紫光集团 核心企业 | H3C 数字化解决方案领导者

H3C统一终端业务管理
解决方案（EAD³）

新华三集团 www.h3c.com

北京总部
北京市朝阳区广顺南大街8号院
利星行中心1号楼
邮编:100102

杭州总部
杭州市滨江区长河路466号
邮编:310052

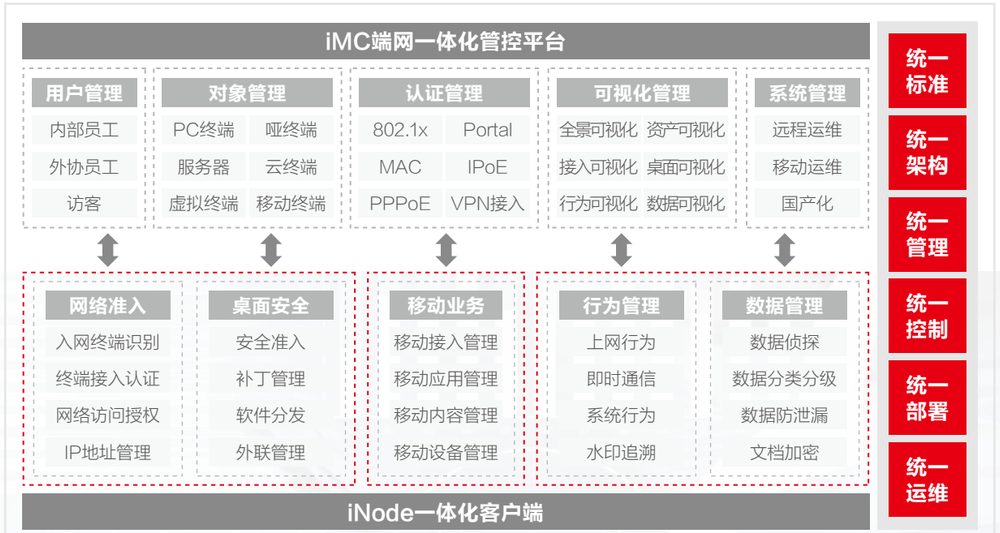
客户服务热线
400-810-0504

CN-192030-20200415-LF-SD-V1.0

方案概述

随着5G、物联网的飞速发展，边缘终端数量急剧攀升，企业内网终端管理变得愈加重要。脆弱的用户终端一旦接入网络，就等于给安全隐患敞开了大门，使危机在更大范围内快速扩散，进而导致网络使用行为“失控”，企业重要数据资产流失、受损。保护用户终端的健康、阻止威胁入侵网络，对用户的网络访问行为进行有效的控制，防止企业终端重要数据流失，是保证企业网络、终端正常运行的前提，也是目前企业急需解决的问题。保障终端合法合规的同时，如何应对海量终端带来的管理压力，实现海量终端有效管控、同时有效降低海量终端管理成本，更是新时代新形势下对终端管理者的新挑战。

紫光旗下新华三集团统一终端业务管理解决方案（EAD³）聚焦网络、桌面、行为和数据，从控制用户终端安全接入网络的角度入手，整合网络接入控制、桌面安全、行为审计、数据保护产品，通过客户端、策略服务器、网络设备以及第三方软件的联动，对接入网络的用户终端实施企业终端管控策略，严格控制终端用户的网络使用行为，全面掌控终端敏感数据分布、流转，有效地加强了用户终端的主动防御能力，为企业网络管理人员提供了有效、易用的管理工具和手段。



方案价值

端网结合，多维度管理，构建一体化终端多维管理体系，全方位守护终端，助力客户迈入终端安全治理新时代。

方案特点

全方位准入控制

EAD³解决方案提供完善的接入控制，可以支持局域网、广域网、VPN、无线各种接入方式，支持包括HUB在内的各种复杂网络、思科等异构网络环境下的部署，保证从任何地点、任何方式下的接入安全。

