公路交通行业云网端一体化安全技术白皮书

编写单位

交通运输部公路科学研究院
中国公路学会交通工程与信息化分会
云南省交通投资建设集团有限公司
云南省交通规划设计研究院股份有限公司
云南省交通科学研究院有限公司
中国公路工程咨询集团有限公司
北京交科公路勘察设计研究院
华为技术有限公司

主编

汪　林、杨春晖、孙秀珍、沈素荣、马　烨、盛　刚

编委会

李振华、杨　童、刘见振、程　剑、文慧智、吕　亮、王国钰、
许智宇、徐旭晶、董方朔、金黎阳、鲁玉春、刘钦鹏、李武东、
杨帅锋、田永强、周　倩

参编人员（排名不分先后）

齐志峰、杨　渝、吕敬富、熊　涛、龚万江、郑　毅、向鹏程、
罗　方、高玉慧、刘惠兴、房　锐、钟　铖、鲍学俊、李　浩、
陈志涛、张开文、和永军、马　聪、张　翔、孙宏贤、李承武、
孙瑞玮、沈　超、李照彬、何培舟、陈佐豪、曹　猛、杨晓寒、
刘丙双、敖日格勒、陈伟玮、王萍萍、刘迟时、欧家成、白瑞思蒙、
刘楠辉、赵　亮、欧阳腊青、郑铁钧、彭　阳、李新元、陶　金

编写单位

交通运输部公路科学研究院
中国公路学会交通工程与信息化分会
云南省交通投资建设集团有限公司
云南省交通规划设计研究院股份有限公司
云南省交通科学研究院有限公司
中国公路工程咨询集团有限公司
北京交科公路勘察设计研究院
华为技术有限公司

目录 / Contents

前言

2019 年 9 月、2021 年 2 月，党中央、国务院先后印发《交通强国建设纲要》《国家综合立体交通网规划纲要》，提出构建安全、便捷、高效、绿色、经济的现代化综合交通体系。截止 2022 年年底，全国国道公路里程 37.95 万公里，省道公路里程 39.36 万公里，高速公路里程 17.73 万公里，稳居世界第一。

随着公路数字化转型逐步加快，路网化、数字化和智能化逐步成为高速公路基础设施建设目标。交通运输部陆续发布了《高速公路联网收费系统优化升级工程方案（全网征求意见稿）》《全国高速公路视频监测优化提升实施方案》，全国联网收费、视频云联网共享等带来了新的安全要求，同时全国高速公路运营单位众多，信息安全管理人员配备不齐，对于如何保障网络信息安全，提出了更大的挑战。

2023 年 4 月交通运输部发布《公路水路关键信息基础设施安全保护管理办法》，同年 6 月 1 日正式要求实施执行，压实了公路运营者主体责任，要求建立公路关键信息基础设施网络安全体系，提升信息安全防护水平。

基于国家产业方针、标准规范及法律法规要求，在交通运输部公路科学研究院、中国公路学会交通工程与信息化分会的指导下，云南省交通投资建设集团有限公司、云南省交通规划设计研究院股份有限公司、云南省交通科学研究院有限公司联合中国公路工程咨询集团有限公司、北京交科公路勘察设计研究院及华为技术有限公司联合创新、在科技赋能行动方案中开始了公路信息安全的相关创新探索，结合公路业务生产、管理、服务等业务应用，涵盖了云平台、网络、安全、终端等产品，探讨云、网、端协同防护、安全智能运营等场景。本白皮书结合高速公路的安全现状，在遵循交通运输部及行业相关的安全规范基础上，提出了云网端一体化安全的网络信息安全理念，基于“智能分析、动态检测、全局防御”的基本原则，打破传统静态、被动、单点的安全防护思路，打造一体化安全体系，实现风险持续检测、威胁主动研判，智能全局防控。希冀本白皮书能为公路信息安全体系建设提供借鉴和参考。

01

公路交通建设发展趋势及安全建设的必要

公路交通建设发展趋势：数字化、网络化、智能化

在高速公路路网化发展过程中，信息系统承担着重要的地位。当前，全国高速公路已形成通信、监控、收费三大机电系统，及隧道机电工程（供电、通风、照明、消防等）。高速公路从信息化、到数字化、智慧化的不断演进发展，是道路承载力、通行能力提升的关键要素。以服务交通运输高质量发展为目标，聚焦智慧物流、智慧出行，以及设施设备数字化、智能化、自动驾驶与车路协同等需求，智慧高速逐步成为未来高速公路发展方向。

当前我国高速公路已从“建设为主”阶段向“建设、养护、管理、服务、安全五位并举”阶段转变。根据交通运输部发布的《交通运输部关于推进公路数字化转型加快智慧公路建设发展的意见》，到 2027 年，公路数字化转型取得明显进展。构建公路设计、施工、养护、运营等“一套模型、一套数据”，实现全生命期数字化。建成“部省站三级监测调度”体系，公路运行效能、服务水平和保通保畅能力全面提升，打造公路出行服务新模式，提升公众满意度。公路市场数据资源充分整合，提升公路领域市场服务和治理能力。建立健全适应数字化的公路标准体系，在国家综合交通运输信息平台架构下，完善公路基础数据库，形成公路数字化支撑保障和安全防护体系。

同时提升公路数字化基础支撑水平，建设完善公路基础数据库。依托国家综合交通运输信息平台部省联动建设，整合公路领域各类既有重点业务信息系统，依托建设与养护数字化，逐步完善公路基础数据库，支撑国家综合交通运输信息平台调度指挥、运行监测、政务服务等功能，全面提升公路服务和管理数字化水平。全面推广公路大数据技术应用。强化公路大数据共建共享、深度融合应用，加快构建与完善相关应用模型和专业算法，发挥数据潜能，强化数据分析、信息提炼、智能深度学习、智慧交互等功能，有力支撑公路数字化转型和产业化升级，壮大公路数字经济。

01 公路交通建设发展趋势及安全建设的必要

在 2023 年 10 月，交通运输部发布《公路工程设施支持自动驾驶技术指南》，推动自动驾驶和智慧公路发展。其中自动驾驶不是狭义的无人驾驶，是车辆以自动的方式持续地执行部分或全部动态驾驶任务的行为，也可称为驾驶自动化。运用自动驾驶技术，以及辅助驾驶技术和公路本身的智能化的交通工程技术的结合，将加大车与路协调融合，对未来自动驾驶和智慧公路技术发展发挥积极作用。《公路工程设施支持自动驾驶技术指南》采用了**“端 - 边 - 云”**相结合的技术架构，建立了公路工程设施支持自动驾驶的技术体系。通过“边”的信息处理与交互，形成边缘云与中心云，分别为路段级、省（区域）级、部（全国）级管理平台提供数据支撑。

在交通运输部印发的《数字交通“十四五”发展规划》中，以数字化、网络化、智能化为主线，以改革创新为根本动力，提出了“交通设施数字感知，信息网络广泛覆盖，运输服务便捷智能，行业治理在线协同，技术应用创新活跃，网络安全保障有力”的六个目标。其中针对网络安全，围绕全链条、全要素、全周期，构建事前防范、监测预警、应急处置三位一体的网络安全防护体系。

与此同时，进入数字经济时代以来，算力成为推动各行业数字化转型，赋能经济蓬勃发展的重要引擎，同时也成为衡量国家综合实力的重要指标之一。随着以 ChatGPT、GPT4 为代表的 AI 大模型的发布，迅速掀起了新一轮人工智能技术的发展浪潮。交通行业把握人工智能技术快速发展的机遇，探索交通大模型研究，提升业务支撑辅助能力，发挥信息资源价值，成为数字化转型的关键能力，同时借助大数据模型可以有帮助安全运维人员有效提升运维效率，降低复杂度，让安全运维效果得到卓著的改善和提升。

公路交通面临的网络安全威胁及挑战

公路交通全面推进数字化转型，云计算和大数据平台在各省交投集团核心业务应用中实施和落地，信息安全问题成为高速公路数字化、智能化发展中的关键点。

近年来，随着国际局势的动荡复杂，网络安全环境愈发严峻，各类攻击事件频发，对关键信息基础设施，公共信息资源以及个人隐私数据都造成了不同程度的危害，如果信息安全防护不当，导致关键信息基础设施被攻击和勒索，可能造成信息泄露或业务系统中断。

- 2020 年，法国某装箱船和供应船运营商遭受 Ragnar Locker 勒索软件攻击，导致其全球货运集装箱预订系统被迫下线。
- 2021 年 5 月，美国某成品油管道运营商遭勒索病毒攻击，旗下承载着美国东海岸近 45% 供油量的输油干线被迫关闭数日，造成巨大损失。
- 2023 年，西北工业大学被境外政府背景黑客长期持续攻击的事件发生，科研成果存在泄露风险。
- 2023 年 4 月，德国某药物研发巨头遭受网络攻击，不得不临时断开了与互联网的连接，避免其 IT 系统遭到入侵。
- 2023 年 7 月，武汉市公安局江汉分局发布警情通报：该中心发现部分地震速报数据前端台站采集点网络设备被植入后门程序。该行为对国家安全构成严重威胁。

- 2023 年 8 月，南昌某高校未采取技术措施保障数据安全，未履行数据安全保护义务。导致 3 万余条师生个人敏感数据被黑客窃取并非法兜售，被罚款 80 万元。
- 2023 年 11 月，OpenAI 开发者大会闭幕不久，遭黑客组织 DDoS 攻击，多次发生严重的业务中断，给依赖该公共大语言模型的开发者、创业公司、企业和用户敲响了警钟。

随着行业数字化转型的快速发展，云、大数据、物联网和移动互联网等 ICT 技术的普及和应用，给各省高速运营业主带来了前所未有的新体验，但是也引入了新的安全问题。近年来，外部 APT（Advanced Persistent Threat，高级持续性威胁）攻击和企业内部违规导致的大规模数据泄露等恶性事件层出不穷。

结合高速公路行业特点，经过调研和交流，目前高速公路行业在数字化转型过程中面临的主要安全风险如下：

- **高速公路管理单位多，层级复杂，权限管控和管理难**

  高速公路收费系统、监控系统自上而下是互联互通的，从部联网中心、省联网中心、省交投集团总部、地市管理处和运营路段分公司，涉及人员众多，层级复杂，身份繁杂且应用权限众多，这对网络安全区域划分和安全防护都提出了较高要求。一旦某个节点发生安全事件，很容易通过网络攻击其他系统，如何快速应急响应，各个层级如何协同管理是公路信息化建设过程中必然面临的问题。

  在《高速公路联网收费系统优化升级方案（征求意见稿）》中，明确提出“提升态势感知能力”，提升预警监测和应急处置机制技术支撑能力。实现态势感知对部联网中心、省联网中心、ETC 发行、客服、区域 / 路段、收费站、ETC 门架系统全面覆盖，实现全网网络安全事件响应、工单流程处置和管理信息反馈等方面工作闭环。

- **业务系统多，网络复杂，同时互联网、第三方网络互访需求，安全边界防护责任重大**

  随着城市发展，高速公路逐步提供出行服务。ETC 发行，客服系统和视频云联网等业务应用，大量业务暴露在互联网侧。由于公路网络覆盖方位广，收费网、视频网、隧道机电网、办公等多张业务网络，同时公路网络与互联网以及其他第三方相关机构存在访问需求，需要防护的边界多，安全围栏需要严防死守，一旦被攻破，安全风险跨网传播，可能影响整个公路业务的运营。

  2022 年 10 月，交通运输部路网监测与应急处置中心发布《联网收费系统网络分区分域管理指南（试行）》，要求各级收费网络管理部门，根据收费联网收费系统的网络业务和系统服务的重要性和受损影响，合理划分网络安全区域，并通过有效技术措施对安全区域进行隔离，综合运用互补的安全措施，确保安全控制策略有效、安全风险影响范围最小，从而构建从外到内的网络安全纵深防御体系。

- **资产众多，海量终端接入，规模愈来愈大，端侧设备难以管理和防护**

  公路业务需要通过大量物联设备采集和处理数据，如摄像头、情报板、传感器、ETC 雷达、抬杆机等，这些物联设备都实现了 IP 化并接入到公路视频监控网络及收费网络中，由于数量庞大，且部署位置多为户外，其安全风险相对数据中心的设备更高，其运维和防护更困难，一旦漏洞或风险被攻击者利用，可能导致数据被非法获取，甚至将这些设备作为跳板进一步攻击到数据中心，给公路业务带来风险和隐患。

01 公路交通建设发展趋势及安全建设的必要

在 2023 年《全国高速公路视频监测优化提升实施方案》中明确提出，加密布设视频点位，高速公路主线视频点位间距原则上不大于每 2 公里 1 对，收费广场、服务设施（含服务区、停车区）应提供覆盖广场整体场区的视频图像。同时要求加强安全管理，对本区域视频云平台、监测设施、网络传输等工作加强安全管理，按照有关规定开展系统等保测评等工作。

同年，交通运输部发布的《公路工程设施支持自动驾驶技术指南》中，明确要求对非授权设备私自连接到内部网络的行为进行检查或限制，能够对终端或用户非授权连接到外部网络的行为进行检查或限制，阻止非授权访问。

» **信息系统越来越复杂，安全运维难以为继**

随着公路业务不断发展，网络规模越来越大，接入对象越来越多，信息系统越来越复杂，给安全防护及运维管理带来巨大挑战。部分高速公路运营单位无专职安全人员或外包安全服务团队，整体安全运维能力不足。部分人员安全意识不足，下载使用个人 U 盘，临时私接更新上传文件，可能给内部网络带来病毒威胁。面对无比复杂的信息化环境，亟需有效的技术或手段，能够快速简化安全运维，提升运维效率，为公路信息化建设和数字换转型保驾护航。

面对上述数字化转型带来的网络安全风险和挑战，在已有工作基础上，以需求为牵引，以目标为导向，以行业标准为依据，聚焦数字技术赋能，基于一体化的安全建设思路，本白皮书提出了云、网、端一体化的安全防护体系，为数字赋能专项行动提供信息安全保障。

02

公路交通云、网、端一体化安全总体架构

2.1 设计思路

基于公路交通信息化发展及安全建设的必要性，结合国家相关法律法规和公路系统的业务特点，公路交通网络安全方案的建设思路如下：

» **依法合规，安全能力合规化：**遵照国家安全相关法律和条例，严格遵从网络安全等级保护基本要求，关键信息基础设施安全保护条例，商用密码应用安全性评估等相关要求及条例，对云平台，网络，终端，数据及应用等不同实体提供安全防护能力，确保国家网络安全相关条例及标准，交通行业相关安全要求及制度在公路行业落地，满足安全合规的要求。

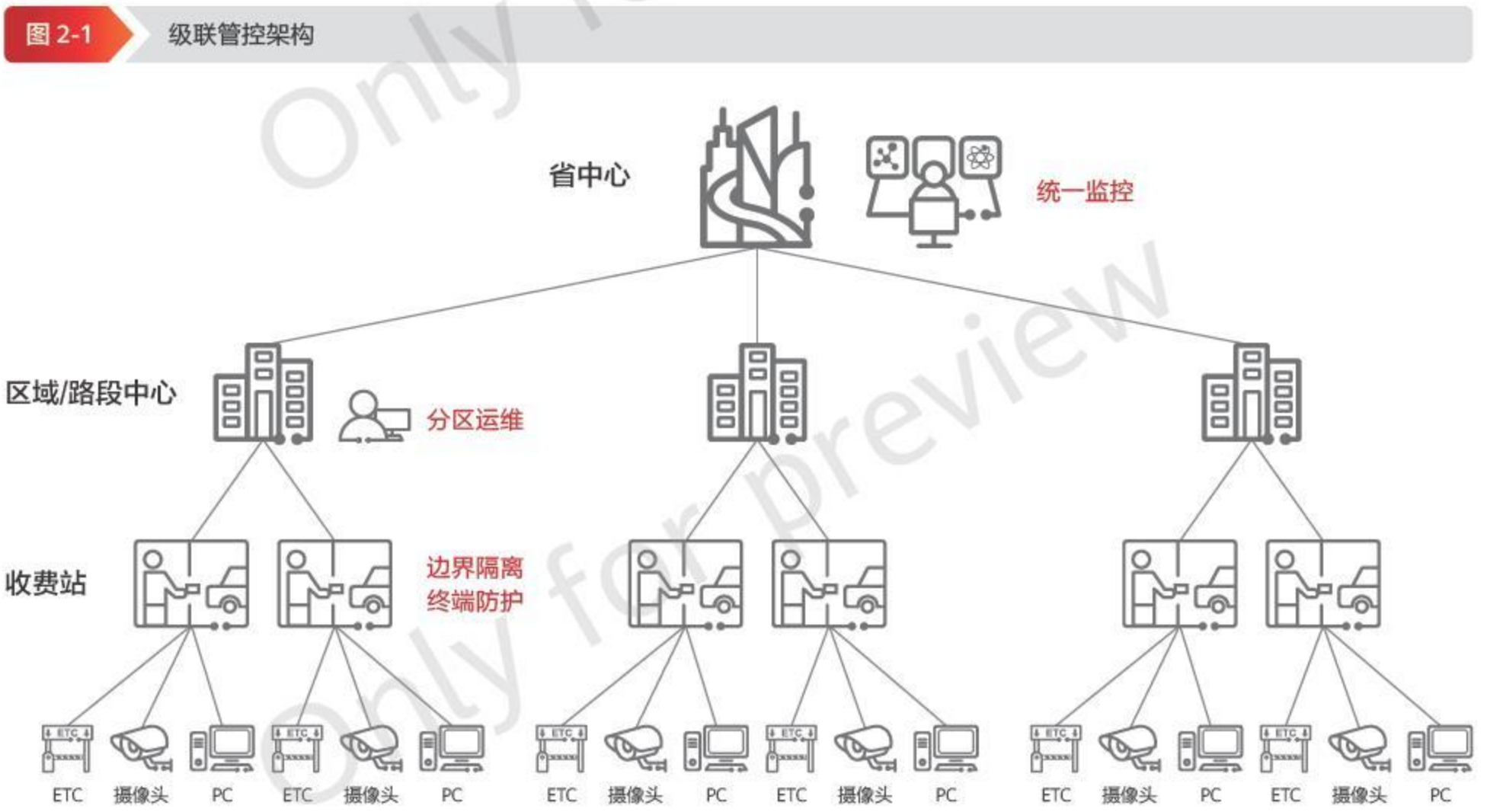
» **云、网、端协同，安全能力体系化：**根据公路交通业务的系统特点，组织架构，运营需求，保障云平台、网络、终端的安全防护的基础上，从体系化的视角，构建云、网、端一体的整体防护架构，提供符合行业特点，公路场景的协同防护能力，保障业务系统安全稳定的同时，能够快速识别风险，检测威胁，联动处置，高效闭环。

