP10资产。

终端防护与响应服务

表 1-5 终端防护与响应服务功能描述

功能	描述
终端识别与管理	● 终端自动识别：提供自动化终端资产清点能力，安装EDR Agent后，该终端即被自动识别。 ● 资产信息管理：自动化统一管理主机列表、进程、端口、组件等终端资产信息。 ● 终端安全管理：智能分析终端安全，呈现终端资产安全分析评分和风险总览。
威胁检测与处置	● 入侵检测：基于行为检测引擎，提供终端行为检测能力，检测暴力破解、异常登录、权限提升等恶意行为。 ● 事件聚合：将离散的勒索类告警事件，基于进程调用链聚合成相应的勒索事件，且支持对其一键处置。

功能	描述
病毒查杀与处置	● 病毒查杀：基于华为第三代反病毒引擎，每日更新病毒特征库，实时更新紧急病毒，提供高质量病毒文件检测能力。 ● 威胁分析：支持对检出的病毒文件进行威胁分析，展示详细的威胁信息，如病毒标识、风险值、置信度等。
主动防御	● 诱饵捕获：基于勒索病毒特征放置诱饵文件，实时检测并及时上报异常行为。 ● 文件防篡改：对重点文件进行访问权限控制并实时检测，及时发现篡改行为。 ● 实时防护：实时扫描全盘目录，及时识别病毒文件并阻断其传送行为。
溯源分析	● 取证分析：采集和存储终端信息，并通过数据挖掘、关联分析等方法，对威胁事件进行取证分析。 ● 攻击可视化：通过EDR（ Endpoint Detection and Response，端点检测与响应）数字化建模、溯源推理算法，实现攻击可视化，精准还原威胁攻击链路。

1.2 部署指南

1.2.1 注册华为乾坤帐号

说明

- 华为乾坤控制台是使用华为乾坤的界面，登录前需要先注册华为乾坤帐号。
- 如果您已有华为乾坤MSP（渠道服务商）创建的租户帐号，可跳过本节内容。

步骤1 访问华为乾坤控制台。

步骤2 在登录页面单击“立即注册”。

根据界面提示完成帐号注册。

----结束

1.2.2 开通服务

前提条件

- 已在配置器SCT上分别购买边界防护与响应服务、等保套餐、终端防护与响应服务，具体请联系代理商。通过购买等保套餐购买漏洞扫描服务和云日志审计服务。
- 已注册华为乾坤帐号，具体操作请参考1.2.1 注册华为乾坤帐号。

背景信息

边界防护与响应服务的开通方式请参见边界防护与响应服务的《服务开通》中“开通服务套餐”章节。

终端防护与响应服务的开通方式参见终端防护与响应服务的《服务开通》中“购买与开通服务”章节。

等保套餐的开通方式请参见本章节。

操作步骤

1. 以租户帐号登录华为乾坤控制台。
2. 在界面右上方单击“订单”，选择“我的套餐”页签。
3. 单击“开通服务”。
4. 单击“根据授权ID激活”，输入“授权ID”，单击“开通”。
   “授权ID”请参考界面提示“查看授权ID获取方式”进行获取。

图 1-4 开通服务界面

5. 查看服务开通情况。
   在“我的套餐”页签下，如果套餐对应的“状态”为“正常”，说明开通成功。

1.2.3 配置天关和防火墙上线

等保合规解决方案需要在客户侧部署天关或防火墙才能正常使用。本方案配套的天关或防火墙的型号，如表1-6所示。

表 1-6 天关或防火墙的型号

设备类型	设备型号
天关	USG65xxE-C：USG6501E-C/USG6502E-C/USG6503E-C
防火墙	• USG65xxE：USG6515E/USG6525E/USG6530E/USG6550E/USG6555E/USG6560E/USG6565E/USG6575E-B/USG6580E/USG6585E • USG65xxE-K：USG6520E-K/USG6560E-K/USG6590E-K

由于边界防护与响应服务、漏洞扫描服务和云日志审计服务均需要使用天关或防火墙，故共用一套上线指南，具体操作请参见《天关和防火墙上线指南》。

1.2.4 快速配置

设备上线后，您还需要在云端或设备中进行相关配置，才能正常使用等保合规解决方案。可以参考如下文档完成快速配置。

表 1-7 参考文档

子服务	手册名称	参照内容	文档获取
边界防护与响应服务	部署指南	• 配置设备安全域 • 配置全局白名单 • 黑白名单授权 • 订阅告警与报告 • 查看威胁事件	部署指南
漏洞扫描服务	部署指南	• 配置VPN接口 • 录入资产 • 授权服务扫描 • 创建漏洞扫描任务 • 查看扫描结果	部署指南
云日志审计服务	部署指南	• 授权日志采集权限 • （可选）添加天关/防火墙 • 添加审计资产 • 配置日志上报 • 验证日志查询	部署指南

子服务	手册名称	参照内容	文档获取
终端防护与响应服务	部署指南	• 服务授权 • 样本获取授权 • 安装EDR Agent • 查看终端资产	部署指南

1.2.5 日常操作

完成快速配置后， 您可以参考如下文档正常使用等保合规解决方案。

表 1-8 参考文档

子服务	手册名称	文档内容简介	文档获取
边界防护与响应服务	用户指南	介绍如何使用边界防护与响应服务。	用户指南
漏洞扫描服务	用户指南	介绍如何使用漏洞扫描服务。	用户指南
云日志审计服务	用户指南	介绍如何使用云日志审计服务。	用户指南
终端防护与响应服务	用户指南	介绍如何使用终端防护与响应服务	用户指南

1.3 维护宝典

- 如何确认天关/防火墙入侵防御（IPS）特征库是否已经更新到最新版本?
  请登录天关/防火墙Web访问界面，具体操作如下：
  a. 选择“系统 > 升级中心”。
  b. 在“特征库升级”中查看入侵防御特征库对应的“当前版本”，确认是否需要升级。

如需升级，请登录华为企业技术支持网站，查阅对应产品的产品文档包。具体配置参见“配置 > 配置指南 > 内容安全 > 入侵防御（IPS）”。

- 如何确认天关/防火墙反病毒特征库（AV，恶意代码库）是否已经更新到最新版本?

  请登录天关/防火墙Web访问界面，具体操作如下：

  a. 选择“系统 > 升级中心”。
  b. 在“特征库升级”中查看反病毒特征库对应的“当前版本”，确认是否需要升级。

  如需升级，请登录华为企业技术支持网站，查阅对应产品的产品文档包。具体配置参见“配置 > 配置指南 > 内容安全 > 反病毒（AV）”。

- 如何确认天关/防火墙用户密码策略是否满足密码长度应大于8位，由数字、大小写字母、特殊字符中的两种或两种以上组成的要求。

  请登录天关/防火墙Web访问界面，具体操作如下：

  a. 选择“系统 > 管理员 > 管理员”。
  b. 单击“新建”，可查看密码规则如下：

     为提升密码安全性，建议密码至少包含以下字符中的3种：<A-Z>，<a-z>，<0-9>，特殊字符（例如!，$，#，%）；密码不能包含两个以上连续相同的字符；且密码不能与用户名或者用户名的倒序相同。

- 如何在天关/防火墙上配置用户密码最小长度?

  请登录天关/防火墙Web访问界面，具体操作如下：

  a. 选择“系统 > 管理员 > 设置”。
  b. 在“密码最小长度”中输入最小长度。

     新建管理员的密码长度必须满足“密码最小长度”的要求。
  c. 单击“应用”。

- 如何在天关/防火墙上配置用户登录失败次数?

  请登录天关/防火墙Web访问界面，具体操作如下：

  a. 选择“系统 > 管理员 > 设置”。
  b. 配置“连续登录失败次数”，管理员帐号认证连续失败次数达到配置的次数时，管理员帐号将被锁定。
  c. 配置“锁定时长”，指定管理员帐号被锁定的时长，锁定时长结束后，管理员帐号将被自动解锁。
  d. 单击“应用”。

- 如何在天关/防火墙上配置设备空闲超时自动退出时间（超时时间不超过30分钟）?

  请登录天关/防火墙Web访问界面，具体操作如下：

  a. 选择“系统 > 管理员 > 设置”。
  b. 在“Web服务超时时间”中输入超时时间。

     Web服务超时时间：若在该时间内无操作，当再次操作时会提示登录超时，需要重新登录。缺省为10分钟。
  c. 单击“应用”。

- 如何在天关/防火墙上设置用户定期更换口令周期（定期更换口令周期不超过90天）?

  请登录天关/防火墙Web访问界面，具体操作如下：

a. 选择“系统 > 管理员 > 设置”。
b. 选中“密码管理”对应的“启用”。
c. 在“密码有效期”中输入密码的有效期90天。
d. 单击“应用”。

- 如何在天关/防火墙上设置非法登录处理措施：连续登录失败5次后锁定帐号/IP地址30分钟（失败次数不大于5次，锁定时间不小于10分钟）？

  请登录天关/防火墙Web访问界面，具体操作如下：

  a. 选择“系统 > 管理员 > 设置”。
  b. 配置“连续登录失败次数”，管理员帐号认证连续失败次数达到配置的次数时，管理员帐号将被锁定。
  c. 配置“锁定时长”，指定管理员帐号被锁定的时长，锁定时长结束后，管理员帐号将被自动解锁。
  d. 单击“应用”。

- 天关/防火墙如何防止鉴别信息在网络传输过程中被窃听?

  天关/防火墙通过web 界面访问，采用 https 方式进行远程管理，防止鉴别信息在网络传输过程中被窃听。

- 如何授予管理用户所需的最小权限，实现管理用户的权限分离?

  当前天关/防火墙已按照“三权分立”原则进行角色划分，已设置系统管理员、审计管理员和安全管理员，授予角色所需的最小权限，并支持用户根据需要修改权限。

  请登录天关/防火墙Web访问界面，具体操作如下：

  a. 选择“系统 > 管理员 > 管理员”。
  b. 编辑对应管理员角色或新建管理员角色。
  c. 单击”确定”。

- 如何将天关/防火墙重要配置数据提供异地数据备份，并定时批量传输至备用场地?

  用户可以根据预算情况部署异地容灾环境，或手工定期导出设备配置并异地保存。

  请登录天关/防火墙Web访问界面，具体操作如下：

  a. 选择“系统 > 配置文件管理”。
  b. 导出当前配置。

- 如何确认华为乾坤用户密码策略是否满足密码长度应大于8位，由数字、大小写字母、特殊字符中的两种或两种以上组成的要求?

  请登录控制台，单击控制台右上角帐号，选择“个人中心 > 个人信息 ”，编辑密码可查看用户密码策略如下：

  – 密码长度不能小于8个字符，大于32个字符。
  – 密码至少包含1个字母和1个数字。
  – 密码不能包含用户名，用户手机号码和电子邮箱帐号。
  – 不能使用密码强度低或常见的密码。

- 如何在华为乾坤上设置用户定期更换口令周期（定期更换口令周期不超过90天）？

  为保障帐号安全，无论是自注册帐号或代建帐号，需要定期修改密码。

系统默认密码有效期为90天，过期前10天每天会发送邮件提示您修改密码，登录页面时也会提示修改密码，具体过程请参见《租户操作指南》的“个人中心设置”章节。

- 如何在华为乾坤上开启用户登录双重验证?

  请登录控制台，具体操作如下：

  a. 单击控制台右上角帐号，选择“个人中心 > 个人信息 ”。
  b. 开启双重验证。开启后，帐号登录时，需要密码、短信双重验证，更能保障帐号安全。

  说明

  开启双重验证的前提是帐号设置了密码并绑定手机号码。

  具体过程请参见《租户操作指南》的“个人中心设置”章节。

- 如何配置访问策略，限制特定的IP地址范围可以访问华为乾坤帐户?

  当前华为乾坤已支持限制特定的IP地址范围访问特定帐户，但当前未对用户开放。用户可以通过提交工单或联系渠道人员申请增加白名单限制。

2 安全重保解决方案

2.1 方案概述

2.1.1 趋势和挑战

在国家重大活动期间，组织单位面临的网络攻击往往呈现攻击力度更大、攻击频率更高、针对性更强等特点。为保证关键信息基础设施及重要信息系统在重大活动期间的稳定运行，各单位需要建立防护、监测、响应的安全机制，确保提前排除网络安全隐患，做好网络应急响应和安全保障工作，避免攻击入侵、感染病毒等网络安全事件的发生。当前安全重保主要面临如下挑战。

- 资产对外暴露面过大，当前主要依靠探测工具进行扫描评估，这种方式效率低，且难以快速定位到最终对外开放的主机与业务，不能有效收敛攻击面。
- 完成风险排查和整改后，依靠人工验证整改效果，耗时费力且验证不充分，缺少多维度评估防御体系风险和有效性的手段。
- 零日攻击日益增长且难以防范，已成为网络安全面临的最严峻的威胁之一，传统防护方式无法实时更新特征库，以降低系统被攻击风险。
- 在重保服务期间，依靠人工驻场分析安全事件、人工关联威胁信息、人工执行防护策略，人工总结提交报告，导致威胁检测不全面，攻击响应不及时，无法实现常态化安全保障的目标。
- 企业存在多个分支机构时，网络覆盖面大、业务系统种类多，因漏洞导致的安全事件频发，企业已有安全措施很难达到风险漏洞管理要求。
- 传统终端安全产品忽视攻击路径分析，无法对威胁事件进行事后溯源，企业不能感知威胁事件发生的原因和过程。因此无法根据威胁发生原因制定对应的防御策略，不能从根本上阻断威胁。

2.1.2 方案简介

华为乾坤推出的安全重保解决方案采用云边一体创新架构，打造一站式云化安全解决方案。如**图2-1**所示，重保安全解决方案由部署在公有云上的云服务和部署在客户网络边界的华为天关防护节点构成，能够帮助用户实现常态化安全保障。

图 2-1 产品架构图

表 2-1 主要服务/模块介绍

部署位置	设备/模块名称	功能介绍
云端	边界防护与响应服务	边界防护与响应服务包括智能分析和处置、安全专家服务两大核心能力，其采用智能大数据分析技术对天关提供的安全日志进行智能分析和处置，同时安全专家深入分析威胁并结合自身经验准确识别复杂威胁并快速响应。 此外边界防护与响应服务还提供资产暴露面风险监测能力，对暴露面进行精确识别和活跃度持续跟踪，帮助用户快速感知暴露面风险。
	重保威胁信息	在重保服务期间通过AI算法分析全网历史攻击行为及攻击方法，精准识别攻击方地址，实时共享历史重保专门威胁信息，有效提升信息的精准度。

部署位置	设备/模块名称	功能介绍
	漏洞扫描服务	漏洞扫描服务是一种针对客户内部资产提供的在线漏洞检测服务。该服务从风险管理角度出发，基于AI算法，结合资产的漏洞扫描结果、资产面临的威胁事件、威胁信息等，整体评估出风险值，帮助客户全面了解资产存在的风险。
	终端防护与响应服务	终端防护与响应服务是针对企业本地终端进行风险检测和处置，防止终端感染和威胁在内网传播的一种服务。它采用云、端协同架构，由云端和安装在终端侧的华为乾坤EDR Agent（后文简称为EDR Agent）软件组成。
企业边界	天关	天关与云端协同工作，作为安全防御节点，既对进出流量进行反病毒、IPS等深度安全检测，为租户本地网络提供边界防护，同时向边界防护与响应服务提供日志，并执行边界防护与响应服务下发的防护策略。

2.1.3 客户价值

风险精准排查

华为乾坤支持对暴露面进行精确识别和活跃度持续跟踪，快速定位到最终对外开发的主机与业务，有效收敛攻击面。

威胁处置快

华为乾坤采用云边一体防御架构，云端分析出威胁后自动化处置，实现威胁秒级处置闭环，大幅提升攻击响应速度。

云端对本地天关提供的安全日志，基于大数据进行智能分析，并结合重保专有威胁信息精准识别威胁，然后协同本地天关进行自动化处置，同时云端安全专家7*24小时在线服务，解决复杂网络安全问题。

识别能力在线自进化

华为乾坤的云端、本地天关的威胁检测和防御能力实时在线升级，威胁一处检出，全局共享，实现分钟级免疫，有效降低零日攻击带来的风险。

云端通过“智能分析+安全专家”实现威胁检测和防御能力的持续快速升级，云端完成升级后，立即向所有本地天关下发防护策略，同步升级所有本地天关的威胁检测和防御能力。通过云端、本地天关协同，实现威胁持续动态检测和全局防御，从而提升防御效果。

