城轨云安全白皮书

文档版本 1.0

发布日期 2021-12-30

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。

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

前言

作为交通强国，城轨数字化跟随我国城轨交通的发展而发展，伴随着世界信息技术的演进而演进，城轨数字化在整个轨道交通系统的建设中发挥着不可或缺的作用。但城轨数字化建设面临着顶层设计缺乏、系统架构陈旧、信息孤岛严重、安全基础薄弱、标准规范缺失等诸多不适应交通强国战略实施的严峻挑战。2016年初，中国城市轨道交通协会专家深刻分析了国内外城轨交通的现状及信息技术发展趋势，率先提出了实现我国城轨数字化建设的“13531”发展蓝图，正式开启了城轨云的新征程。

数字化时代也是网络安全事件频发的时代。城市轨道安全关系民生，加快推动轨道交通系统的安全建设势在必行。近年来，国家不断通过法律法规及相关政策的出台，持续推动城市轨道交通系统安全体系的建设。因此，构建智能、有效、合规的城轨云解决方案是城轨行业数字化发展的必然趋势，而解决方案的安全考量就成了其健康发展和有序建设的重中之重。

为了将华为对城市轨道行业网络安全的思考与建设经验分享给业界，华为特推出《城轨云安全白皮书》（简称“白皮书”），向业界推广其安全管理框架，以求相互了解与借鉴，共同推动城轨行业的开放与发展。

本白皮书面向城轨行业的广大读者群，致力于帮助客户了解城轨行业上云的必然趋势，同时提供上云过程以及云上运营时的安全指导，辅助城轨客户创造一个高效、安全的云环境。

目 录

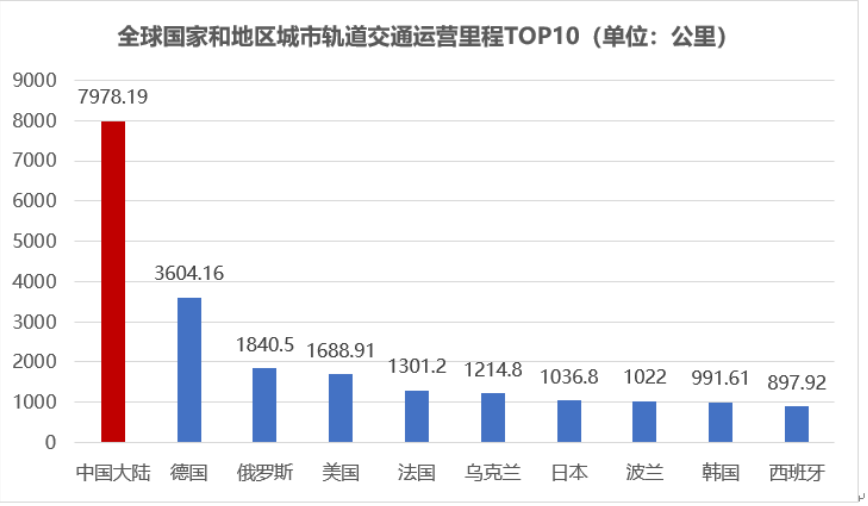
1 以城轨云为新起点，开启智慧城轨建设

1.1 智慧城市轨道是未来发展的大趋势

- **中国城轨已开通的运营里程数世界领先**

  截至2020年底，全球共有77个国家和地区的538座城市开通城市轨道交通，运营里程达到33346.37公里。其中，中国大陆地区（不含港澳台）以7978.19公里的总运营里程排名全球第一。

图 1-1 全球国家和地区城市轨道交通运营里程 TOP10

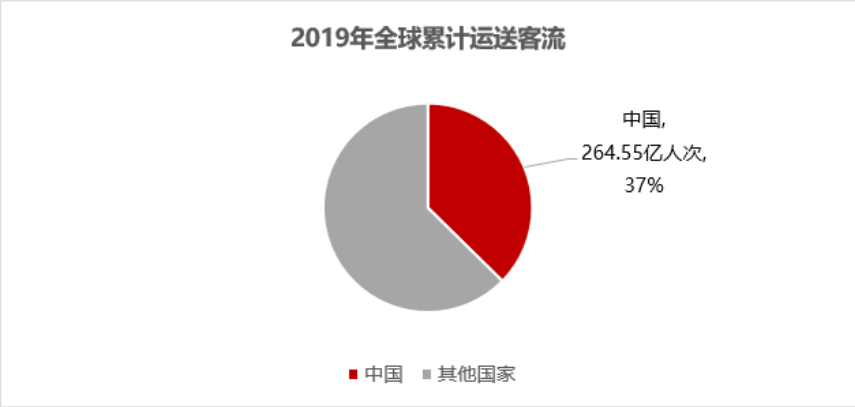


资料来源：《都市快轨交通》前瞻产业研究院

- **中国累计客运量世界领先**

  根据中国城市轨道交通协会和维基百科的客流数据统计和计算，2019年，全球地铁和轻轨累计运送客流707.94亿人次，其中中国（含港澳台）以264.55亿人次的总客运量居全球首位。