» **统一运营，安全能力智能化：**结合公路组织架构，省中心统一安全监管，区域 / 路段中心分区运维防护的需求，提供分层管控，多方运维的统一运营架构，构筑职责清晰，操作简单，运维高效的数字化，智能化安全运营平台。安全运营平台借助安全大模型能力，融合安全运营专家经验，筛选高价值事件，发现未知威胁，联动安全设备，实现时间的溯源和调查取证，自动处置。

2.2 云、网、端一体化安全架构

基于省级公路交通业务系统的组成架构，可划分三个层级，分别是省中心，区域 / 路段中心以及收费站，如图 2-1 所示。

图 2-1 级联管控架构



» **省中心：**省中心是公路交通信息化建设的核心，是业务上云，数字化转型的平台底座，监督全省公路交通运行状况，协调各路段之间信息交互，相关信息的调取等。在安全防护层面，省中心负责全网统一监控，情报同步，跨区域协同防护等职责。

» **区域 / 路段中心：**区域 / 路段分中心一般由路段经营管理单位设在其管理中心，与路段收费、监控分中心合并设置。与各个收费站、服务区、养护工区等建立路段通信网，并接入省骨干通信网，实现与省中心的联网通信。在安全防护层面，区域 / 路段中心担负所属区域 / 路段内的风险识别、威胁检测及响应处置等安全运维职责，同时向省中心同步安全态势及情报等信息。

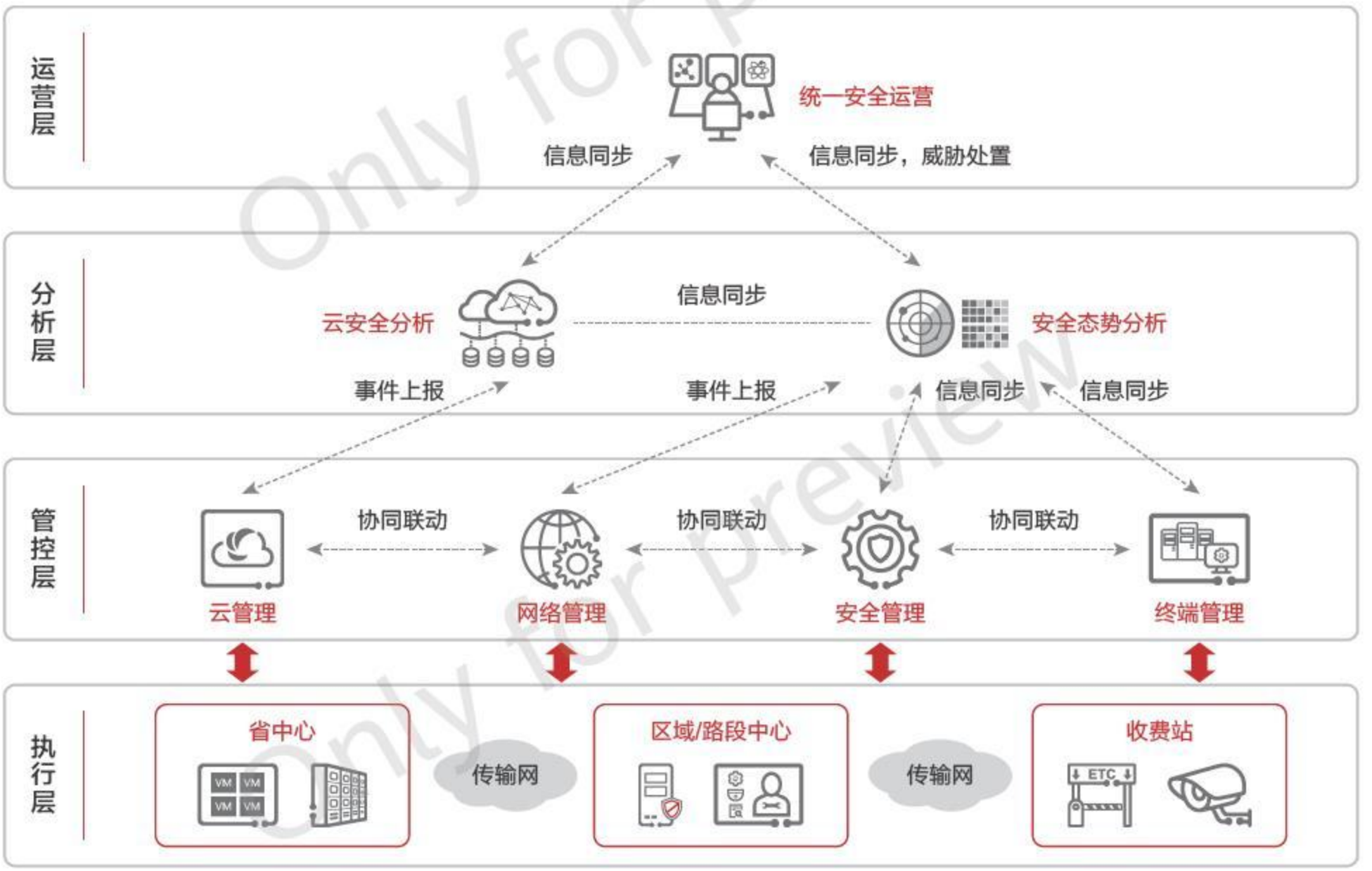
» **收费站：**在高速公路沿线的收费站、服务区、养护工区等合并设置基层通信站点，作为接入层汇聚节点，与收费站广场、隧道、外场监控网络形成接入网，并通过路段通信网连接到区域 / 路段中心。收费站部署各类物联终端及业务主机，风险暴露面较大，需要通过资产识别，准入管理，安全防护等手段消减安全风险。同时，收费、视频、监控等不同业务需要隔离防护，避免安全风险跨区传播。

随着公路交通基础设施数字化程度的不断提升，省中心的平台支撑能力持续增强，业务系统集中上云，同时收费站向少人化，无人化发展。信息安全建设应基于业务架构及发展趋势，采用可持续演进的架构，将安全的平台能力集中建设在省中心，通过探针、网关及安全设备将安全能力下沉到区域及收费站。区域 / 路段中心按需从省中心申请安全资源及能力，减少本地部署的安全实体设备，便于安全运维架构随着业务架构灵活调整，随着公路持续建设按需扩容，避免安全重复建设，提搞安全资源的利用率。

同时，安全建设并非是独立的工程，而是随着业务系统同步规划、同步建设，同步发展的，与应用系统，云平台，网络，终端是强关联的。通过与云平台、网络、终端的协同联动，将各实体的安全能力形成合力，形成多维纵深的，级联管控的，自动化操作的体系化安全架构是公路交通的安全建设重点。

基于上述级业务架构及演进趋势，公路交通系统信息安全体系不仅要实现从云平台、网络、终端等实体的安全防护，还应将各实体的安全能力统一调度和管理，提供一体化，可视化，全局化的安全防护能力，实现统一安全运营和协同防护，提升安全运维效率，我们将整体安全架构分为运营层，分析层，管控层和执行层，其架构如图 2-2 所示。

图 2-2 云、网、端一体化安全架构



其中各个逻辑层次的说明参考表 2-1。

表 2-1 各个逻辑层次说明

层次	说明
执行层	执行层是指参与业务交互的物理设备及运行在物理设备之上的应用软件，由省中心云平台，区域 / 路段中心的网络以及收费站的各类终端三个部分组成，每个部分均包含各自的安全设备，如防火墙、探针、IPS、终端安全软件、云安全资源池等。终端包括物联终端（ETC，抬杆机等）、办公终端、摄像头、工控机 /PLC 工控组件等类型。网络由各类业务网（收费网、视频网、监控网等）及收费站 - 区域 / 路段 - 省中心的骨干传输网组成。省中心云平台主要包括云平台自身安全及平台上的租户安全。执行层在整体架构中负责收集资产信息、流量信息、日志信息、安全信息等，并上传至安全分析系统，同时接受控制器下发的授权管理和阻断策略，对存在安全风险终端、用户、流量进行自动或人工的处置。
管控层	管控层由终端管理、网络 / 安全控制器、云管理平台组成。终端管理负责收集终端资产信息、终端状态、终端安全日志，并对终端进行安全处置。网络 / 安全控制器通过南向 NETCONF（Network Configuration Protocol，网络配置协议）、SNMP（Simple Network Management Protocol，简单网络管理协议）等接口，统一管理控制物理和虚拟网络，完成网络配置的自动化下发。同时北向与安全分析平台对接，完成安全威胁的自动化闭环。云管理平台负责云业务的部署，以及虚拟网络、虚拟机创建、安全组件的下发等服务。管控层在架构中，向下对执行层进行管理控制，向上和安全分析平台进行协同，提供溯源等信息，管控层从分析层接受授权、阻断、查询策略，并下发给执行层，是实现自动化阻断和溯源的关键部件。
分析层	分析层由网络安全态势感知平台、云安全分析平台组成。网络安全态势感知平台收集终端和网络的信息，并进行分析，实现网络侧的态势感知，通过多级租户方式向区域 / 路段中心提供态势感知能力。云安全分析平台负责收集云平台、应用、数据的安全信息，完成云自身安全威胁分析。分析层在整体架构中通过智能算法对所有信息进行综合分析和研判，并将全网的安全态势进行统一呈现，对于需要处置的事件下发给控制器进行处理，是云网端一体防护架构的核心。
运营层	运营层由省中心统一安全运营系统构成。统一安全运营系统承担全省 ICT 系统的统一运维和运营管理功能，从运营角度实现对安全事件的溯源，工单派发，闭环处置等安全生命周期管理。通过部署安全运营中心，收集网络安全态势感知平台和云安全分析平台的事件信息，进行关联分析和威胁统一呈现，响应处置。统一安全运营系统实现对网络设备、安全设备、系统、主机、中间件、数据库、存储、应用、虚拟化等多种资产的安全事件、设备运行状态、网络通信流量、资产脆弱性、网络安全防护能力等数据的采集和集中管理和全网安全态势可视化。运营层可以通过安全大模型学习专家运维经验，对海量安全数据进行去重，聚合，关联及分析，通过各类 AI 模型检测网络中的未知类型的攻击以及新型病毒等，并自动联动安全设备进行自动化处置。

03 公路交通云、网、端一体防护安全解决方案

公路交通云网端一体化防护主要针对终端、网络、云平台等多个维度部署安全组件，实现安全防护。多维度的安全防御组件是云网端一体化安全解决方案的基础，满足国家等级保护合规要求。基于云网端一体防护解决方案架构，通过各个层次的配合和协同，可以较好地实现公路交通系统的等级保护，关基防护等合规化要求。在一体防护的架构下，解决方案设计内容包含多维纵深防护、安全协同联动及统一安全运营等三个部分，下面将逐一进行介绍。

3.1 云网端一体化防护基础：多维纵深防护

多维纵深防护是指从省中心的云平台安全，链接省 - 区域 - 收费站的传输网络安全，再到收费站的终端安全的三层纵深防御，其中省中心云平台作为承载公路交通核心业务系统稳定运行的基础平台，需提供云平台自身的安全防护以及云内租户的安全防护能力。传输网络为全省公路交通业务提供大带宽，高可靠的网络服务，需要考虑网元自身的安全，网络管理运维等安全问题。终端安防护能力是基于网络准入的基础上，对物联终端提供流行为分析以及对 PC、服务器类智能终端提供防勒索病毒等防御能力。

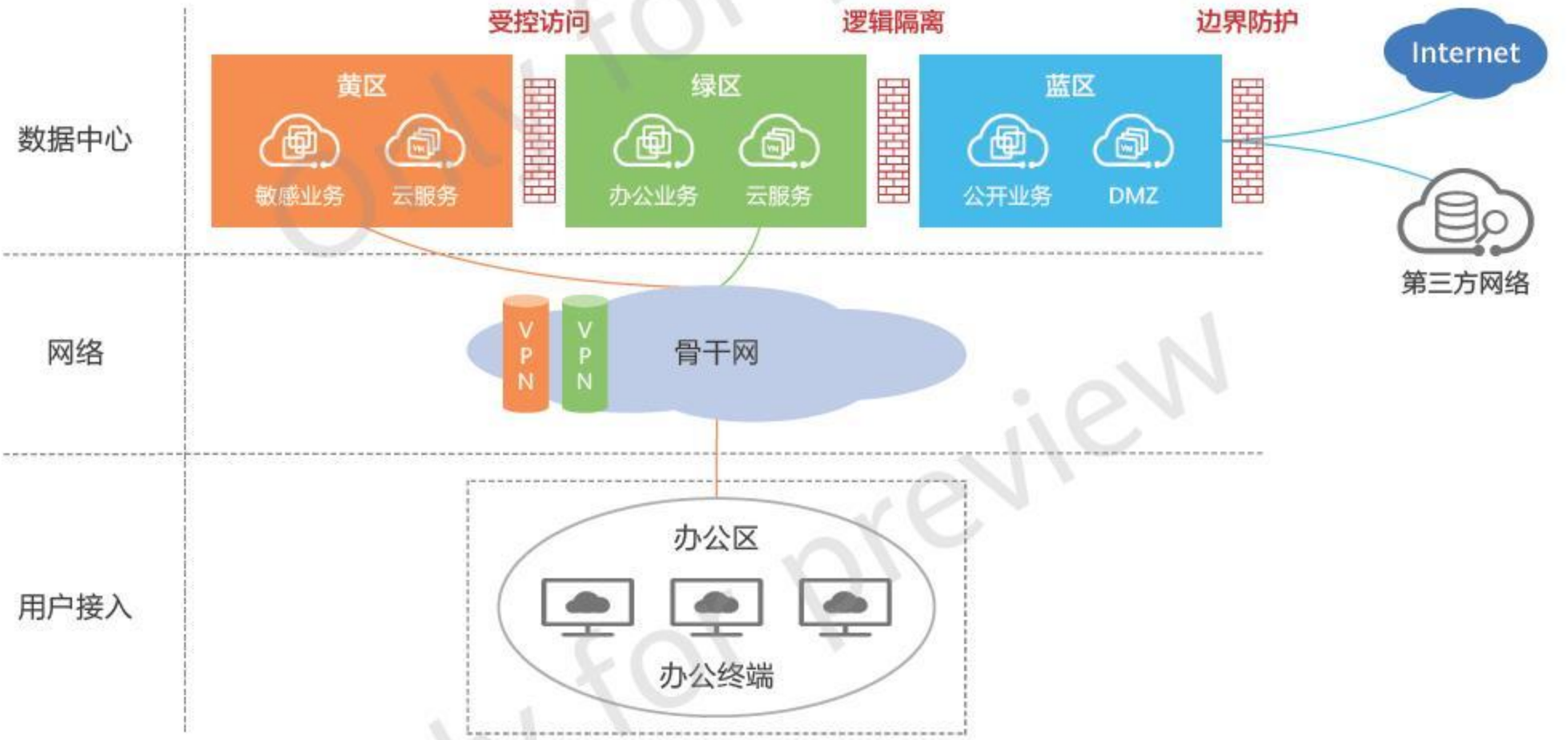
3.1.1 云平台安全方案设计

省中心的云平台需要为部署在云上的业务系统提供安全防护能力，边界保护是云安全的核心，多层级边界对不同区域的应用及数据提供不同等级、不同粒度的安全防护。结合公路业务及数据安全防护需求，云平台按照业务特性及敏感程度，可规划为敏感业务域（黄区）、内部管理域（绿区）、外部服务域（蓝区），每个域部署不同的专业系统。如下图所示：

- **黄区：**涉密数据，包含敏感信息，主要面向内部特定用户使用，不对外进行信息交互，是高等级安全区域，涉及的业务系统如干部管理，涉密公文等。
- **绿区：**非涉密数据，不包含敏感信息，主要面向内部用户，与外部按需受限交互，是中等级安全区域，安全与效率平衡，涉及业务系统如办公 OA 等。
- **蓝区：**外部公开数据，面向外部用户，对外发布公共信息与服务，共享为主，效率优先，是低等级安全区域，涉及业务系统包括门户网站，公众 APP 等。

在省中心云平台中，不同业务区的隔离管控如图 3-1 所示。

图 3-1 业务分区架构



数据中心云平台分为三个区域：

最外层的蓝区是部署外部公开的业务的区域，为公网用户提供访问服务，需要按照 DMZ（demilitarized zone，非军事区）的防护标准进行边界访问控制及防护。

中间绿区是办公业务区，部署 OA 相关系统，主要为内网用户提供办公业务服务，与蓝区之间逻辑隔离，蓝区业务不能直接访问绿区，但绿区可以向蓝区同步数据。

内侧是部署敏感业务的黄区，以涉密非公开数据和业务为主，与绿区之间受控访问，通过严格的白名单访问策略管理绿区和黄区之间的交互，确保黄区数据不外泄的同时，能够从绿区同步业务所需数据。

每个区域中的安全防护能力由云平台的云租户安全服务提供，云租户安全以安全服务的形式提供，基于云管平台的安全服务目录，实现安全能力的申请、审批、部署等，如图 3-2 所示。

图 3-2 资源域的安全防护能力

云安全服务聚焦灵活调度安全资源，弹性扩展、自助申请等特点。各种基于云虚拟设备的安全防护手段，涵盖了云安全能力的事前监测、事中处理与事后审计全生命周期，并互相协同工作，形成一个完整的云内安全事件响应闭环。

安全服务化主要以云租户安全组件的形式提供安全能力，利用快速、弹性分配资源的优势，安全也能够作为服务的形式向用户提供，用户能够根据自身需求按需自助开通、并自定义安全策略配置。

根据上述需求，云平台将成熟安全能力进行服务化适配，统一作为安全资源在云管理平台呈现和管理，为用户业务提供不同安全服务，满足不同业务上云后的等保合规要求及定制化安全防护需求。安全即服务是云数据中心区别于传统数据中心安全业务部署与管理的关键需求，涉及云上用户与应用系统的安全运行防护、云租户间安全隔离防护、地址重叠（VPC 间）、云租户内应用系统间安全隔离、云应用系统不同组件间安全访问控制等多个方面。安全服务化主要是云管理平台通过 API 调用实现对应安全服务的编排调度、订单及管理，为云上用户及业务提供统一的服务目录。用户可按需在云管平台上选择安全服务，独立的服务实例将自动下发至用户 VPC 内部，以实现安全资源灵活调度、动态扩展、按需快速交付，全面满足云用户对业务安全部署的要求。

