北信源VRV®

股票代码:300352

北京北信源软件股份有限公司

基于可信终端的安全管理平台

可行性分析报告

二〇一九年十月

目 录

1．项目概况

本项目将服务于国家安可与大数据战略，贯彻落实《网络安全法》、《国家网络空间安全战略》以及系列政策、法规、决策文件的指导精神，将大数据与网络安全、国产化平台安全紧密融合，面向可信终端的安全管理，打造“安全基线+安全服务”一体化的网络安全解决方案。根据国家网络安全等级保护和 SM 信息系统分级保护的相关国家标准，从安全通信网络、安全区域边界、安全计算环境、安全管理中心等方面，构建不同等级的基线安全防护体系；从安全运维管理入手，利用大数据技术和平台，提供大数据平台支撑的安全服务和积极防御能力，有效抵御持续变化的安全威胁。为此，开发并建设大数据驱动的可信终端安全管理平台，以系统性地解决国产化平台终端的安全管理问题。项目周期为 15 个月，拟于 2019 年第四季度开始，至 2020 年底结束。

通过本项目，能够为国家安可战略提供强有力的技术和产业支撑，解决国产可信终端的网络安全问题，满足国家网络安全等级保护和分级保护的要求，消除可信终端“裸奔”存在的安全风险，有效应对日益增长的网络安全威胁，保障国家关键信息基础设施安全。而且，还引领可信终端安全技术、产品和市场的发展方向，并推动终端安全特别是可信终端安全标准的制定，规范行业的发展，带动我国网信事业的发展，巩固北信源在终端安全管理领域的国内龙头地位，以及在安可方向的领先地位。

2．项目背景

2.1 安全可信已成国家战略

随着《国家网络空间安全战略》和《网络安全法》等一批政策、法律、法规的发布实施，安全可信已经上升到国家战略高度，保卫网络安全就是保障国家主权，而自主可控、安全可信就是保障网络安全、信息安全的基本前提。自主可控是中国信息化产业发展的必经之路，也是我国产业迈向全球价值链中高端的必然之选。随着国际范围内网络安全局势升级和信息技术产业竞争加剧，自主可控作为落实网络强国和军民融合战略、提升国家网络信息安全能力的关键举措，重要性日益凸显。国产信息技术保障国家信息安全，自主可控助推民族 IT 产业腾飞。

强力推进国产自主化建设应用，是国家信息化发展战略的大势所趋。

党的十八大以来，以习近平同志为核心的党中央对信息化和网络安全重大问题做出一系列重大决策、提出一系列重大举措，推动我国网信事业取得了历史性成就。习总书记多次在重要场合强调自主可控的重要性，建设网络强国要以自主创新为基石，关键核心技术是国之重器，要下定决心、保持恒心、找准重心，加速推动信息领域核心技术突破。要建设网络强国，必须掌握核心技术，强调安全可控，必须做到对网络空间安全的可管、可防、可控，必须紧紧牵住核心技术自主创新这个“牛鼻子”，构建安全可控的信息技术体系，这对推动我国经济高质量发展、保障国家安全都具有十分重要的意义。

而且，贸易摩擦、“中兴事件”表明核心技术受制于人将为大国崛起带来阻碍；进一步地，国外软、硬件的预装“后门”也会带来网络信息安全隐患，只有把关键核心技术掌握在自己手中，才能从根本上保障国家经济安全、国防安全和其他安全。在这样的背景下，国家政策强力推动自主可控相关行业的国产化替代，领域也由此前的党政军市场进一步扩大到国计民生行业，包括金融、石油、电力、电信、交通、航空航天、医疗、教育等涉及国计民生的重大行业。国产化替代的加速推进将为自主可控领域的成长提供强劲动力。

2.2 可信终端安全问题亟待解决

随着安全可信国家战略的实施，国产可信终端的发展取得了长足的进步，在政府、教育、军队和军工领域得到了较为广泛的部署和应用。这虽然杜绝了境外IT产品人为设置后门的风险，但可信终端在信息安全方面非常薄弱。信息安全建设必须紧贴整个国产化替代过程，确保平滑过渡，不出现大的安全漏洞，能够有效抵御网络攻击。因此，近年来各安全厂商陆续发布了产品，并解决了可信终端的部分安全问题，国产化平台安全产品进入了发展的快车道。北信源也立足自身优势，针对可信终端与服务器乃至整个国产化信息系统，打造基于大数据的“安全基线+安全服务”的可信终端安全管理体系和整体解决方案，开发大数据驱动的可信终端安全管理平台，以系统性地解决可信终端面临的安全问题。