图 1-2 2019 年全球累计运送客流



资料来源：《2020年世界城市轨道交通运营统计与分析综述》

中国城轨的运营里程和累计客运量均已处于世界领先地位，随着中国城市轨道规模的持续扩大，城市轨道急需通过数字化转型来提高效率、降低成本。同时，国家“十四五”规划提出了要加快城市轨道交通的数字化升级革新，并且相继出台了《交通强国建设纲要》《数字交通发展规划纲要》等系列文件，为城市轨道交通的数字化转型保驾护航。

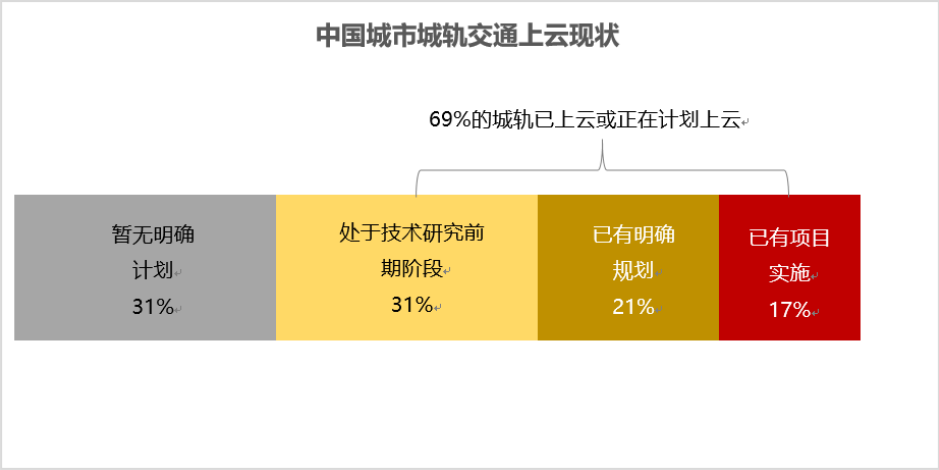
1.2 城轨云成为智慧城轨的支撑平台

2016年初，中国城市轨道交通协会专家深刻分析了国内外城市轨道交通的现状及信息技术发展的趋势，率先提出了实现我国城轨信息化建设的“13531”发展蓝图，即打造1个门户（智慧地铁的门户网站），构建3个中心（生产/应急指挥中心、乘客服务中心和企业管理中心），拓展5个领域（运营生产、运营管理、企业管理、建设管理和资源管理），依托3张网络（安全生产网、内部服务网和外部服务网），搭建1个平台（城市轨道交通云平台）。随着“13531”蓝图的发展，正式开启城轨云应用的新征程。

- **国内各城市城轨上云现状**

  RT轨道交通于2020年对中国42座城市轨道交通运营商展开大规模调研活动。根据调研结果显示，目前国内参与调研的城轨中，有69%的城轨已上云或正在计划上云。

图 1-3 中国城市城轨交通上云现状



资料来源：《 2020年中国城轨云应用现状和发展调研报告 》

城轨云是城市轨道交通未来的发展方向，中国轨道交通系统的建设进程也将随着发展全面步入数字化时代。

2 构建完善的网络安全体系成为推进智慧城轨建设的基石

2.1 智慧城轨转型面临的网络安全挑战

近年来，伴随着城市轨道交通的持续发展，国内城市轨道交通信息化程度不断攀升。随着信息化与轨道交通自动化的深度融合，轨道交通自动化与控制网络也向着分布式、智能化的方向迅速发展，越来越多基于TCP/IP的通信协议和接口被采用，实现了各子系统的互联互通、资源共享，进一步提升了自动化水平。城市轨道交通信息系统的集成化、智能化程度越来越高，业务运行过程对信息系统的依赖性日益增强，因此，轨道交通业务面临的网络安全挑战也变得越来越大。

近年来全球各地轨道交通网络安全事件频繁发生，包括：

- **波兰（2008）：罗兹市有轨电车运营调度系统入侵事件**

2008年1月14日，14岁黑客侵入波兰罗兹市有轨电车运营调度系统，并利用遥控装置改变数辆有轨电车的行驶方向。此举不但导致被操纵电车的候补车厢脱轨，还导致12名乘客受伤，所幸此次事件没用造成人员伤亡。