3.1.2 网络安全方案设计

网络安全建设是一个系统工程，除了要提高外部防护能力，更应该加强自身安全能力的建设。在公路交通网络的安全建设中，需要着重考虑网元设备自身的安全性以及网络管理运维能力，下面将对网元可信和网络管理运维方案进行阐述。

3.1.2.1 网元可信

在公路交通网络中，网络交换机、路由器、防火墙部署在数据中心、骨干传输网、接入网等关键位置，构成了数据世界的高速公路和桥梁，因此设备自身的安全性至关重要，如果被攻击可能导致内网被控制、流量被监听、数据被篡改等严重风险。因此设备自身需具备安全可信能力，在产品设计、开发、运行阶段均需规划安全可信能力，覆盖设备硬件、操作系统以及软件应用等部件，强化设备的内生安全能力，增加设备应对威胁攻击的能力。

可信启动提供了一种安全机制，可以有效阻止在启动过程中加载并运行未经授权的应用。启动程序通过签名公钥验证软件的数字签名，确保所加载软件的完整性和可信性，只有通过签名校验的镜像文件才允许被加载和运行。在启动过程中的任何阶段，一旦签名验证失败，启动过程都会被立刻终止，如图 3-3 所示。

图 3-3 可信启动流程

网元设备的可信启动分为 3 个阶段。

1. 在生产装备阶段：通过统一的签名平台对软件包进行签名，得到对应的签名文件与根证书。将签名文件烧录到对应的 Flash 存储介质上，将根证书烧录到芯片内部不可更改的部分，将片内引导程序内置于 SoC（System on Chip，片上系统）内部的 BootROM 中，该 BootROM 具备不被非法篡改的物理属性。至此，设备芯片内部完成了可信根环节。
2. 在硬件启动阶段：系统上电或复位后 CPU 首先执行 BootROM，由 BootROM 对 BIOS（Basic Input Output System，基本输入输出系统）与根公钥进行哈希校验以确保其完整性。如果哈希校验失败，则拒绝启动 BIOS，直接复位系统；如果哈希校验成功，则启动 BIOS，信任链转移到 BIOS。
3. 在软件启动阶段：BIOS 用证书信息对操作系统进行签名验证。验证通过则加载运行，信任链继续传递给操作系统，验证不通过则拒绝继续启动。操作系统启动后，从软件包指定位置读取 APP 软件，然后对软件 APP 进行校验。如果校验失败，则拒绝继续启动；如果校验成功，则启动 APP 软件。

上述过程实现层层逐级校验，建立从芯片可信根到产品应用软件的完整信任链，实现可信启动，保证软、硬件不被篡改，出现任何错误都记录日志并重启。

网元设备的三平面隔离

如前文所述，网元设备做为构建网络的节点，其自身的安全性尤为重要，通过对当前各类网元设备的分析和研究，依据不同功能平面进行隔离防护，提升网元设备自身的健壮性。网元设备可以划分为管理平面、控制平面、数据平面等三大平面，三个平面互不影响，但是又都相互依赖，缺一不可。不同平面的功能如表 3-1 所示。

表 3-1 网元设备的三平面功能

名称	解释
数据平面（Data Plane）	也叫转发平面或用户平面，处理和转发设备不同端口上各种类型的数据，如 L2、L3、ACL、QoS、组播、安全防护等各种具体的数据处理转发过程，数据平面通过硬件转发表项实现流量转发，例如 FIB 表、VLAN 表等。
控制平面（Control Plane）	用于控制和管理所有网络协议的运行，提供了数据平面所必需的各种网络信息和转发查询表项，例如 OSPF、BGP、IS-IS、ARP、IGMP、IPv6、MPLS 等协议。
管理平面（Management Plane）	面向系统操作维护人员（或外部第三方管理软件），提供输入输出，用户管理，License，管理对象的监控、配置、告警、统计等，不直接对系统的运行状态产生影响，例如 SSH、SNMP、CLI、NETCONF 等。

» 如果数据平面不隔离，攻击者可能通过发送大量的非法数据报文攻击网元设备，可能导致网元的 CPU、内存等资源过量消耗，控制平面无法申请到资源、无法进行有效的配置和处理，导致业务受损。

» 如果控制平面不隔离，攻击者可能利用网络协议漏洞攻击网元设备，可能导致非法提权，进而对其他平面进行控制，或发起拒绝服务攻击导致网元设备无法正常工作。
» 如果管理平面不隔离，攻击者可能通过系统或第三方软件漏洞攻击网元设备，非法获取配置权限，更改网元设备配置，导致业务错误或受损。

所以，每个平面都要考虑部署相应的安全策略，以防范承载网络可能受到的攻击。推荐的安全防护手段如下：

» 数据平面安全
  • 配置安全访问控制列表，过滤掉已知网络攻击数据包。
  • 应对典型协议报文的攻击进行防护，包括但不限于 Ping of Death 攻击（利用长度超大的 ICMP 报文对系统进行的拒绝服务攻击）、SYN Flood 攻击（利用 TCP 的三次握手机制建立大量半链接，持续消耗系统资源的攻击）、Teardrop 攻击（通过发送携带错误分片标志位和偏移字段的报文导致系统异常的攻击）、Smurf 攻击（通过将 ICMP 应答请求报文的回复地址设置成受害网络的广播地址，导致目标系统异常的攻击）、Land 攻击（通过发送具有相同源地址和目标地址的欺骗数据包，导致目标设备异常的攻击），配置防护策略，如进行限速、过滤、丢弃。

» 控制平面安全
  • 配置安全防护及访问策略，对设备控制、流量管理及其他业务流量进行安全管控。
  • 针对路由协议，应启用路由协议认证功能，确保与可信的设备进行交互，同时启用协议自有或网元设备增补的安全防护能力，提升路由协议交互的安全性。
  • 按需配置各类表项的规格限制，例如，最大条目路由限制等，预防可能遭受的路由冲击，导致网元设备瘫痪。

» 管理平面安全
  • 根据最小权限分配原则对设备管理账号进行权限管理、定期口令更新与留档审计。
  • 登录设备应使用 SSHv2 等安全协议，并通过 ACL 限制可远程管理设备的 IP 地址段；网管系统应采用 HTTPS 等安全协议，采集协议应采用 SNMPv2c 或以上版本。
  • 关闭设备上不必要的服务及端口，例如 HTTP（Hypertext Transfer Protocol，超文本传输协议）、FTP、TFTP 等，若有使用需求，应在受控的条件下使用，使用结束后回退到关闭状态。

基于上述三个平面的防护及隔离设计，能够有效提升网元设备自身的安全性和可靠性，为公路网络建设提供可信的网元基础设施。

3.1.2.2 网络管理运维

在网元可信的基础上，为了更好的保障网络安全，网络管理应具备基础网元管理，网络可视管理及网络智能诊断功能。

» **基础网元管理**

公路沿路通信网设备通过 Telemetry 技术，实时采集设备数据并上送至网络管理平台，通过智能故障识别算法对网络数据进行分析，精准展现网络实时状态，并能及时有效地定界故障以及定位故障发生原因，发现影响业务的网络问题，保障用户网络体验。同时支持 SNMP v1/v2c/v3、CLI（命令行）、Web 网管、SSHv2.0、NETCONF、ICMP 等多样化的

管理和维护方式，可满足对接不同管理平台和维护管理需要，包括但不限于如下能力：

1) 网元安全态势呈现，并对网元安全状态进行评分，识别高风险网元并优先处置。
2) 安全配置核查能力，及时发现不合规的安全配置项（如弱口令策略、弱加密算法、不安全协议等），并给出指导支撑用户修复。
3) 运维面入侵感知能力，及时发现口令暴力破解、异常登录行为、非法账号创建等行为，避免网络业务被非法控制和恶意破坏。
4) 基本的安全响应处置能力，如封堵 IP、禁用账号等，支持安全事件的快速响应和应急处置，并针对网元下发响应动作。
5) 采集网元上的日志、配置、安全事件等信息，并上送到网管，作为网管上安全配置核查、运维入侵检测、安全态势呈现的信息输入。
6) 具备系统面入侵监测能力，及时发现非法提权、关键文件篡改、Rootkit 攻击等行为，避免网络设备被非法控制，并上报网管。
7) 具备接收网管下发的安全响应策略并在网元上进行执行闭环的能力。

» **网络可视管理**

网络可视管理是指通过拓扑发现功能，实时监控所有网元设备的运行状态，并根据网络运行环境变化优化网络参数及配置，保证网络以最优性能运行，网络可视管理包括以下功能

拓扑自动发现：将网元设备自动添加到拓扑视图中，同时可以发现网元间的链路。可以控制拓扑的图层显示，例如拓扑上的所有链接，只显示光纤，其他不显示等。

拓扑告警显示：拓扑告警支持使用不同的颜色或图标表示网络状态。告警的颜色可以用户自定义配置。

» **网络故障诊断**

网络故障诊断功能包括故障定界、根因分析以及预测性诊等功能。

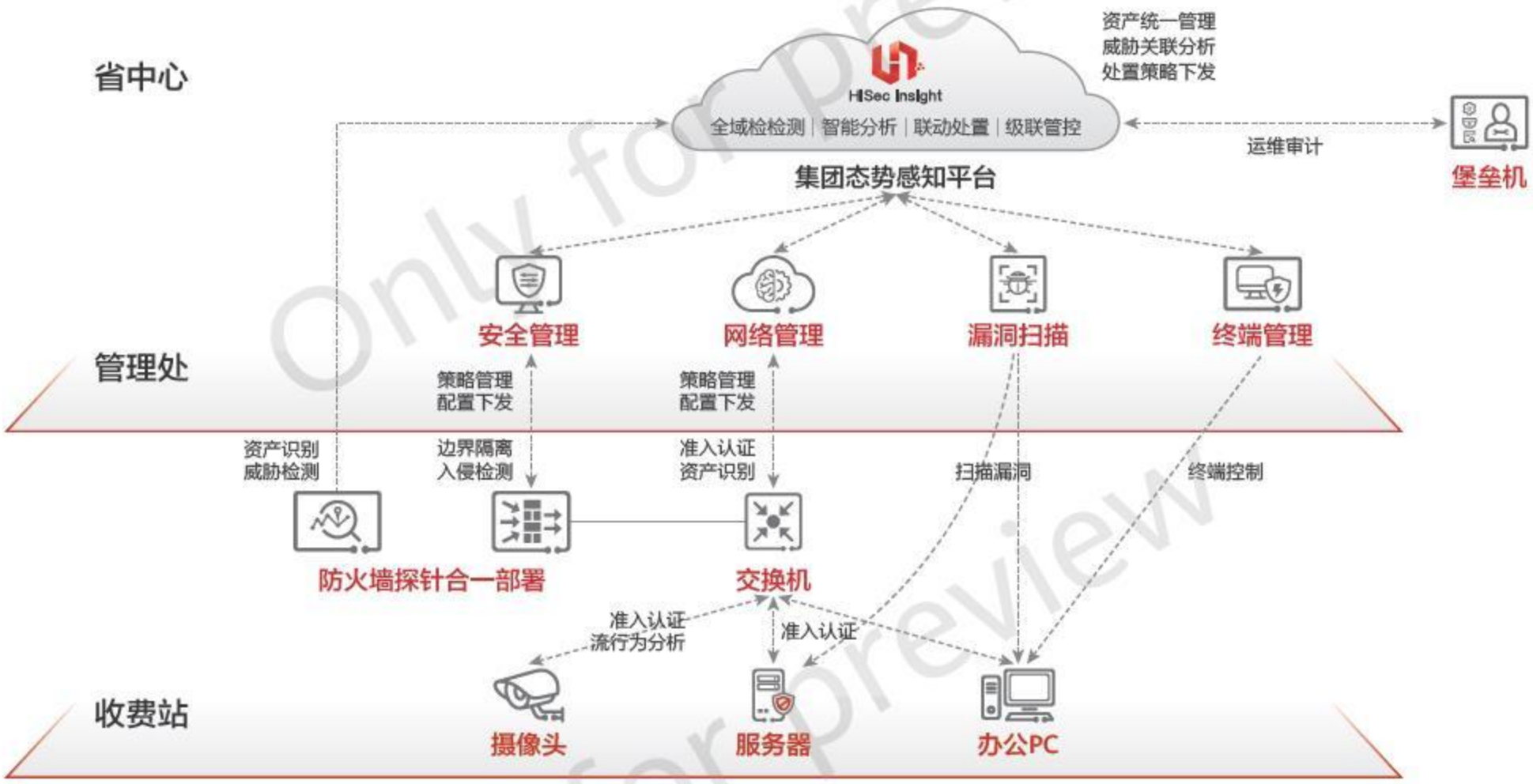
- 故障定位：网络发生故障时会出现业务中断、业务丢包、业务时延变大的现象，直接影响用户体验。导致故障的原因可能有很多种，故障定位功能快速定位到故障发生的设备及端口，通过自动恢复或人工恢复方式快速恢复业务。
- 根因分析：当导致网络故障的问题比较复杂时，需要通过人工分析海量日志和告警，逐步排查故障原因，拖延了故障恢复时间，根因分析功能能够对设备信息进行聚集、并借助 AI 能力快速从海量信息中通过关联分析及历史配置对比等方式快速分析故障原因，为运维人员提供关键的故障原因等信息，辅助恢复业务网络。
- 预测性诊断：预测性诊断能够对经常发生的故障进行学习和统计，通过 AI 技术对网络状态进行预测，做到故障预防。

3.1.3 终端安全方案设计

3.1.3.1 终端识别及准入

公路交通网络中，尤其是收费站及路侧，数量庞大的终端设备处于无准入管理，无安全防护的状态，攻击者可能利用仿冒设备，冒充合法的终端接入网络，实施非法监听和非授权访问等操作。通过对终端设备的认证及准入控制，能够有效消减终端设备带来的风险，其实现流程如图 3-4 所示。

图 3-4 统一终端管理方案



终端安全防护方案包含终端准入认证、终端资产识别、终端威胁检测，终端态势统一呈现四部分功能。

1. 终端准入认证

   接入交换机承担终端准入认证网关功能，为不同类型终端设备提供差异化的准入认证能力。

   如摄像头等物联设备，无法安装终端认证软件，需要通过 MAC（Media Access Control，媒体接入控制）地址认证方式接入，MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何客户端软件。设备在启动了 MAC 地址认证的端口上首次检测到用户的 MAC 地址以后，即启动对该用户的认证操作。

   PC 和服务器等智能终端设备通过 802.1X 接入网络，802.1X 协议是基于 Client/Server 的访问控制和认证协议。它可以限制未经授权的用户 / 设备通过接入端口访问网络。

   通过终端的准入控制功能，可以实施检测资产的入网状态：如已经授权的合法终端以及尚未授权的待入网终端。终端的在线状态：如当前是否在线，以及上一次在线时间等信息。通过对终端资产的状态的管理和感知，识别异常终端及异常状态。

2. 终端资产识别

   传统的资产识别方式是通过资产探针对网段进行遍历扫描，发现设备后通过 NMAP（Network Mapper，网络端口扫描工具）等工具进一步识别资产的类型，但是通过此类主动扫描方式进行检测存在一定盲区，无法 100% 覆盖网络中的

所有资产。本方案中通过接入交换机的准入认证获取资产 IP，并结合被动指纹识别及交换机内置的主动探测相结合的方式保证资产 100% 覆盖的同时，能够高精准识别现网终端设备。

3. 终端威胁检测

资产识别及准入控制措施能够有效识别仿冒、私接等问题，但是仍无法避免一些高明的攻击者绕过认证体系，例如修改 MAC 地址或硬件识别信息等，同时，攻击者可以通过漏洞或近端物理攻击获取终端设备的控制权限再攻击内部网络。为了提升终端设备的安全防护能力，需要对其流量进行分析，从而判断终端可能存在的安全风险。

除了流行为的异常检测，还需对终端设备的漏洞进行识别，对设备的弱口令等风险进行检测，同时 PC、服务器等智能终端设备安装终端安全软件进行病毒查杀和异常检测。

通过多维度的检测和关联分析，能够精准识别终端上的安全风险，并对风险进行告警和处置。

4. 终端态势统一呈现

采集到终端信息，准入状态，安全状态后，会将信息同步到态势感知平台，与网络安全事件进行关联分析和统一呈现，提升检测准确度，让运维人员快速定位到问题终端。

3.1.3.2 终端防勒索

通过终端的准入管理及安全防护，可以缓解仿冒，私接及被外部入侵的风险，但由于终端的外设及接口难以有效监控和管理，存在通过 U 盘、光盘等外部存储介质感染病毒程序的风险，根据《2023 年恶意软件准备和防御报告》的调查结果，如图 3-5 所示，勒索软件等病毒软件成为企业面临的头号威胁。

公路交通网络中，收费站、区域中心、省中心是网络互通的，任何一处的终端设备一旦感染勒索病毒等高危病毒，可能通过内部网络扩散到核心业务区，导致收费，监控，视频等相关业务受损，甚至业务中断。因此终端设备的防勒索病毒能力尤为重要，是关乎整体公路交通安全的关键能力。

图 3-5 企业面临的 TOP 安全威胁

勒索软件攻击模式主要有以下两个特点：

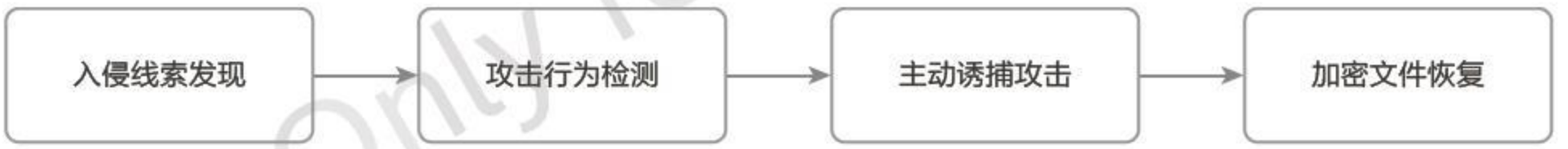
1. 为了快速拿到赎金或形成威慑，攻击和加密速度极快。
2. 通过恢复用户核心业务数据来获取赎金，攻击者一定会加密用户业务数据。