四合一全面漏扫

- 云端提炼多种场景化模板，支持按需选择模板进行更具针对性的扫描。
- 支持系统漏洞扫描、WEB漏洞扫描、数据库扫描、弱密码扫描，四合一全面检测资产脆弱性。

终端威胁感知全，检测快，判定准，处置优

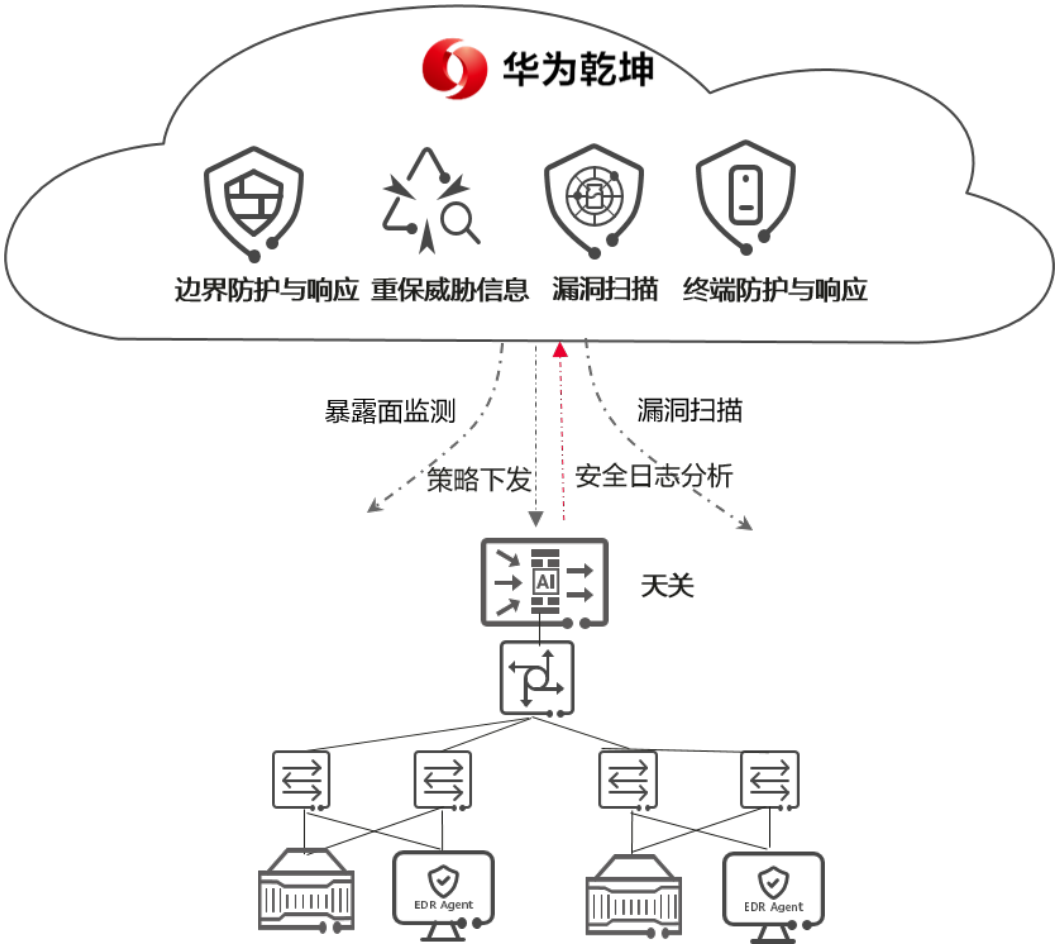
- 轻量级软件EDR Agent部署在租户端侧，全面覆盖安全日志采集点，能够实时感知终端上的异常行为。当其与云端网络断连后，仍可提供主动防御能力，进行有效防护
- EDR Agent内置防病毒引擎和行为检测引擎，根据全攻击路径检测规则，对终端上的文件和目录进行毫秒级检测，快速判定威胁。针对勒索病毒，EDR Agent采用诱饵捕获技术，在病毒入侵初期即可精准识别风险，向云端及时上报异常事件。终端防护与响应服务实时同步威胁信息，检出新威胁后及时更新威胁特征库，增强对全网的安全防护能力。
- 基于海量数据库和智能检测算法，云端能够检出常规签名无法检测到的恶意样本，发现多种WAF（Web Application Firewall，网站应用程式防火墙）绕过手段，对抗未知和变种威胁。
- 终端防护与响应服务可联动边界防护与响应服务，进行威胁分析和封禁外部攻击源，为租户提供最优阻断方案，全方位抵御安全风险。云端采用智能化技术，当攻击发生时，可自动挖掘同一攻击链上所有威胁事件，提供一键快速处置方式。

2.1.4 应用场景

某单位为了在重保期间做好安全保障工作，需要提前评估当前网络面临的安全风险，但资产对外暴露面过大，当前的排查方法效率低，且难以快速定位到最终对外开放的主机与业务，不能有效收敛攻击面。单位的网络覆盖面大，无法全面检查漏洞并精准修复。在保障期间总是依靠人员驻场对安全事件进行分析、验证、处置，导致威胁检测不全面，攻击响应不及时，对终端的威胁行为也无法快速判定。

采用如**图2-2**所示的安全重保解决方案即可解决上述问题。

图 2-2 应用场景



采用华为乾坤的安全重保解决方案可以实现：

- 边界防护与响应服务采用流量实时分析技术与云端探测相结合的方式，对暴露面进行精确识别和活跃度持续跟踪，做到暴露面一目了然且有据可查。
- 边界防护与响应服务对天关提供的安全日志，基于大数据、重保威胁信息等进行智能分析，精准识别威胁，并根据分析结果协同天关进行自动化处置。同时云端安全专家7*24小时在线服务，解决复杂网络安全问题。帮助用户全面检测威胁并快速响应，实现常态化安全保障。
- 漏洞扫描服务基于华为威胁信息库和机器学习智能评估技术，计算漏洞风险评分。漏洞评分越高，风险越高，用户可以根据评分精准修复。
- 终端防护与响应服务可以对终端上的文件和目录进行毫秒级检测，快速判定威胁。

2.1.5 关键特性

天关

表 2-2 天关功能描述

功能	描述
本地网络边界防护	天关部署在租户网络边界，通过入侵防御、反病毒、DNS过滤等技术守护本地安全，并向云端提供安全日志。天关可以执行以下防护动作： ● 对流量进行入侵防御检测，全方位防御各种威胁行为。 ● 对流量进行反病毒处理，有效避免病毒文件引起的数据破坏、权限更改和系统崩溃等情况的发生。 ● 对流量进行DNS过滤，全面控制域名访问。

边界防护与响应服务

表 2-3 边界防护与响应服务功能描述

功能	描述
自动化分析	云端基于分析模型对安全日志进行分析判定，并根据判定结果执行不同的处置。租户可依靠云端的自动化分析能力提升防护响应速度。 自动化分析以后，可以有如下几种处置方式： ● 事件命中误报模型，则此事件状态变更为误报。 ● 事件命中告警自动确认模型、威胁分析等模型，则自动化分析将请求安全响应执行相应的处置。 ● 在自动化分析的基础上，安全专家进一步分析处置事件。
安全响应	提供安全事件的响应闭环能力，主要包括下发黑名单、发送告警两种安全响应动作，租户可利用云端的安全响应能力有效提高安全事件的闭环效率。 针对以下场景提供下发黑名单、发送告警两种安全响应动作： ● 自动化分析判定后可以自动处置的事件，自动化分析将请求安全响应下发黑名单或发送告警。 ● 自动化分析判定后需要安全专家处置的事件，安全专家分析后可通过Portal页面的事件管理菜单人工下发黑名单或发送告警。 ● 租户在租户门户中下发黑名单。
云端专家精准分析	云端专家整合安全能力，快速准确识别复杂威胁： ● 现网对抗经验固化到云端，不断增强云端安全能力。 ● 最新漏洞分析、云端智能签名生产，快速应对新型威胁。 ● 专家针对发现的每一条安全告警进行统一分析，运用云端各种安全能力，解决最新“疑难杂症”。

功能	描述
资产暴露面风险监测	采用流量实时分析技术与云端探测相结合的方式，对暴露面进行精确识别和活跃度持续跟踪，快速感知暴露面风险，做到一目了然且有据可查。
极致体验	● 定期安全报告：定期自动生成周报、月报，并通过邮件发送至用户邮箱。 ● 事件紧急通知：通过短信、邮件两种方式通知用户。 ● 安全态势大屏：提供全局的攻击防御大屏展示。

漏洞扫描服务

表 2-4 漏洞扫描服务功能描述

功能	描述
漏洞扫描	漏洞扫描支持系统扫描、应用扫描等多种扫描类型，并为扫描出的漏洞提供修复建议。同时支持漏洞扫描报告下载。
资产发现	基于客户提供的IP网段，主动发现网段内的联网资产。经客户确认后，支持资产一键录入，提高资产梳理效率。
漏洞管理	以漏洞视角呈现每个漏洞的详细信息和关联资产。 ● **详细信息**包括漏洞名称、漏洞编号、漏洞优先级评级VPR和修复建议等。 漏洞优先级评级VPR（Vulnerability Priority Rating）用来表示漏洞修复优先级，是漏洞扫描服务基于漏洞利用代码成熟度、漏洞公布时长、产品的覆盖率、CVSS评分等多维度数据，通过机器学习算法计算的漏洞风险评分。分数越高，说明越需要优先修复。 ● **关联资产**能够帮助客户快速定位到风险资产，使漏洞修复更有针对性。
边界漏洞免疫（自动消减处置措施）	一般情况下，漏洞是通过在资产上安装补丁进行修复。当客户的实际环境无法满足安装补丁的条件，又希望降低被攻击风险时，可以利用天关/防火墙的入侵防御（IPS）能力，设置漏洞关联的IPS签名动作为“阻断”，通过在边界拦截异常流量，缓解漏洞被利用的风险。漏洞关联的IPS签名ID会被查询出来，显示在漏洞详情的界面中。 天关/防火墙侧的IPS签名动作一般有“告警”和“阻断”两种。 ● 如果签名动作为“阻断”，则表示天关/防火墙会阻断异常流量。漏洞被利用的风险低。 ● 如果签名动作为“告警”，则表示天关/防火墙只产生告警，不会阻断异常流量。漏洞可能会被利用。 天关/防火墙侧的IPS签名动作是根据长期运营数据统计结果进行设置的，请不要随意修改。如果一定要修改，请在右上角的帐号下，单击“我的工单”，提交工单寻求解决方法。 **说明** 使用本功能时，天关/防火墙需要联网，且可以自动升级特征库，以便保持特征库为最新版本。

重保威胁信息

表 2-5 重保威胁信息功能描述

功能	描述
威胁信息中心	支持全球恶意IP、恶意域名、恶意文件、漏洞信息等威胁信息的快速检索，数据详情包括但不限于威胁类型、风险级别、置信度、场景信息、地理位置、关联历史事件、关联恶意信息、相关文章等信息。
安全研究	定期发布威胁周报、威胁预警、热点威胁信息等文章，帮助客户了解近期关键安全事件。
高性能信息查询接口	提供高性能的全球恶意IP、恶意域名、恶意文件、漏洞信息、URL分类等威胁信息的查询接口，辅助自动化分析人员进行分析取证及处置，提升运维效率。

终端防护与响应服务

表 2-6 终端防护与响应服务功能描述

功能	描述
终端识别与管理	● 终端自动识别：提供自动化终端资产清点能力，安装EDR Agent后，该终端即被自动识别。 ● 资产信息管理：自动化统一管理主机列表、进程、端口、组件等终端资产信息。 ● 终端安全管理：智能分析终端安全，呈现终端资产安全分析评分和风险总览。
威胁检测与处置	● 入侵检测：基于行为检测引擎，提供终端行为检测能力，检测暴力破解、异常登录、权限提升等恶意行为。 ● 事件聚合：将离散的勒索类告警事件，基于进程调用链聚合成相应的勒索事件，且支持对其一键处置。
病毒查杀与处置	● 病毒查杀：基于华为第三代反病毒引擎，每日更新病毒特征库，实时更新紧急病毒，提供高质量病毒文件检测能力。 ● 威胁分析：支持对检出的病毒文件进行威胁分析，展示详细的威胁信息，如病毒标识、风险值、置信度等。
主动防御	● 诱饵捕获：基于勒索病毒特征放置诱饵文件，实时检测并及时上报异常行为。 ● 文件防篡改：对重点文件进行访问权限控制并实时检测，及时发现篡改行为。 ● 实时防护：实时扫描全盘目录，及时识别病毒文件并阻断其传送行为。

功能	描述
溯源分析	● 取证分析：采集和存储终端信息，并通过数据挖掘、关联分析等方法，对威胁事件进行取证分析。 ● 攻击可视化：通过EDR（ Endpoint Detection and Response，端点检测与响应）数字化建模、溯源推理算法，实现攻击可视化，精准还原威胁攻击链路。

2.2 部署指南

2.2.1 注册华为乾坤帐号

说明

- 华为乾坤控制台是使用华为乾坤的界面，登录前需要先注册华为乾坤帐号。
- 如果您已有华为乾坤MSP（渠道服务商）创建的租户帐号，可跳过本节内容。

步骤1 访问华为乾坤控制台。

步骤2 在登录页面单击“立即注册”。

根据界面提示完成帐号注册。

----结束

2.2.2 开通服务

前提条件

- 已在配置器SCT上分别购买边界防护与响应服务**专业版**、重保威胁信息、漏洞扫描服务、终端防护与响应服务，具体请联系代理商。
- 已注册华为乾坤帐号，具体操作请参考**2.2.1 注册华为乾坤帐号**。

操作步骤

请参照如下文档分别开通边界防护与响应服务、重保威胁信息、漏洞扫描服务、终端防护与响应服务。

表 2-7 参考文档

子服务	手册名称	具体章节	文档获取
边界防护与响应服务	服务开通	“开通商用服务（线下）> 租户身份开通 > 开通服务套餐”	开通服务套餐

子服务	手册名称	具体章节	文档获取
漏洞扫描服务	服务开通	“开通线下购买的套餐”	开通线下购买的套餐
终端防护与响应服务	服务开通	“购买与开通服务”	购买与开通服务
重保威胁信息	服务开通	“开通商用套餐”	开通商用套餐

2.2.3 绑定重保套餐

背景信息

您需要将边界防护与响应服务**专业版**套餐与重保威胁信息套餐绑定，才能正常使用安全重保解决方案。

操作步骤

步骤1 登录华为乾坤控制台

步骤2 单击“订单”，选择“我的套餐”页签，

步骤3 查看当前边界防护与响应服务**专业版**套餐。

步骤4 **可选:** 单击操作栏的“绑定重保”，将专业版套餐与重保威胁信息套餐绑定。

----结束

2.2.4 配置天关和防火墙上线

安全重保解决方案需要在客户侧部署天关才能正常使用，本方案配套天关USG6603F-C、USG6606F-C，具体操作请参见《天关和防火墙上线指南》中“**USG6000F-C天关上线**”章节。

2.2.5 快速配置

设备上线后，您还需要在云端进行相关配置，才能正常使用安全重保解决方案。可以参考如下文档完成快速配置。

表 2-8 参考文档

子服务	手册名称	参照内容	文档获取
边界防护与响应服务	部署指南	• 配置设备安全域 • 配置全局白名单 • 黑白名单授权 • 订阅告警与报告 • 查看威胁事件	部署指南
漏洞扫描服务	部署指南	• 配置VPN接口 • 录入资产 • 授权服务扫描 • 创建漏洞扫描任务 • 查看扫描结果	部署指南
终端防护与响应服务	部署指南	• 服务授权 • 样本获取授权 • 安装EDR Agent • 查看终端资产	部署指南
重保威胁信息	不需要在云端进行配置。		

2.2.6 日常操作

您可以参考如下文档使用安全重保解决方案。

表 2-9 参考文档

子服务	手册名称	文档内容简介	文档获取
边界防护与响应服务	用户指南	介绍如何使用边界防护与响应服务。	用户指南
漏洞扫描服务	用户指南	介绍如何使用漏洞扫描服务。	用户指南
终端防护与响应服务	用户指南	介绍如何使用终端防护与响应服务	用户指南
重保威胁信息	用户指南	介绍如何使用重保威胁信息。	用户指南

3 防勒索解决方案

3.1 方案概述

3.1.1 趋势和挑战

勒索软件是不法分子通过加密文件等方式劫持用户文件，借此索要钱财的一种恶意软件。勒索软件变种多、更新快，难以防范，据权威报道，勒索软件会造成企业巨额经济损失和重要数据的泄露，已升级成为全球网络领导者最关心的网络威胁。

网络安全建设作为现代企业治理的一个重要课题，在勒索病毒的猛烈攻势下面临着严峻的挑战。

- 攻击规模化组织化，应对难

  在勒索软件巨大利益的驱使下，专业勒索组织形成，并向其他攻击者售卖勒索服务，形成完整产业链。这降低了勒索软件的攻击成本和门槛，极大提高了勒索软件的攻击频率，增加企业被攻破的概率。

- 未知威胁不断涌现，检测难

  随着威胁手段和攻击技术的不断提高，勒索软件不断衍生出大量变种软件。然而传统安全产品仅采用威胁特征库匹配技术，只能识别已知威胁，无法有效检测不断涌现的勒索变种。

- 恢复成本高昂，危害大

  由于勒索软件含有大量加密算法，企业遭遇攻击后，业务中断时间长，恢复成本高。面对勒索软件，企业不仅需要承担赎金损失，还会面临商誉、商业机会、法律诉讼、人力和时间成本等连带损失。这对于很多企业，特别是中小型企业来说，是毁灭性打击。

3.1.2 方案简介

在深入分析勒索软件特点和防勒索建设困境后，华为乾坤推出了防勒索解决方案。华为乾坤防勒索解决方案采用云边端一体的创新架构，构建了以资产为核心的纵深防御体系，针对勒索软件攻击链特征，实现对勒索事件的层层防护，全方位保障企业网络安全。

图 3-1 华为乾坤防勒索解决方案架构图

如图3-1所示，华为乾坤防勒索解决方案由部署在云端的服务、部署在客户网络边界的天关/防火墙和部署在电脑、服务器等企业终端上的华为乾坤EDR Agent（后文简称为EDR Agent）软件组成。同时它根据用户诉求提供可选的安全托管服务和保险理赔服务。各个组件的功能介绍如表3-1所示。

表 3-1 组件功能介绍

部署位置	组件名称	功能介绍
云端	边界防护与响应服务	使用天关/防火墙为租户的本地网络提供边界防护，并基于天关/防火墙提供的日志进行智能分析和处置，持续保护企业内网安全。云端通过集成告警自动确认、威胁分析等检测模型，智能识别租户本地网络的潜在威胁并完成自动化处置，从而帮助租户简化本地运维，提升安全防护实效。
	终端防护与响应服务	针对企业本地终端进行风险检测和处置，防止终端感染和威胁在内网传播。支持文件本地备份恢复，在恶意进程修改用户文件前将文件备份至本地存储区，在文件被加密后由云端下发文件恢复指令至终端，一键恢复被加密文件。