- **美国（2016）：旧金山市政地铁系统感染勒索软件**

2016年11月25日，旧金山系统遭受攻击，售票系统屏幕显示“你们被黑了，数据都在我们手上，想要恢复正常，就联系XXXXX吧。“ 导致自动售票机被迫关闭，旅客在周六可以免费乘坐轻轨。

- **英国（2020）：地铁营销系统遭受网络钓鱼攻击事件**

2020年12月，英国地铁公司证实了其营销系统被黑客攻击，该系统被用来向客户发送钓鱼信息。英国地铁公司的客户收到了来自“Subcard”的电子邮件，内容是处理所谓的地铁订单，其中包括一个恶意链接，需要客户确认订单信息。通过该恶意链接，导致很多客户的姓名被泄露。

- **加拿大（2020）：温哥华公共交通机构TransLink遭勒索软件Egregor攻击**

2020年12月，加拿大温哥华市公共交通机构TransLink遭勒索软件Egregor攻击，导致温哥华居民无法使用Compass地铁卡，也无法使用售票亭购买的车票。导致TransLink长达两天的运营瘫痪。

城市轨道交通系统每天承载上千万人的出行，一旦出现网络安全事故将直接影响人民的正常生活，造成的损失不可估量。因此，需要高度重视城市轨道交通的网络安全风

险。但由于城市轨道交通在早期建设中缺乏网络安全体系化规划，随着信息化建设的飞速发展，严重落后的安全防护能力为行业的发展带来隐患。因此，在智慧转型过程中通过构建完善的城市轨道系统网络安全体系以提升网络安全能力迫在眉睫。

2.2 政策推动轨道交通网络安全体系建设提速

近年来，国家政府和各级管理单位高度重视城市轨道交通行业面临的网络安全问题，相继出台一系列的网络安全管理和保障政策，推动安全体系的建设。

- 2016年，工信部发布《工业控制系统信息安全防护指南》，以推动全国工控系统安全体系建设。
- 2017年，《中华人民共和国网络安全法》正式施行，关键信息基础设施的运行安全受到法律保护。
- 2017年7月，国家互联网信息办公室发布《关键信息基础设施安全保护条例（征求意见稿）》，该条例明确将交通行业列入关键信息基础设施保护范畴。
- 2019年，公安部发布《信息安全技术网络安全等级保护基本要求》，以加强通用信息系统安全防护体系的建设。
- 2020年，城轨协会发布《城市轨道交通云平台网络安全技术规范》《智慧城市轨道交通信息技术架构及网络安全规范》和《中国城市轨道交通智慧城轨发展纲要》，以推进城市轨道交通安全防护体系的建设。

《中国城市轨道交通智慧城轨发展纲要》作为城轨行业下一时期（2020年-2035年）“智慧城轨”发展的技术政策、技术规范、发展规划和实施计划的指导性文件，提出城轨行业从业者需贯彻“系统自保、平台统保、边界防护、等保达标、安全确保”的策略，系统地采用可信安全与智能协同的技术，同步规划城轨云、同步建设网络安全纵深防护体系，保障城轨云持续稳定运行，建立自主可控的城轨云平台，构建网络安全纵深防护体系，建成适应云平台体系架构的运行维护体系和运行管理机制。

2.3 构建城市轨道交通网络安全体系需解决的问题

由于城市轨道交通行业的特殊性以及传统烟囱式的专网建设形式，导致城规行业在构建城市轨道交通网络安全体系时面临巨大挑战。

- 分支多，管理难

  轨道交通的安全建设涉及线路、车站、车辆段等多分支，应用系统维护管理分散，难以统一管理和自动升级维护。
- 安全弱，不生效

  安全设备购买后未正确配置，导致设备旁落或透明转发，无法阻断和隔离威胁，信息安全监管缺乏，以台账式管理为主。
- 资产多，看不清

  城轨行业部门庞杂、供应商繁多，导致不同业务系统、不同线路、不同车辆段的PC终端、哑终端、摄像头终端等海量设备无法集中管控，实现统一准入管理。
- 传播快，防不住

  城规行业可能面临大量勒索病毒和挖矿病毒的威胁，一旦感染，蔓延迅速，影响多条线路的多个系统，导致业务中断。

3 城轨云解决方案助力客户构建网络安全体系

3.1 城轨云采用多层次纵深安全防御体系，以实现城轨云解决方案的安全合规

城轨云解决方案是以等级保护为基本要求，以《城市轨道交通云平台网络安全技术规范》为建设指引，同时结合城市轨道交通的网络安全管理现状，构建一套合规、协同、智能且有效的解决方案，以有效支撑轨道交通行业智慧转型。