针对第一个特点，我们主要的应对理念是防御前移，建立实时的分层防御机制，尽早断开攻击者的入侵链路，不断增加攻击者的成本和难度。从基于 NDR（Network Detection and Response，网络威胁检测与响应）的高级入侵线索发现（如 0-Day 漏洞利用），到 XDR（ExtendedDetection and Response，可扩展威胁检测与响应）及 IOA（Indicator of Attack，攻击指标）高级威胁检测引擎等不同维度检测方法的检测，对勒索病毒进行识别和阻断，再到文件加密行为的拦截，每一层的防御机制均针对勒索攻击的关键动作，缓解勒索软件攻击带来的影响。

针对第二个特点，需要抓住勒索软件攻击的必然行为“文件加密攻击”，通过主动诱捕技术使攻击意图显现并在加密用户数据前确认威胁行为并及时阻断，在“用户数据早晚会被加密”的假设下为用户提供加密文件恢复兜底方案，稳定恢复到加密前的状态，确保用户数据零损失。

终端防勒索方案流程如图 3-6 所示。

图 3-6 终端防勒索方案流程



1. 入侵线索发现

   边界突破是新型勒索软件进入目标系统的关键环节，外联 C&C 通信是控制目标系统的重要手段，传统的 IPS/IDS 仅能阻断已知攻击行为，但面对 0-Day 漏洞和加密流量攻击却束手无策，本白皮书中入侵线索发现通过以下关键技术识别新型的，未知的攻击行为：

   - 无监督学习 + 细粒度动态特征基线 + 统计分析发现 0-Day 漏洞线索、未知加密流量攻击线索，不依赖任何标签，基于场景化建模的思路，利用 30+ 统计工具、孤立森林、极值理论等方法，将已知攻击场景（20+）的数据泛化到对未知攻击行为的发现上，从而全面发现攻击线索。
   - 因果关联分析 + 监督树算法 + 统计分析进行事件建模，从海量的告警中识别隐蔽攻击，例如：代码执行漏洞、慢速暴破等，精度可达 99.9%。
   - 风险传播算法 + 行为相似度模型进行关系建模，持续发现类似的攻击模式和受害基础设施。

2. 攻击行为检测

   对于绕过边界防御的勒索软件攻击，IOA 行为检测引擎毫秒级实时检测终端上的异常行为模式，辅助内存威胁溯源图与网络侧的攻击线索实时深度联动，通过图因果关联模型、时序关联模型、时间关联模型、统计关联模型等精准研判 0-Day 漏洞利用成功、PowerShell 攻击投递、钓鱼入侵成功等攻击场景，精准识别威胁实体，通过 XDR 与网关、终端

联动实现毫秒级的攻击阻断能力。对于已经运行起来的勒索软件载体，同样通过内存溯源图，启发式的方式锁定威胁根节点，组合 400+ 流行勒索软件家族的深度学习和关联分析，大数据挖掘关键因果链条，叠加信任传播算法和静态文件检测引擎，可有效实现对勒索软件变种和未知勒索软件加密前的实时精准研判。

3. 主动诱捕攻击

文件攻击（加密、破坏等）是勒索攻击的必然动作，也是整个勒索攻击检测链条上的关键检测环节。如何在用户正常办公和业务无感知状态下全天候自动保护客户关键数据资产免受损失是本方案的技术要点，主要有以下几点：

- 部署诱饵文件：基于流行勒索软件家族攻击模式深度研究和用户办公行为模式学习，部署勒索专用静态 / 动态诱饵文件，通过内核级接口调用，使勒索病毒调用文件检索接口时，优先返回诱捕文件路径，并基于诱饵文件状态第一时间感知攻击行为。
- 快速精准研判：基于 AI 的海量勒索文件攻击模式学习算法，实时精准区分勒索攻击和用户正常操作，不影响用户操作体验的同时实现对文件恶意操作行为精准阻断。
- 内核级毫秒级处置：基于终端内存图锁定恶意进程链，调用内核接口，快速终结病毒进程，阻断攻击行为。

4. 加密文件恢复

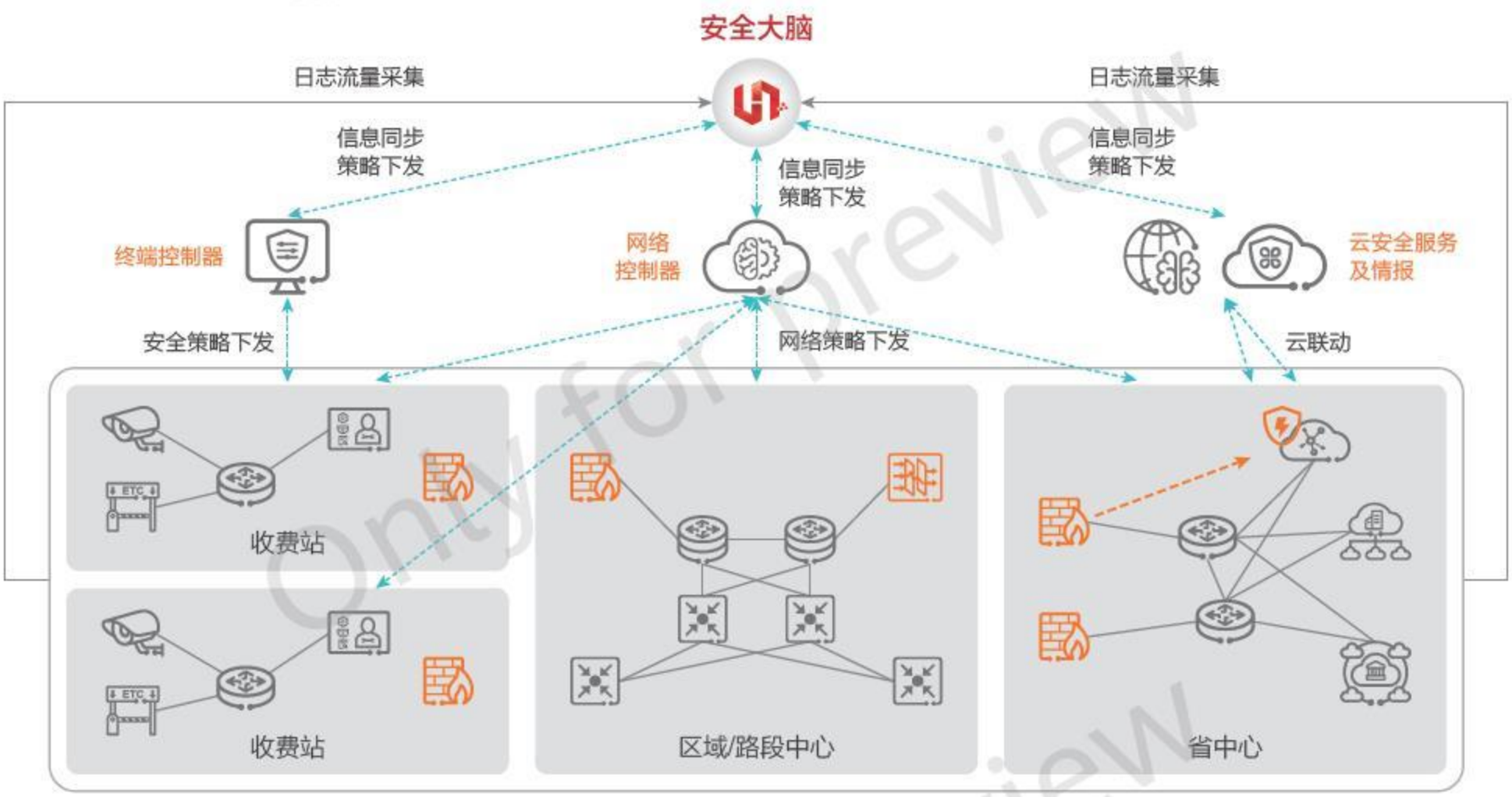
当攻击行为已经发生，检测滞后的情况下，通过轻量级勒索回滚方案恢复加密文件，保障数据零损失。相比较其他完全备份方式，轻量级勒索回滚方式具备如下特点：

- 存储资源占用小：事件触发增量备份及差异化备份，只有当关键文件修改事件发生时内核层才会将该文件备份到保护区内。
- 实时备份：当检测到勒索程序后，将文件正好恢复到被加密时间之前的点，不会有文件版本差异。
- 自动化：当检测到勒索程序后，自动恢复用户被加密的文件，无需用户手工选择备份版本恢复。

3.2 云网端一体化防护关键：安全协同联动

上一节介绍了终端、网络、云平台的纵深防御策略，基于全局防御理念，公路交通网络安全还需建立统一的安全管理中心，基于云网端一体防护的架构，对全网资产、平台和应用进行持续监控，通过大数据和智能算法进行统一安全分析，掌控全网的安全态势，通过云网安的协同与联动，实现对威胁的精准溯源和近源处置，其方案架构如图 3-7 所示。

图 3-7 云网端一体安全协同防护方案



1. 全面收集终端、网络、边界、云（平台，应用，数据等）的状态、日志和流量信息，进行综合分析和研判，安全态势全域统一呈现。为了提升安全事件分析的精准度，需要收集尽可能多的信息，特别是终端（含服务器）的信息，流量的信息，安全日志的信息。这些信息分别散落在不同的网络区域，需要把端、网、云的安全相关信息进行统一收集，以获得更全面的待分析数据。在信息收集的时候，需要遵循的原则是：尽可能搜集全面，但同时要考虑成本，例如流量探针的设置，要考虑在流量集中的位置进行部署，或者复用网络 / 安全设备自身的能力，减少独立探针的部署数量，因为收费站的数量数百计，在收费站每多增加一台设备，成本就会增加数百倍。在信息收集之后，还需要有智能算法对信息进行综合分析和研判，提升威胁告警的准确度，并在完成分析之后，将全网的态势信息统一呈现。

2. 从多个维度对风险进行动态评估和评分，基于评分结果进行授权管理。为了对核心资产进行安全防护，在初次认证通过之后，需要对终端和用户的风险进行实时地评估，评估的维度要包含终端、网络和用户行为等信息。基于多维的评估结果，对用户风险给与评分，当评分低于一定的阈值后，结合用户的身份对用户权限进行调整，实施降级、阻断等操作。

3. 能够通过 IP 地址快速溯源。发现威胁后，需要找到真正的攻击源或受感染主机。在规划良好，静态分配 IP 地址的场景下，通过 IP 地址很容易找到威胁源。但在动态分配 IP 地址场景下，特别是无线化后，人员流动频繁的场景，例如会议室无线场景、移动巡检场景，很难通过 IP 地址直接定位到主体。通过安全态势感知和网络控制器的协同联动，能够快速定位感染的主体，进行下一步处理，消除威胁。

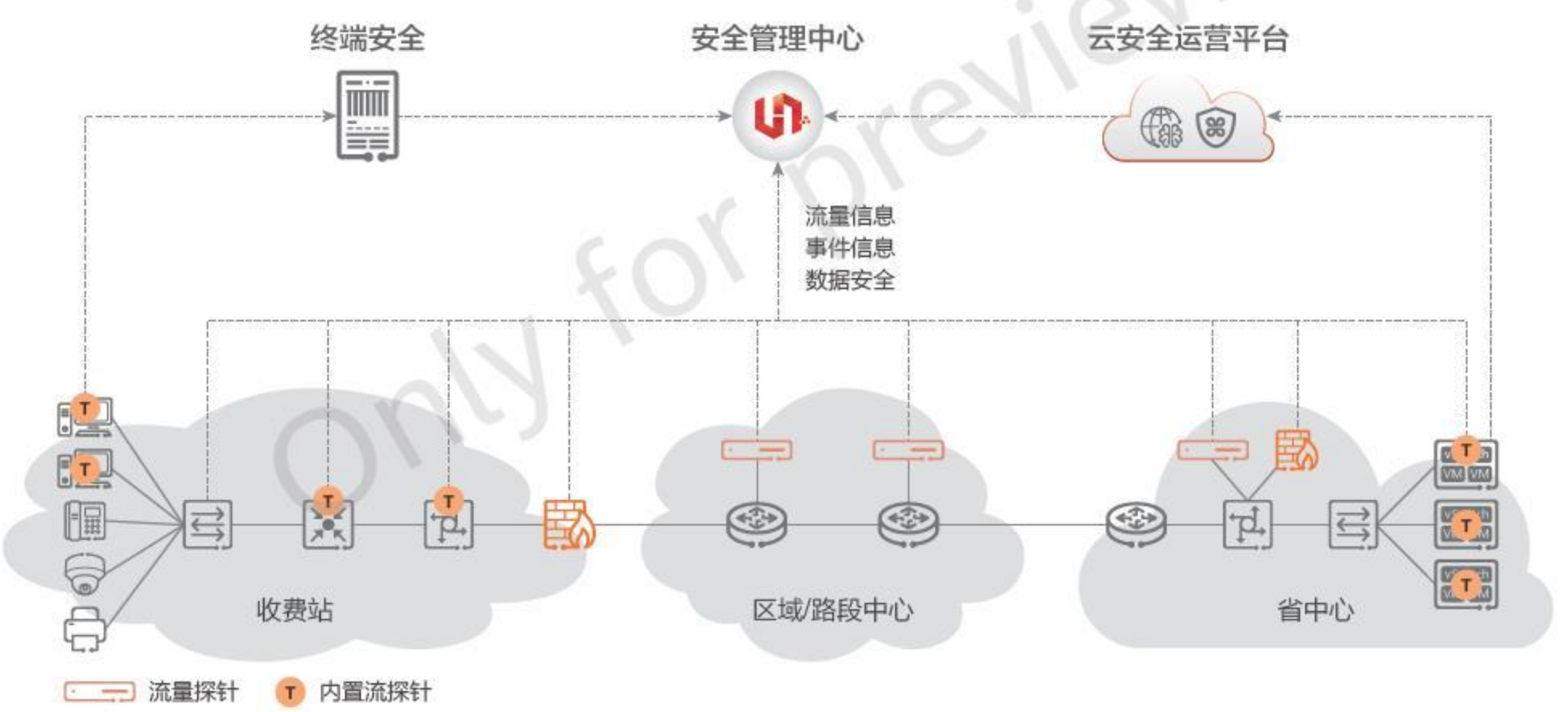
4. 自动找到精准的遏制位置，实现威胁判定后快速处置，防止扩散。当识别到严重威胁时对威胁进行遏制，以避免威胁进一步扩散到其他位置。进行遏制的位置会有多种选择，如果位置选择过高，威胁会继续扩散同区域内的其他资产上，因此必须选择尽可能接近攻击源且在可控制范围内的设备。如果通过手工对接入位置进行排查，可能需要查找多台网络及安全设备的日志或表项才能定位到威胁源，还有可能涉及跨部门的协同，往往需要数小时或数天，效率低下。所以，通过分析层、管控层、执行层设备之间的自动化协同联动，实现威胁源快速定位，近源快速处置的能力，有效提升运维效率。

云网端一体安全协同防护方案主要分为三阶段，统一安全分析，精准溯源和近源处置。通过持续收集全网全量的流量信息，以及终端的安全、漏洞等安全事件信息，进行统一的安全关联分析，提升安全分析准确率，减少重复或者无效的告警，并对于威胁源进行精准溯源，根据溯源后的位置进行近源快速阻断，防止威胁横向扩散。

3.2.1 统一分析

统一安全分析的核心思想是尽可能多的收集网络和安全设备的日志、事件信息，在网络的各个节点采集网络流量信息，将资产、网络、安全、云租户、威胁事件共享，云内和云外信息统一共享，并基于 AI 威胁分析模型进行大数据关联分析，减少无效告警，提升威胁告警精准率，实现云内和云外威胁一屏呈现，全网安全态势统一分析，提升安全运维效率。解决方案部署示意如图 3-8 所示。

图 3-8 统一安全分析



在所有可能的攻击路径上部署探针采集流量信息，采集各级安全设备的事件、告警信息、与云安全管理平台对接获取云内告警信息，与终端安全服务器对接采集终端安全日志及告警信息，将采集到的这几类数据进行大数据关联分析，消除冗余的威胁告警，提升威胁告警精准度。

- **通过内置探针或独立探针采集全网流信息：**在收费站、区域 / 路段中心、数据中心分级部署探针采集全网流信息，尽量多的采集全网流信息。
- **通过云安全管理平台获取云内的威胁信息：**安全管理中心和云安全运营平台对接，从云安全运营平台获取租户安全信息、威胁事件、资产信息等信息。
- **通过终端安全软件收集终端合规信息：**在智能终端上部署终端安全软件进行安全合规检测，安全管理中心与终端安全服务器对接收取终端合规信息。
- **通过资产扫描、漏洞扫描获取资产数据和漏洞信息：**安全管理中心通过资产探针、漏洞扫描等设备收集全网的资产数据和漏洞信息。
- **通过日志采集器获取全网的事件、日志数据：**安全态势平台和网管、云平台对接，收集全网的网络、安全设备，如防火墙的安全事件、告警、日志等数据。