2.3 大数据与网络安全进入深度融合期

一方面，根据国家互联网应急中心（CNCERT/CC）发布的2018年年度报告和

2019年半年报，2018年，我国境内感染计算机恶意程序的主机数量约为1256万个，位于境外的约3.2万个计算机恶意程序控制服务器控制了我国境内约1101万台主机，被篡改网页和植入后门的政府网站分别达到618个和1339个。而仅在2019年上半年，境内感染网络病毒的终端数就达到68万余个，被篡改网页和植入后门的政府网站分别达到62个和71个，国家信息安全漏洞共享平台共协调处置了1402起涉及我国政府部门以及银行、民航等重要信息系统部门以及电信、传媒、公共卫生、教育等相关行业的漏洞事件。这说明我国政府等敏感行业的关键信息基础设施，由于涉及到国家安全和社会稳定，已成为境外黑客组织、间谍情报机构和敌对势力的重要攻击目标。

另一方面，大数据发展也已成国家战略，习总书记强调推动实施国家大数据战略，加快完善数字基础设施，推进数据资源整合和开放共享，保障数据安全，加快建设数字中国。在此背景下，大数据技术和平台以及相关人才队伍迅速发展壮大。而在网络安全领域，随着数字基础设施的发展，要处理分析的数据指数级增长，安全威胁的攻击和隐藏等行为方式也发生了显著的变化，这都需要大数据技术和平台来支撑。大数据与网络安全的融合，已从概念期进入到了深度融合期。

在国产化替代的进程中，特别是党政军的国产化替代进程，涉及国家信息基础设施和重要信息系统，必然会成为各种网络攻击的重点目标。因此，信息安全建设必须紧贴整个替代过程，确保平滑过渡，不出现大的安全漏洞，能够有效抵御针对国产自主可控计算机的网络攻击。本项目面向企业私有云的应用场景，构建大数据驱动的网络态势感知平台，实现了大数据与网络安全的深度融合，满足了用户在基于大数据的网络安全管理、网络安全态势感知、应用性能分析和企业管理方面的迫切需求。

3．项目必要性分析

3.1 自主可控领域网络安全市场空间巨大

近年来，随着《网络安全法》的颁布实施，国家相关部委也纷纷发文，强力推进自主可控进程。2016年12月，《“十三五”国家信息化规划》中，提出全面增强信息领域核心技术设备自主创新能力，打造自主先进的技术体系，构建先进、安全、可控的核心技术与产品体系。《国家网络空间安全战略》中，指出网络安

全是国家安全的核心，核心技术装备应安全可控，建立实施网络安全审查制度，提高产品和服务的安全性和可控性。由此可见，自主可控和国家信息安全紧密相关，是中国信息化产业发展的必经之路，也是国家安全战略的要求。

按照计划，“十三五”期间将完成国家计划推进领域的国产化替代，之后将在国计民生行业推进，而且，这一进程因今年的贸易摩擦升级有望进一步加速。当前我国芯片、操作系统、数据库等核心元件国产占有率相对较低，未来“党政军+国计民生”八大行业的国产化替代将为国产软硬件及网络安全行业带来巨大发展空间。

3.2 落实网络安全等级保护（以下简称“等保 2.0”）的重要举措

终端安全管理符合国家法律法规和标准的强制要求。在网络安全等级保护和分级保护中，终端安全管理是关键的技术手段，是相关国家标准的强制要求。政府、军工、金融和能源等涉及国家安全行业的信息系统，必须安装终端安全管理产品。而且，随着网络安全威胁的日益严重，很多大中小企业信息系统也都安装了终端安全管理产品。在刚刚发布的等保2.0标准中，安全区域边界、安全计算环节和安全管理中心，均对终端安全管理和大数据与网络安全的融合提出了明确的技术要求。本项目打造大数据与国产化平台可信终端安全融合的安全解决方案，既是对用户迫切安全需求的应答，也是落实等保2.0的重要举措。

3.3 符合公司战略发展的迫切需求

北信源是专业从事信息安全的国家级高新技术企业，主营业务为信息安全软件产品的研发、生产、销售及技术服务，为政府机关、军工、金融和能源等国家重点行业及企事业单位提供信息安全产品和整体解决方案。作为主要为政府、军工等行业用户提供终端安全解决方案的厂商，自主可控已成为公司的重点战略发展方向，近年来持续加大了在自主可控领域的投资，不但与中标麒麟、银河麒麟等操作系统厂商建立战略合作关系，还不断将原有领先的终端安全技术向国产化平台迁移，主动适配不同型号的自主可控计算机，开发了主机监控审计、网络准入控制、终端安全登录和电子文档安全管理等满足国产化平台安全需求的终端安全管理技术和产品。本次投入到自主可控计算机安全领域，研发突破新技术进一步提升安全管理能力，有效整合、升级换代现有的国产化平台产品，为自主可控