图 3-1 城轨云解决方案总体架构

- **等级保护，安全能力合规化**

  等保方案保障建设的基本思路是：严格参考等级保护的标准和思路，对现状进行分析，对发现的问题进行加固改造。在设计阶段时，参考《信息系统等级保护安全设计技术要求》，从安全计算环境、安全区域边界、安全通信网络和安全管理中心等方面落实安全保护技术要求，建立“可信、可控、可管”的安全防护体系，使得系统能够按照预期运行，免受网络攻击和破坏。建成后的安全保障体系将符合国家等级保护标准，能够为城市轨道交通系统稳定运行提供有力保障。城轨云安全架构从云平台统一承载业务和安全部署设计方案统筹考虑，对所有业务系统提供满足等保2.0三级要求的系统环境。

- **多维联动，安全能力协同化**

基于等保合规的云平台，结合城市轨道交通行业安全现状及需求，构建网安协同、端安协同、云安协同的多维协同安全体系，通过联动方案强化各个安全设备之间的协同性，提升安全防护效率，扩大安全防护能力，使不同维度的安全能力形成纵深协同的安全能力，实现真正有效实用的城市轨道交通系统的安全防护体系。

- **智能运营，安全能力智能化**

  城市轨道交通系统线路多而复杂，安全设备部署分散，对安全运维管理带来挑战。为提升城轨云客户安全运维的能力，华为为客户提供统一安全运营平台。该平台与威胁事件的识别、防御、检测、响应、恢复等安全环节进行联动，构建端到端的安全运维体系，提升安全运营的智能化水平。

- **纵深防御，安全能力有效化**

  城轨云解决方案为城轨客户的通信网络、区域边界、计算环境，综合采用访问控制、入侵防御、恶意代码检测、安全审计、防病毒、传输加密、数据备份等多种技术和措施，实现业务应用的可用性、完整性和保密性，实现综合的安全管理能力。同时充分考虑各种技术的组合和功能的互补性，合理利用措施，从外到内形成一个纵深的安全防御体系，保障系统整体的安全能力。

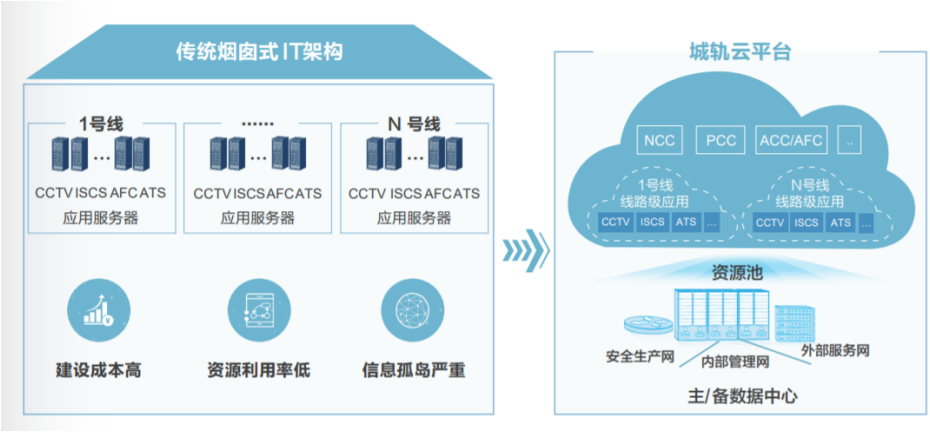
3.2 城轨云解决方案点对点解决客户诉求

- **分支多，管理难**

  轨道交通的安全建设涉及线路、车站、车辆段等多分支，应用系统维护管理分散，难以统一管理和自动升级维护。

为解决城轨行业存在的上述问题，城轨云平台统一承载了ISCS（综合监控系统）、AFC（自动售检票系统）、PIS（乘客信息系统）、ATS（信号监控系统）和CCTV（综合安防系统）等多应用系统，突破当前城轨业务系统的烟囱式发展，整合平台、融合资源，实现运营全局化与业务协同化、数据和业务标准化与归一化、资源和架构统一化与平台化，真正实现资源共享，按需调配，弹性扩展，助力客户实现从线路运营向线网运营的转变。