部署位置	组件名称	功能介绍
	漏洞扫描服务（可选）	从风险预防角度出发，检测企业资产安全状况，高效精准地识别潜在漏洞，为客户提供专业的修复建议，帮助客户降低资产安全风险。
边界	天关/防火墙	作为安全防御节点，既对进出流量进行反病毒、IPS等深度安全检测，为租户本地网络提供边界防护，同时向边界防护与响应服务提供日志，并执行边其下发的防护策略。
终端	EDR Agent	主要负责收集并向终端防护与响应服务上报终端上的租户登录、进程运行/创建、目录/文件访问日志、DNS请求信息，执行预置的主动防御策略和云端下发的防御策略与文件恢复指令。
/	安全托管服务（可选）	与区域安全合作伙伴一起为客户提供7*24小时的安全托管服务。
	保险理赔服务（可选）	为用户提供勒索赎金兜底服务，具体参考太平洋财险公司提供的华太安理赔产品。

3.1.3 客户价值

华为乾坤防勒索解决方案是专为企业客户打造的解决方案，可以满足企业客户应对勒索软件攻击的网络安全需求。

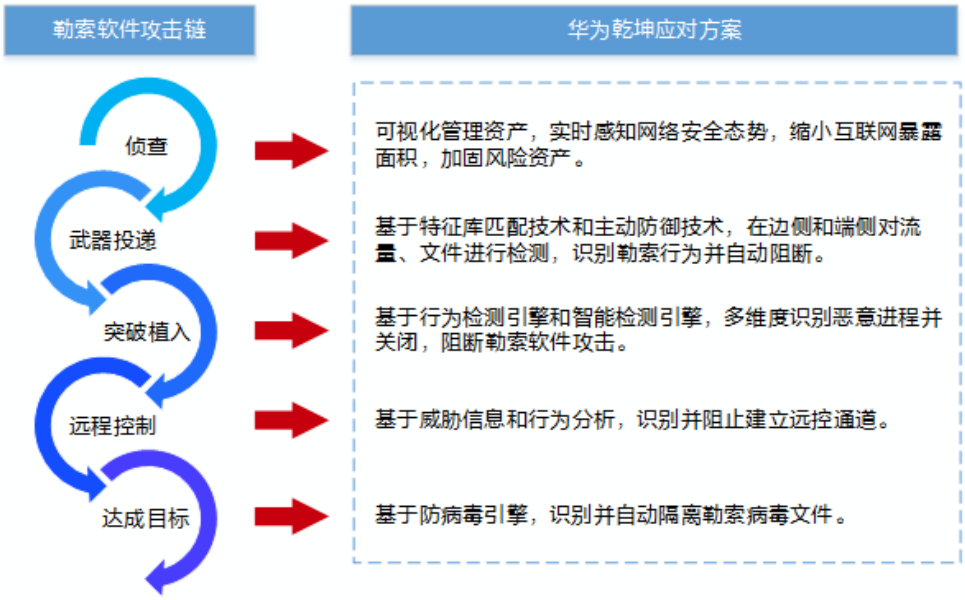
- 多维评估

  提供自动化终端资产清点能力，统筹管理主机列表、进程、端口、组件等资产信息。自动识别资产后，华为乾坤防勒索解决方案可以基于实时威胁信息，持续扫描资产暴露面，对资产进行脆弱性评估、漏洞优先级评估、防护有效性评估等多维度评估，全面感知资产状态，及时预警勒索病毒并提供针对性建议，做到智能引导闭环。

- 全面防护

  华为乾坤防勒索解决方案采用云边端一体的创新架构，基于四大立体防护体系和七大检测引擎，全面覆盖企业终端和边界的安全日志采集点，全面感知安全态势，构建纵深防御体系。如**图3-2**所示，在深入分析勒索病毒攻击链特点后，华为乾坤防勒索解决方案在攻击链各个阶段均部署应对方案，层层拦截勒索病毒，秒级检测勒索入侵，全方位守护企业网络安全。

图 3-2 勒索软件攻击链及应对方案



- 智能响应

  采用边端联动处置的创新方案，自动挖掘同一攻击链上所有勒索事件，提供一键快速处置方式，为租户提供最优阻断方案，全方位抵御安全风险。处置勒索软件后，华为乾坤防勒索解决方案基于知识图谱的攻击可视化技术，支持进程、注册表、文件、网络连接等溯源操作，用于支撑风险全面加固和勒索事件深度清理，防止同一勒索事件重复发生。

3.1.4 典型应用

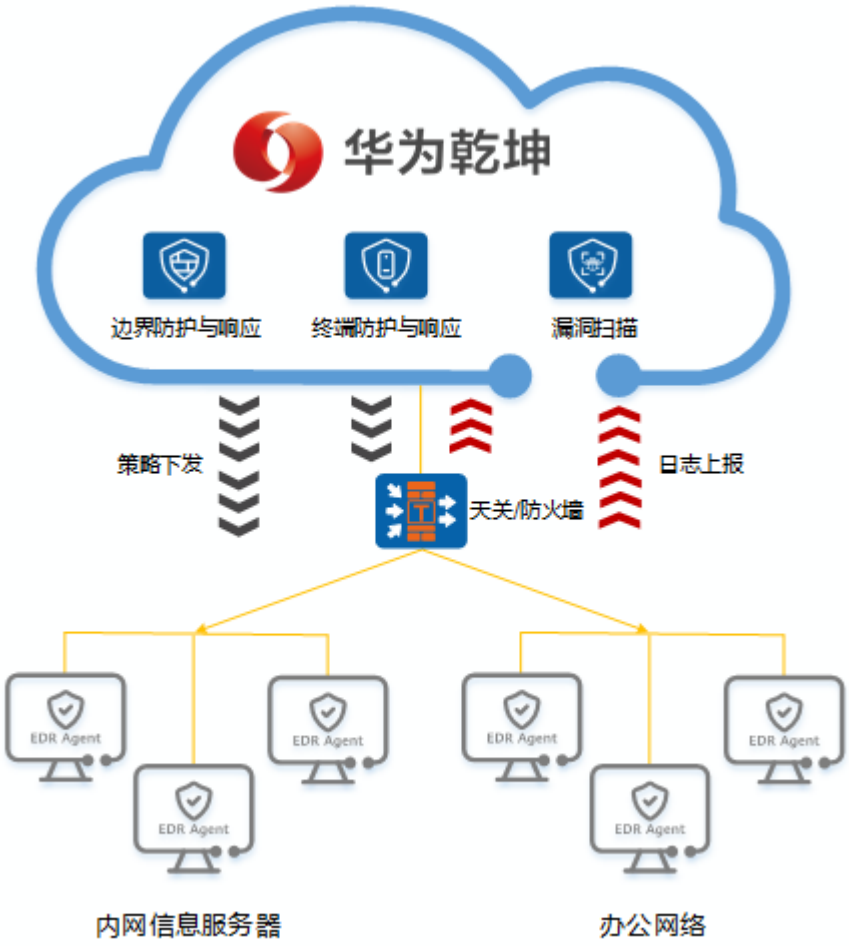
3.1.4.1 中小型企业联网场景

中小型企业缺乏安全投资和安全运维人员，通常只购买最基本的安全设备，但也因没有专业运维人员而无法发挥作用。不法分子因勒索软件攻击成本低廉而常常进行无差别攻击，面对此类安全防护能力几乎空白的企业，勒索入侵成功率极高，可迅速导致整个信息系统不可用，业务长时间中断，并造成企业重大经济损失。随着勒索软件的泛滥，中小型企业日常业务的可持续性存在高风险，因此防勒索建设也成为此类型企业必须面对的课题。

此类型企业防勒索建设的主要诉求包括：

- 由于安全资金和安全运维人力短缺，不想购买多种安全设备。
- 没有安全运维能力，希望将“防勒索建设”外包出去，保障日常业务运营不中断。

图 3-3 中小型企业联网场景



采用华为乾坤防勒索解决方案，可以帮助企业实现：

- 仅需在企业互联网出口部署一台天关/防火墙，在企业终端上安装EDR Agent软件，即可通过云端自动下发的防勒索能力，有效阻止勒索软件入侵和留存，保障企业日常业务运营。
- 获取云端自动处置能力和安全专家服务，进行自动化运维，大幅减轻企业的安全运维压力。

3.1.4.2 大型企业集团多分支互联场景

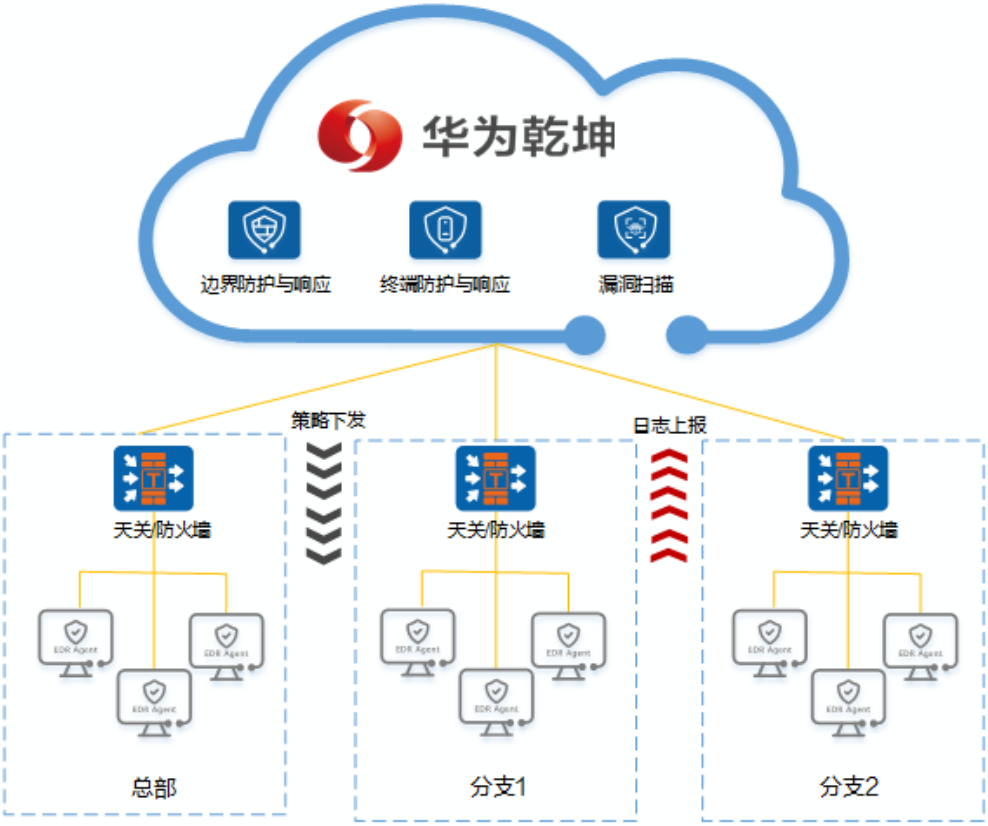
大型企业集团业务一般遍及全国，在全国多省市设有分支，且分支之间业务来往频繁。此类型企业一般在集团总部设有小型的网络安全部门，但分支基本没有专门的安全运维人员。由于分支机构庞大且分支间互联网数据传输频繁，总部安全人员难以准确感知集团整体安全态势，通常存在多项风险。大型企业集团因为资金雄厚，是攻击者勒索入侵的主要目标，一旦被攻破，将面临被索要大额赎金和企业声誉下滑的艰难情境。

此类型企业安全建设的主要诉求包括：

- 简化本地运维：因企业分支机构庞大和安全运维成本受限，无法为每个分支派驻安全运维人力，希望能够在不影响勒索防护质量的情况下减轻企业安全运维压力。

- 实现统一防护：能够对分支机构网络防护全部覆盖，及时了解每个分支的安全状况，可以统筹分析全集团的勒索事件，并统一响应、及时阻断威胁。

图 3-4 大型企业集团多分支互联场景



采用华为乾坤防勒索解决方案，可以帮助企业实现：

- 利用云端的智能分析和处置能力提升自动运维效率，自动拦截勒索事件，隔离病毒文件。云端安全专家及时提供安全服务，有效简化本地运维。
- 通过在每个分支的互联网边界处部署一台天关/防火墙作为安全防御节点，同时在每台终端上部署EDR Agent软件，全面覆盖企业安全日志采集点，结合云端的安全服务实现对所有分支网络的统一防护。
- 借助云端对安全事件的统筹分析，及时自动响应阻断威胁，并将安全告警通过邮件发送至总部安全管理员。总部安全管理员可针对性进行应急响应，解决严重的勒索事件，并借助安全报表了解整体的网络安全态势，把握全集团的网络安全动态。

3.1.5 关键特性

表 3-2 关键特性

特性类型	特性名称	简介
边界防护与响应服务	本地网络边界防护	天关/防火墙部署在租户网络边界，通过入侵防御、反病毒、DNS过滤等技术守护本地安全，可以执行以下防护动作： ● 对流量进行入侵防御检测，全方位防御各种威胁行为。 ● 对流量进行反病毒处理，有效避免病毒文件引起的数据破坏、权限更改和系统崩溃等情况的发生。 ● 对流量进行DNS过滤，全面控制域名访问。
	租户数据安全处理	● 数据授权：在用户授权前提下，本地天关/防火墙仅提供用户授权范围内的数据。 ● 加密传输：本地天关/防火墙采用HTTPS或TLS协议将日志提供到云服务平台。 ● 加密保存：使用华为公司密钥管理中心（KMC）加密组件对数据进行加密，加密后存储在云端。 ● 处理原则：仅供云服务平台运营专家进行威胁分析和溯源。 ● 信息隔离：每个客户都有自己的服务账号，基于账号接收分析报表和短信，不同客户间信息隔离。
	自动化分析	云端基于分析模型对威胁事件进行分析判定，并根据判定结果执行不同的处置。租户可依靠云端的自动化分析能力和安全专家简化本地运维，提升防护实效。 自动化分析以后，可以有如下几种处置方式： ● 事件命中误报模型，则此事件状态变更为误报。 ● 事件命中告警自动确认模型、威胁分析等模型，则自动化分析将请求安全响应执行相应的处置。 ● 在自动化分析的基础上，安全专家进一步分析处置事件。
	安全响应	提供安全事件的响应闭环能力，主要包括下发黑名单、发送告警两种安全响应动作，租户可利用云端的安全响应能力有效提高安全事件的闭环效率。 针对以下场景提供下发黑名单、发送告警两种安全响应动作： ● 自动化分析判定后可以自动处置的事件，自动化分析将请求安全响应下发黑名单或发送告警。 ● 自动化分析判定后需要安全专家处置的事件，安全专家分析后可通过Portal页面的事件管理菜单人工下发黑名单或发送告警。 ● 租户在租户门户中下发黑名单。

特性类型	特性名称	简介
	云端专家精准分析	云端专家整合安全能力，快速准确识别复杂威胁： ● 现网对抗经验固化到云端，不断增强云端安全能力。 ● 最新漏洞分析、云端智能签名生产，快速应对新型威胁。 ● 专家针对发现的每一条安全告警进行统一分析，运用云端各种安全能力，解决最新“疑难杂症”。
终端防护与响应服务	终端识别与管理	● 终端自动识别：提供自动化终端资产清点能力，安装EDR Agent后，该终端即被自动识别。 ● 资产信息管理：自动化统一管理主机列表、进程、端口、组件等终端资产信息。 ● 终端安全管理：智能分析终端安全，呈现终端资产安全分析评分和风险总览。
	威胁检测与处置	● 入侵检测：基于行为检测引擎，提供终端行为检测能力，检测暴力破解、异常登录、权限提升等恶意行为。 ● 事件聚合：将离散的勒索类告警事件，基于进程调用链聚合成相应的勒索事件，且支持对其一键处置。
	病毒查杀与处置	● 病毒查杀：基于华为第三代反病毒引擎，每日更新病毒特征库，实时更新紧急病毒，提供高质量病毒文件检测能力。 ● 威胁分析：支持对检出的病毒文件进行威胁分析，展示详细的威胁信息，如病毒标识、风险值、置信度等。
	主动防御	● 诱饵捕获：基于勒索病毒特征放置诱饵文件，实时检测并及时上报异常行为。 ● 文件防篡改：对重点文件进行访问权限控制并实时检测，及时发现篡改行为。 ● 实时防护：实时扫描全盘目录，及时识别病毒文件并阻断其传送行为。
	溯源分析	● 取证分析：采集和存储终端信息，并通过数据挖掘、关联分析等方法，对威胁事件进行取证分析。 ● 攻击可视化：通过EDR（Endpoint Detection and Response，端点侦测与回归）数字化建模、溯源推理算法，实现攻击可视化，精准还原威胁攻击链路。
漏洞扫描服务（可选）	资产发现	基于客户提供的IP网段，主动发现网段内的联网资产。经客户确认后，支持资产一键录入，提高资产梳理效率。 目前仅适用于A类/B类/C类私有IP地址网段和资产IP白名单范围内的资产发现。
	漏洞扫描	漏洞扫描支持系统扫描、应用扫描等多种扫描类型，并为扫描出的漏洞提供修复建议。同时支持漏洞扫描报告下载。

特性类型	特性名称	简介
	漏洞管理	以漏洞视角呈现每个漏洞的详细信息和关联资产。 ● **详细信息**包括漏洞名称、漏洞编号、漏洞优先级评级VPR和修复建议等。 漏洞优先级评级VPR（Vulnerability Priority Rating）用来表示漏洞修复优先级，是漏洞扫描服务基于漏洞利用代码成熟度、漏洞公布时长、产品的覆盖率、CVSS评分等多维度数据，通过机器学习算法计算的漏洞风险评分。分数越高，说明越需要优先修复。 ● **关联资产**能够帮助客户快速定位到风险资产，使漏洞修复更有针对性。
	边界漏洞免疫（自动消减处置措施）	一般情况下，漏洞是通过在资产上安装补丁进行修复。当客户的实际环境无法满足安装补丁的条件，又希望降低被攻击风险时，可以利用天关/防火墙的入侵防御（IPS）能力，设置漏洞关联的IPS签名动作为“阻断”，通过在边界拦截异常流量，缓解漏洞被利用的风险。漏洞关联的IPS签名ID会被查询出来，显示在漏洞详情的界面中。 天关/防火墙侧的IPS签名动作一般有“告警”和“阻断”两种。 ● 如果签名动作为“阻断”，则表示天关/防火墙会阻断异常流量。漏洞被利用的风险低。 ● 如果签名动作为“告警”，则表示天关/防火墙只产生告警，不会阻断异常流量。漏洞可能会被利用，建议您联系华为乾坤运营人员（如：提交“工单”），重新设置签名动作。