多因素结合身份认证

自研新华三e盾软令牌，提供免费、安全的动态口令服务，可用于网络接入用户认证、设备管理用户认证。

除支持自建账号，还可与丰富的第三方认证数据源联动，譬如第三方LDAP/AD用户、第三方RADIUS用户、第三方数据库用户、第三方WEB系统用户。EAD³还支持身份与接入终端的MAC地址、IP地址、所在VLAN、接入设备IP、接入设备端口号等信息进行绑定，支持智能卡、数字证书认证、动态令牌，增强身份认证的安全性。

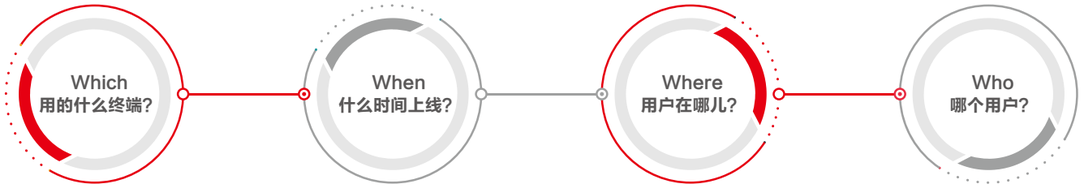
终端可信环境感知

根据管理员配置的安全策略，用户可以从系统配置、网络配置、软件配置、进程管理、外设管理、终端操作、上网行为、数据流转等多个维度对终端状态数据进行实时采集。各项采集指标权重可根据场景灵活调整，基于百分制为终端实时评分，评价结果一目了然，并且可以主动或被动方式为第三方应用提供终端实施评价数据，最终为客户构建完备的终端状态感知体系、实时评价体系。

精细化的权限控制

在用户终端通过病毒、补丁等安全信息检查后，EAD³可基于终端用户的角色，向安全联动设备下发事先配置的接入控制策略，按照用户角色权限规范用户的网络使用行为。终端用户的所属VLAN、ACL访问策略、是否禁止使用代理、是否禁止使用双网卡等安全措施均可由管理员统一配置实施。

可以对终端进行精准类型识别、厂商识别



姓名	用户组	终端类型	SSID	接入地点	接入时间	接入规则
Will	财务部	PC	移动IT_1X	财务部	工作时间	财务部访问规则
Will	财务部	iPad	移动IT_MEETING	会议室	工作时间	会议室访问策略
Frank	访客	Android	移动IT_GUEST	大厅	工作时间	Internet
Frank	访客	Mac OS	移动IT_MEETING	会议室	工作时间	禁止接入
Jerry	研发	Android	移动IT_1X	研发	工作时间	研发实验室

灵活方便的执行方式

EAD³按照网络管理员配置的安全策略区别对待不同身份的用户，定制不同的安全检查和处理模式，包括监控模式、提醒模式、隔离模式和下线模式。用户可以根据自己的实际需要，为VIP客户、内部员工、外来访客等不同人群，定义不同的安全策略执行方式。

桌面资产及外设管理

EAD³解决方案提供了对终端资产全方位的监控和管理的功能，可以对终端软硬件使用情况、变更情况进行监控，同时还支持终端资产的配置管理和软件的统一分发、远程桌面控制，实现对桌面资产的有效管理。EAD³解决方案还提供了对U盘和其他外设的管理功能，可以对终端用户的各种外设进行控制，有效防止重要信息的泄密，同时提供U盘文件的监控功能，可以查看重要文件通过U盘拷贝时，有无存在不当使用行为。

终端行为审计

终端行为审计系统实时追踪终端电脑的操作行为，监控网络资源的使用和敏感信息的传播，准确掌握终端系统的安全状态，并生成各项统计报表，为泄密事件的事后溯源提供了有力支持。