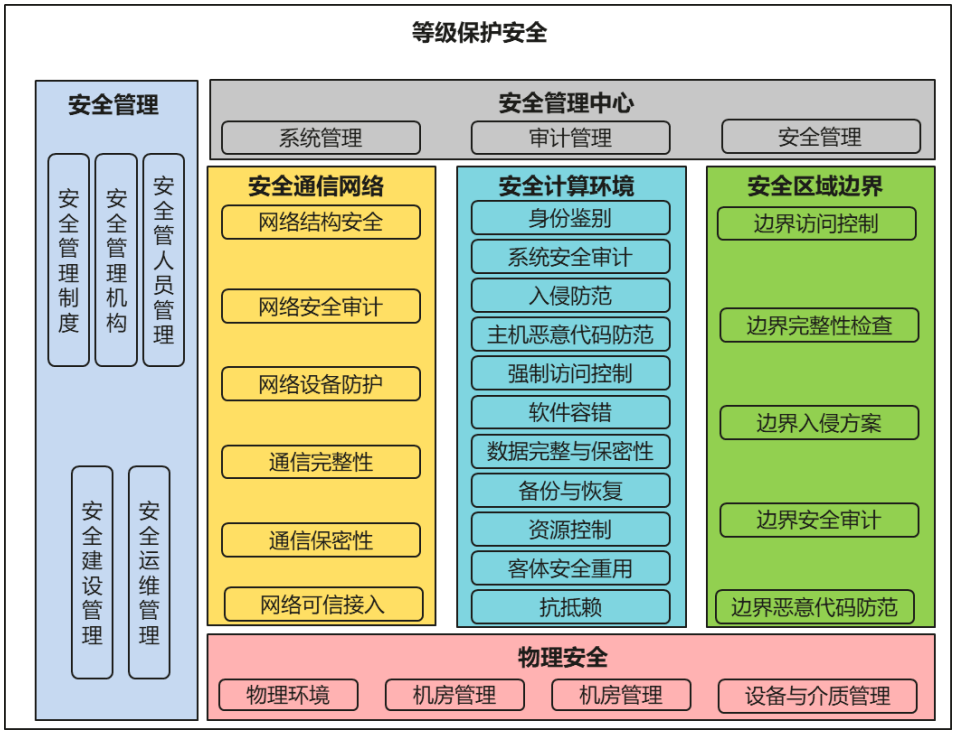
图 3-2 城轨云平台助力客户实现从线路运营向线网运营转变



同时，华为依据《信息系统等级保护安全设计技术要求》，从通信网络安全、计算环境安全、区域边界安全、安全管理平台及安全管理五个领域出发，设计城轨云平台的安全能力，从而为城轨客户提供满足等保2.0三级要求的云平台。

在此基础上，城轨客户可按照等保2.0的要求构建其内部统一的安全管理体系，统一管理线路、车站、车辆段等多分支及相关应用系统，解决“分支多，管理难”的问题。

图 3-3 等保 2.0 管理体系

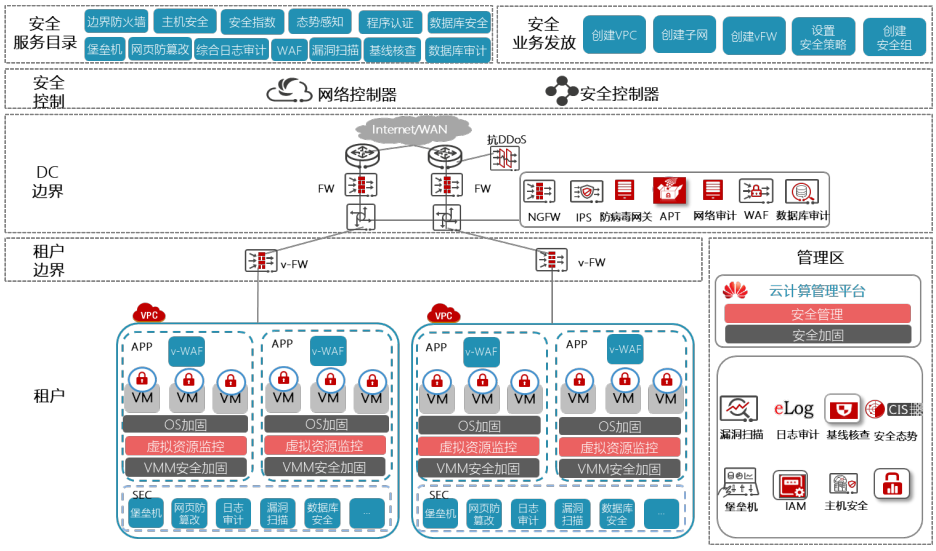


- **安全弱，不生效**

  安全设备购买后未正确配置，导致设备旁落或透明转发，无法阻断和隔离威胁，信息安全监管缺乏，以台账式管理为主。

为解决城轨行业存在的上述问题，城轨云解决方案依据《信息系统等级保护安全设计技术要求》，搭建城轨云的技术框架，为城轨客户按照等保2.0的要求建立其内部统一的安全管理体系提供基础。