计算机打造一体化的终端行为与数据安全管理体系和平台，巩固北信源在国内终端安全管理/数据安全管理领域的龙头地位。

4. 项目可行性分析

4.1 项目与国家相关战略和政策高度一致

本项目与国家安可战略高度一致，是落实国家安全可战略的具体举措，也与国家《网络空间安全战略》、《网络安全法》、信息安全等级保护制度和信息系统分级保护制度中的具体技术要求相吻合。项目紧贴国产化替代进程，为国产可信终端的安全保驾护航。确保国产可信终端的安全可靠运行，定将会得到政府的大力支持与扶持。近年来，国家在研发投入、知识产权保护、政府补助等方面对企业提供了大力支持，国产化平台生态体系逐步完善，安可实施进程得到了稳步推进。

4.2 公司在终端安全与大数据领域拥有雄厚的技术基础

北信源的终端安全管理技术和产品在业界一直独占鳌头，国内市场占有率自2006年以来连续十二年名列第一。面向企业内网安全和终端安全，从网络准入控制、操作系统安全、数据安全、恶意代码防御到大数据安全分析，均拥有国内领先的重大核心技术。

在大数据领域，公司先后中标公安信息网安全监测大数据平台、人民银行总行一体化终端安全管理、三峡集团综合安全管理平台和楚天云统一安全态势感知平台等项目，在行业私有云的大数据安全方面具有得天独厚的技术和部署优势，研发了大数据应用安全审计平台、大数据网络安全管理平台等产品，拥有丰富的依托公有云或私有云建设大数据安全平台的成功经验。而且，通过行业终端大数据安全分析北京市工程实验室的建设，进一步提升了公司在大数据安全方面的技术和人才实力。

4.3 公司在可信终端安全方面拥有深厚的技术积淀

公司自 2012 年起开始参与国家“核高基”项目，即开展一系列信息安全产品国产化适配研发。立足于终端安全，以内网安全、数据安全、边界安全为切入

点，突破、多项关键技术，先后研发了基于国产化平台的主机监控与审计系统、终端安全登录系统、电子文档安全管理系统、打印刻录监控与审计系统等多款国产化安全产品。目前，公司与可信华泰、中标麒麟、银河麒麟等安可产品厂商均建立了战略合作关系，协助厂商完善底层 API 和安全管理接口，了解这些 API 接口的技术细节，为终端安全管理产品的能力持续提升打下了坚实的基础。

2018 年以来，国家相关部委高度重视安可推进进程，印发了专门的国产化信息设备名录，公司所研发完成的多款国产化平台产品，包括主机监控与审计系统、专用服务器审计系统、终端身份鉴别系统、打印刻录安全监控与审计系统和网络防病毒系统均进入该目录。特别是在可信终端安全方面，终端安全技术与可信计算技术已完全融合，这充分体现了公司在安可领域的深厚技术积淀。

4.4 公司拥有优质的客户资源

公司凭借较为完整的终端安全管理产品线、紧贴国内用户需求的产品功能及业界较高的产品性能，赢得了众多用户的信赖，产品被广泛应用于政府、军队、军工、能源和金融等重要行业领域，终端安全管理产品客户端数量已超过数千万点，管理的企业网络达数万个，涉及各行业上千家用户。这些行业部门都是北信源的优质客户，其信息系统绝大多数属于国家关键信息基础设施，同时也是需要完成国产化替代的信息系统。随着国产化替代进程的推进，这将给本项目系列产品的推广、部署和应用，带来非常积极的效果，使得 Windows 平台的终端安全管理产品无缝过渡到国产操作系统平台的终端安全管理产品，确保行业信息系统的安全。

公司将会以现有客户群体为基础，推广大数据驱动的可信终端安全管理平台系列产品，在原有安全产品、服务的基础上进一步为客户提供国产化平台上的安全防护技术、产品和服务，持续提升客户价值。

4.5 公司拥有覆盖广泛的营销服务体系

公司目前在北京设有总部技术支持中心。总部技术支持中心采取“一站式”服务结构体系，统一服务窗口，并且在广东、上海、江苏、陕西等多个省市建立了营销服务网点，可方便进行本地化的现场技术服务。公司凭借这一广覆盖、快响应的营销服务体系，能够帮助客户快速了解产品的功能和使用方法，降低新产