系统行为

- 窗口标题日志
- USB外发日志
- 打印操作记录
- 文件操作日志
- 程序使用日志
- 屏幕追踪及屏幕录像

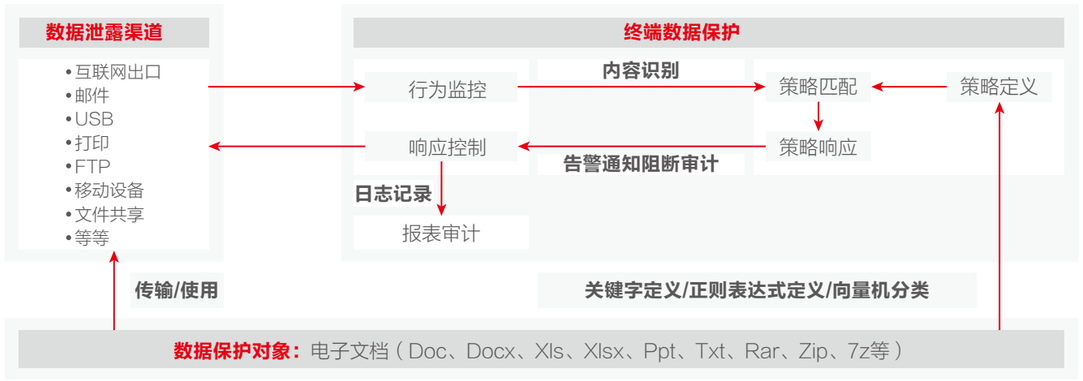
上网行为

- 网页浏览记录
- 聊天行为记录
- 文件上传记录
- 论坛发贴记录
- 邮件收发记录
- FTP监控日志

新华三EAD终端行为审计原则：管理审计并重，行为内容兼顾

终端数据保护

数据保护解决终端敏感数据泄密问题。信息安全时代，数据代表着最强大的生产力。EAD³通过领先的终端扫描技术、数据分类技术、内容识别技术，让用户终端敏感数据可视、可控，从源头上阻断敏感数据通过各种途径泄露。

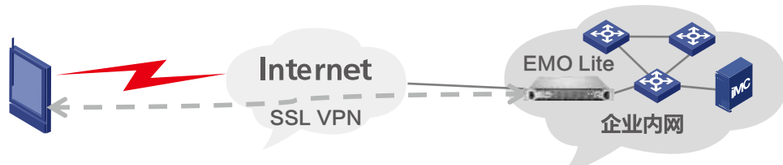


一体化客户端

通过统一的、可定制、可装配式部署的iNode客户端，为用户提供网络准入、桌面安全、行为审计、数据管理等全方位终端业务管理服务，可极大提升用户使用体验，降低后期运维难度。

便捷运维能力

EAD³解决方案提供了远程协助能力，管理员可远程执行终端维护操作。终端用户和系统管理员共享终端桌面，实时交互，完成远程运维操作。同时提供移动运维APP，系统管理员可随时随地接入并实施运维。



- 内网、外网随时随地接入
- 安全的SSL VPN连接通道，杜绝入侵风险
- 通过PC、PAD、SmartPhone便捷运维

多种层次的高可用性

EAD³解决方案提供了双机冷备、双机热备以及分布式集群功能，可以避免单台EAD³服务器宕机引起的认证中断，同时还支持单机故障的逃生方案，临时允许客户端不用认证就可以使用网络，保证了经济敏感用户的利益。

扩展开放的解决方案

EAD³解决方案为客户提供了一个扩展、开放的结构框架，最大限度的保护了用户已有的投资。EAD³广泛、深入的和国内外防病毒、操作系统、桌面安全等厂商展开合作，融合各家所长；EAD³与第三方认证服务器、安全联动设备等之间的交互基于标准、开放的协议架构和规范，易于互联互通。