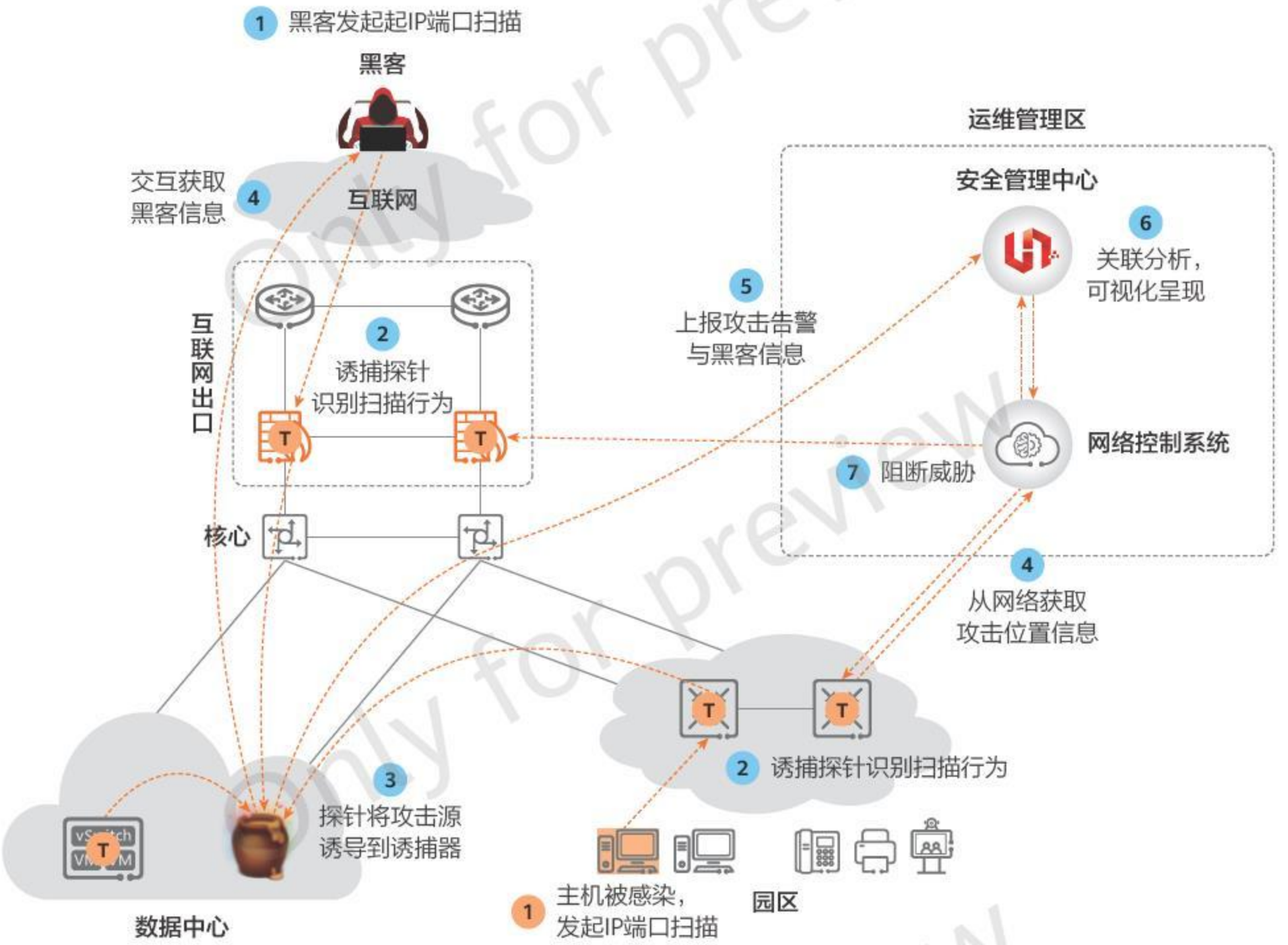
3.2.2 精准溯源

随着攻防技术的不断发展，攻击者的入侵方式更加多样化。不法分子可能利用网络漏洞窃取用户的重要数据，攻击者会向目标主机发送特定的攻击数据包或执行恶意行为。如果能追踪这些攻击数据包的来源，定位攻击者的真实位置和相关信息，受害主机不但可以采用应对措施，如在合适位置过滤攻击报文，同时可以对攻击者采取反向遏制或威慑。通过云网端协同的网络及安全策略的分析，可以精准溯源攻击路径，定位攻击者。如图 3-9 所示。

公路云、网、端协同防护方案中通过以下几种途径获取威胁源：

1. 从网络管理系统或云平台获取攻击者的真实位置，确定攻击路径，为风险处置提供精准的数据。
2. 态势感知平台通过网络控制器获取终端信息（IP、MAC、资产属性等），定位到相关终端位置。
3. 态势感知平台通过蜜罐获取攻击者的接入位置，及时发现攻击者信息。

图 3-9 精准溯源



1. 黑客从互联网向外部服务发起扫描探测或内网被感染主机发起横向扫描。
2. 互联网出口防火墙，内置诱捕探针，识别黑客的扫描行为；接入网交换机内置诱捕探针，识别异常主机的扫描行为。
3. 诱捕探针把攻击源诱导到诱捕器蜜罐。
4. 蜜罐识别攻击行为，通过交互获取攻击行为信息；网络控制器获取主机位置，定位终端接入位置信息。
5. 蜜罐向安全管理中心上报攻击告警信息；网络控制器向安全管理中心上报终端接入位置信息。
6. 安全管理中心进行关联分析，展示攻击信息或中毒终端接入位置信息。
7. 安全管理中心联动网络控制器联动网络安全设备进行精准阻断。

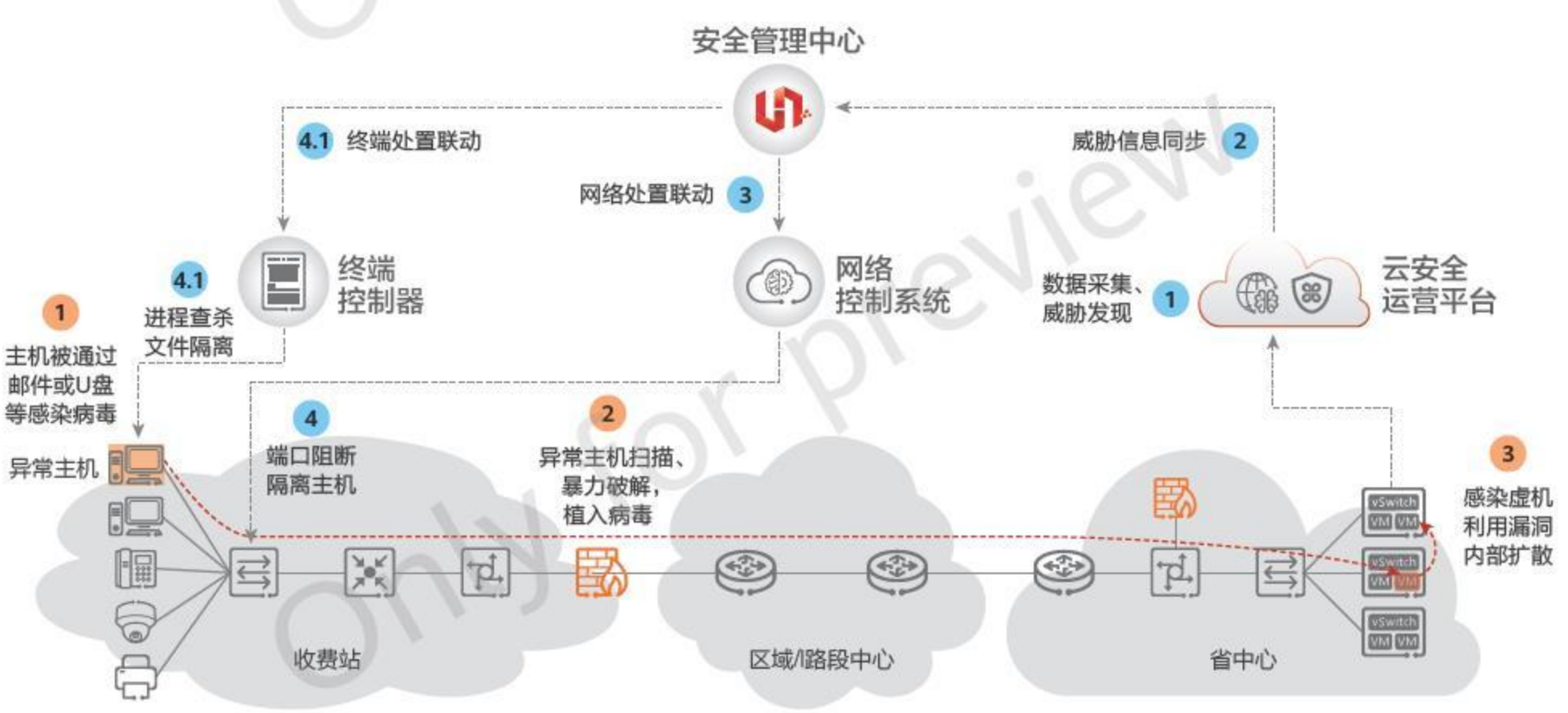
3.2.3 近源阻断

安全态势感知平台发现威胁后，需快速处置威胁，通过自动化的手段提升威胁事件的处置效率，避免威胁扩散。威胁处置原则如下：

» **阻断点自动识别：**安全和网络联动，自动识别最佳阻断点。
» **近源阻断，降低风险：**在最靠近攻击源的设备上进行阻断，避免威胁扩散。
» **威胁自动或人工处置：**对于判断准确率高的威胁，可采用自动化处置的方式阻断威胁，对于检测率不准确的威胁，采用手工处置的方式，避免误阻断影响正常业务。

如图 3-10 所示，省中心发现病毒，通过溯源，在收费站接入层交换机快速近源处置。

图 3-10 近源阻断



病毒扩散过程

1. 主机通过 U 盘等感染病毒。
2. 异常主机通过扫描、暴力破解，虚机被植入病毒。
3. 感染虚机利用漏洞，向省中心云平台业务主机横向扩散。

风险处置流程

1. 风险分析发现：云安全运营平台采集数据，发现数据中心的威胁信息，并进行处置。
2. 安全态势统一呈现：安全管理中心和云安全运营平台协同，由安全管理中心汇总云上云下的威胁告警，进行全网威胁统一可视化呈现。
3. 威胁精准近源处置：安全管理中心精准溯源，根据攻击路径，联动网络控制器及终端控制器处置风险。
4. 威胁隔离阻断：网络控制器向接入交换机下发策略，对主机进行隔离或阻断。同时对终端控制器下发进程查杀，文件隔离的策略，在终端上终结病毒文件。通过云网端联动，威胁近源处置，威胁平均遏制时间由小时级缩短到分钟级，在靠近威胁的地方快速阻断，避免威胁扩散。

3.3 云网端一体化防护大脑：统一安全运营

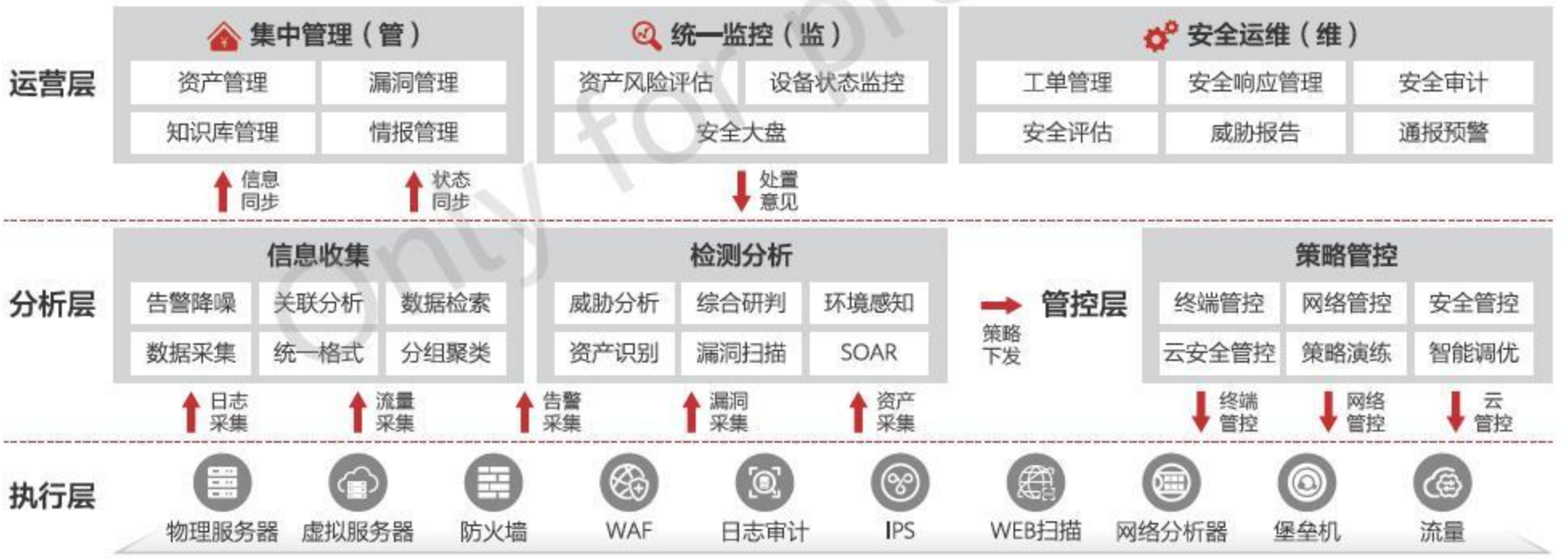
3.3.1 公路安全运营方案概述

安全运营指通过已有的安全系统、工具来生产有价值的安全信息，通过组织人、工具（平台、设备）、发现安全问题、验证问题、分析问题、解决问题并持续迭代优化的过程。公路的安全运营体系包括安全管理制度，安全技术体系，安全支撑服务，安全监督及考核等内容。安全管理制度包括组建安全运营团队，制定安全管理规章制度，开展安全意识教育及安全技能培训等。安全技术体系是指采用等保安全防护，多维纵深防护、云网端协同防护等安全技术手段，从基础安全和新技术安全两方面进行安全防护，形成多维度、体系化的纵深防御架构。安全运维支撑指通过集中管理，统一监控，运维活动，实现安全的集中运营控制与有效管理，确保公路安全运营保障体系的有效落地。安全监督及考核指通过开展常态化安全验证手段，如周期性安全漏洞扫描、基线核查、渗透测试、攻防演练等工作，保证安全管理、安全技术和安全措施的有效性，通过一系列安全运营评价指标，衡量评价安全运营质量水平，持续改进，实现安全质量的螺旋上升。本文主要阐述安全运维支撑平台的架构及实践。安全管理制度、安全监督考核等内容不作为本文重点，相关标准及规范可参考城轨协相关安全要求。

3.3.2 公路交通安全运营平台设计

公路网络分支多，站点多，安全设备数量庞大，同时随着业务发展及公路持续建设，新建收费站，区域及路段中心扩容导致安全策略变更频繁。安全运营建设虽然投资大，但防御效果不佳，部分安全设备无法 100% 发挥作用，安全运维严重依赖安全人员的专业技能以及对各类安全设备的熟练操作，依靠大量的人工操作保障安全体系的运营。一个智能化、自动化的安全运营平台能够对海量的安全数据自动采集和治理。通过设备之间的协同联动自动完成庞杂的分析、取证、响应等操作，针对不同的业务场景做出准确、合理、高价值的分析，为运维人员提供决策依据。运维人员只需聚焦于最终的决策判断，并执行处置动作。基于上述问题，城市轨道交通安全运营平台根据云网安架构划分为四层架构，分别是执行层，分析层，管控层和运营层，其架构如图 3-11 所示。

图 3-11 安全运营平台架构



» **执行层**

执行层也是安全数据的生产者和安全策略的执行者，网络中所有生成安全信息的实体和软件都属于执行层，这些安全数据涵盖了网络中能够检测到的所有安全日志和告警信息，通过对执行层数据的分析能够对现网安全状态进行评估和感知。

» **分析层**

执行层产生的海量安全信息是威胁分析的基础，分析层通过安全大数据平台的组件能力对安全数据进行统一格式化处理，并通过降噪，归并去重，分组聚合，关联分析，建立索引等方式对数据进行治理和加工，为运营层的调用及检测分析提供数据基础。

» **管控层**

管控层负责对全网终端、网络、云的安全策略的管控，根据业务应用互访关系自动编排和部署安全策略。对部署策略的合规性检查，业务影响评估，以及策略的冗余分析尤为重要。通过部署控制器对安全设备进行统一管理，策略的自动编排和智能调优，能够有效提升安全资源的管理和运维水平，提高安全运营效率，如图 3-12 所示。

图 3-12 管控层

» **运营层**

安全运营是以资产为保护对象展开的一系列管理，监控，运维操作。运营层分为集中管理，统一监控，安全运维三部分功能。

a. 集中管理

集中管理包括对资产，漏洞，知识库及情报的管理，对于资产的精准识别和全量探测是安全运营的必要前提。

资产的漏洞为网络攻击提供了可行性，能够标识资产的脆弱性，通过对漏洞的及时管理能够有效降低攻击成功的可能性。安全设备的检测能力依赖知识库的覆盖广度和时效性，对漏洞库，病毒库，补丁库等知识库集中管理能够有

效发挥安全设备的检测能力。情报是辅助威胁判定的重要信息，通过关联 0Day 漏洞，新型攻击事件等情报，提前做好预防，必要时通过手动更新知识库的方式进行专项防护。

b. 统一监控

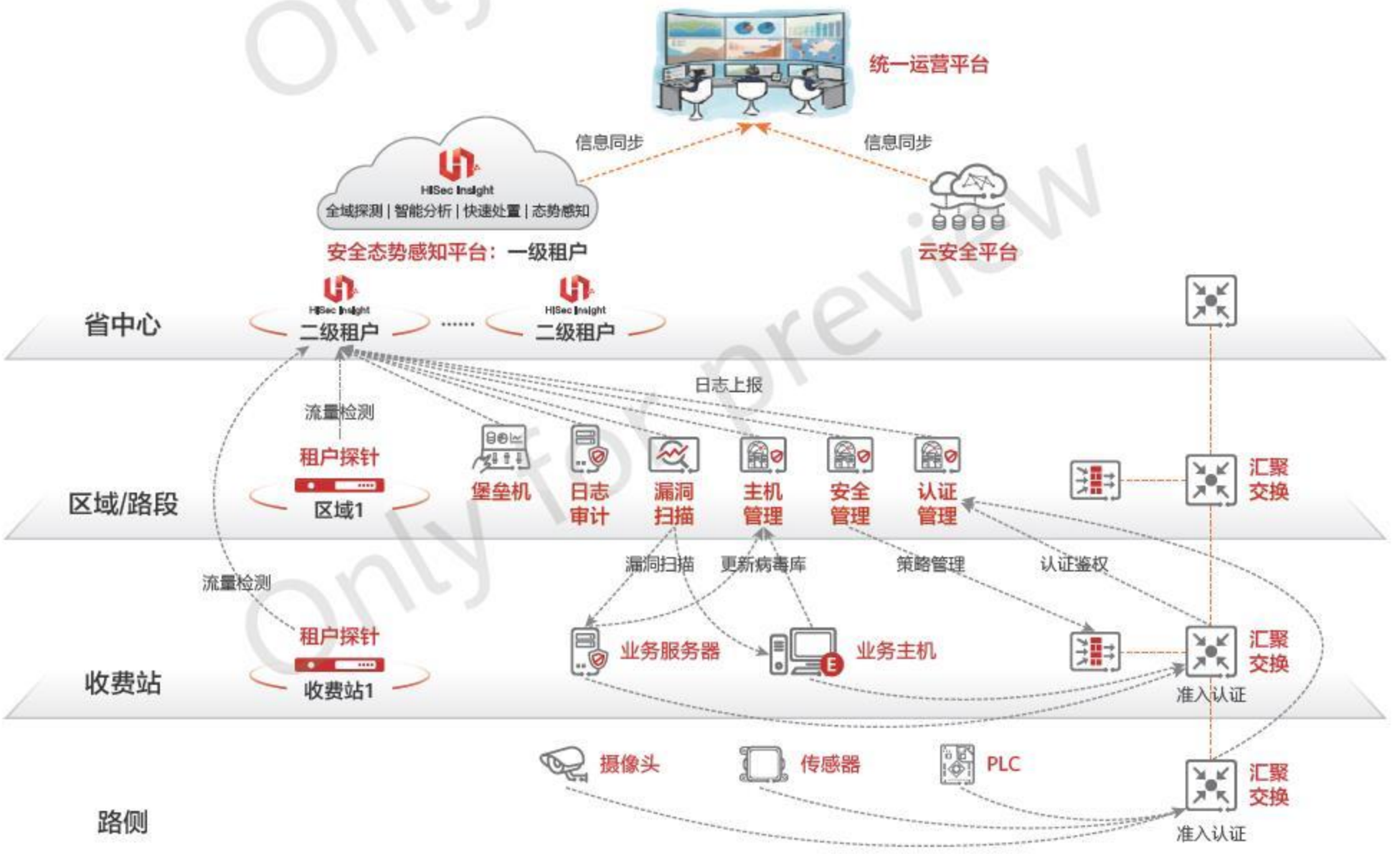
统一监控包括资产风险评估，设备状态监控，态势感知以及可视化展现等功能，在资产的集中管理的基础上，结合业务系统及信息资产的重要性，对资产进行风险评估，对可能导致生产业务受损的关键资产进行识别和风险评估，为下一步安全运维操作提供处置依据。公路场景中，不同区域 / 路段可能属于不同的业主，需要各自分区运维，网络和专业系统的运行环境及防护重点有所不同。在实际运维过程中，多个区域 / 路段中心的场景化安全监控平台与一个集中的安全监控平台的级联方式，会取得较好的整网的安全态势感知效果。

c. 安全运维

安全运维是支撑安全运营平台体系化运转的核心能力，包括安全基线配置运维、告警管理、事件分析、响应处置、通报预警、溯源取证、威胁报告输出及工单管理等功能。公路安全运营过程中将大量的分析，取证，响应等人工处置操作以及专家经验转化成程序和脚本自动化完成，最大化安全设备的防护能力，可以有效减少运维人员的学习及培训成本，提升运维效率，同时降低误操作及误判的概率。