品推广的难度。同时，公司依托多年积累的成熟经销商体系，可以快速实现新产品在中小企业客户中的推广，提高市场推广和技术支持能力。

5．项目实施内容

5.1 概述

本项目资金将全部用于大数据驱动的可信终端安全管理平台系列产品的研发和市场推广，具体包括：（1）**大数据驱动的可信终端安全管理平台研发**，面向不同国产化平台的可信终端，研发可信终端安全管理系统、可信服务器安全加固与审计系统、基于大数据的网络安全管理系统、基于大数据的安全态势感知系统、基于大数据的应用性能分析系统、基于大数据的安全运维管理系统等 6 款产品，拟申请 20 项发明专利，涉及研发场地装修改造费、设备购置费、研发及技术人员支持费用、第三方合作研发费用等；（2）**大数据驱动的可信终端安全管理平台的市场营销**，涉及销售人员薪酬、线上线下广告投放、展会等市场推广活动以及运营维护费用等。

本项目面向行业（企业）私有云或信息系统，将构建大数据驱动的“安全基线+安全服务”一体化的网络安全管理体系，既满足标准合规要求，又可有效抵御安全威胁，如图 1 所示。其中，安全基线就是依据国家网络安全等级保护和分级保护的相关标准，主要针对安全区域边界、安全计算环境和安全管理中心，从网络准入控制、操作系统安全监控、用户实体行为分析、应用与数据安全、威胁检测与响应、基于大数据的网络安全管理等方面，通过上述可信终端安全管理系统、可信服务器安全加固与审计系统、基于大数据的网络安全管理系统、基于大数据的安全态势感知系统和基于大数据的应用性能分析系统等 5 款产品，形成符合标准的各级基线安全防护能力。安全服务则通过基于大数据的安全运维管理系统产品，建立大数据安全运维管理中心，实现网络安全监控、威胁情报获取、安全运维和动态安全防护配置，形成积极的动态防御能力，有效抵御持续变化的安全威胁。

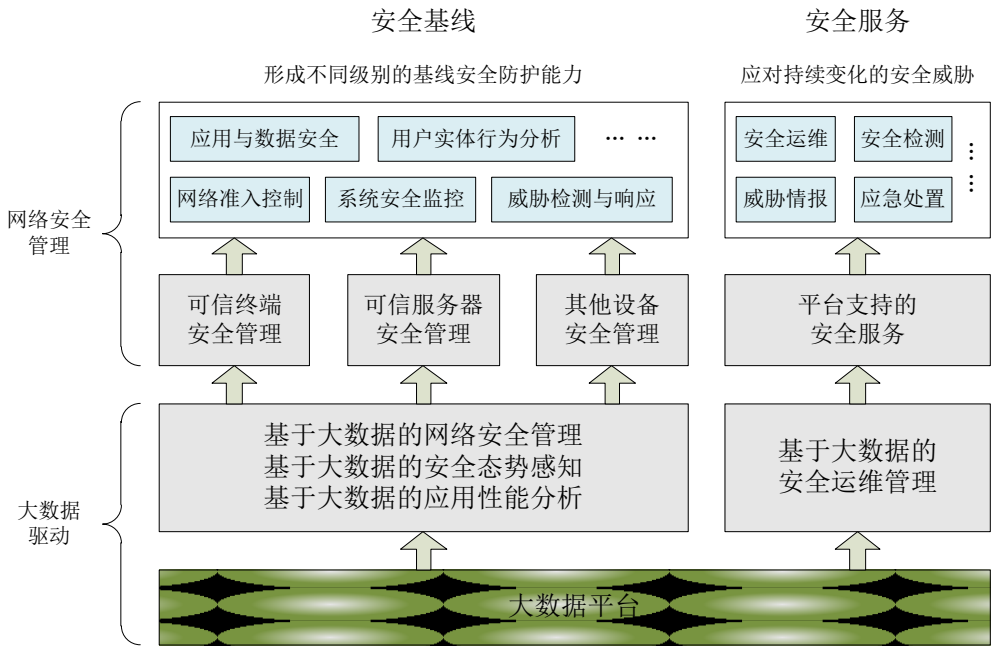

图 1 大数据驱动的网络安全管理体系

5.2 大数据驱动的可信终端安全管理平台

该平台由可信终端安全管理系统、可信服务器安全加固与审计系统、基于大数据的网络安全管理系统、基于大数据的安全态势感知系统、基于大数据的应用性能分析系统和基于大数据的安全运维管理系统等 6 个系统组成，具体如图 2 所示。其中，可信终端安全管理系统和可信服务器安全加固与审计系统分别用于对国产化平台的可信终端和可信服务器进行安全管理，可独立部署与应用，同时为大数据共性技术支撑模块提供来自可信终端和可信服务器的原始数据；大数据共性技术支撑模块是四个大数据安全系统的公共部分，负责大数据的采集、预处理、传输、存储和展示；基于大数据的网络安全管理系统、基于大数据的安全态势感知系统、基于大数据的应用性能分析系统和基于大数据的安全运维管理系统等四个大数据系统，基于大数据共性技术支撑平台，面向不同的安全应用领域，通过不同的大数据安全分析模型，形成相应的安全功能与能力。