案例

谋局全网 纵深防御

——中国银行大规模部署H3C EAD终端准入控制解决方案

作为中国四大国有银行之一的中国银行是中国唯一持续经营超过百年的银行，也是中国国际化和多元化程度最高的银行。

中国银行网络规模庞大，地理位置分散，导致计算机终端使用过程中存在应用、管理、安全等多方面问题，网络准入机制薄弱、内网边界模糊并且存在违规外联行为风险。终端杀毒等必备软件无法管理安装状态、病毒库更新频率低，在整个内网形成重大安全隐患。

新华三EAD终端准入控制方案从网络准入、终端桌面管理、终端安全保护等方面，立体化保护中国银行内部网络和末端节点，切实满足客户需求。目前EAD部署包括中国银行总行及超过半数的各省分支行，覆盖终端范围超过数十万点。EAD通过对入网终端进行安全检查，网络内原先部署的杀毒软件和桌面管理系统安装率达到了要求，保护了前期投资，有效的落实了网络安全规范要求。对非授权终端做到了准入控制，外来终端需要经过审核才能接入网络，大大减少了金融系统机密泄露的风险。内部员工使用用户名和密码接入网络，并对认证记录进行了保存，网络使用情况做到了有据可查。

新华三EAD终端准入控制方案从网络和终端两个层面保障了中国银行内部网络的安全性，访问的合规性，问题的可回溯性。

无序到有序 十二年守护

华夏银行H3C EAD终端准入控制系统稳定运行十二年

华夏银行是一家成立于1992年的股份制银行。截至2018年9月，总资产规模达2.61万亿元，在全国108个地级以上城市设立了42家一级分行，营业网点总数达1006家，形成了“立足经济发达城市，辐射全国”的机构体系。

华夏银行总行内部使用的办公终端多种多样，缺乏统一有效的安全检测防范机制，难以对全公司的桌面计算机进行有效的安全管理，可能给网络的安全运行留下大量的安全隐患；各类办公文件、移动存储介质也缺乏管控与审计机制。

针对华夏银行总行存在的问题，新华三深入客户办公场景，把握客户核心需求，经过长期论证和可行性分析，最终制定贴近客户的解决方案，为华夏银行总行办公网部署新华三EAD终端访问控制系统。系统覆盖总行办公网数千终端，通过准入控制、桌面安全的集中管理，确保华夏银行网络安全相关的管理要求落到实处，提升整体运维效率，有效降低办公网各类安全风险，提高办公网络业务续航能力。

护网先锋 守护底线

光大银行规模应用H3C EAD终端准入控制方案

中国光大银行是中国国内第一家国有控股并有国际金融组织参股的全国性股份制商业银行。截至2018年12月31日，中国光大银行已在境内设立分支机构1252家，实现境内省级行政区域服务网络的全覆盖，机构网点辐射全国136个经济中心城市 。

光大银行内部办公终端数量多、网络环境复杂，终端准入与安全问题日趋严峻。防止非授权终端接入公司网络，对接入网络的终端如何进行安全管理与审计，加强远程协助手段来解决日常办公问题，都成为急需解决的问题。

通过部署EAD终端准入控制方案，与LDAP和网络设备联动，实现对所有接入公司网络的终端进行统一的准入身份验证和合规检查，只有通过身份认证及合规检查的设备才能接入并正常访问网络。管理员可随时掌握终端运行状态，通过提供各种安全措施及运维工具，有效提升光大银行IT部门对各类故障问题的处理效率，进而大幅提升员工的工作效率,保障业务的实时性。

三位一体 助力电力信息化

四川电力全网应用H3C EAD构建终端三位一体立体防护体系

四川省电力公司是国家电网公司的全资子公司，国有特大型企业，以电网经营为核心业务，负责四川省境内主要电网规划、建设、运营和电力供应。2005年末，公司资产总额达484亿元，拥有电力生产、设计、施工、修造、科研及学校等企事业单位45个，职工总人数28958人，供电面积约16万平方公里，占四川省国土总面积的33.55%，供电人口约6640万人，约占全省总人口的78.4%。