基于上述安全运营平台架构，公路场景下安全运营部署架构如图 3-13 所示。

图 3-13 安全运营部署架构



- **省中心：**省中心作为统一监管单位，承担全省的统一安全监管职责，是安全运营管理的核心枢纽，部署统一安全运营平台、云安全管理平台、安全态势感知平台。其中态势感知平台为区域 / 路段中心提供租户式态势感知能力。
- **区域 / 路段中心：**在省中心的监管下，承担以区域为单位进行分区防护和运维管理职责，部署探针、堡垒机、日志审计、漏洞扫描、终端管理、安全管理、认证管理等安全设备，区域内所有公路网络提供安全防护能力。区域路段中心部署的租户探针，将流量信息及告警数据上报给至所属态势感知租户下。认证管理系统联动路段、收费站、路侧的交换机，实现全路段内资产的准入及是被管理。
- **收费站：**受管理处安全监管和防护，管理处将安全能力下沉到收费站，为收费站的终端，服务器，网络提供安全防护能力，包括设备准入认证、流量安全检测、安全策略管理、主机安全，漏洞扫描等。

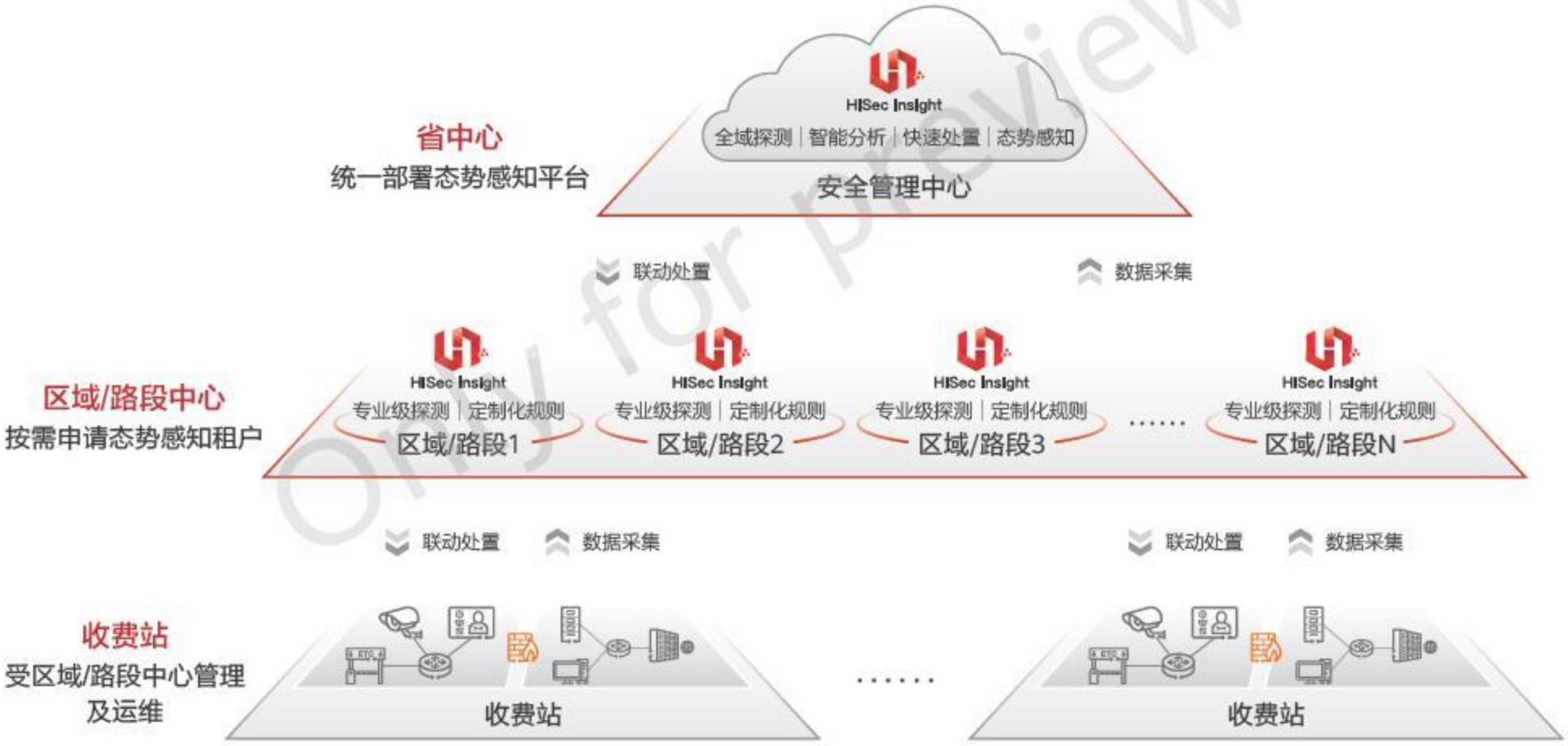
3.3.3 态势感知级联管控

公路交通网络由于省中心统一监管，区域 / 路段分区防护的两级管理现状，以及收费质量提升场景下态势感知全网覆盖的要求，态势感知平台需要多级部署。

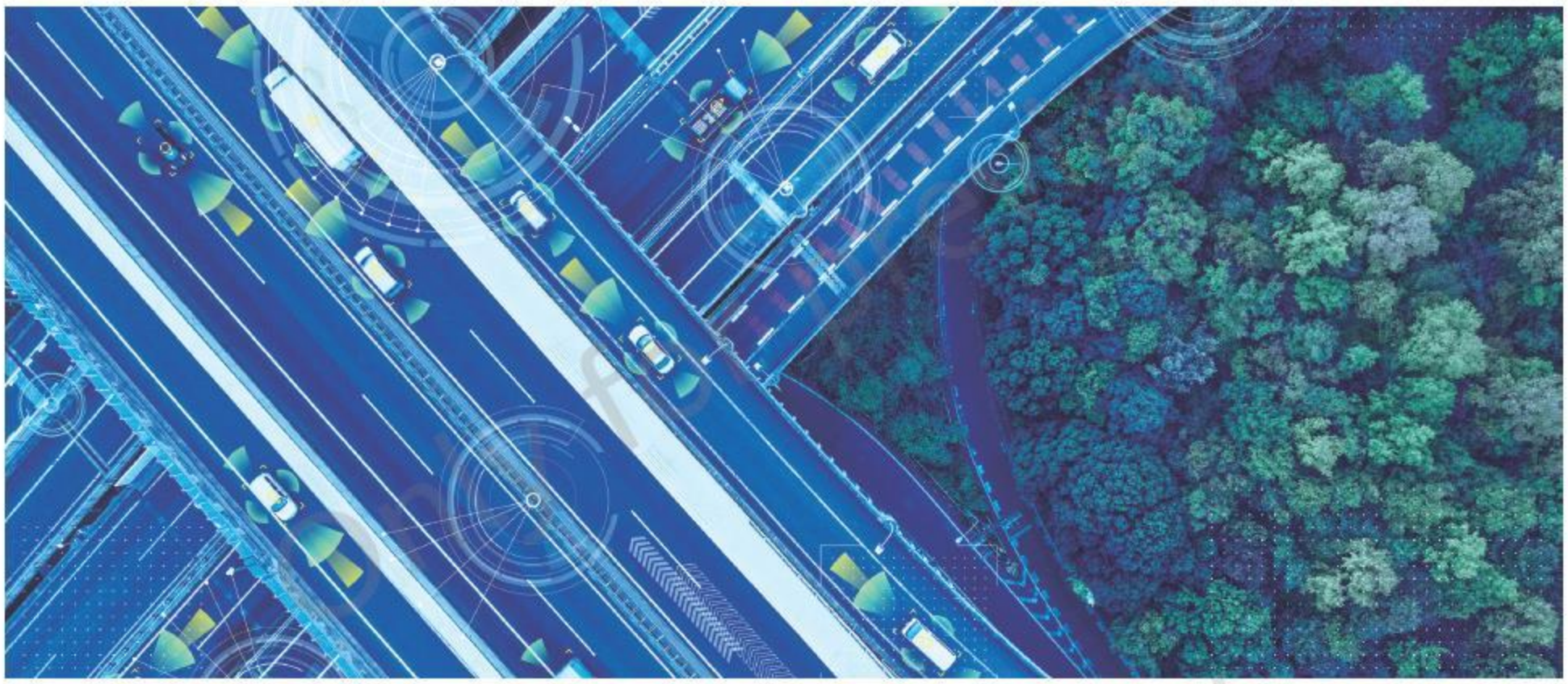
传统的态势感知级联方式是两套态势感知平台通过相互调用接口实现上下级平台之间的交互和信息同步，但这种方式存在信息同步不及时，状态不一致，可扩展性差，升级管理复杂等问题。因此新一代的态势感知平台通过同一套态势感知平台的多租户的方式提供态势感知平台的级联管控能力。

多租户作为实现分布式运维和云化部署的关键特性，能够提供基于租户的数据采集、处理、分析和呈现，同时实现同级租户之间的账号，资源，以及运维界面之间的隔离，下级租户的数据能够被上级租户实时全面掌握，非常适合公路场中省中心全局统一监管，区域中心分区运维的组织架构，其架构如图 3-14 所示。

图 3-14 省中心态势感知平台



- **省中心（一级租户）：**能够实时全局查看所有区域中心（二级租户）所有威胁事件以及事件处置状态，资产信息及资产准入及在线状态。省中心管理员可以根据不同区域的安全态势及威胁情报，统筹考虑其他区域的安全运维策略，实施跨区协同及情报共享。
- **区域 / 路段中心（二级租户）：**能够实时全局查看所在区域中心的威胁事件以及资产信息，但不能查看上级租户或其他平级租户的任何信息，不同二级租户之间的信息完全隔离。
- **收费站：**按照《高速公路联网收费系统优化升级工程方案》中的要求，态势感知能力要覆盖到收费站级，探针要部署到收费站，每个管理处都管理着下属数十个收费站，为了简化运维和降低组网成本，本方案中采用了防火墙和探针合一部署的架构，实现有防火墙的地方就能覆盖态势感知能力，真正实现了态势感知能力全网覆盖的同时降低了安全投资成本。



3.3.4 安全大模型辅助安全运营

安全防护效果不仅取决于各类安全防护设备的部署，更取决于对安全设备，网络环境，业务访问过程的持续的监测，常态化的运维以及高效的处置闭环能力，这要求安全运维人员具备较高的安全技术水平，丰富的实践经验以及长时间的专注工作。因此企业或机构往往因为没有安全运维人员，或安全运维人员能力不足而导致安全运维效率低下，威胁处置不及时，网络中病毒泛滥等情况。

而随着 AI 大模型的出现和持续演进，为安全运营提供了新的解决思路，即通过大模型的学习能力，训练符合行业场景的安全数据，并结合专家经验和指导，生成智能的安全运维模型，辅助安全运维人员完成繁琐的检测，分析，溯源，处置，闭环等运维等操作。

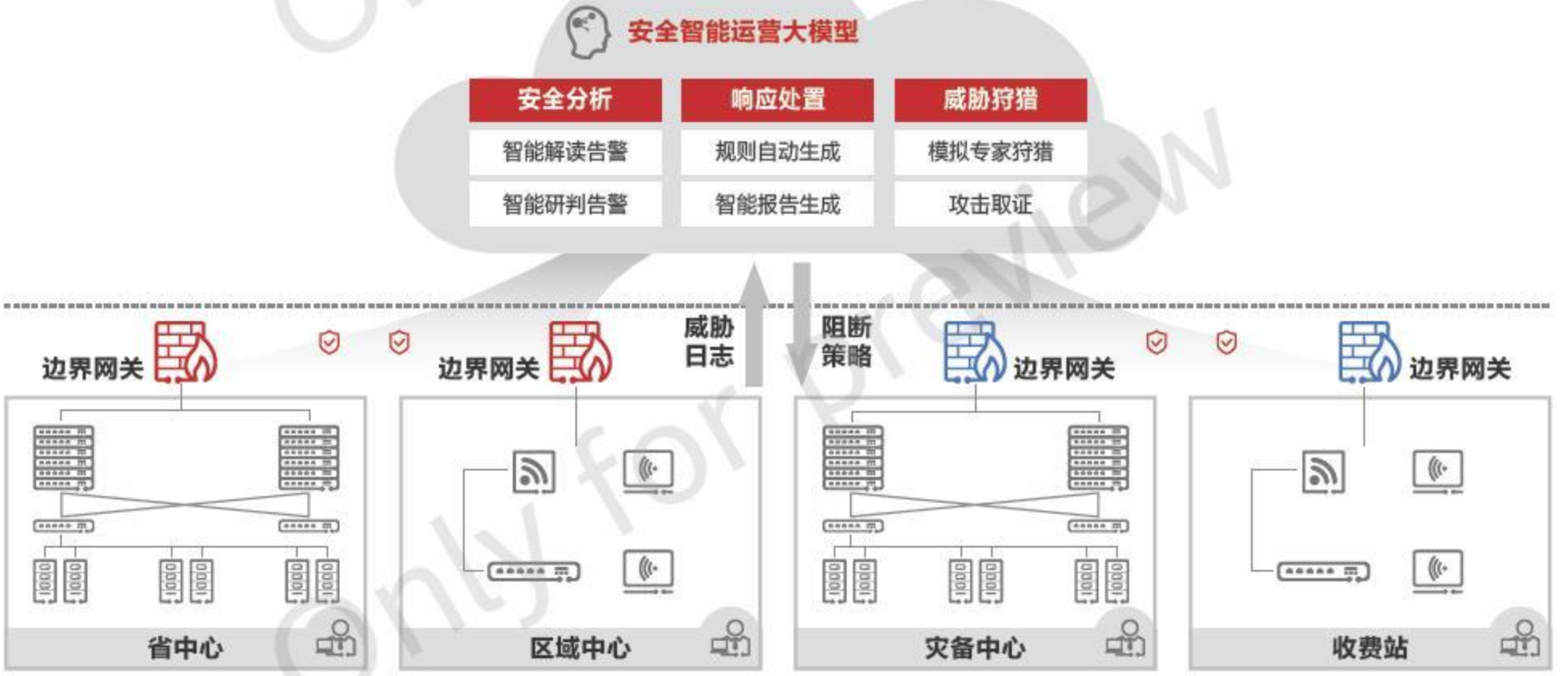
安全大模型不仅可以出色的完成智能辅助运营能力，还可通过大模型探测网络的脆弱性，通过学习各类病毒、工具以及人的攻击行为模式，识别网络最有可能遭受的攻击以及安全的薄弱点，并进行针对性的防护。

下面我们逐一介绍安全智能运营及安全智能对抗两个大模型进行介绍：

» **安全智能运营大模型**

安全智能运营大模型分为安全分析，响应处置，威胁狩猎三个功能，其架构如图 3-15 所示。

图 3-15 安全智能运营大模型



a. 安全分析功能：

①. 智能解读告警：现网安全设备及应用系统每天生产亿级别的告警及安全信息，难以通过人工进行全量分析，大模型通过学习及专家辅导后，能够读懂告警信息，并提炼相关关键字段进行统计、上下文分析，关联等，并自动形成索引，供后续智能研判告警使用。

②. 智能研判告警：通过智能解读告警，大模型经获取了海量的安全告警信息后，融合安全运营专家经验，通过威胁推理，综合研判，从中筛选出高价事件及相关的攻击链条，将威胁平均检测时间从数小时降低到分钟级，极大提升威胁识别效率

b. 响应处置功能：

①. 规则自动生成：基于智能研判告警的结果，关联网络拓扑、相关资产及漏洞信息，自动生成安全处置策略，并通过模拟仿真运行方式判断安全规则对现网业务的影响及对威胁的处置效果，当达到预期要求后，自动生成安全处置规则及策略，下发给可联动的安全设备进行威胁处置。

②. 智能报告生成：能够周期性生成月、周、日报，并基于不同安全运维人员差异化需求生成不同内容的安全报告。

c. 威胁狩猎功能：

①. 模拟专家狩猎：大模型会学习已知的各类攻击事件及攻击模式，从中总结出常用的攻击手段及攻击意图，尤其是对 APT 攻击的每个步骤进行深度挖掘，通过对工具或恶意程序的二进制逆向分析及共行为的识别，能够检测出常规安全软件及设备无法检测出的高级威胁事件，这类威胁事件通常由具备较强专业技能的个人或组织对目标发起针对性的长期渗透攻击。