3.2 部署指南

3.2.1 注册华为乾坤帐号

说明

- 华为乾坤控制台是使用华为乾坤的界面，登录前需要先注册华为乾坤帐号。
- 如果您已有华为乾坤MSP（渠道服务商）创建的租户帐号，可跳过本节内容。

步骤1 访问华为乾坤控制台。

步骤2 在登录页面单击“立即注册”。

根据界面提示完成帐号注册。

----结束

3.2.2 开通服务

前提条件

- 已在配置器SCT上分别购买边界防护与响应服务、终端防护与响应服务和漏洞扫描服务（可选），具体请联系代理商。
- 已注册华为乾坤帐号，具体操作请参见《租户操作指南》中的“帐号注册”章节。

背景信息

边界防护与响应服务的开通方式请参见边界防护与响应服务的《服务开通》中“开通服务套餐”章节。

终端防护与响应服务和漏洞扫描服务（可选）的开通方式请参见本章节。

操作步骤

1. 以租户帐号登录华为乾坤控制台。
2. 在界面右上方单击“订单”，选择“我的套餐”页签。
3. 单击“开通服务”。
4. 单击“根据授权ID激活”，输入“授权ID”，单击“开通”。
   “授权ID”请参考界面提示“查看授权ID获取方式”进行获取。

   图 3-5 开通服务界面

5. 查看服务开通情况。
   在“我的套餐”页签下，如果套餐对应的“状态”为“正常”，说明开通成功。

3.2.3 配置天关或防火墙上线

华为乾坤防勒索解决方案需要在客户侧部署天关或防火墙才能正常使用。本方案配套的天关/防火墙的型号及上线指导，如表3-3所示。具体操作请参见《天关和防火墙上线指南》。

表 3-3 天关或防火墙的型号

设备类型	设备型号
USG6000E-C天关	● USG63xxE-C：USG6301E-C/6302E-C/6303E-C ● USG65xxE-C：USG6501E-C/USG6502E-C/USG6503E-C
USG6000F-C天关	USG6603F-C、USG6606F-C
USG6000E防火墙	● 防火墙USG61xxE：USG6106E ● 防火墙USG63xxE：USG6305E/USG6306E/USG6308E/USG6309E/USG6312E/USG6315E/USG6322E/USG6325E/USG6332E/USG6335E/USG6350E/USG6355E/USG6365E/USG6385E/USG6395E ● 防火墙USG6303E：USG6303E ● 防火墙USG65xxE：USG6515E/USG6525E/USG6530E/USG6550E/USG6555E/USG6560E/USG6565E/USG6575E-B/USG6580E/USG6585E ● 防火墙USG65xxE-K：USG6520E-K/USG6560E-K/USG6590E-K ● 防火墙USG63xxE-B：USG6308E-B/USG6318E-B/USG6338E-B/USG6358E-B/USG6378E-B/USG6388E-B/USG6398E-B ● 防火墙USG6xxxE-Exx：USG6000E-E03/USG6000E-E07 ● 防火墙USG66xxE：USG6610E/USG6620E/USG6630E/USG6650E/USG6680E/USG6605E-B/USG6620E-K/USG6640E-K ● 防火墙USG67xxE：USG6712E/USG6716E
USG6000F防火墙	● 防火墙USG65xxF：USG6525F/USG6555F/USG6565F/USG6585F/USG6585F-B/USG6520F-K/USG6560F-K/USG6590F-K/USG6510F-D/USG6530F-D/USG6510F-DK/USG6510F-DL/USG6530F-DL ● 防火墙USG66xxF：USG6615F/USG6625F/USG6635F/USG6655F/USG6685F/USG6620F-K/USG6650F-K ● 防火墙USG67xxF：USG6710F/USG6715F/USG6725F/USG6710F-K ● 防火墙USG6000F-Exx：USG6000F-E01/USG6000F-E03/USG6000F-E05/USG6000F-E07/USG6000F-E09/USG6000F-E12/USG6000F-E15/USG6000F-E20

3.2.4 快速配置

设备上线后，您还需要在云端或设备中进行相关配置，才能正常使用华为华为乾坤防勒索解决方案。可以参考如下文档完成快速配置。

表 3-4 快速配置参考文档

子服务	手册名称	参照内容	文档获取
边界防护与响应服务	部署指南	• 配置设备安全域 • 配置全局白名单 • 黑白名单授权 • 订阅告警与报告 • 查看威胁事件	部署指南
终端防护与响应服务	部署指南	• 服务授权 • 样本获取授权 • 安装EDR Agent • 查看终端资产	部署指南
漏洞扫描服务（可选）	部署指南	• 配置VPN接口 • 录入资产 • 授权服务扫描 • 创建漏洞扫描任务 • 查看扫描结果	部署指南

3.2.5 日常操作

您可以参考如下文档使用防勒索解决方案。

表 3-5 参考文档

子服务	手册名称	文档内容简介	文档获取
边界防护与响应服务	用户指南	介绍如何使用边界防护与响应服务。	用户指南
终端防护与响应服务	用户指南	介绍如何使用终端防护与响应服务。	用户指南
漏洞扫描服务	用户指南	介绍如何使用漏洞扫描服务。	用户指南

4 安全分支解决方案

4.1 方案概述

4.1.1 趋势和挑战

随着技术和行业数字化的发展，企业分支办公、分支零售、分支物流、分支连锁等场景越来越多。为了更快抓住商机，企业正通过网络云化方式快速部署网络，实现分支业务快速上线或变更。

网络云化是网络服务化的实现手段，正如IaaS让企业不再重复建设基础设施那样，网络云化后，企业不用关心建设网络需要什么样的架构、在哪里建设网络、功能如何实现，只需要关心企业实现商业价值的时候，网络需要提供什么样的功能，这使得企业彻底获得网络云化带来的好处，更加聚焦业务。

企业分支网络云化过程中，面临着不少挑战：

- 分支部署慢：传统部署难以满足业务灵活部署的诉求

  传统的分支业务部署速度慢，从业务申请到开通往往需要长达1～3个月的时间。同时云化趋势下，企业业务更新发展迅速，传统网络部署方式难以满足快速上线和业务变更的要求。

- 管理运维难：设备激增，人工配置低效且易错，运维效率低下

  传统模式下，需要专人现场对设备进行管理，但随着企业分支跨地域分布越来越广泛，设备类型越来越多，设备数量激增，导致管理难度大、成本高。此外，随着业务不断增多和业务云化，WAN网络中分支到分支、公有云、私有云的流向更加复杂，传统网络运维方式已难以适应业务的发展。

- 应用体验差：海量应用带宽共享，业务冲突导致体验不佳

  随着Internet的普及，网络的覆盖范围和网络质量有了很大的提高，Internet成为许多企业除了传统专线之外新的重要选择，但是Internet网络本身并不能保障服务质量。此外传统网络对业务不感知，无法获知应用的状态，当遭遇突发流量链路拥塞或质量劣化的时候，往往会造成关键业务体验无法保障。

- 安全威胁多：传统被动防御已无法满足当前企业安全诉求

云化趋势下，企业提供服务的同时遭受到的攻击形态越来越多变。随着企业资产类型变多，风险暴露面增大，企业对分支安全的要求越来越高，传统依靠人为被动防御的手段已无法满足企业主动防御的诉求。企业需要尽早识别攻击行为，迅速做出反应，将损失降至最低。

4.1.2 方案简介

华为乾坤安全分支解决方案融合了云管理网络和边界防护与响应、威胁信息、终端防护与响应、云日志审计等服务，是一套面向企业WAN、LAN、WLAN以及安全的全方位网络管理方案，并以SaaS云服务形式提供给用户，为企业降低了运维复杂度、节省管理成本、确保端到端安全。

华为乾坤安全分支解决方案打造了一站式、可体验的网安融合方案，帮助企业实现了多分支统一管理和安全防护的愿景。方案的主要亮点如下：

- **全网统一管控：**提供多分支统一网络管理、监控、运维和报表服务。
- **极简组网架构：**出口网关和智能防火墙ALL-in-One，网安融合减少运维复杂度；分支内提供“小行星”组网，网络架构三层变两层，引流绿色低碳分支网络。
- **Wi-Fi智能调优：**Wi-Fi场景化识别和调优，智能漫游，保障关键用户和应用体验。
- **零信任准入控制：**精细化的权限控制；终端智能识别，防仿冒防私接；安全态势联动，快速隔离失陷终端。
- **分支安全实时防护：**使能边界安全防护，安全风险时网络实时阻断、精准溯源；在线漏洞扫描，精准地识别潜在漏洞；联动网络快速封禁中毒终端，阻断横移，减少损失。
- **SD-WAN应用保障：**基于链路质量、带宽利用率、应用级别智能选路；双发选收、智能A-FEC，保障实时视频不卡顿；支持报文压缩去重，节省用户开支。

4.1.3 客户价值

华为乾坤安全分支解决方案是专为企业客户打造的网安融合方案，不仅帮助企业业务快速上线，还提供丰富的故障诊断和巡检工具，同时提供主动防御能力，切实提升分支安全防护实效。

- **分支按需互联，全网统一管控**
  - 为用户提供基本的广域互联能力，支持总部、分支、公有云业务灵活连接、轻松互访。
  - 提供分支/园区网络统一管理和监控能力，设备状态可视可管，Wi-Fi、局域网和广域网间支持设置统一的安全策略。
- **极简部署，智能运维**
  - 设备支持多种即插即用方式开局，适应不同的网络场景，网络策略一键下发，大幅降低网络部署难度，缩短业务上线周期。
  - 出口网关和智能防火墙ALL-in-One，实现网安融合，并提供“小行星”组网，网络架构三层变两层，简化用户组网，减少运维复杂度。
  - 用户接入过程全旅程可视，故障可实时回溯，接入问题分钟级定位，多维度评估Wi-Fi网络质量，主动优化网络和用户漫游体验。
- **零信任准入控制**
  - 提供多种准入认证方式，可灵活进行认证策略和授权策略配置，对准入权限进行精细化控制，保障网络接入安全。

  - 终端智能识别和检测，避免仿冒或私接终端，联合安全态势，可以对失陷终端快速隔离。
- **分支安全实时防护**
  - 分支网络边界部署安全设备（防火墙），提供入侵防御、反病毒能力，云端自动威胁处置，一处检出全局免疫。
  - 分支终端部署EDR Agent软件，快速封禁中毒终端，阻断横移，减少损失。
- **关键应用保障**
  - 基于首包识别和业务感知技术能快速识别应用，支持通过自定义应用规则识别特殊应用。
  - 基于TCP FPM（TCP Flow Performance Measurement，TCP流性能测量）、IP FPM（IP Flow Performance Measurement，IP流性能测量）等技术进行应用质量和链路质量检测，基于应用质量、带宽利用率、应用优先级等进行智能选路，保障关键应用业务体验。
  - 支持双发选收、智能A-FEC，可以保障实时视频不卡顿，提供极致的用户体验。

4.1.4 方案架构

背景信息

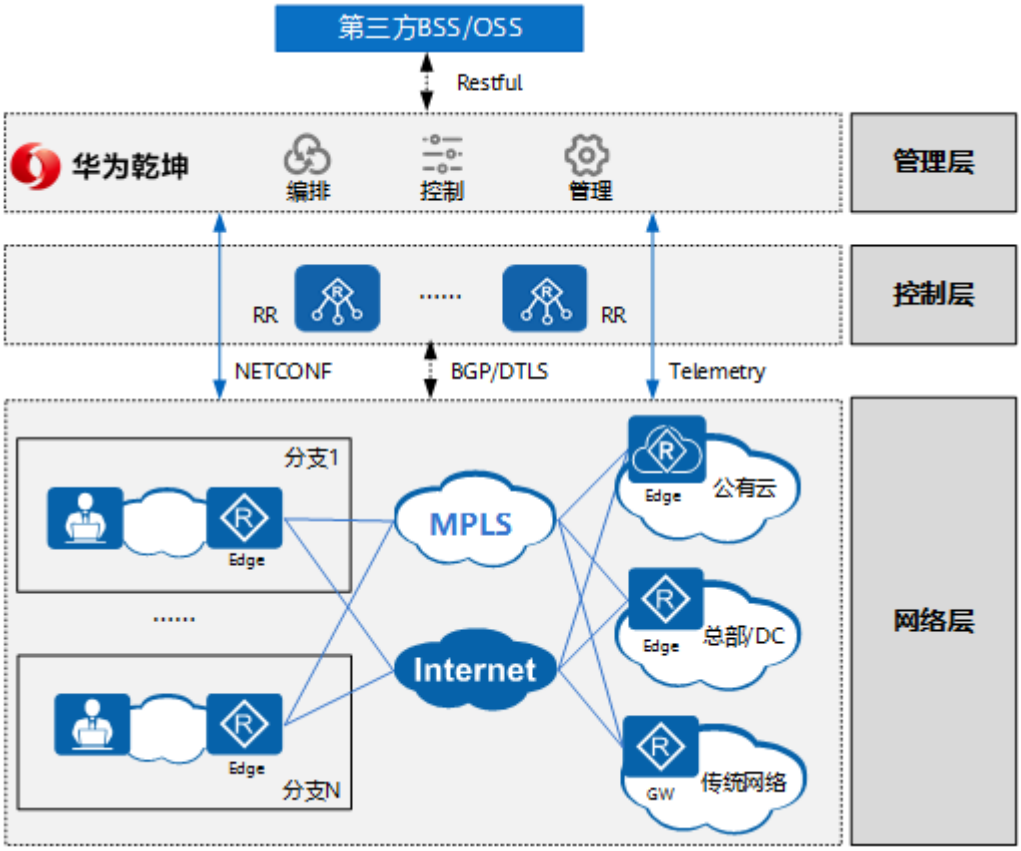
对于多园区/分支网络，通常会采用SD-WAN或IPsec VPN来实现分支间互联。

- SD-WAN：属于一种动态的VPN，可以按需在站点间建立隧道，动态发布路由。SD-WAN通过在站点间建立GRE隧道来创建VPN通道，同时支持在GRE隧道上进行IPsec加密，以实现隧道的加密安全。另外SD-WAN可以基于应用、策略选择质量较优的链路发送数据，实现基于应用、策略的智能选路。
- IPsec VPN：属于一种静态的VPN，通过在站点之间建立IPsec隧道来创建VPN通道，根据配置静态网段引流到VPN隧道中，实现站点间的业务通过VPN隧道进行访问。

基于 SD-WAN 的架构介绍

基于SD-WAN的华为乾坤安全分支解决方案总体架构如图4-1所示，主要包括管理层、控制层、网络层。

图 4-1 安全分支网络互联架构模型（SD-WAN）



- **第三方BSS/OSS**

  华为乾坤开放了北向API接口，可以将SD-WAN纳入到已有的BSS/OSS等第三方业务编排系统，实现SD-WAN的集成和灵活定制。

- **管理层**

  管理层的核心是华为乾坤云平台，主要提供网络编排和管理能力，支持端到端业务处理。

  – 网络编排：负责SD-WAN面向业务的网络模型抽象、编排和配置自动化发放，主要包括企业WAN组网和各种网络策略相关的业务编排。通过对网络模型的抽象和定义，屏蔽SD-WAN部署和实现的技术细节，使网络配置和业务发放更加简易、灵活。

  – 网络管理：负责网络层设备的统一管理与运维，包括统一配置网络业务；采集设备告警、日志等信息；基于链路、应用、网络的性能数据采集、统计和分析；基于网络拓扑、告警管理、性能监控等方式多维度统计和呈现运维信息。

- **控制层**

  控制层的核心组件是RR（Route Reflector，路由反射器），主要负责控制网络层的路由转发和拓扑定义。其功能主要包括：VPN路由的分发和过滤、VPN拓扑的创建和修改、站点间Overlay隧道的创建和维护等。相比传统网络完全的分布式控制方式，这种集中式的控制实现了企业WAN控制平面和转发平面的分离，简化了网络运维操作，减少了网络配置错误几率，提升了企业WAN的运维效率。

- **网络层**

从业务角度来说，企业的分支、总部和数据中心以及在云上部署的IT基础设施等都可以统称为企业的站点。用于不同站点WAN互联的网络设备以及中间的WAN一起构成了SD-WAN的网络层。

从网络功能层次划分，SD-WAN网络可以分为Underlay网络和Overlay网络两层。

- Underlay网络：即物理网络，是由路由器等网络设备通过运营商提供的物理线路互联组成的WAN，常见类型有MSTP专线、MPLS VPN以及Internet等。
- Overlay网络：即虚拟网络，是在一张物理网络上构建出一张或多张虚拟的逻辑网络。不同的虚拟网络虽然共享物理网络中的设备和线路，但虚拟网络中的业务与物理网络中的业务相互解耦。虚拟网络的多实例化，既可以服务于同一租户的不同业务（如多个部门），也可以服务于不同租户。