随着电力信息化的发展，网络规模的扩大，终端用户数量越来越多，业务越来越复杂，管理成本越来越高，运维管理越加依赖于信息网络平台，从而对网络管理，边界安全，网络可靠性，服务质量的要求越来越高。一个安全可靠的网络必须满足条件之一就是确保接入网络的用户合法、终端合规，且网络上的流量清楚明晰，便于控制。

为了实现上述要求,在四川省电力公司通过部署新华三iMC网络管理平台及EAD终端准入系统,对网络设备进行可视化管理，同时对接入网络的终端进行准入控制,只有合规的终端才能够接入网络，并在运行过程中进行实时监控,对出现安全隐患的终端主动进行隔离等。

新华三 iMC EAD功能特性为用户提供了从网络端点接入控制入手，通过对用户终端系统补丁的安装情况、防病毒软件版本、敏感软件的安装和运行情况、终端流量的异常变化进行检查和监控，加强网络终端的主动防御能力，控制病毒、蠕虫的蔓延。EAD通过准入客户端、策略服务器、接入设备以及防病毒软件的联动，可以将不符合安全要求的终端限制在“隔离区”内，防止“危险”终端对网络造成威胁，避免“易感”终端受病毒、蠕虫的攻击。它构建了融合网络、用户、终端的三维全网边界防护体系，最终为用户提供端到端的安全接入防护。

电子围栏严防跨区域办理业务

H3C EAD助力山西农信移动业务腾飞

山西省农村信用社是由省委、省政府直接领导和管理的地方性金融机构，自1945年成立迄今已有七十余年的历史。共有省、市、县、乡四级机构3182个。资产总额、存贷款余额均居全省金融机构之首。

山西省农信3/4G网络无线业务平台主要为全省流动服务车和各农商行助农终端业务提供无线准入服务，随着各县级行社对移动准入的业务需求不断增加，对现有平台提出支持离线地图定位功能，可在系统平台看到下属联社每个接入终端的接入位置，实现对移动终端设备的定位，并且在超出指定范围后提供告警，及时发现跨区域移动营销行为，并将移动终端下线处理。依托新华三统一终端业务管理解决方案，通过EAD准入控制系统联动离线地图，成功将客户需求落地，实现网络对业务有效支撑，提升整体管理效率。

海南省政府 做中国政务移动化“第一个吃螃蟹的人”

新华三为海南搭建电子政务外网移动端接入平台

要成为中国政务移动化“第一个吃螃蟹的人”，需要魄力与实力兼备。作为中国最年轻的省份，1988年建省的海南也是电子政务领域最具魄力和活力的省份之一，其2014年投入使用的电子政务外网乃是中国第一批电子政务外网。所以，海南省成为中国政务移动化“第一个吃螃蟹的”，并不让人吃惊，何况背后更有着新IT领军企业新华三移动IT解决方案给予的实力保障。

更上层楼：全国首个能随身携带的政务办公系统

由新华三负责承建的海南电子政务外网，支撑起了一个承载着丰富业务类型且覆盖面极广的省内政务公用网络平台，极大提升了海南省包括民政厅、商务厅、海事局、国土环境资源厅、科学技术厅、审计厅、水务厅、交通运输厅、住房和城乡建设厅、监察厅、教育厅、农业厅等在内的多个机关单位的业务流程办理效率，推动了海南政府从职能部门向服务部门的转变进程。但当50余家省直机关、19个市县和洋浦开发区的办公业务全部接入之后，电子政务外网PC终端接入方式已然满足不了公务员群体的办公需求，这直接促使海南省政府决定再次携手新华三“更上一层楼”。

为满足海南省各级政府机关以及派驻机构对电子政务外网的无缝联结需求，新华三首先对电子政务外网PC终端安全接入进行了相应的改造和扩容，满足市县级PC终端通过802.1X、Portal以及SSL VPN三种接入方式便捷、快速、安全地接入电子政务外网资源的需求，推动电子政务应用不断向网络设备水平参差不齐的一线基层延伸。