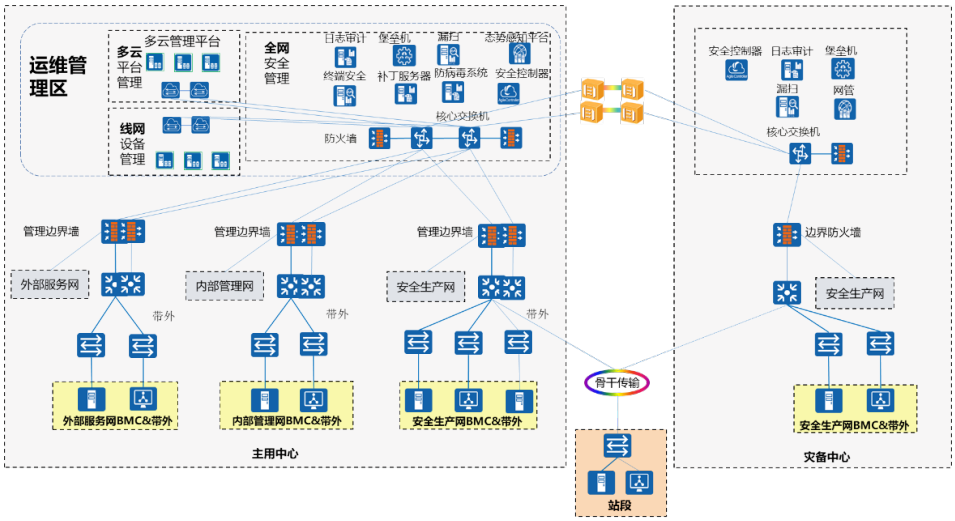
图 3-4 云等保方案技术要求框架



在设计城轨云解决方案整体的安全架构时，华为充分考虑了城规业务的管理现状，将安全管理中心的设计融入到整体的解决方案，并作为整体解决方案的核心，承接整体

业务的安全分析、安全审计、安全运维管理等功能，为城轨客户提供资产可视化的风险管理能力，有效解决“安全弱，不生效”的问题。

图 3-5 安全管理中心设计示意图



1. 统一系统管理

城轨云解决方案提供了一套全面的网络运维管理系统（eSight设备），帮助城轨客户实现集中统一管理，对系统的资源和运行进行配置和管控，包括：用户统一身份管理、系统资源配置与监控、系统运行异常监控等。

2. 集中审计管理

城轨云解决方案集成了统一的安全审计、日志审计、主机安全审计等安全服务功能。通过部署日志审计系统对分布在系统各个组成部分的安全审计机制进行集中管理，包括：根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等；对安全审计员进行严格的身份鉴别，并只允许其通过特定的命令或界面进行安全审计操作。具体的集中审计内容包括：日志监控、日志管理、审计分析等。

3. 统一漏洞扫描

城轨云平台部署了漏洞扫描系统，通过扫描等手段对指定的虚拟机或者物理机系统的安全脆弱性进行检测，发现可利用的漏洞的一种安全检测（渗透攻击）行为，并提供及时的安全防护。漏洞扫描系统和防火墙、入侵检测系统互相配合，通过对网络的扫描，平台管理员能了解平台的安全设置和运行的应用服务，及时发现安全弱点，客观评估网络风险等级。平台管理员能根据扫描的结果更正网络安全弱点和系统中的错误设置，在黑客攻击前进行防范。

4. 安全检测设计

城轨云解决方案中对安全监测也进行了考虑和设计，其中包括部署在安全管理中心的态势感知平台（Hisec Insight）、安全控制器、漏洞扫描系统、日志审计、堡垒机等，以帮助城轨客户能够有效应对可能的安全威胁。