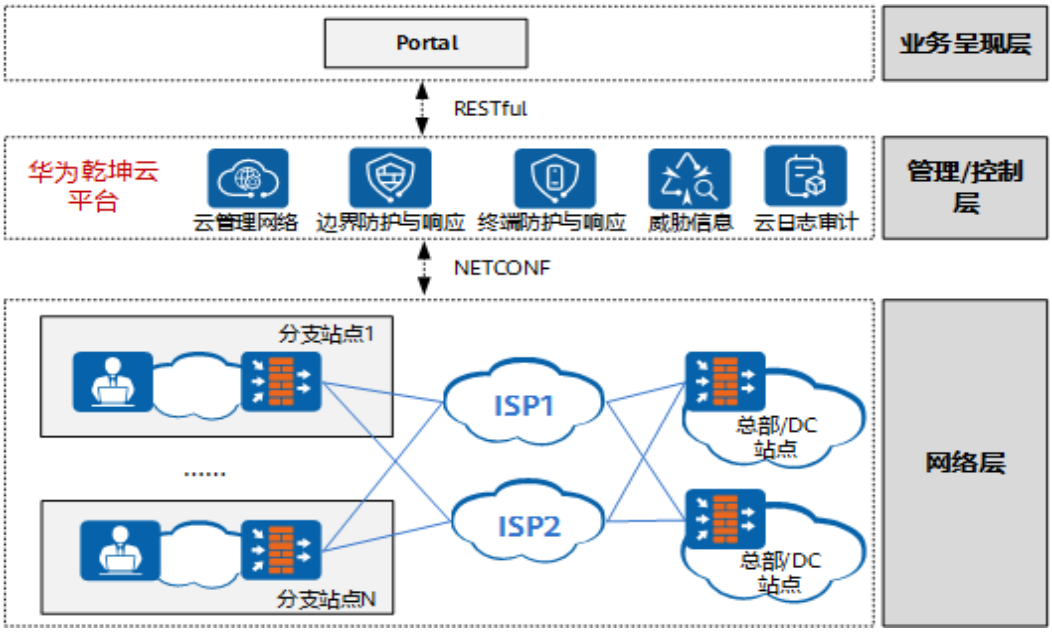
从网络设备的功能定位划分，网络层主要由Edge和GW两类设备构成。

- Edge：是站点的出口CPE设备（Customer Premise Equipment）。Edge的本质是SD-WAN隧道的发起和终结点，也可以看做SD-WAN网络的边界点。Edge之间的Overlay隧道可以构建在任意的有线或者无线的Underlay WAN网络上。
- GW：是连接SD-WAN站点和其他网络（如传统VPN）的网关设备。通过GW可以实现SD-WAN网络与传统网络、公有云网络间的互通。

基于 IPsec VPN 的架构介绍

基于IPsec VPN的华为乾坤安全分支解决方案总体架构如图 安全分支网络互联架构模型所示，主要包括业务呈现层、管理/控制层、网络层。

图 4-2 安全分支网络互联架构模型（IPsec VPN）



- **业务呈现层**

  华为乾坤提供了面向企业、MSP等不同用户角色的Portal界面，Portal中展示了完整的网络端到端业务处理和配置流程，业务呈现层将最终用户的诉求传递到华为乾坤云平台。

- **管理/控制层**

网络管理/控制层主要提供设备一站纳管（通过Netconf协议纳管）、统一运维能力，同时基于智能算法实现威胁检测、自动处置、安全策略统一下发，保障重点业务平稳运行。

对于多分支/园区场景，华为乾坤提供了IPsec VPN互联网络编排能力，通过华为乾坤云平台对站点间VPN的模型进行编排、业务发放。

- **网络层**

  网络层由物理设备组成，是企业WAN的基础物理组网。基于场景诉求，选择合适的出口设备，主要包括防火墙和第三方VPN网关。

  - 防火墙：主要适用于金融、物流、办公等高安全场景，采用防火墙做出口设备，可以做分支、总部的出口设备。
  - 第三方VPN网关：多分支场景，总部网络一般已部署（已存在第三方VPN网关设备），此时分支设备需要和第三方VPN网关对接，只能通过IPsec VPN与第三方VPN网关对接。

4.1.5 典型组网

华为乾坤安全分支组网由园区AP、交换机和出口网关组成，由华为乾坤云管理平台统一管控。分支间以及分支与总部、分支与云之间支持通过VPN互联，常见的广域互联技术包括SD-WAN和IPsec VPN互联技术，前者推荐**路由器（AR）**作为出口网关设备，后者推荐**防火墙**作为出口网关设备。

4.1.5.1 互联技术选型

SD-WAN和IPsec VPN作为云园区网络解决方案出口互联的两种技术，有不同的适用场景和特性差异，在选择时，要充分考虑两种技术对场景的匹配度，选择合适的技术进行方案设计和部署。

SD-WAN和IPsec VPN特性的关键差异点如表4-1所示。

表 4-1 SD-WAN 和 IPsec VPN 关键差异点

特性		SD-WAN	IPsec VPN	备注
组网	Hub-Spoke	支持	支持	-
	Full-Mesh	支持	支持	IPsec VPN mesh互联限制比较多，如仅FW支持、仅支持32个站点、出口必须是公网地址。
	分层组网	支持	不支持	分层组网主要用于站点规模非常多时的互联组网场景。
部署	多Hub站点/Hub多出口	支持	支持	IPsec VPN方案中仅FW设备支持。
	站点出口为第三方设备	不支持	支持	SD-WAN方案Spoke、Hub节点必须都为AR设备。
	分支多链路上行	支持	支持	IPsec VPN方案多链路时，也只能同时建一条隧道。

特性		SD-WAN	IPsec VPN	备注
	网关设备双机出口	支持	不支持	-
	U盘开局	支持	不支持	-
	邮件开局	支持	不支持	-
	DHCP option开局	支持	支持	FW不支持DHCP option方式开局。
	注册查询中心方式开局	支持	支持	-
功能	分支和Hub建立多条VPN隧道，流量可以负载分担/主备	支持	不支持	-
	智能选路（基于应用、链路质量选路）	支持	支持	-
	隧道IPsec加密	支持	支持	-
	分支、Hub间动态路由发布	支持	不支持	-
	链路限速	支持	支持	-
	分支互访	支持	支持	-
支持的规模	站点规模（单租户）	5000	5000	-
支持的网关设备	AP	不支持	不支持	-
	AR（非SD-WAN款型）	不支持	不支持	-
	AR（SD-WAN款型）	支持	不支持	支持SD-WAN的AR款型请参见云管理网络的《服务开通》中“**开通云管理网络套餐**”章节。
	FW	不支持	支持	-

关于SD-WAN和IPsec VPN方案的选择，可以参考如下规则和建议：

必须选择SD-WAN技术的场景

- 分支、总部站点多链路上行，分支、总部需要多隧道建链实现多VPN隧道的主备或者负载分担。
- 需要基于应用、链路质量进行智能选路。

- 有多区域/多中心站点（每个区域相当于一个总部），需要跨区域进行分层互联的复杂互联场景。
- 园区间有多部门业务隔离的诉求，对WAN侧也需要进行隔离，需要部署多VPN的互联。

必须选择IPsec VPN技术的场景

- 小微门店仅部署AP，AP做出口网关。
- 金融、物流、办公门店等只考虑用FW做出口网关场景。
- Hub节点为第三方VPN网关。

其他建议

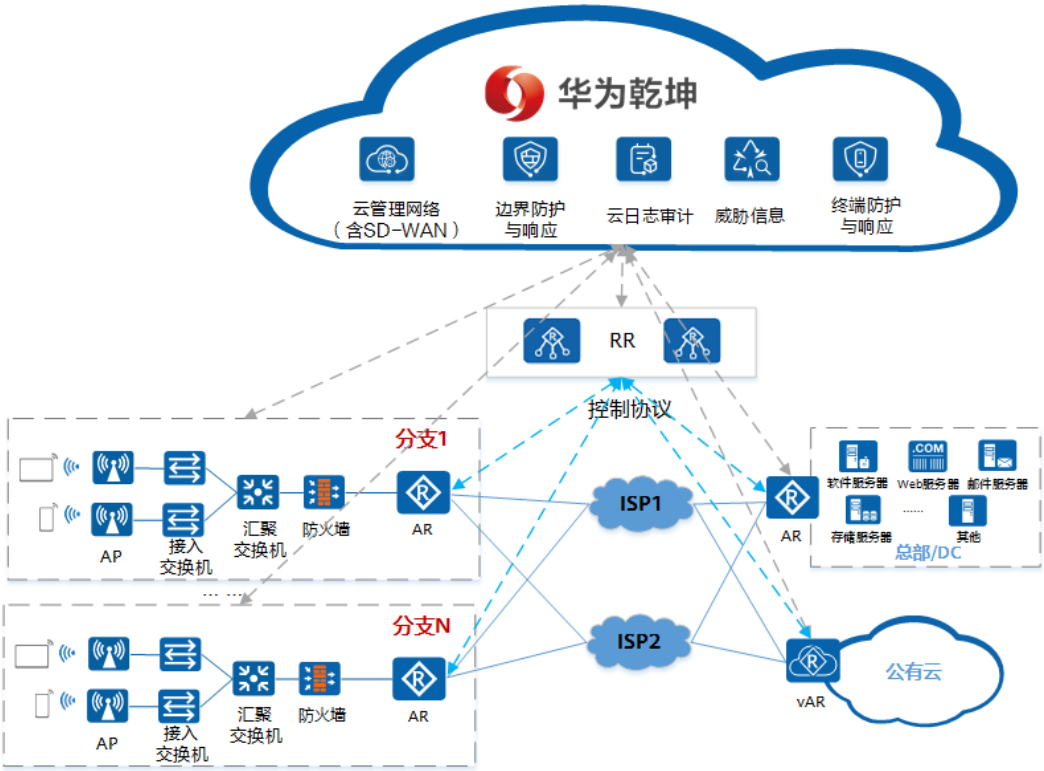
- IPsec VPN主要适合于中小型海量分支的互联，SD-WAN可以支持中小型分支的互联，同时也可以支持大中型园区的互联，通过动态的方式发布园区路由，在大中型园区互联场景下更具灵活性、扩展性。
- 如果仅有单链路和单总部的场景，则建议配置轻量化的IPsec VPN，同时也可以支持更多的设备类型，方便灵活组网。
- 针对多Hub节点场景（一个总部多个公网出口也为多个Hub节点），分支如果只需要和一个Hub节点建链，则可以考虑用FW的IPsec VPN方案。
- 部署SD-WAN方案时，如果同时需要高级安全如IPS、威胁分析、反病毒等，则可以通过AR下挂FW的方案实现。
- 针对FW、AR部署时，SD-WAN方案可以在满足站点规模的前提下，都可以替代IPsec VPN的方案，但实际可以根据部署的成本、代价、灵活性、扩展性，选择具体的方案。

4.1.5.2 SD-WAN 方案组网

该方案面向大型连锁企业、高校、多分支办公园区等场景，提供SD-WAN服务，实现企业复杂组网需求，保障应用体验，同时支持LANWAN融合、威胁分析与处置等能力，一站统管，降低企业的管理难度。

方案组网

图 4-3 AR 路由器作为出口网关



如图4-3所示，方案采用云边端一体创新架构。

- 云端部署云管理网络（含SD-WAN特性）和边界防护与响应等服务，为用户提供设备云化管理、网络极简开局、SD-WAN智能选路、智能运维、威胁自动分析处置等能力。
- 本地网络出口网关采用AR路由器，实现了分支与分支、分支与总部/数据中心（DC）、分支与云之间通过SD-WAN的互访；边界部署安全设备（天关），持续保护企业分支安全。
- 在PC、服务器等企业终端部署EDR Agent软件，云端时刻感知资产终端风险，防止终端感染和威胁在内网传播。

组网模型

SD-WAN使用的是动态的VPN，可以按需在站点间建立隧道，动态发布路由。SD-WAN组网的站点互联模型和出口互联模型如下所示。

- **站点互联模型**

  园区LAN-WAN融合场景的SD-WAN组网方案支持三种站点互联模型：Full-mesh、Hub-spoke、分层组网。不同互联模型所支持的组网规模不同，如表4-2所示，需要根据企业网络中需要互联的站点数量或规模来选择对应的互联模型。

图 4-4 SD-WAN 互联模型（Full-mesh）

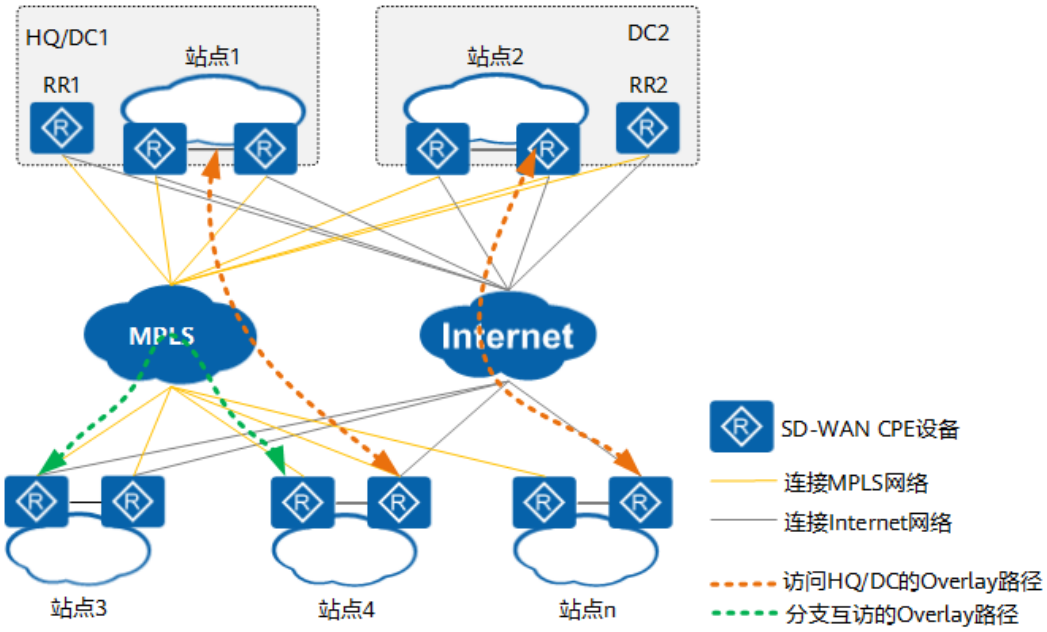


图 4-5 SD-WAN 互联模型（Hub-spoke）

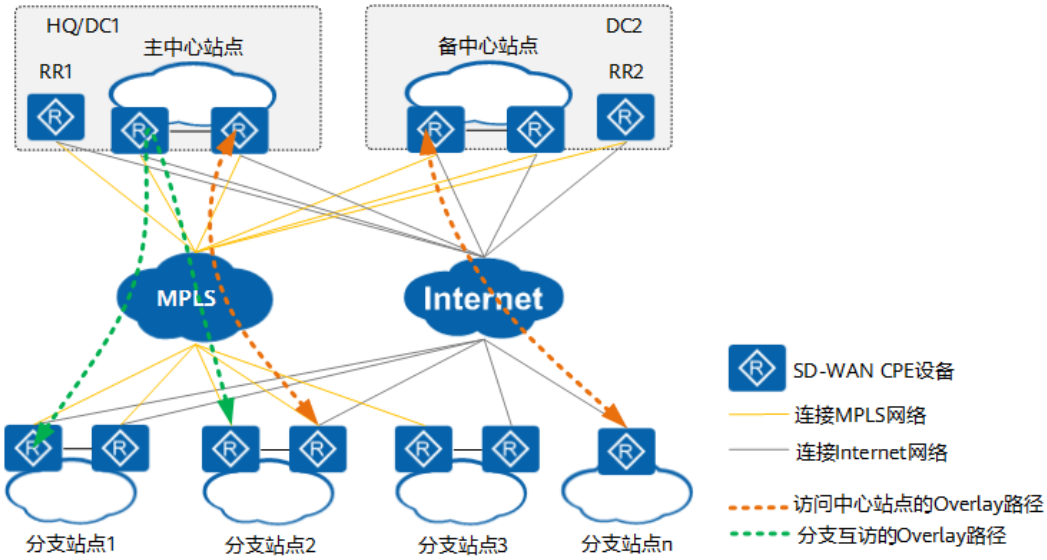


图 4-6 SD-WAN 互联模型（分层组网）

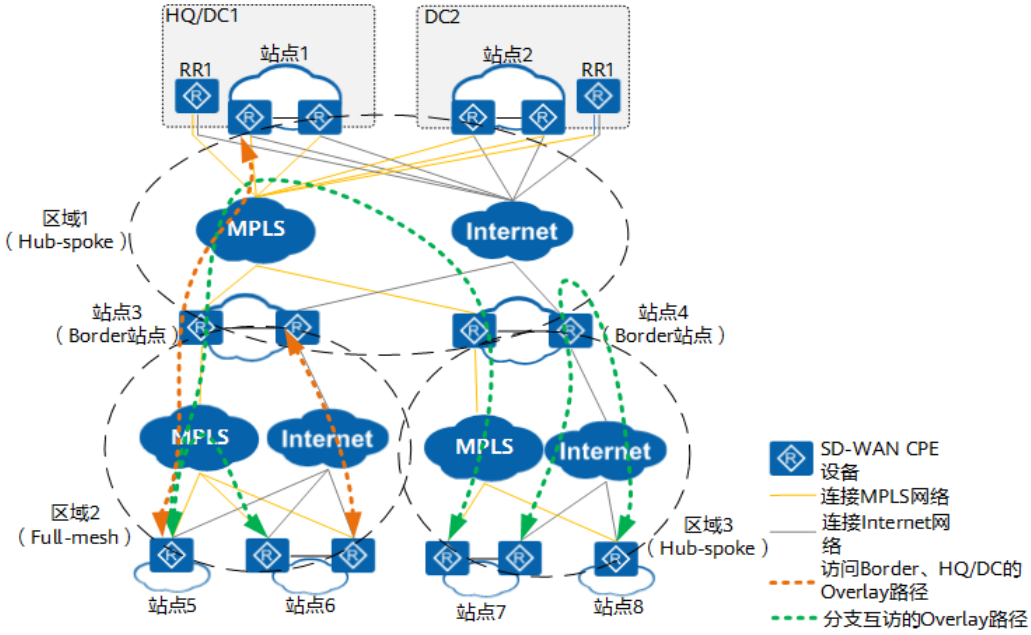
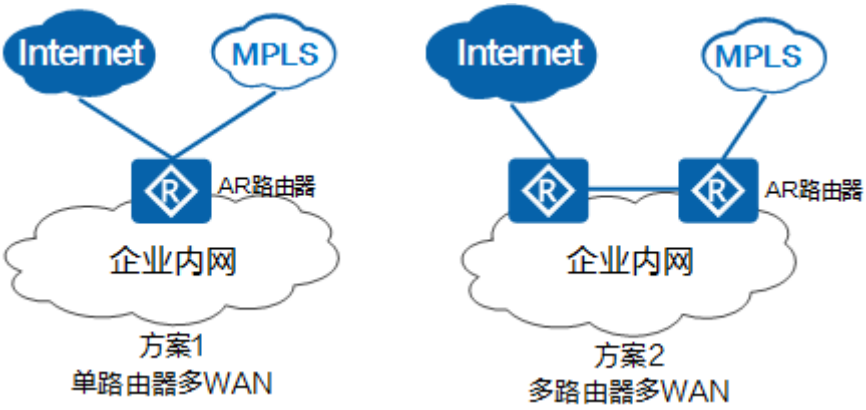