而在现有H3C iMC智能管理中心基础之上，新华三开始尝试为海南电子政务外网搭建移动端接入平台，让公务员群体可通过自有的移动智能终端便捷快速地访问海南省电子政务外网资源，同时帮助海南政府将Windows应用快速迁移至移动端，并避免移动业务开展过程中各个环节的安全风险。

无懈可击：不为安全牺牲便捷，不因便捷模糊安全

新华三搭建的移动端接入平台，成功规避了因设备本身、用户使用习惯、应用下载与操作以及数据传输等等可能引发的安全隐患，从而让这个全国首个能随身携带的政务办公系统，变得无懈可击。

例如，在移动设备准入上，新华三部署的iMC　EIA系统，提供DHCP指纹识别、Http Agent识别和MAC OUI识别三种具有较高识别度和可靠性的终端设备类型识别方式，同时还实现了基于接入场景的准入控制策略。

也就是说，用户的接入权限，不再仅由用户的身份决定，用户类型、网络类型、接入地点、接入时间、终端类型、终端操作系统、终端归属等条件，均可能影响用户的接入权限。网络管理员可以利用iMC　EIA系统提供的接入策略引擎，实现合适的人、使用合适的设备、合适的网络、在合适的地点和时间，获得合适的网络访问权限，最大限度的保证政务外网的安全。

同时，移动内容管理（MCM）系统确保业务单位数据不被外泄，支持对下载至移动终端的单位数据进行管理，包括控制文档分发、控制邮件分发，为业务提供单位文档安全阅读环境，避免单位数据被动泄密。

而在安全性能之外，新华三的移动终端接入平台同时也满足了公务员群体与政府IT管理人员对政务移动化“易用”与“易管”的需求，并未因安全而牺牲便捷，或者因便捷而模糊安全。

移动政务：后电子政务时代的新潮流

作为“第一个吃螃蟹的人”，海南省政府与新华三合作的政务移动化取得了极大成功。带着可装进公文包的政务办公系统跑基层、访民情，随时随地调研资料、提交报告、进行业务办理等等，已成为海南省上到省政府、下到街道办公处的公务员群体办公常态。这种与时俱进的办公方式不仅受到了公务员群体的欢迎，也被群众所称道，与政府相关的各种手续流程、审批流程得以“提速”，群众亦是政务移动化的受益者。

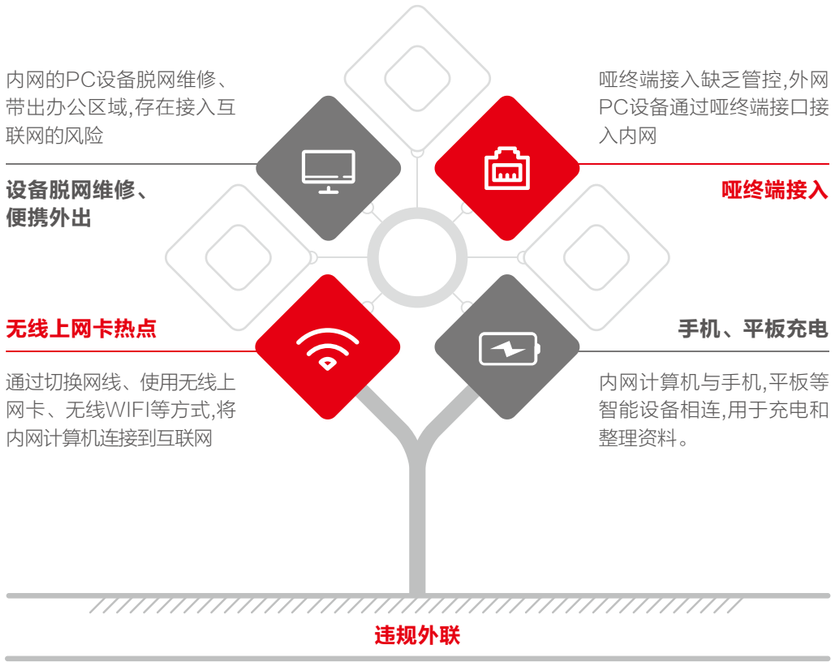
可以预料的是，不久的将来，由海南省开启的中国政务移动化潮流必将汹涌而至，海南的成功经验将作为政务移动化的最佳实践而被不断借鉴与复制。