- **资产多，看不清**

  城轨行业部门庞杂、供应商繁多，导致不同业务系统、不同线路、不同车辆段的PC终端、哑终端、摄像头终端等海量设备无法集中管控，实现统一准入管理。

为解决城轨行业存在的上述问题，城轨云解决方案融入了统一安全运营中心，可对城轨客户的云上、云下业务系统进行统一安全运营管理。

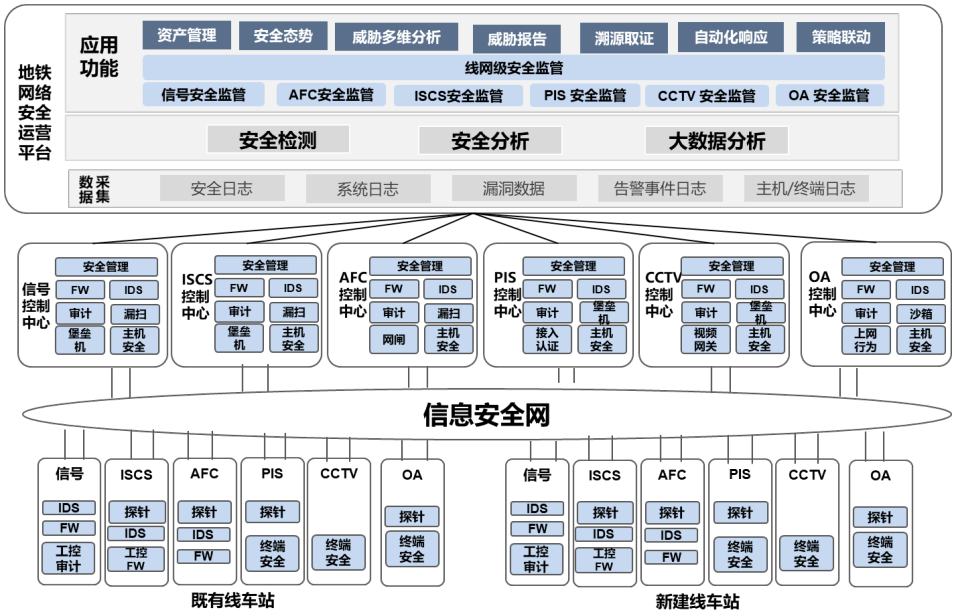
1. 线网级运营平台

接收来自各专业系统的资产信息、漏洞信息、威胁信息，进行全网统一态势感知及关联分析，发现高危威胁后全网通报预警，并自动下载外网最新补丁、知识库，供全网下载更新。

2. 专业级运营平台

结合不同的专业系统、应用场景，设置对应的关联规则，实现个性化、定制化的安全防护，结合通用系统安全，优化网络安全配置，实现策略联动、网安协同。

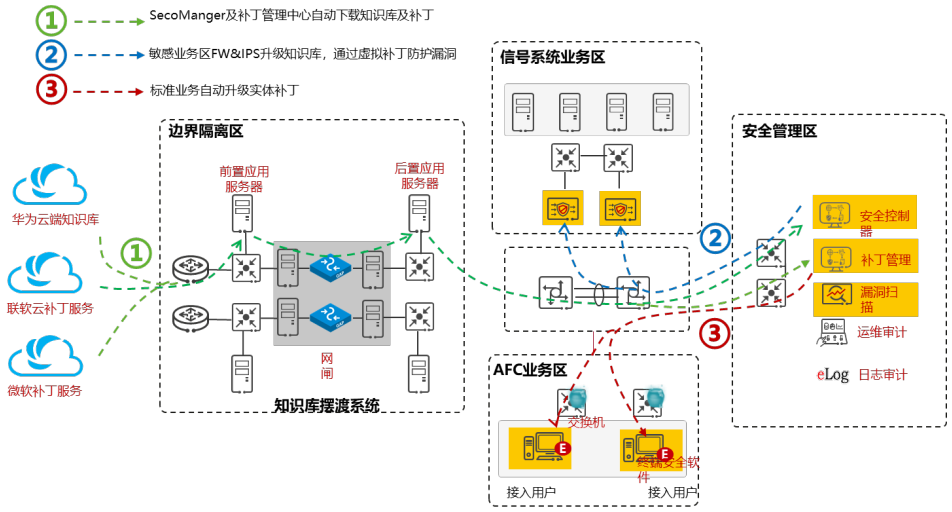
图 3-6 统一安全运营平台方案设计及部署规划



统一安全运营中心可以实现零运维、免安装补丁的优势，从而在确保安全的同时，还能尽可能的减少城轨客户的人力成本。

- 零运维：知识库和补丁的下载、摆渡（外网到内网）、升级等操作全部实现自动化，简化运维，避免误操作。
- 免安装（补丁）：虚拟补丁方案场景可以不用安装实体补丁，从网络层面有效阻断漏洞被利用的渠道。