表 4-2 SD-WAN 互联模型支持的场景

互联模型	站点规模	适用场景
Full-mesh	站点≤200	• 网络规模比较小 • 分支间流量比较大
Hub-spoke	站点≤1000	• 中等规模网络 • 流量主要是分支访问总部，分支间的互访可以通过总部互访
分层组网	站点≤2000	网络规模大，有多个区域中心，通过多个区域中心将整个网络连通起来

- **出口互联模型**
  - 对于中小型酒店、门店、商超等场景，网络规模比较小，出口组网采用单设备和单链路即可满足要求，如图4-7中的方案1
  - 对于大型商超、普教场景，网络规模较大，对可靠性要求高，可以采用双设备或双链路组网方案，如图4-7中的方案2。

图 4-7 互联出口组网模型（路由器做出口网关）

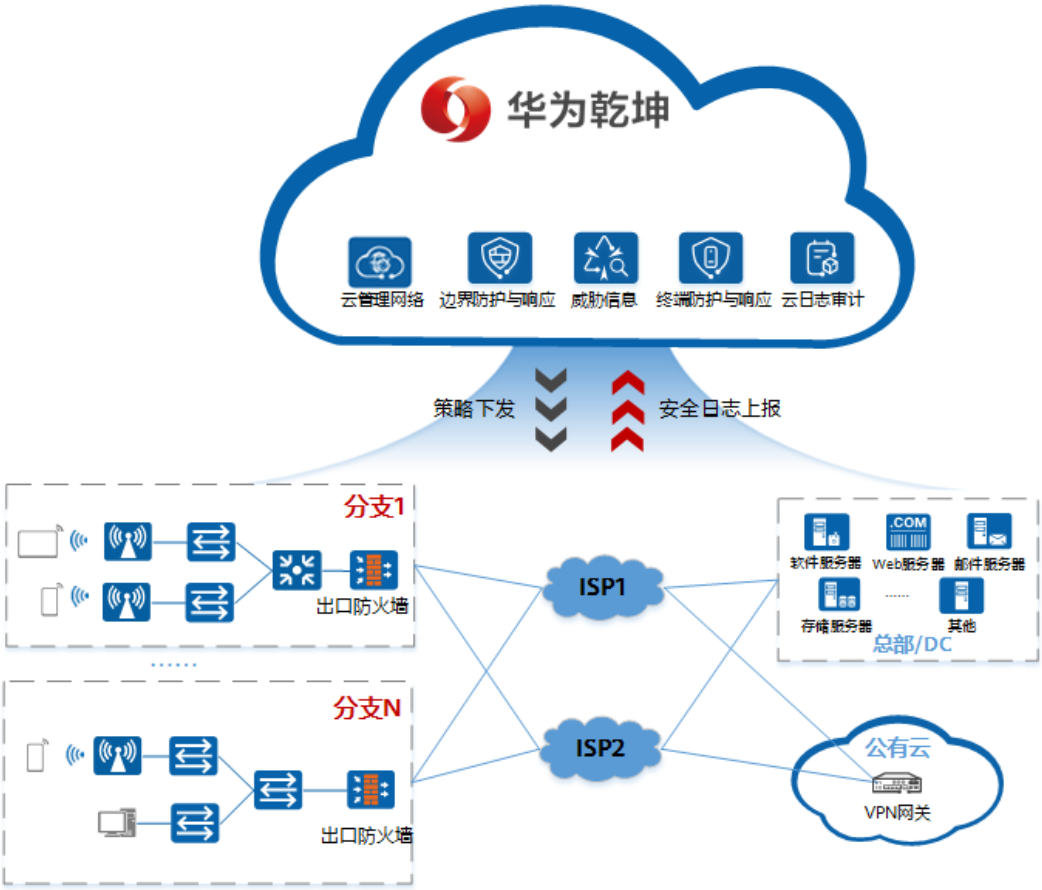


4.1.5.3 IPsec VPN 方案典型组网

该方案面向零售门店、酒店、教育行业，提供LANWAN融合、出口网关和智能防火墙ALL-in-One、威胁分析与联动处置等能力，同时满足客户对网络、安全和监管需求，为用户提供极致性价比。

方案组网

图 4-8 防火墙作为出口网关



如图4-8所示，方案采用云边端一体创新架构。

- 云端部署系列云服务，支持设备云化管理、威胁自动分析处置、安全策略一键下发，支持网络极简开局、智能运维。
- 本地网络边界部署安全设备（天关），提供入侵防御、反病毒、DNS过滤等能力，持续保护企业分支安全；提供DHCP、NAT、IPsec VPN分支上网以及分支互联/上云能力。
- 在PC、服务器等企业终端部署EDR Agent软件，云端时刻感知资产终端风险，防止终端感染和威胁在内网传播。

组网模型

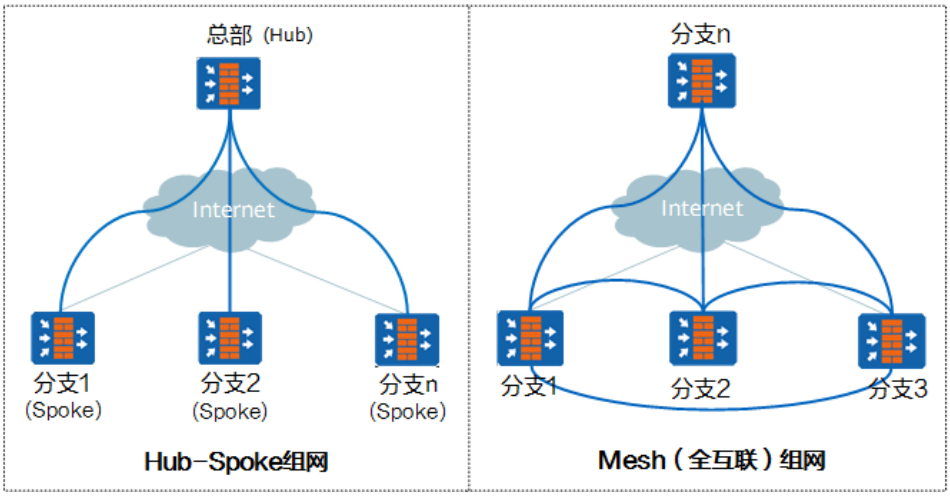
IPsec VPN属于一种静态的VPN隧道，在网络规划时，需要先确定组网模型，确定网络拓扑关系。

- **站点互联拓扑模型**

  对于使用IPsec VPN，站点间的互联拓扑模型均可分为Hub-Spoke和Mesh两种模型，如图 互联拓扑模型所示，需要根据实际需求选择合适的互联拓扑模型。

  - Hub-Spoke模型适用于大规模的分支互联，但分支的互访，也无法满足所有分支都可以互访，仅支持部分分支间互访，建议针对大型、有互访诉求的分支，按需开启互访的能力。
  - Mesh组网模型主要受限于整体网络的规模，无法适合海量分支场景下有分支互访的诉求，仅建议在少量分支互联的场景下应用（如分支站点<32个）。

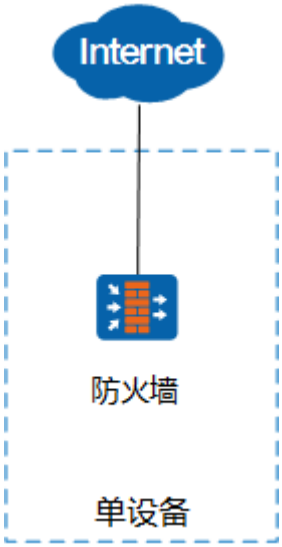
  图 4-9 互联拓扑模型



- **出口组网模型**

  出口组网仅支持单设备单链路模式，且只支持通过云管模式上云，如图4-10所示。

图 4-10 互联出口组网模型



4.1.6 应用场景

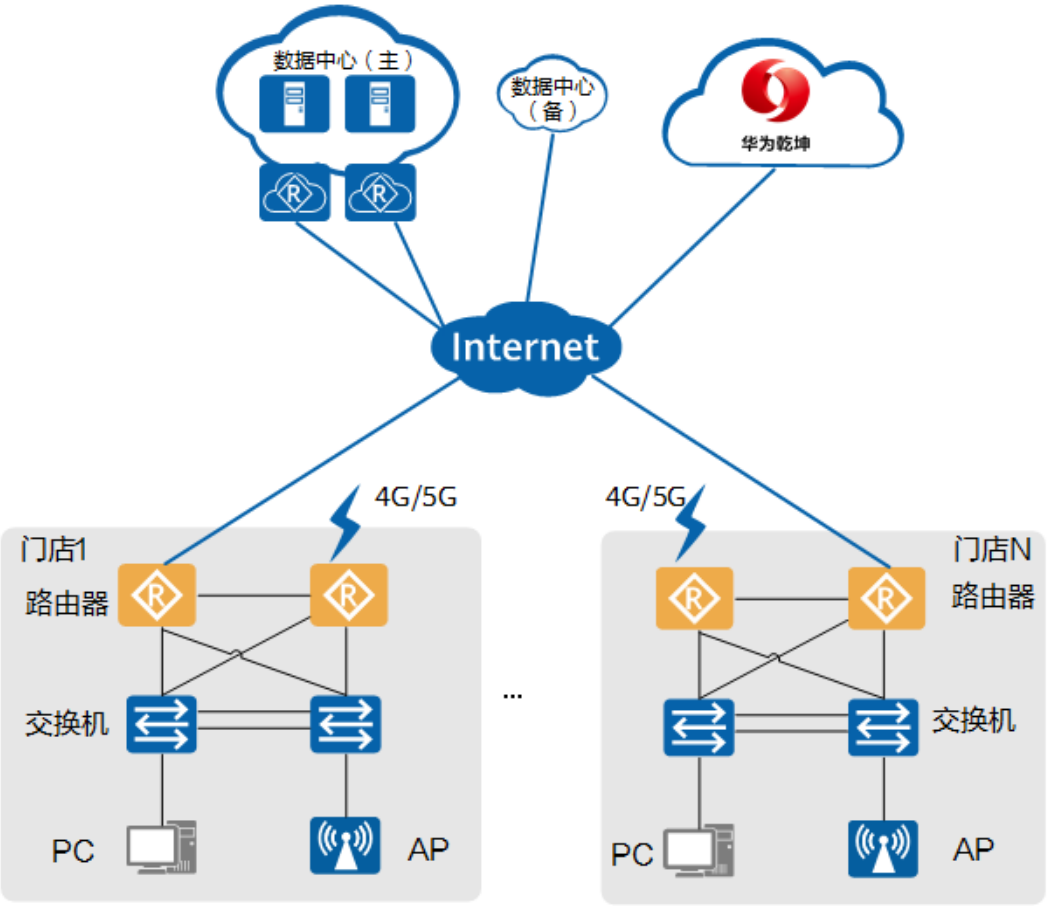
4.1.6.1 连锁餐饮业（AR）

某头部连锁餐饮店，在全国约有4000+家门店，门店网络分为专网（Staff Network）和客网（Guest Network）两个网络，当前已实现LANWAN融合统一管理。

用户希望通过SD-WAN实现分支与分支、分支与数据中心、分支与云之间全场景随需互联。在实现过程中主要面临的困难包括：

- 成本高：专网和客网硬件隔离，专网改造成本高，均为有线网络。
- 运维难：无法统一运维监控可视化以及智能运维，依赖人工运维，运维效率低。
- 可靠性低：出口路由器单台部署，存在单点故障问题，可靠性低。

图 4-11 连锁餐饮组网图



如图4-11所示，采用华为乾坤安全分支解决方案，可以帮助连锁门店实现：

- LAN-WAN融合，统一管理和控制AP、交换机、路由器等多种设备，LAN侧和WAN侧业务统一管理和控制。
- 设备支持多种即插即用方式开局，适应不同的网络场景，网络策略一键下发，大幅降低网络部署难度，缩短业务上线周期。
- 丰富SD-WAN策略，提升应用体验，应用识别、智能选路，QoS精细化调度。
- 出口路由器双机部署，可靠性有效提升。

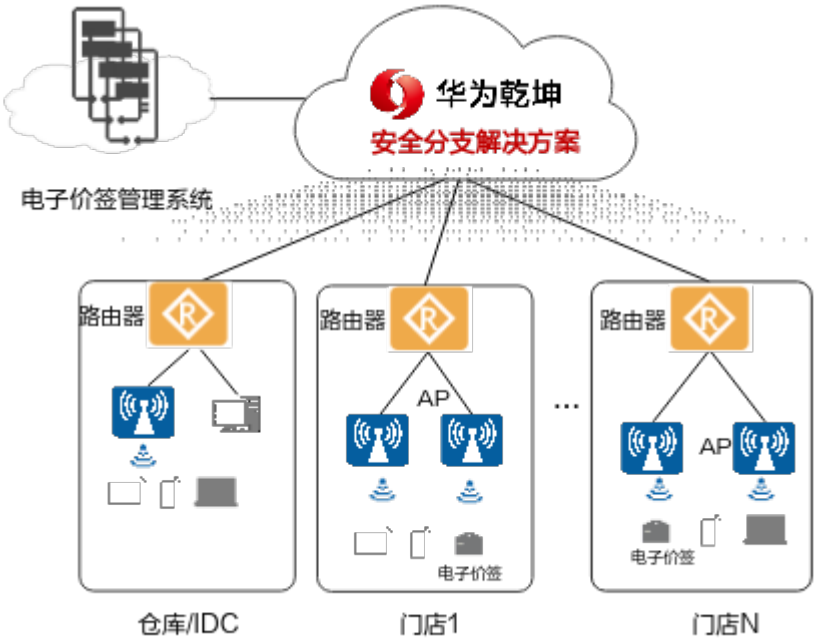
4.1.6.2 零售业（AR）

某零售集团在中国400多个城市拥有超过4000家店铺，涉猎的商品包括保健产品、美容产品、香水、化妆品、日用、食品、饮品、电子产品、洋酒及机场零售业务。

该集团要求门店尽快扩张，业务数据需要接入总部和云数据中心，目前面临的主要困难包括：

- 4000+门店数量庞大，设备管理复杂。
- 缺乏专业IT人员，网络建设和运维能力匮乏，一旦网络故障无法及时响应，影响访客体验。
- 门店缺乏基本的安全防护手段，门店收银系统时常面临网络安全风险。

图 4-12 零售门店组网图



如图 零售门店组网图所示，采用华为乾坤安全分支解决方案，可以帮助零售集团实现：

- 网络和出口安全统一管理，分支门店状态实时可视。
- 设备即插即用，无需工程师现场调测，一家门店部署时间由1周降为1天，让网络部署不再成为门店扩张的瓶颈。
- 有线无线智能运维，故障远程指导定位解决。
- 安全问题实时阻断，门店安全优先保障。

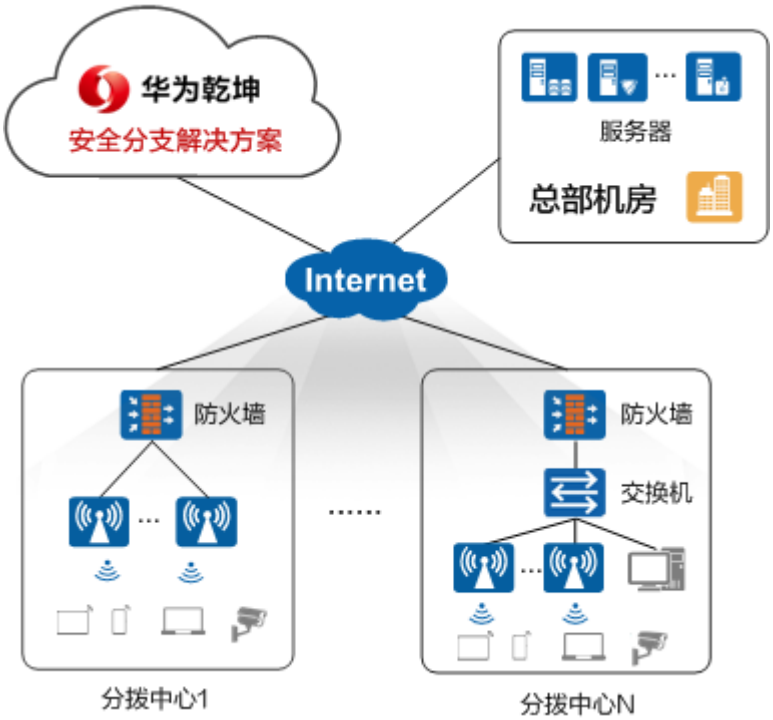
4.1.6.3 物流业（FW）

某物联公司主要从事运输、仓储、搬运、包装、配送等工作，在全国10多个省份有200+家分拨中心。

该司希望分拨中心和总部之间能够进行业务互访，同时分拨中心实现无线全覆盖。在实现过程中主要面临的困难包括：

- 分拨中心的位置分散，分拨中心管理员完全不具备IT知识，远程业务部署的效率低下。
- 各分支网络无法统一管理，网络状态不可见，一旦故障，无法及时闭环，从而导致用户无法查看物流信息，引发大面积的投诉。