专机需专用，违规无遁形

新华三H3C EAD帮助广东税务实现终端防违规外联

国家税务总局广东省税务局于2018年6月15日挂牌成立，标志着原广东省国家税务局、原广东省地方税务局正式合并，税务局负责贯彻执行国家和省有关税收工作的方针政策和法律法规，制定地方各税、费的征收管理办法；承担组织实施地方税、共享税及社会保险费、文化事业建设费和省人民政府、国家税务总局委托征收的其他基金（费）的征收管理责任。

一直以来，税务内网都有着严格的网络安全管理要求，对整个税务系统的内部人员都有着严格的管理规范。但由于税务人员分散，规模庞大，部分基层单位的税务人员信息化水平不够高，导致税务终端的使用存在风险隐患。广东省税务局及各地市税务单位，对全网终端的准入管理，防违规外联需求迫切，希望通过技术手段，彻底规避员工有意无意的网络访问违规问题，包括非法终端入网，私接共享，无意内网外联等问题。如下图：



新华三iMC-EAD终端管理方案，为用户量身设计方案，解决内网安全准入、设备脱网维修、非法私接共享、手机充电等违规外联问题，通过技术手段彻底规避违规风险，从源头上阻止员工泄密的可能。最终通过新华三EAD终端管理方案，帮助用户守护网络边界底线。

精准识别 按需接入

奇瑞捷豹路虎汽车采用H3C EAD终端准入控制解决方案

奇瑞捷豹路虎汽车有限公司成立于2012年11月由奇瑞汽车股份有限公司和英国捷豹路虎汽车共同出资组建而成，是国内首家中英合资的高端汽车企业。

随着企业规模的不断扩大，员工数量激增，网络接入终端及接入方式的多样化，奇瑞捷豹路虎汽车有限公司对多场景、细粒度管理的准入需求越来越急迫。新华三深入企业内部，详细了解企业网络准入管理的业务流程，与客户共同探讨分析准入机制的最优方案，最终为客户定制出一套符合奇瑞捷豹路虎汽车有限公司现状并对未来发展趋势具有充分弹性空间的终端准入方案。方案从终端类型精准识别入手，从接入者身份、接入时间、接入方式、接入位置等多个维度，制定详细的准入策略，切实满足客户复杂的准入需求。

项目的成功实施部署，覆盖了数千员工日常工作中网络访问的各种准入场景，提高了IT部门运维管理的效率，为客户网络安全、高效、平稳的运行，提供了坚实的基础。

创新应用，加速数字化转型

H3C EAD助力乐山电子政务外网打造网络准入新标杆

“十三五”以来，随着网络新技术的发展以及我国政府职能的不断转变，我国的电子政务进入新的发展阶段，跨地域、跨部门、跨系统的信息共享、业务协同以及智慧政务等成为了各地电子政务的重点建设内容。2017年11月26日，中共中央办公厅、国务院办公厅印发了《推进互联网协议第六版（IPv6）规模部署行动计划》（厅字〔2017〕47号）（以下简称《IPv6规模部署》），要求各级地方政府积极开展电子政务外网IPv6升级改造；为贯彻落实《IPv6规模部署》，根据国家、省、有关电子政务外网技术路线以及国家、省有关文件要求，结合乐山市电子政务外网网络建设实际，明确提出，所有内部办公终端接入电子政务外网需要认证，实现电子政务网和互联网逻辑隔离；统一市级部门互联网出口，确保网络安全，杜绝内网敏感信息发生外泄到互联网。