图 3-7 统一安全运营平台应用场景示例

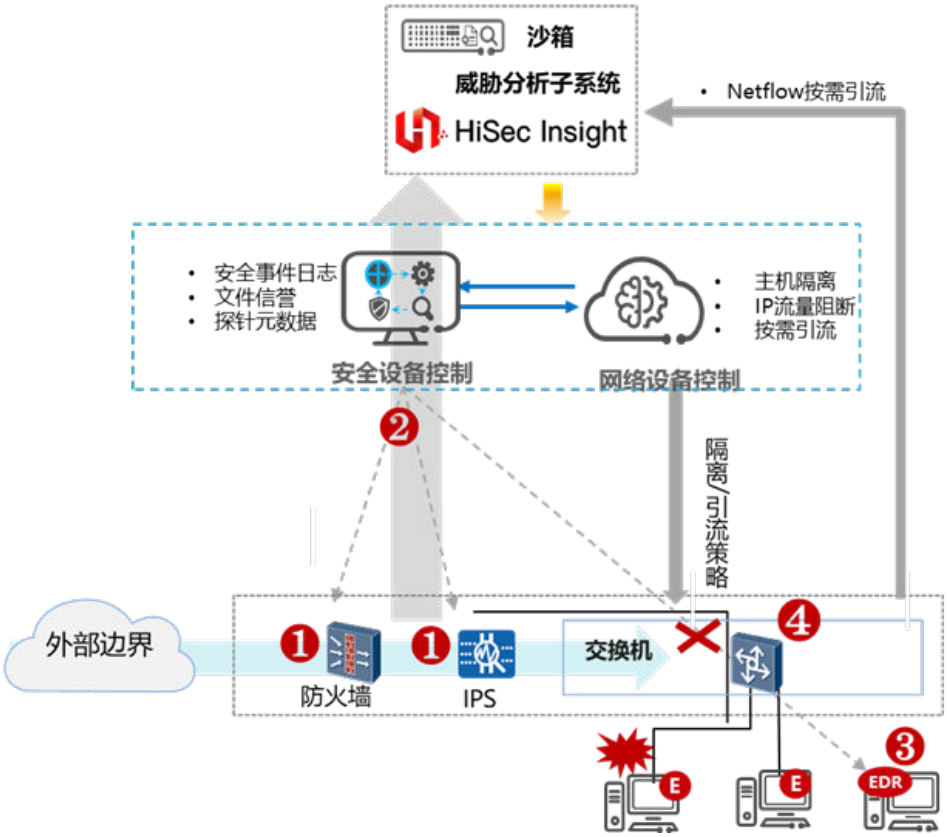


- **传播快，防不住**

  城规行业可能面临大量勒索病毒和挖矿病毒的威胁，一旦感染，蔓延迅速，影响多条线路的多个系统，导致业务中断。

为解决城轨行业存在的上述问题，城轨云解决方案基于“网络安全联动防护，威胁自动处置闭环”为原则，通过基础防御、联动防御、终端防御，层层设防，抵御来自外部的威胁。

图 3-8 网络安全联动防御体系



1. 基础防御：边界安全设备提前预设安全策略，实现已知威胁防御和隔离。
2. 联动防御：安全分析子系统联动安全设备，动态ACL策略进行新增威胁拦截。
3. 终端防御：终端检测响应EDR在主机内检测异常行为，与安全分析子系统联动终端EDR进行隔离、删除、进程杀灭或阻断。

4 华为提供多方位安全服务，协助客户推动安全能力建设

4.1 等保 2.0 咨询服务

《智慧城市轨道交通信息技术架构及网络安全规范》-“第三部分：网络安全”明确要求安全生产网中部署的系统应达到等保2.0三级，内部管理网的系统应达到等保2.0二级。城轨云解决方案的安全架构从云平台统一承载业务和安全部署设计方案统筹考虑，对承载在云平台上的业务系统统一提供满足等保2.0三级要求的底层安全环境，并为核心业务系统提供遵从等保要求的设计方案。

此外，华为的等保2.0合规方案可协助城轨客户的业务系统在城轨云上实现等保2.0合规。该方案为城轨客户提供全栈的安全防护体系和丰富的安全服务，帮助客户高质量满足等级保护要求。关于等保2.0咨询服务的详情，请参见“**等保合规安全解决方案**”页面，同时该页面提供等保合规2.0白皮书下载的链接，客户可自行下载，提前针对等保2.0要求进行自评估。

4.2 管理检测与响应服务

华为根据其30年安全经验的积累，致力于协助城轨客户建立由管理、技术与运维组成的安全风险管控体系。通过云服务的方式，帮助城轨客户实现对安全风险与安全事件的监控，及时采取有效措施降低安全风险，减少安全事件带来的损失，同时结合城轨客户反馈的安全需求对用户安全防护进行持续改进。城轨客户可选择的管理检测与响应服务包括：

- 安全方案设计服务：结合用户云上业务，量身定制云安全体系，输出安全解决方案。
- 安全检查服务：协助客户制订安全防护体系，包括安全服务的规格、数量、策略。
- 安全加固服务：对虚拟服务器进行全面安全基线加固，指导用户根据渗透测试结果进行Web应用加固。
- 应急响应服务：对安全事件进行应急处理，帮助客户快速恢复业务并进行溯源。
- 安全监控服务：对服务器进行7*24小时安全响应，及时发现潜在威胁。

- 安全防护服务：根据用户业务，组合安全产品进行防护，帮助用户达到最大的防御效果。

5 结语

华为公司始终秉持着“以客户为中心”的核心价值观，为此华为向企业提供了城轨云安全解决方案，以帮助客户构建完善的云上安全体系，同时，华为致力于与相关组织共同研究和探讨城轨安全的发展方向，打造一个开放、协作、共赢的城轨云安全生态圈，不遗余力地推动行业和社会进步。