图 4-13 物流分拨中心组网图



如图 物流分拨中心组网图所示，采用华为乾坤安全分支解决方案，可以帮助物联公司实现：

- 分拨中心设备即插即用，WLAN网络云端规划，配置一键下发，分钟级网络交付。
- 200+分拨中心网络状态云端集中可视，分支通过部署安全设备实时检测威胁，一旦故障云网联合定位，故障远程处理，运维效率大幅提升。

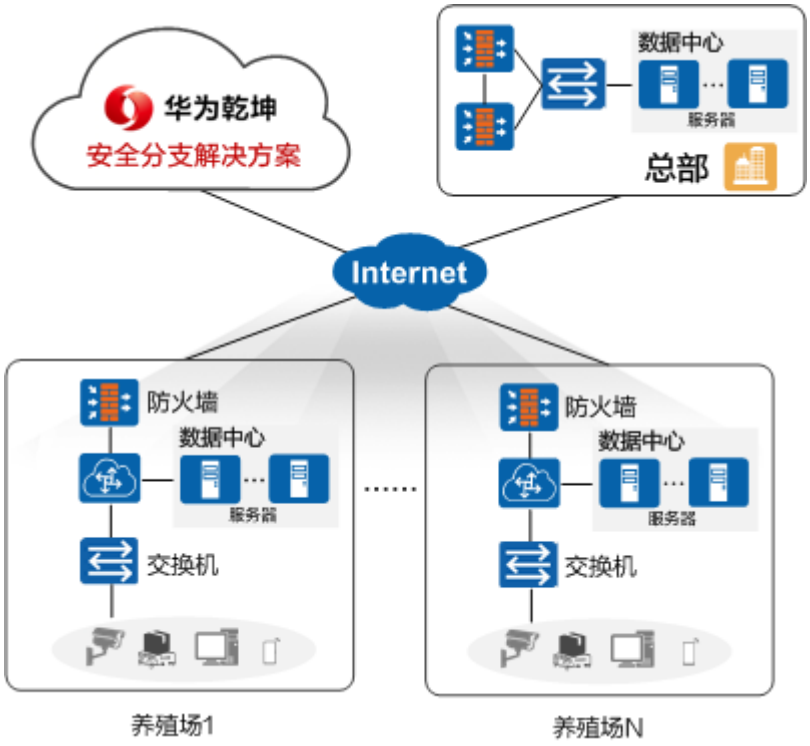
4.1.6.4 畜牧业（FW）

某大型畜牧业公司以生猪养殖为核心，集饲料加工、种猪育种、生猪养殖、屠宰加工等于一体。目前拥有2000+家养殖场，遍布全国各地。

该公司希望采用自动化技术替代人工方式，提升整个企业养殖管理效率，打造智慧牧场新标杆。在实现过程中主要面临的困难包括：

- 各地养殖场无法集中管理，各类IoT设备繁多，管理复杂度高。
- 牧场每天产生数以亿计的养殖数据，牲畜对温度、湿度等数据比较敏感，一旦场内服务器遭遇威胁攻击，可能导致养殖停滞，给牧场带来巨大经济损失。
- 设备维护依靠IT人员现场勘察，而养殖场本身对外来生物管控严格，一般要求提前2天进行封闭消毒。一旦设备故障，定位成本高、耗时很长。

图 4-14 畜牧养殖场组网图



如图 畜牧养殖场组网图所示，采用华为乾坤安全分支解决方案，可以帮助畜牧业公司实现：

- 集中运维，远程管理：少量网络工程师统一集中运维全国所有的养殖场网络，零接触设备替换、升级、远程管理。
- 终端安全管理：自动物料器、温湿度传感器、AGV小车、视频监控等物联数据实时检测，异常终端隔离，全方位保障圈舍环境调控、精准饲喂和疫病监测。
- 物联应用优先保障：AGV小车等终端接入过程全旅程可视，多维度评估Wi-Fi网络质量，主动进行智能调优，保障牧场网络应用体验。

4.1.7 关键特性

表 4-3 华为乾坤安全分支解决方案关键特性

特性类型	特性名称	简介
云管理网络	站点管理	支持按站点管理网络，可以查看网络拓扑、调整拓扑结构、配置站点业务。
	设备管理	支持纳管网络设备（交换机、AP、AR、WAC）、安全设备（防火墙）。
	准入认证	提供了802.1X、Portal、MAC等多种认证方式，可按需对接入用户进行策略管控。

特性类型	特性名称	简介
	IPsec VPN	提供一种静态VPN，通过在站点之间建立IPsec隧道来创建VPN通道，实现分支与分支、分支与总部、分支与云之间的业务互访。
	SD-WAN	● 提供一种动态VPN，可按需在站点间建立隧道，动态发布路由。通过站点间建立GRE隧道来创建VPN通道，同时支持在GRE隧道上进行IPsec加密，实现分支与分支、分支与总部、分支与云之间的业务安全互访。 ● 支持基于应用、策略选择质量较优的链路发送数据，实现基于应用、策略的智能选路。
	网络环境监控	支持网络健康度评估、网络问题分析、无线智能去噪。
	用户体验保障	支持用户旅程回放、协议回放、用户问题分析。
	应用分析	支持全网应用数据监控，保障网络应用畅通无阻。
	智能调优	支持智能无线射频调优、智能无线漫游。
边界防护与响应服务	本地网络边界防护	天关/防火墙部署在租户网络边界，通过入侵防御、反病毒、DNS过滤等技术守护本地安全，可以执行以下防护动作： ● 对流量进行入侵防御检测，全方位防御各种威胁行为。 ● 对流量进行反病毒处理，有效避免病毒文件引起的数据破坏、权限更改和系统崩溃等情况的发生。 ● 对流量进行DNS过滤，全面控制域名访问。
	租户数据安全处理	● 数据授权：在用户授权前提下，本地天关/防火墙仅提供用户授权范围内的数据。 ● 加密传输：本地天关/防火墙采用HTTPS或TLS协议将日志提供到云服务平台。 ● 加密保存：使用华为公司密钥管理中心（KMC）加密组件对数据进行加密，加密后存储在云端。 ● 处理原则：仅供云服务平台运营专家进行威胁分析和溯源。 ● 信息隔离：每个用户都有自己的服务账号，基于账号接收分析报表和短信，不同用户间信息隔离。

特性类型	特性名称	简介
	自动化分析	云端基于分析模型对威胁事件进行分析判定，并根据判定结果执行不同的处置。租户可依靠云端的自动化分析能力和安全专家简化本地运维，提升防护实效。 自动化分析以后，可以有如下几种处置方式： ● 事件命中误报模型，则此事件状态变更为误报。 ● 事件命中告警自动确认模型、威胁分析等模型，则自动化分析将请求安全响应执行相应的处置。 ● 在自动化分析的基础上，安全专家进一步分析处置事件。
	安全响应	提供安全事件的响应闭环能力，主要包括下发黑名单、发送告警两种安全响应动作，租户可利用云端的安全响应能力有效提高安全事件的闭环效率。 针对以下场景提供下发黑名单、发送告警两种安全响应动作： ● 自动化分析判定后可以自动处置的事件，自动化分析将请求安全响应下发黑名单或发送告警。 ● 自动化分析判定后需要安全专家处置的事件，安全专家分析后可通过Portal页面的事件管理菜单人工下发黑名单或发送告警。 ● 租户在租户门户中下发黑名单。
	云端专家精准分析	云端专家整合安全能力，快速准确识别复杂威胁： ● 现网对抗经验固化到云端，不断增强云端安全能力。 ● 最新漏洞分析、云端智能签名生产，快速应对新型威胁。 ● 专家针对发现的每一条安全告警进行统一分析，运用云端各种安全能力，解决最新“疑难杂症”。
终端防护与响应服务	终端识别与管理	● 终端自动识别：提供自动化终端资产清点能力，安装EDR Agent后，该终端即被自动识别。 ● 资产信息管理：自动化统一管理主机列表、进程、端口、组件等终端资产信息。 ● 终端安全管理：智能分析终端安全，呈现终端资产安全分析评分和风险总览。
	威胁检测与处置	● 入侵检测：基于行为检测引擎，提供终端行为检测能力，检测暴力破解、异常登录、权限提升等恶意行为。 ● 事件聚合：将离散的勒索类告警事件，基于进程调用链聚合成相应的勒索事件，且支持对其一键处置。
	病毒查杀与处置	● 病毒查杀：基于华为第三代反病毒引擎，每日更新病毒特征库，实时更新紧急病毒，提供高质量病毒文件检测能力。 ● 威胁分析：支持对检出的病毒文件进行威胁分析，展示详细的威胁信息，如病毒标识、风险值、置信度等。

特性类型	特性名称	简介
	主动防御	● 诱饵捕获：基于勒索病毒特征放置诱饵文件，实时检测并及时上报异常行为。 ● 文件防篡改：对重点文件进行访问权限控制并实时检测，及时发现篡改行为。 ● 实时防护：实时扫描全盘目录，及时识别病毒文件并阻断其传送行为。
	溯源分析	● 取证分析：采集和存储终端信息，并通过数据挖掘、关联分析等方法，对威胁事件进行取证分析。 ● 攻击可视化：通过EDR（Endpoint Detection and Response，端点侦测与回归）数字化建模、溯源推理算法，实现攻击可视化，精准还原威胁攻击链路。
威胁信息服务	威胁信息检索	支持全球恶意IP、恶意域名、恶意文件、漏洞信息等威胁信息的快速检索，数据详情包括但不限于威胁类型、风险级别、置信度、场景信息、地理位置、关联历史事件、关联恶意威胁信息、相关文章等信息。
	安全研究	定期发布情报周报、情报预警、热点情报等文章，帮助用户了解近期关键安全事件。
	高性能威胁信息查询接口	提供高性能的全球恶意IP、恶意域名、恶意文件、漏洞信息、URL分类等威胁信息的查询接口，辅助自动化分析人员进行分析取证及处置，提升运维效率。
	重保威胁信息	在重保服务期间通过AI算法分析全网历史攻击行为及攻击方法，精准识别攻击方地址，实时共享历史重保专项威胁信息，有效提升信息的精准度。
云日志审计服务	日志接收/解析/存储/查询	● 支持接收不同类型资产（如服务器/终端、网络设备、安全设备、业务系统等）所产生的日志，将日志留存在云端，实现日志的集中管理和存储。 ● 支持解析多种格式及多种来源的日志，将其标准化。 ● 支持日志审计留存在云端，支持180天的日志留存时长。 ● 支持用户按需实时查询日志信息，查询条件包含时间、日志级别、日志类型、资产名称、源/目的IP地址和端口等。
	审计资产管理	● 支持增加多种类型的资产，如服务器、终端设备、网络设备、安全设备等，并对资产的等级进行标识，为用户判断是否需要进行日志审计提供参考信息。 ● 支持灵活管理需要审计的资产。
	日志审计统计数据可视化	● 支持查看当前所有日志数量以及各日志级别的日志数量。 ● 支持按时间段查看日志容量使用趋势和日志数量趋势，如近7天、近一个月。 ● 支持查看当前审计的资产数量及类型。 ● 支持查看每天上报日志最多的TOP10资产。

4.2 部署指南

4.2.1 部署注意事项和要求

部署约束和注意事项

只部署分支园区的网络，以及分支与分支互连，分支与总部互连。关于总部园区的网络不在本文档中建设和部署。

部署前要求

- 已完成**总部园区**的建设和部署。
- 已完成云管理网络套餐和安全服务套餐的购买。**各个服务需要单独购买，按需购买。**

  在安全分支解决方案场景下，在分支网络建设完成后，可以叠加使用安全服务。本场景支持的安全服务类型如下：
  - 边界防护与响应服务
  - 终端防护与响应服务
  - 威胁信息服务
  - 云日志审计服务

4.2.2 开通服务

安全分支解决方案由云管理网络和一系列安全服务组成。如果成功购买了**云管理网络套餐**和**安全服务套餐**，需要先激活套餐，才能正常使用各服务功能。

服务的开通步骤具体请参见表 服务套餐开通。

表 4-4 服务套餐开通

开通服务	套餐描述	开通步骤参考
云管理网络	• 支持试用套餐开通 • 支持云管理网络商用套餐开通 • 支持CloudCampus产品套餐开通	参见云管理网络的《服务开通》。
边界防护与响应服务	• 支持试用套餐开通 • 支持商用套餐开通（线下）	参见边界防护与响应服务的《服务开通》。
威胁信息服务	• 支持试用套餐开通 • 支持商用套餐开通（线下）	参见威胁信息服务的《服务开通》。

开通服务	套餐描述	开通步骤参考
终端防护与响应服务	• 支持试用套餐开通 • 支持商用套餐开通（线下）	参见终端防护与响应服务的《服务开通》。
云日志审计服务	• 支持试用套餐开通 • 支持商用套餐开通（线下）	参见云日志审计服务的《服务开通》。

4.2.3 部署分支网络

实现分支互联的方式不同，分支网络部署步骤也存在差异：

- 通过**IPsec VPN方式**实现分支互连时，分支网络的部署步骤请参见表4-5。

  说明

  使用IPsec VPN方式实现分支互连，分支网络的出口网关是**防火墙**。有以下注意事项：
  - 云管理网络的“网络规划与设计”工具无法使用，请您**手动完成数据规划和网络开局。**
  - 防火墙采用云管模式上云，并手动配置安全策略。

  表 4-5 分支网络的部署步骤

步骤	步骤描述	文档参考
1	完成设备上云（被云平台纳管）和网络手动开局。	云管理网络的《网络部署》中如下几个章节。 • 部署流程 • 软件安装 • 硬件安装 • 网络手动开局 • 设备注册上线
2	根据场景需要，配置第三方设备接入，完成网络业务和用户准入认证配置。	云管理网络的《网络部署》中如下几个章节。 • 设备管理 • 业务配置 • 准入管理
3	配置分支与总部、分支与分支间的互连。	云管理网络的《网络部署》中“IPsec VPN互联”章节。

- 通过**SD-WAN方式**实现分支互连时，分支网络的部署步骤请参见表4-6。

表 4-6 分支网络的部署步骤

步骤	步骤描述	文档参考
1	站点及设备管理	云管理网络的《网络部署》中“**SD-WAN互联**”章节。
2	创建基础网络	
3	创建虚拟网络	
4	创建流量策略	
5	智能运维	

4.2.4 部署分支安全服务

安全分支场景下，当分支网络建设完成后，可以叠加使用一系列安全服务。本场景支持的安全服务有：边界防护与响应服务、终端防护与响应服务、威胁信息服务和云日志审计服务。请根据自身实际诉求，按需部署安全服务，具体参见**表 安全服务的部署步骤**。

表 4-7 安全服务的部署步骤

部署的服务	部署步骤	步骤描述	文档参考
边界防护与响应服务	1	配置防火墙上线。	边界防护与响应服务的《**部署指南**》。 **须知** **需要注意的是：** 叠加安全服务时，建议检查配置，如果防火墙已完成设备上云，则无需重复以上操作。 当使用IPsec VPN分支场景时，防火墙使用云管模式上云；当使用SD-WAN分支场景时，防火墙使用传统模式上云。
	2	在使用服务能力之前，配置基础业务： ● 配置设备安全域 ● 配置全局白名单 ● 授权黑白名单 ● 查看威胁事件	
威胁信息服务	-	无需部署操作，开通后可正常进行威胁信息搜索和查询。	-
终端防护与响应服务	-	● 安装EDR Agent ● 查看终端资产	终端防护与响应服务的《**部署指南**》。
云日志审计服务	1	配置防火墙上线。	云日志审计服务的《**部署指南**》。 **须知** **需要注意的是：** 叠加安全服务时，建议检查配置，如果防火墙已完成设备上云，则无需重复以上操作。 当使用IPsec VPN分支场景时，防火墙使用云管模式上云；当使用SD-WAN分支场景时，防火墙使用传统模式上云。
	2	添加审计资产和日志上报。	

4.2.5 常见维护操作

4.2.5.1 网络日常操作

安全分支场景下，分支网络部署成功后，可以在云端进行网络集中化管理，还可以基于多种智能算法和大数据技术实现网络高效运维。

包括网络大屏展示、设备上报数据等，详细的运维操作指导请参见云管理网络的《网络运维》。

4.2.5.2 安全日常操作

安全分支场景下，华为乾坤提供了一系列安全服务，如边界防护与响应服务、终端防护与响应服务、威胁信息服务和云日志审计服务。此类服务提供了诸多识别威胁、阻断威胁的能力，详细的操作指导请参见表 安全服务操作。

表 4-8 安全服务操作

安全服务	操作描述	文档参考
边界防护与响应服务	介绍如何使用边界防护与响应服务，包括处置威胁事件、管理黑白名单、查看安全报表等。	边界防护与响应服务的《用户指南》。
威胁信息服务	介绍如何使用终端防护与响应服务，包括检索威胁信息、查看威胁情报等。	威胁信息服务的《用户指南》。
终端防护与响应服务	介绍如何使用网络威胁与评估服务，包括查看终端安全、配置威胁检测策略、处置威胁事件等。	终端防护与响应服务的《用户指南》。
云日志审计服务	介绍如何使用云日志审计服务，包括审计资产管理、日志查询和导出等。	云日志审计服务的《用户指南》。

5 安全办公园区解决方案

5.1 方案概述

5.1.1 趋势和挑战

随着越来越多的企业将其运营数字化，海量的设备接入办公园区网络。由于缺乏准入控制技术，入网终端的安全状态与使用者身份未知，无法保障终端入网安全可信，这就导致内网数据泄露等事件频发。与此同时，企业面临的网络安全风险也越来越大，由于人的行为具有不确定性，电脑、服务器等终端作为直接与人交互的装置，面临更多的安全风险，往往是整个网络安全防护流程中最薄弱的环节。近年来针对终端的攻击行为层出不穷，攻击者不仅可以从外部入侵，还可以直接从企业内部发起攻击，导致终端感染。感染的终端接入办公园区网络，会导致威胁在内网迅速扩散，造成企业重大经济损失。