由于电子政务外网和互联网出口使用一条物理链路，为确保电子政务外网数据安全，乐山市电子政务外网采用EAD多网逻辑隔离技术实现电子政务外网和互联网逻辑隔离，保证在同一时间内，只能接入一个网络区域，明确划分各个委办单位间的业务接入边界。并且让网络运维人员对接入用户的身份与行为进行实名认证与智能管理，做到事前、事中、事后有据可查、权责明晰。值得一提的是，该方案同时实现了“终端复用”，让各单位不需要购置新的终端设备来实现网络隔离。实现了在“好用”的同时，达到三级等保建设标准的目标。避免电子政务敏感数据外泄的隐患，有效保护内网安全。

采用逻辑隔离技术实现一网多用，降低建设多套物理网络成本。通过准入控制、逻辑隔离等技术，确保电子政务网终端安全相关的管理要求做到“可落地、可执行、可检查、可优化”。 提供对边界安全防护灵活完善的解决方案，防止非法外联、非法接入和非法信息泄漏等破坏边界完整性行为的发生。

安心守护，保障网络安全接入

H3C EAD助力陕西电信护网行动

中国电信集团有限公司是国有特大型通信骨干企业，中国电信拥有全球规模最大的宽带互联网络和技术领先的移动通信网络，具备为全球客户提供跨地域、全业务的综合信息服务能力和客户服务渠道体系，陕西电信是中国电信股份有限公司在陕西省设立的省级分公司，是陕西省内主导的全业务通信运营企业。

随着5G、物联网等新技术的快速发展应用，电信运营商也在不断丰富自己的业务，内部新建的业务系统繁多，包括boss系统、客服系统等业务支撑系统，还包括OA、CRM系统等常规办公系统，同时各个网络中的桌面电脑以万计。系统上积累了大量的客户信息、生产数据和运营信息，　　公司内部面临着非法终端接入、涉密业务数据泄露、计算机资产难以统一管理等诸多严峻挑战，加之国家安全等保政策的管理要求，因此建立一套统一的网络访问控制系统显得特别重要。

为了保护内网访问安全，基于新华三统一终端业务管理解决方案，通过入网身份检查，不同用户访问权限控制，终端可控软件管理、防止内网PC违规外联等技术手段，实现内部办公网络安全接入。

该方案的成功部署，确保网络接入可管可控，为运营商的网络安全建设使命保驾护航，最大化释放网络价值。并且符合国家安全等保要求、符合国家信息网络安全政策法规。

助力人工智能，建设美好世界

科大讯飞通过H3C EAD实现终端合规接入

科大讯飞股份有限公司成立于1999年，是知名的智能语音和人工智能上市企业。自成立以来，长期从事语音及语言、自然语言理解、机器学习推理及自主学习等核心技术研究并保持了国际前沿技术水平。

随着科大讯飞企业规模的扩大，网络接入的终端数量越来越多，终端类型及接入方式也越来越多样化，各类终端缺乏网络用户识别、准入控制机制。如何保障各类终端用户安全接入是科大讯飞面临的一个挑战。新华三与科大讯飞经过多次深入交流，依托新华三统一终端业务管理解决方案，为其量身定制了终端准入控制方案。该方案确保科大讯飞可以按照用户角色、设备类型、接入时间、接入地点等条件自由定义不同的接入场景，对网络访问权限做精细化控制。同时满足科大讯飞多种接入形式、多种终端类型、多种用户角色的统一运维管理需求，确保终端安全策略在整个企业网络无缝地执行。

项目的成功实施部署为科大讯飞近万名员工提供各种准入场景，提高了IT部门运维管理的效率，为客户网络安全、平稳的运行保驾护航。