②. 攻击取证：在威胁狩猎过程中，大模型会对必要的攻击行为或痕迹进行取证，提高攻击者被发现的风险，并为后续可能的法律追究提供取证信息。

» **安全智能对抗大模型**

网络安全的本质是攻击者与防守方之间的持续的，高强度的对抗和博弈，安全智能对抗大模型通过学习攻击者的攻击模式和过程，总结出常见的攻击套路和攻击方式，并进行针对性的防护，其架构如图 3-16 所示。

图 3-16 安全智能对抗大模型

首先，大模型对所保护的网络进行模拟探测，识别出网络中存在安全漏洞及薄弱环节，结合常见的渗透方式生成可执行的工具脚本，并对漏洞实施探测和结果评价。

其次，基于探测结果，大模型针对探测行为进行威胁建模，并结合网络拓扑，应用互访关系，安全策略配置等生成最佳的联动处置策略，协同各类安全设备进行应急响应处置，并对受影响的业务应用进行恢复。

最终，通过安全智能对抗大模型发现并消减了网络中存在的安全风险，持续提升网络安全健康度。

» **安全大模型对安全运营的提升效果**

基于上述两个安全大模型能力，对安全运营能力的提升主要体现在以下几点

a. 告警降噪

对海量安全告警进行聚合和消噪，减少 95% 的低价值或无效告警信息，并提升告警准确度。

b. 实时响应

对海量数据进行实时分析和处理，快速做出响应，将 MTTD（mean time to detect，平均检测时间）有数小时降低到分钟级。

c. 自动处置

通过专家经验模型和 AI 推理能力，实现 96% 以上安全事件的自动化处置。

d. 运维效率

通过与传统人工运维效率的对比，安全大模型对整体安全运维效率的提升在 160 倍以上。

04 云南交投安全建设实践

云南省交通投资建设集团有限公司（简称云南交投），是云南省省属国有企业，是云南综合交通体系建设主力军、云南综合交通投融资主平台、云南综合交通全产业链经营主体。截止 2022 年底，建成通车高速公路 6180 公里，占全省通车里程 10249 公里的 60.3%。产业涵盖了公路、铁路、水运、航空等综合交通的规划设计、投资建设、运营管理、经营开发、物资贸易、交通科技等全产业链领域。

云南交投积极主动贯彻落实新发展理念，全面推进实施《科技赋能三年行动方案（2022-2024 年）》，进一步优化科技创新布局，落实好集团公司党委双赋能，强“两翼”，全面提升“投融建管营”能级，推进数字赋能专项行动的安排部署，形成“云上交投”数字品牌，一批数字产品实现市场化应用，数字应用和数字经济业态初步形成。

4.1 安全建设目标

根据数字交投“十四五”发展规划要求，需达到网络安全保障有力，等级保护合规率大幅提升，行业网络信任体系初步建立，关键信息基础设施和关键数据资源保障水平有效提升，安全防护和维护政治安全能力显著增强，主动防护、纵深防御的行业网络安全综合防范体系基本建立。

结合云南交投数字赋能行动规划，建立健全网络安全管理体系，明确各部门各单位网络安全管理职责，建立完善的基础制度，覆盖安全管控、组织机构、规范标准、安全技术、安全运营等五个重点部分，保障集团安全有序的发展，并对安全建设提出了针对性的目标。

1. **全面提升预警监测和应急处置机制技术支撑能力：**针对网络边界扩大，应用集中上云，数据融合共享，实现安全态势感知能力全网覆盖，提升安全预警能力，横向覆盖终端、网络、云平台，纵向覆盖省中心，管理处，收费站。
2. **护航交投数字化转型，数据安全能力有效提升：**针对数字化转型带来的数据安全风险，提供切实可行的安全防护能力，结合云南的区域特点，针对敏感数据，跨国数据，个人隐私数据等，实现高敏感业务安全优先，非敏感业务效率优先，切实提升数据安全保护能力。
3. **贴合交投发展规划，安全管理制度切实落实：**针对愈发严峻的外部网络态势及国际局势，国家公路发展规划，集团业务演进路线，切实落实常态化安全运营动作和管理制度，提升运维效果，及时识别风险并处置闭环，持续净化集团网络环境。
4. **积极响应并遵守国家安全政策，安全标准规范严格执行：**针对数字化转型后的新环境，梳理规范化的网络安全标准，为终端入网，资源申请，开放权限，审批审计等全流程提供简要明确，可执行，可监督，可审计的安全标准规范。

4.2 当前成果及整体规划

云南交投在《科技赋能三年行动计划（2022-2024）》通过三个阶段的规划，分步骤完成安全能力的建设，如图 4-1 所示。

图 4-1 安全能力建设

» 阶段一，打基础：安全能力合规化建设

2022 年，遵照国家网络安全方面的法律和条例，严格参考等级保护的思路和标准，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，对终端，网络，边界，云平台，数据等不同实体提供安全防护能力。针对安全现状分析发现的问题进行加固改造，为系统稳定运行提供有力保障。云南交投逐步完成了云平台等保三级防护，关键信息基础设施保护，商用密码应用安全评测要求等一系列安全建设，打造了牢固的安全及合规基础，为已经上云及正在上云的业务应用提供了必要的安全防护能力。

» 阶段二，建能力：安全能力体系化建设

2023 年，在一阶段的建设基础上，云南交投端到端打通了数据安全、云平台安全、网络安全及终端一体化管理体系，构筑了数云网端一体化防护能力，包括建立了级联管控的统一态势感知平台；全网资产可视、可控，可管的统一资产管理能力；针对敏感数据及办公数据的零信任访问体系；收费网，视频网，监控之间数据安全交换能力；同时优化了安全管理制度，输出了为后续建设提供标准的标准规范文档，并启动了人才培养计划，为云南交投科技赋能行动提供人才储备。

» 阶段三，提效益：安全能力智能化建设

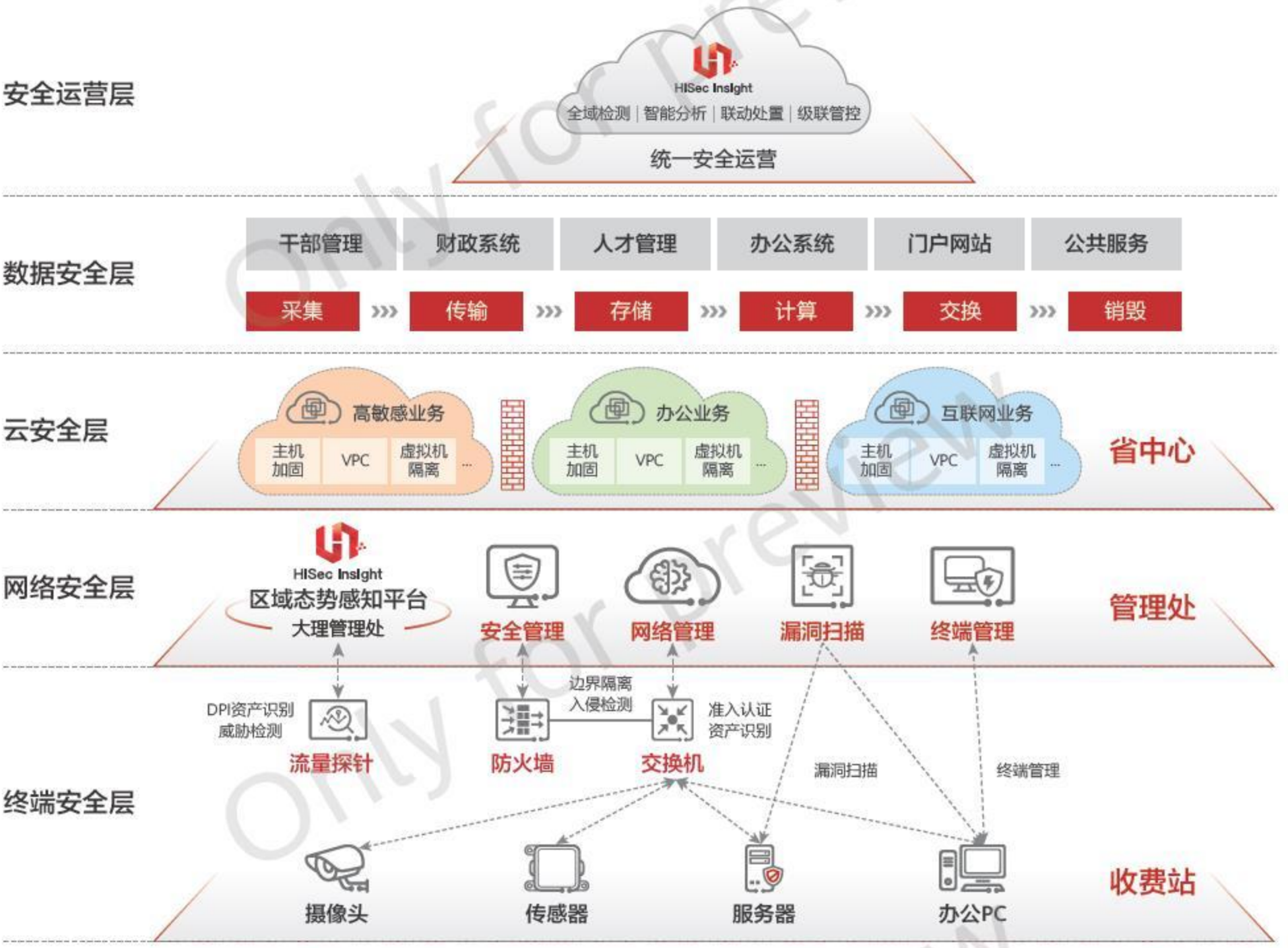
完成阶段二的建设内容后，云南交投已建成体系化的安全防护能力，但仍需结合数字化转型后的业务发展及需求，不断优化和完善整体安全运行体系。随着业务系统的规模上云，海量数据的融合共享，安全需要进一步结合应用和数据进行精细化，场景化的优化，包括应用系统的零信任改造，安全能力的服务化调用，以及持续优化的安全运营平台等。同时云南交投抢抓“一带一路”、面向印度洋国际陆海大通道、面向南亚东南亚辐射中心建设等重大战略机遇，持续优化数据安全防护体系，基于云南特色，研究跨国数据安全交互方案，通过集中管理，统一监测，安全运维，实现从威胁事件的识别、防御、检测、响应、恢复等安全环节进行闭环管理，构建端到端的安全运维体系，提升安全维护的数字化、智能化水平。

4.3 安全建设实践及成效

云南交投数、云、网、端一体化安全建设方案

基于云南交投集团安全防护需求，信息安全体系不仅要实现从终端、网络、云平台、业务应用到数据平台等实体的安全防护，还应将网络、安全、云平台的组件和安全能力统一调度和管理，提供一体化、可视化、全局化的体验，实现统一安全运营和协同防护，提升效率。云南交投安全架构分为安全运营层，数据安全层，云安全层、网络安全层以及终端安全层，其架构如图 4-2 所示。

图 4-2 数、云、网、端一体化安全架构



» **安全运营层**

安全运营层部署在省中心，承担集团统一运维和运营管理功能，从运营角度实现对全网安全事件的统一监管、情报同步、跨区协同等功能。通过部署安全运营中心，采集数据安全信息，云平台安全信息，网络安全信息，以及终端安全信息进行智能分析，综合呈现，并提供多级管控平台，是交投安全体系的核心。

» **数据安全层**

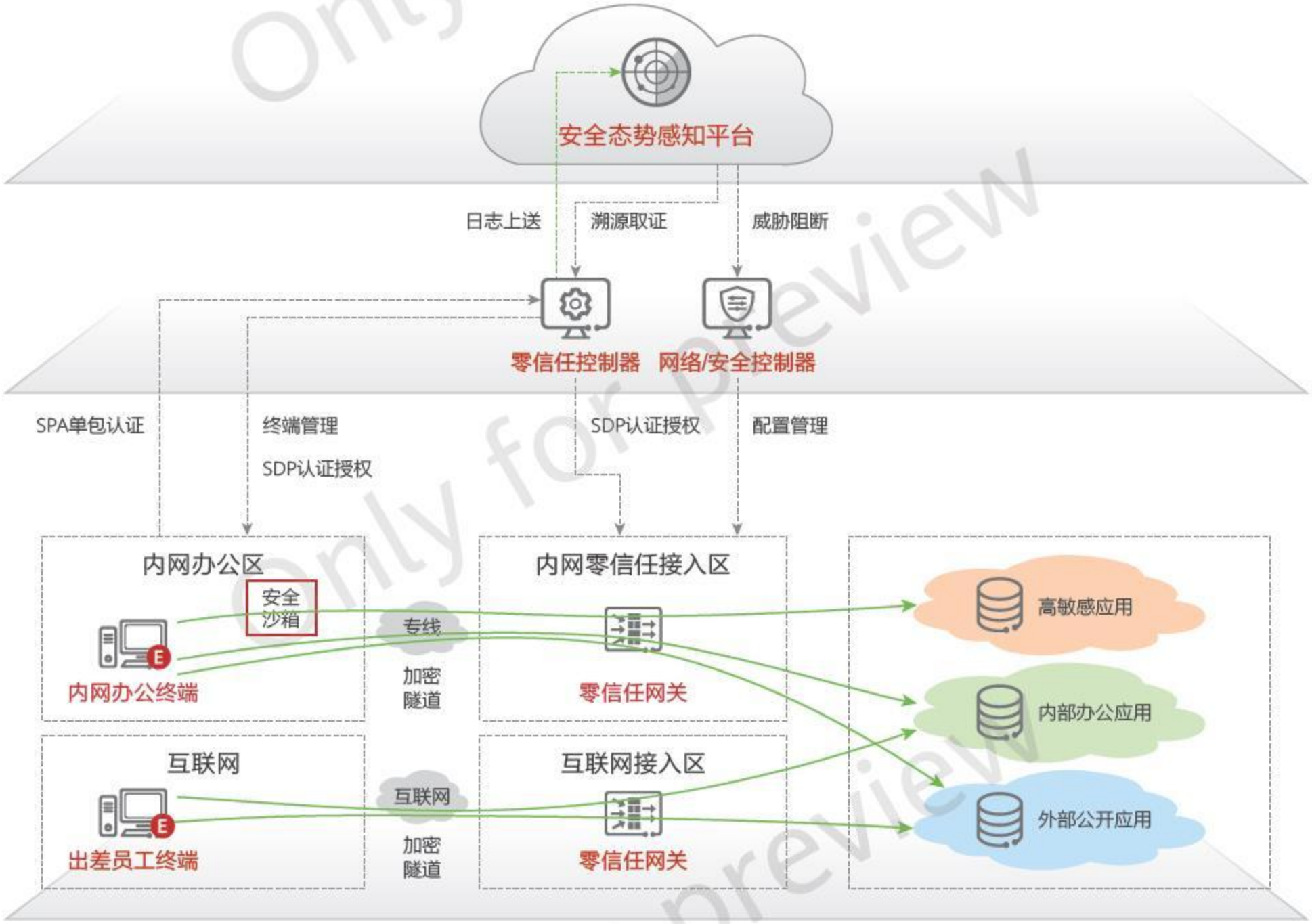
交投业务存在部分高敏感业务和数据，例如干部管理、财务等业务系统的数据密级较高，需要提供数据安全防护能力，避免数据丢失，泄露以及损毁，数据安全层通过对数据的分级分类，零信任访问控制，安全沙箱等能力，从技术层面上确保高敏感数据被合法使用，非敏感数据被高效使用，确保每个业务和数据能够根据防护需求被安全、合规、可信的访问和使用。

云南交投对业务应用进行了分区规划，例如财务及干部管理等应用因其业务及数据的敏感程度，被划分到安全密级高

的黄区，办公应用属于内部公开的普通办公数据，被划分到安全密级中等的绿区，门户网站等业务应用及数据属于外部公开的信息，被划分到可对公网公开的访问的蓝区。

结合零信任安全体系，构筑持续认证，动态授权，精细管理的数据安全访问架构，如图 4-3 所示。

图 4-3 数据安全访问架构

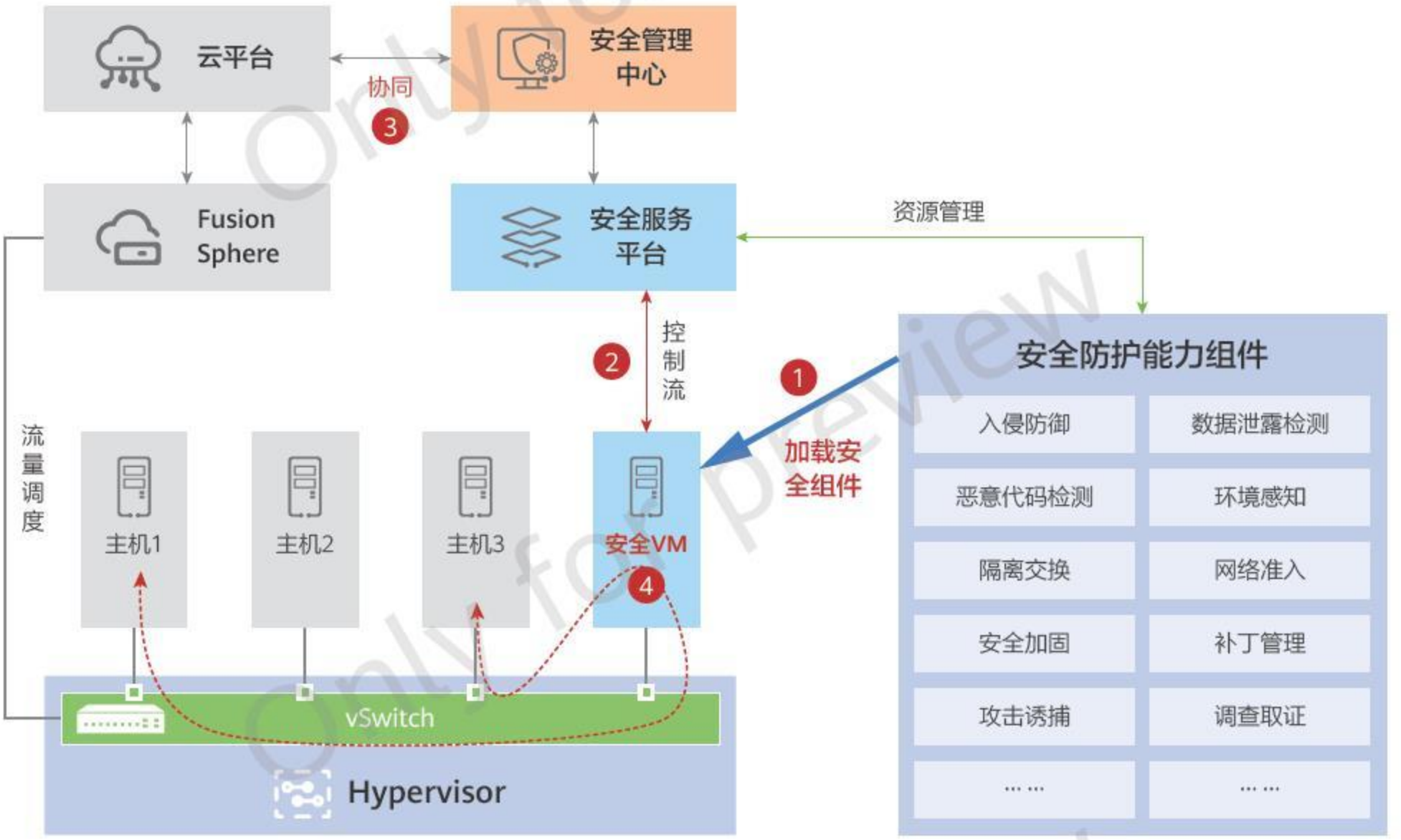


» **云安全层**

云南交投数字化转型的一个核心要素就是应用和数据的云化部署，云内业务系统的安全防护通过云平台内生安全服务来保障。云南交投采用云原生安全架构，构筑了统一管理，按需申请，便捷部署的云原生安全防护能力。