企业办公园区网络当下面临着不少挑战：

- 等保2.0合规要求

  根据等保2.0合规要求，凡是达到等保三级及三级以上的企业，在安全计算环境中必须采用多因子认证，做到威胁终端可溯源。

- 网络接入和IT账号管理割裂

  传统办公园区存在多套身份管理系统管理，导致权限割裂管理、终端检查方案割裂，且本地AD数据无法同步至云上。

- 访客WiFi缺乏管理

  传统办公园区直接开放SSID或PSK供访客接入，无审计定位，无溯源方案，无法针对访客进行二次经营管理。

- 业务安全策略难以适应环境变化

  工作在非传统办公环境中，例如居家办公，需要为相同用户在不同环境接入时提供不同的安全策略，因此需要基于接入位置、时间、终端类型等配置网络策略，传统业务安全策略难以实现策略灵活部署。

- 缺乏对终端持续检测的能力

传统办公园区在设备入网前严格检查，但是入网后对终端就不再进行持续看管，即使设备合规状态变化了也无从知晓。缺乏对对终端安全威胁的检测和发现能力。

5.1.2 方案简介

华为乾坤安全办公园区解决方案融合了云管理网络和终端防护与响应服务，聚焦园区办公场景，为企业提供实时感知终端安全态势、动态调整网络准入策略的能力，持续保障办公安全。如图所示，安全办公园区解决方案由部署在云端的网络云准入服务和部署在电脑、服务器等企业终端上的华为乾坤EDR Agent（后文简称为EDR Agent）软件组成。各个组件的功能介绍如表5-1所示。

图 5-1 华为乾坤安全办公园区解决方案架构图

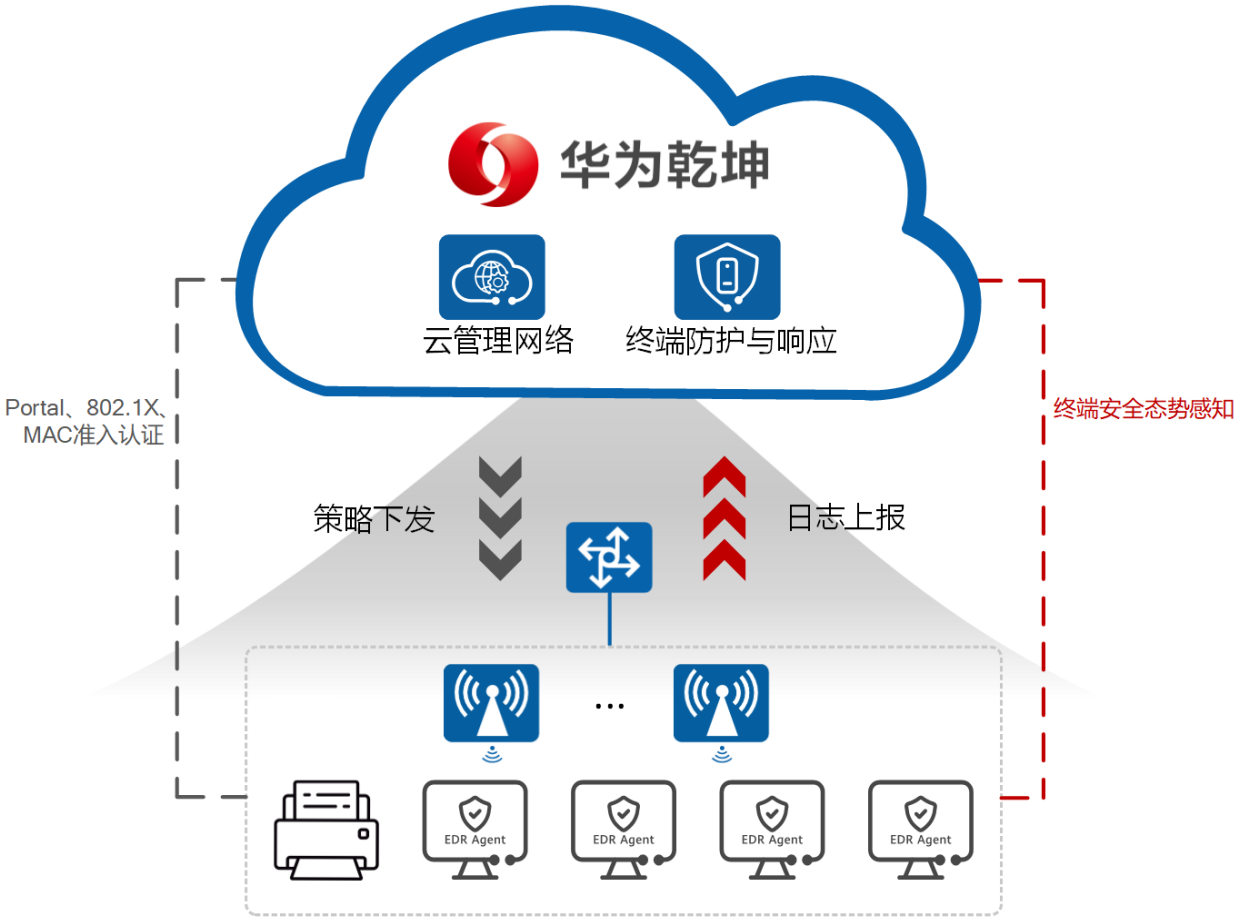


表 5-1 组件功能介绍

部署位置	组件名称	功能介绍
云端	云管理网络	针对接入企业网络的内部员工和访客的终端使用合适的方式进行合法性校验，并针对用户身份给予相应的网络权限规划。华为乾坤云准入服务提供了802.1X、Portal、MAC等多种认证方式，可按需对接入用户进行策略管控。 联动终端防护与响应服务，已安装EDR Agent的终端资产评分如小于云准入服务中定义的分数，则拒绝该终端接入企业网络。
	终端防护与响应服务	针对企业本地终端进行风险检测和处置，防止终端感染和威胁在内网传播。此外，根据病毒等级对资产风险持续进行评分。
终端	EDR Agent	主要负责收集并向终端防护与响应服务上报终端上的用户登录、进程运行/创建、目录/文件访问日志、DNS请求信息，执行预置的主动防御策略和云端下发的防御策略。

5.1.3 客户价值

零信任准入控制

- 提供多种准入认证方式，可灵活进行认证策略和授权策略配置，对准入权限进行精细化控制，保障网络接入安全。
- 终端智能识别和检测，避免仿冒或私接终端，联合安全态势，可以对失陷终端快速隔离。

提升终端防御能力

- 轻量级软件EDR Agent部署在租户端侧，全面覆盖安全日志采集点，能够实时感知终端上的异常行为。当其与云端网络断连后，仍可提供主动防御能力，进行有效防护。
- EDR Agent内置防病毒引擎和行为检测引擎，根据全攻击路径检测规则，对终端上的文件和目录进行毫秒级检测，快速判定威胁。针对勒索病毒，EDR Agent采用诱饵捕获技术，在病毒入侵初期即可精准识别风险，向云端及时上报异常事件。终端防护与响应服务实时同步威胁信息，检出新威胁后及时更新威胁特征库，增强对全网的安全防护能力。
- 基于海量数据库和智能检测算法，云端能够检出常规签名无法检测到的恶意样本，发现多种WAF（Web Application Firewall，网站应用程式防火墙）绕过手段，对抗未知和变种威胁。
- 云端采用智能化技术，当攻击发生时，可自动挖掘同一攻击链上所有威胁事件，提供一键快速处置方式。

极简部署，智能运维

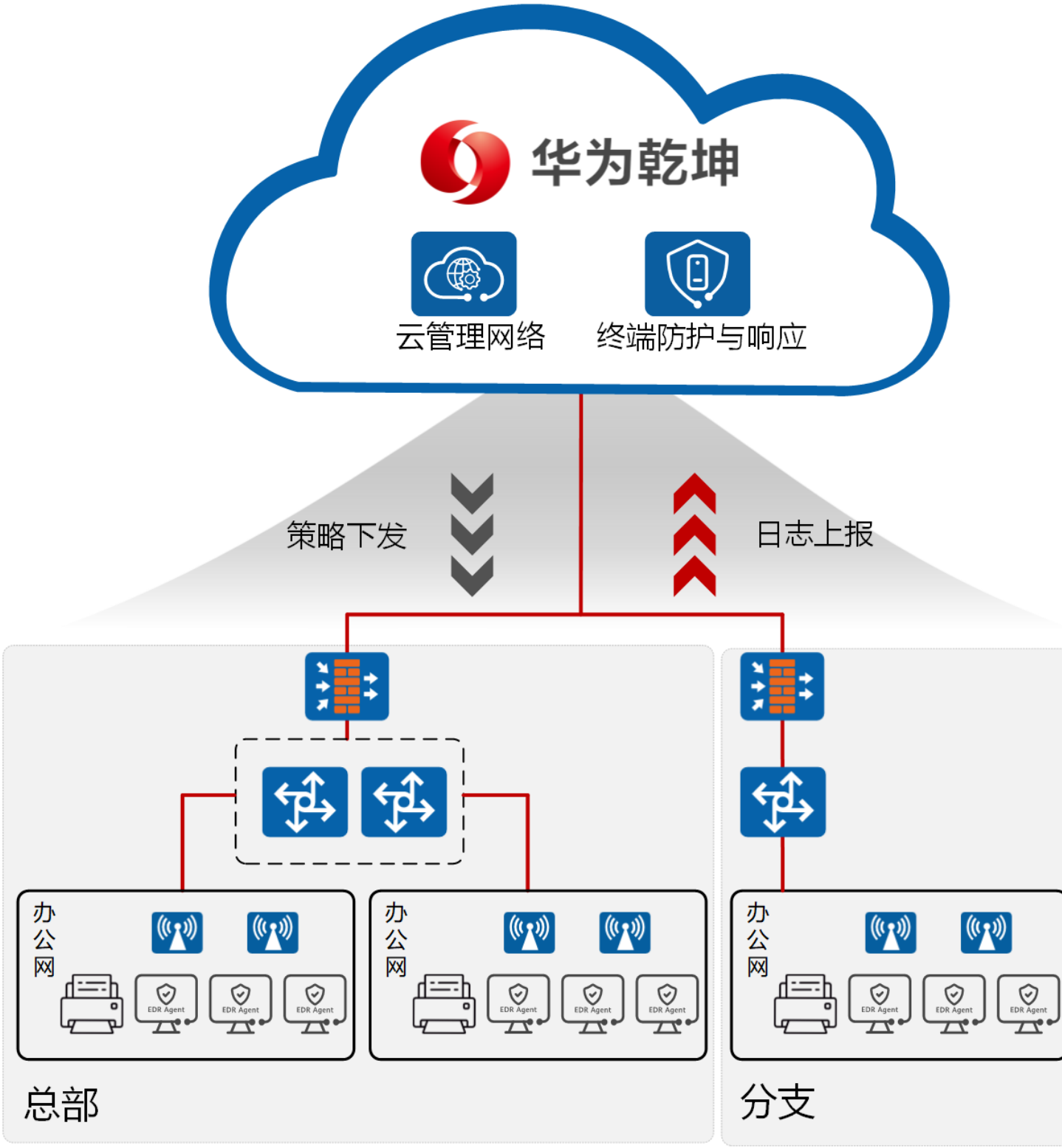
- 用户接入过程全旅程可视，故障可实时回溯，接入问题分钟级定位。
- 轻量级软件EDR Agent部署在终端，全面覆盖安全日志采集点，能够实时感知终端上的异常行为。当其与云端网络断连后，仍可提供主动防御能力，进行有效防护。

5.1.4 典型应用

某企业的分支机构规模和人员规模在逐步扩大，办公园区中接入的终端数量也逐步增加。企业当前缺少对接入网络的终端进行准入控制的手段，导致接入网络的终端的安全状态与使用者身份未知，无法保障终端入网安全可信。此外，企业终端目前缺少有效的安全防护面临着被病毒攻击的隐患。终端失陷后，病毒将在内网横向传播感染更多终端，最终造成企业系统瘫痪、数据遭遇破坏或丢失的后果，企业将蒙受巨大损失。

采用如**图1 园区办公场景**所示的安全园区解决方案即可解决上述问题。

图 5-2 园区办公场景



采用华为乾坤安全办公园区解决方案可以实现：

- 丰富的接入认证方式。基于不同的使用场景，提供多样化的接入认证方式为不同类型的终端用户进行用户身份合法性校验，并针对用户身份给予相应的网络权限。

- 确保入网终端安全可信。已安装EDR Agent的终端资产评分如小于云准入服务中定义的分数，则拒绝该终端接入企业网络。
- 提高终端安全能力。EDR Agent内置防病毒引擎和行为检测引擎，根据全攻击路径检测规则，对终端上的文件和目录进行毫秒级检测，快速判定威胁。

5.1.5 关键特性

表 5-2 华为乾坤安全办公园区解决方案关键特性

特性类型	特性名称	简介
云管理网络	站点管理	支持按站点管理网络，可以查看网络拓扑、调整拓扑结构、配置站点业务。
	设备管理	支持纳管网络设备（交换机、AP、AR、WAC）、安全设备（防火墙）。
	准入认证	提供了802.1X、Portal、MAC等多种认证方式，可按需对接入用户进行策略管控。
	IPsec VPN	提供一种静态VPN，通过在站点之间建立IPsec隧道来创建VPN通道，实现分支与分支、分支与总部、分支与云之间的业务互访。
	网络环境监控	支持网络健康度评估、网络问题分析、无线智能去噪。
	用户体验保障	支持用户旅程回放、协议回放、用户问题分析。
	应用分析	支持全网应用数据监控，保障网络应用畅通无阻。
	智能调优	支持智能无线射频调优、智能无线漫游。
终端防护与响应服务	终端识别与管理	● 终端自动识别：提供自动化终端资产清点能力，安装EDR Agent后，该终端即被自动识别。 ● 资产信息管理：自动化统一管理主机列表、进程、端口、组件等终端资产信息。 ● 终端安全管理：智能分析终端安全，呈现终端资产安全分析评分和风险总览。
	威胁检测与处置	● 入侵检测：基于行为检测引擎，提供终端行为检测能力，检测暴力破解、异常登录、权限提升等恶意行为。 ● 事件聚合：将离散的勒索类告警事件，基于进程调用链聚合成相应的勒索事件，且支持对其一键处置。
	病毒查杀与处置	● 病毒查杀：基于华为第三代反病毒引擎，每日更新病毒特征库，实时更新紧急病毒，提供高质量病毒文件检测能力。 ● 威胁分析：支持对检出的病毒文件进行威胁分析，展示详细的威胁信息，如病毒标识、风险值、置信度等。

特性类型	特性名称	简介
	主动防御	● 诱饵捕获：基于勒索病毒特征放置诱饵文件，实时检测并及时上报异常行为。 ● 文件防篡改：对重点文件进行访问权限控制并实时检测，及时发现篡改行为。 ● 实时防护：实时扫描全盘目录，及时识别病毒文件并阻断其传送行为。
	溯源分析	● 取证分析：采集和存储终端信息，并通过数据挖掘、关联分析等方法，对威胁事件进行取证分析。 ● 攻击可视化：通过EDR（Endpoint Detection and Response，端点侦测与回归）数字化建模、溯源推理算法，实现攻击可视化，精准还原威胁攻击链路。

5.2 部署指南

5.2.1 注册华为乾坤帐号

说明

- 华为乾坤控制台是使用华为乾坤的界面，登录前需要先注册华为乾坤帐号。
- 如果您已有华为乾坤MSP（渠道服务商）创建的租户帐号，可跳过本节内容。

步骤1 访问华为乾坤控制台。

步骤2 在登录页面单击“立即注册”。

根据界面提示完成帐号注册。

----结束

5.2.2 开通服务

前提条件

- 已在配置器SCT上分别购买云管理网络、终端防护与响应服务，具体请联系代理商。
- 已注册华为乾坤帐号，具体操作请参考2.2.1 注册华为乾坤帐号。

操作步骤

请参照如下文档分别开通云管理网络与终端防护与响应服务。

表 5-3 参考文档

子服务	手册名称	具体章节	文档获取
云管理网络	服务开通	“开通线下购买的套餐”	开通线下购买的套餐
终端防护与响应服务	服务开通	“购买与开通服务”	购买与开通服务

5.2.3 快速配置

部署终端防护与响应服务

安全办公园区场景下，终端需要部署终端防护与响应服务，部署步骤请参见。

表 5-4

部署的服务	步骤描述	文档参考
终端防护与响应服务	• 服务授权 • 样本获取授权 • 安装EDR Agent • 查看终端资产	终端防护与响应服务的《部署指南》

部署准入认证

安全办公园区场景下，主要包括三种方式的认证技术：802.1X认证、Portal认证和MAC认证。由于这三种方式的认证原理不同，各自适合的场景也有所差异，实际应用中，可以根据场景部署选一种合适的认证方式，也可以部署几种认证方式组成的混合认证。同时，华为乾坤云管理网络支持联动终端防护与响应服务，实现终端风险动态感知，网络零信任准入。准入认证的部署步骤请参见表5-5。

表 5-5 准入认证的部署步骤

步骤	步骤描述	子服务	文档参考
1	基于不同的场景与需求，选用合适的准入认证方式。	云管理网络	云管理网络的《网络部署》中“准入认证”的如下几个章节。 ● 准入认证介绍 ● 用户准入认证配置指南
2	联动终端防护与响应服务，实现终端风险动态感知，网络零信任准入。	云管理网络	云管理网络的《网络部署》中“准入认证”的联动EDR感知终端安全态势章节。

5.2.4 日常操作

您可以参考如下文档使用安全办公园区解决方案。

表 5-6 参考文档

子服务	手册名称	文档内容简介	文档获取
云管理网络	用户指南	介绍如何使用云管理网络。	《网络运维》
终端防护与响应服务	用户指南	介绍如何使用终端防护与响应服务。	《用户指南》