云原生安全能力即云平台结合自身架构及组件能力，与安全组件深度定制，提供的高效、便捷、服务化安全组件能力，云租户根据需求申请云安全服务，云平台将云安全组件加载到云租户所在 VPC 或 VM 上，其架构如图 4-4 所示。

图 4-4 云安全服务架构

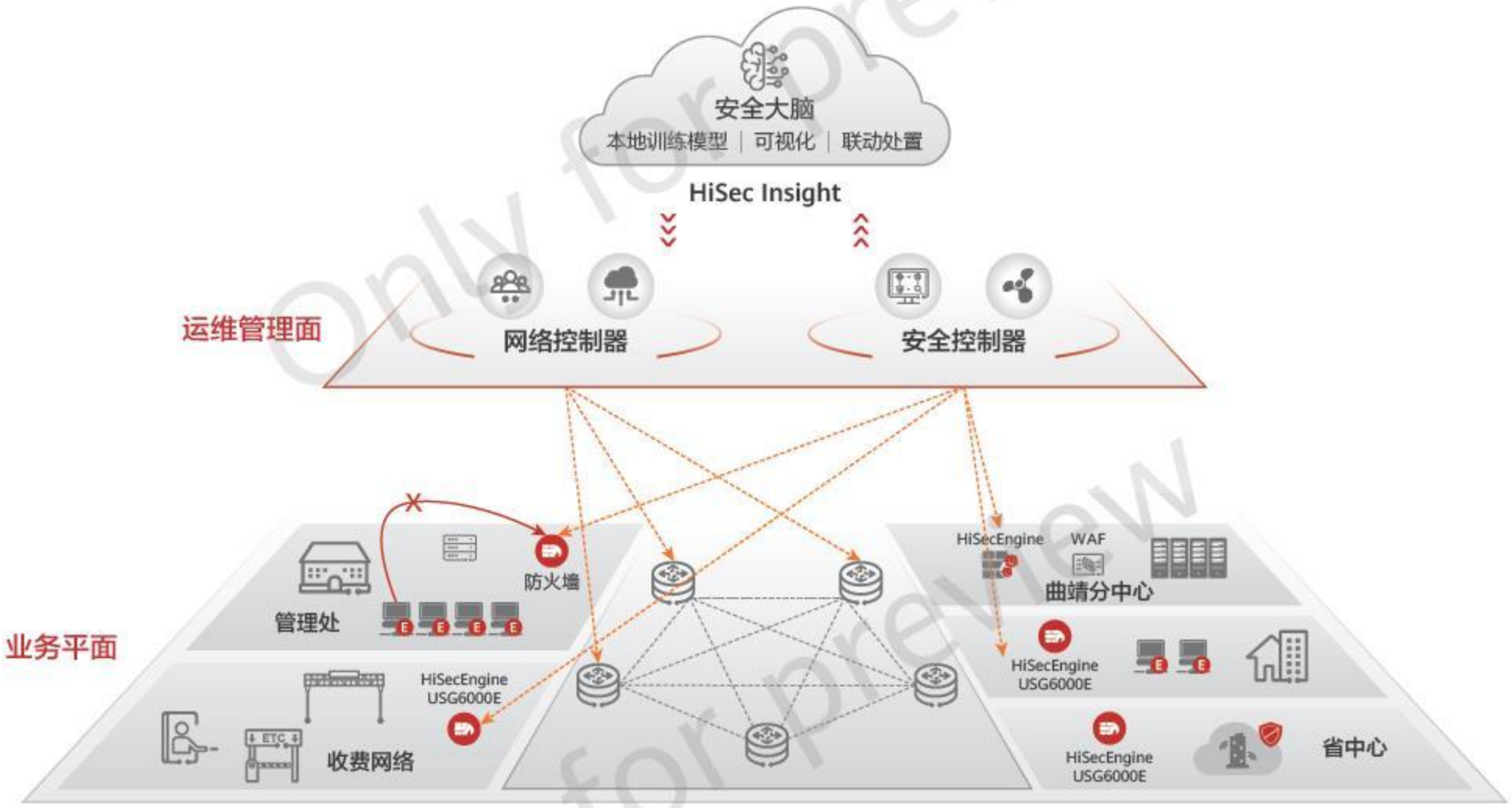


云原生安全能力有别于采用独立安全资源池的方案：通过核心交换机引流，将云平台用户的云上业务流量通过 EIP 牵引到云外安全资源池内进行清洗和过滤的方式。云原生安全不需要进行不必要的引流操作，无需暴露内部 IP，安全能力更丰富，约束更少。

» **网络安全层**

交投的信息化建设不仅包含省中心的数据中心云平台，还包含管理处（区域中心 / 路段中心）、收费站及隧管所等区域。为了更高效，可靠的实施运维管理，云南交投在已有业务网络架构的基础上，构筑了运维管理平面，与业务平面逻辑隔离，当业务平面的服务器或终端设备被攻破后，不会将风险扩散到网络设备及安全设备上。当业务平面遭受网络攻击导致网络阻塞后，可通过运维平台快速对网络进行运维和处置，其架构如图 4-5 所示。

图 4-5 网络安全架构



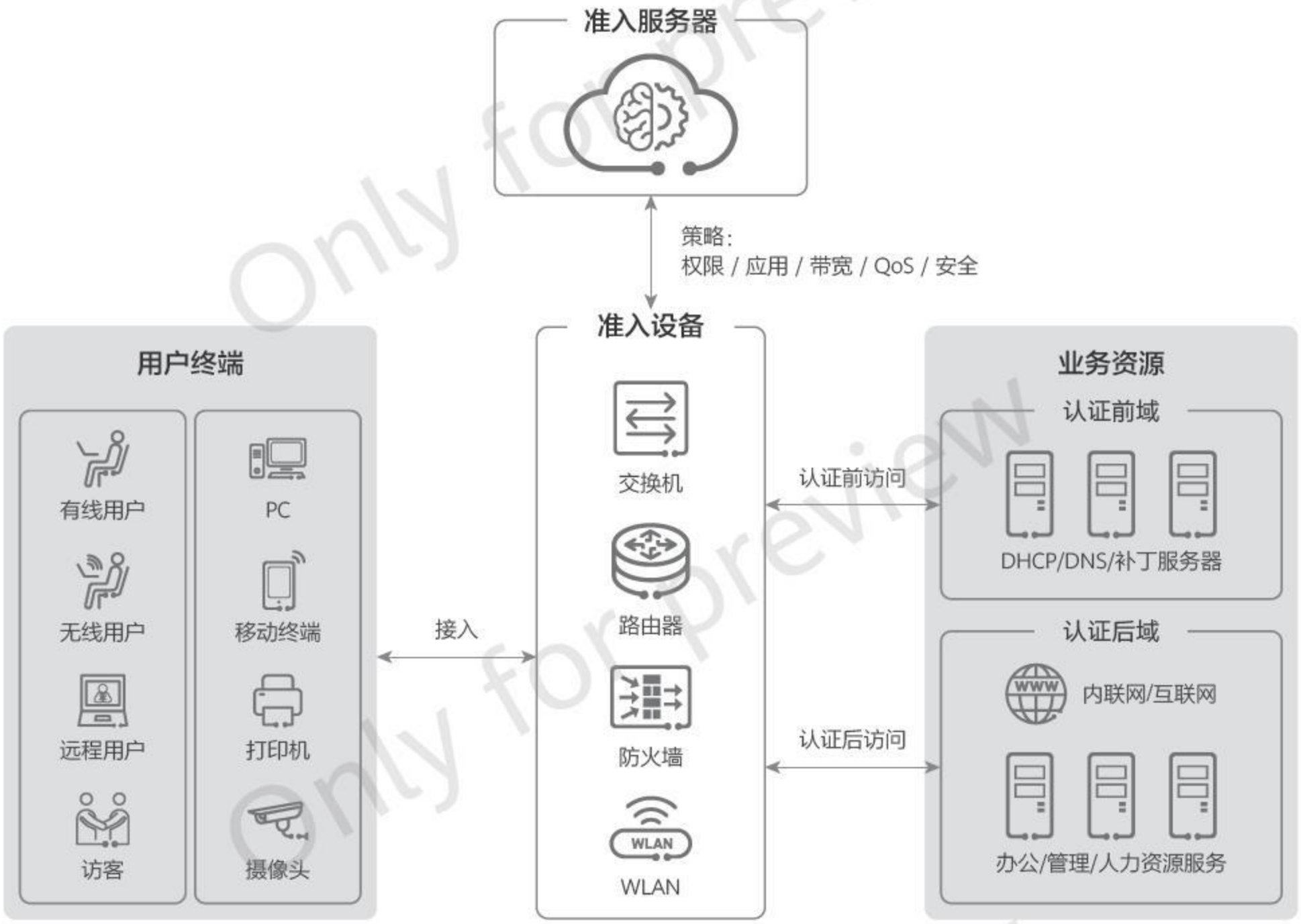
所有网络设备及安全设备的运维管理入口统一接入运维管理平台，业务平面所有资产无法直接访问网络设备及安全设备，当业务平面发生阻塞或故障时，不影响运维平面的网络，通过网络控制器快速诊断网络问题并恢复，通过安全控制器快速诊断安全问题并恢复，有效提升了云南交投网络的可靠性与可维护性。

» 终端安全层

云南交投网络终端准入控制的方案由三个组件组成，如图 4-6 所示。

- **用户终端：**各种终端设备，例如 PC、服务器、打印机、摄像头等。
- **准入设备：**准入设备是终端设备访问网络的认证控制点，对接入网络的终端发起认证要求，并将终端提交的用户信息上报给准入服务器进行认证。准入设备是准入策略的执行者，按照制定的准入策略实施相应的控制动作（如允许接入网络或拒绝接入网络）。准入设备可以是交换机、路由器、无线接入点、VPN 网关或其他安全设备。
- **准入服务器：**准入服务器是网络准入控制的大脑，主要功能是实现对终端的认证和授权，用于确认尝试接入网络的终端身份是否合法，并指定终端所能拥有的网络访问权限。准入服务器通常分为认证服务器（如 RADIUS（Remote Authentication Dial-In User Service，远程身份验证拨号用户服务）服务器）和用于存储用户身份信息的用户数据源服务器。

图 4-6 网络准入控制的技术架构



网络准入控制系统把业务资源分为两类：认证前域和认证后域。顾名思义，认证前域即终端设备在完成认证之前可以访问的区域。该区域主要部署 DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）服务器、DNS（Domain Name System，域名系统）服务器、补丁服务器等。在终端通过认证前，准入设备只允许终端访问认证前域的资源。其他核心资产，即认证后域的资源，如各种业务系统等，只允许认证通过的终端访问。网络准入控制的工作流程如下。

a. 终端身份认证请求：终端发送自己的身份凭证给准入设备。
b. 终端身份认证：准入设备将终端的身份凭证发送给准入服务器进行身份认证。
c. 终端身份校验：准入服务器收到终端的身份凭证后，进行身份校验，确定终端身份是否合法，并将校验结果及准入策略下发给准入设备。
d. 终端策略授权：准入设备根据准入服务器的校验结果对终端实施准入控制，例如允许或者禁止终端访问网络；或者对终端进行更加复杂的管控动作，如提高或降低终端的转发优先级、限制终端的网络访问速率等。

云南交投安全建设成效

云南交投在安全建设工程中，对业务应用进行了分区规划，将敏感业务，办公业务，外部服务业务分别划分到黄，绿，蓝三个区域，实现了不同层级的访问控制，提升安全防护效果的同时保障业务的使用体验。基于省中心 - 区域 / 路段 - 收费站的业务架构，采用了租户式级联管控态势感知平台架构，提升省中心监管能力的同时保障区域 / 路段的分区运维效率。发挥网络 + 安全的协同能力，充分利旧现网交换机设备，通过交换机与网络控制器及态势感知平台联动，实现了准入控制，资产识别，终端流行为分析能力等能力，保护前期投资的同时，提升了安全防护效果。

云南交投安全建设实践的整体成效如下所示：

- **一处检测、全网免疫：**云南交投八个管理处中任意一处检测到恶意文件，都会将恶意文件的 MD5 等情报信息同步到省中心态势感知平台，省中心将情报同步到其他管理处，其他管理处遇到相同恶意文件时，无需进行检测，直接阻断即可，实现一处检测，全网免疫的效果。
- **级联管控、按需扩容：**云南交投在对大理管理处等八个管理处建设了二级态势感知平台能力，在未来两年内还会增加 4 个管理处的安全建设。随着云南交投业务的持续发展，管理处存在合并以及增加的需求，通过虚拟化的租户式的态势感知平台能力，无需为管理处单独部署硬件态势感知平台，只需要在省中心态势感知平台上按需扩容和申请资源即可，能够灵活适配云南交投业务架构，按需扩容。
- **近源处置、消减风险：**态势感知平台检测为风险后，通过安全控制器和网络控制器，向防火墙及交换机下发处置策略，能够在最接近威胁源的网络节点进行处置操作，最大程度消减安全风险和影响。
- **非授权数据看不到：**为了便于内网办公区员工及出差或居家办公员工能够安全可信合规的访问不同的业务系统，云南交投集团部署了 20000 个零信任客户端以及 2000 个安全沙箱，为全集团员工提供安全合规访问黄区和蓝区应用的接入能力，以及为部分员工提供需要访问黄区的带有安全沙箱功能的接入终端。
  零信任接入网关作为应用代理，在识别用户的权限后会通过 Portal 页面展示用户有权限访问的业务系统入口，对于没有授权访问的业务系统不会显示任何访问入口，杜绝了非授权用户越权访问的风险。
- **敏感数据丢不了：**访问黄区高敏感应用的终端部署了终端安全沙箱，能够通过预先配置的策略，在访问高敏感应用时自动开启安全沙箱，所有访问数据和下载的数据均落盘在安全沙箱内，安全沙箱内的数据无法外发至网盘等网络介质，只能在本地访问，关闭沙箱后，数据被加密保存，即使硬盘丢失，数据也是加密状态，不会发生信息泄露。
- **资产可视、可控、可管：**资产信息、资产入网状态、资产在线状态、资产安全状态，资产所属区域等信息统一呈现，一目了然，同时可对异常资产进行退网、阻断等操作，实现了全网资产的可视、可控、可管。

05 总结与展望

近年来，我国网络安全产业规模快速增长、产品体系相对完善、创新能力逐步增强、发展环境明显优化，但在终端、网络、边界、云平台、应用和数据等各个实体安全中，不同安全企业各有所长。云南交投集团联合华为公司，整合安全合作厂商，结合业界先进理论和技术，以工程化的视角，在业界率先定义公路交通云网端一体化安全集成架构，消除网络访问行为的不可预测带来的安全风险，构建从用户、设备、应用、数据等的信任链，为后续公路交通自主安全的建设和安全运营提供指导和参考。云网端一体化防护的理念不同于传统边界“打补丁”式的防护，是基于“体系化”的思路，将安全可信融入云、网、端、应用等系统，从系统的视角解决安全问题。因此，云网端一体化更像是一个安全生产，需要通过融合不同细分领域的优秀安全产品，通过系统化的安全集成设计，构建更加专业的安全体系。业内任何一家安全厂商都难凭“一己之力”做到全方位领先，构建安全生态是首要之选，结合公路交通场景实践验证是重中之重。同时，随着安全大模型的持续发展和相关技术的完善，必然探索更加高效，精准，自动化，智能化的模型训练技术和方法，并联合更多合作伙伴推动技术的发展也应用场景的拓展，实现人工智能技术的可持续发展。

云南交投抢抓“一带一路”，面向南亚东南亚辐射中心建设等重大战略机遇，坚持应用牵引，数据赋能，需求导向，实用高效，市场主导，产业培育的发展原则，通过《科技赋能三年行动计划》在集团公司已有云平台基础上，升级完善算力基础设施和平台扩容，构建安全可控“交投云”，建立较为完善的云服务支撑体系，为集团公司数字经济发展，数字化转型，数字赋能，数字交通等提供基础性保障和支撑。

网络安全和信息化是一体之两翼，驱动之双轮，必须统一谋划，统一部署，统一推进，统一实施。公路交通云网端一体化安全体系建设任重道远，仍需行业伙伴协作前行，共期未来。

06

缩略语

缩略语	英文全称	中文全称
APT	Advanced Persistent Threat	高级持续性威胁
BIOS	Basic Input Output System	基本输入输出系统
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DNS	Domain Name System	域名系统
HTTP	Hypertext Transfer Protocol	超文本传输协议
IOA	Indicator of Attack	攻击指标
MAC	Media Access Control	媒体接入控制
MTTD	Mean Time to Detect	平均检测时间
NDR	Network Detection and Response	网络威胁检测与响应
NETCONF	Network Configuration Protocol	网络配置协议
NMAP	Network Mapper	网络端口扫描工具
RADIUS	Remote Authentication Dial-In User Service	远程身份验证拨号用户服务
SNMP	Simple Network Management Protocol	简单网络管理协议
SoC	System on Chip	片上系统
XDR	ExtendedDetection and Response	可扩展威胁检测与响应