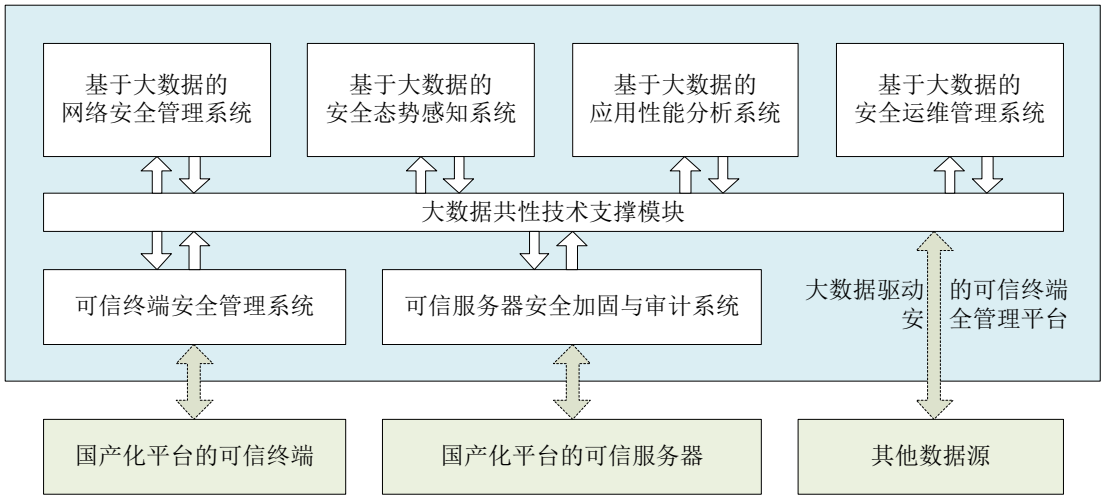

图 2 大数据驱动的可信终端安全管理平台组成结构

5.2.1 可信终端安全管理系统

可信终端安全管理系统针对国产化平台的可信终端，融合可信计算技术，从网络准入控制、系统监控、应用安全、数据安全及威胁检测等方面，实现对可信终端的全层次细粒度安全管理，保障可信终端安全。同时，也使可信终端成为信息系统的关键数据采集点，为信息系统的大数据网络安全管理、态势感知和安全运维管理提供强有力支撑。系统结构如图 3 所示。

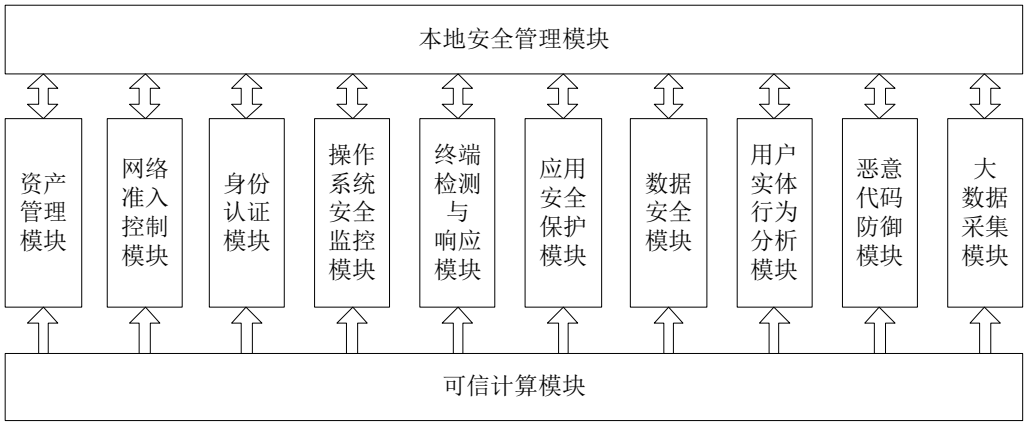

图 3 可信终端安全管理系统结构

该系统支持可信计算双体系结构，基于防护监管一体化策略，以内核层 HOOK 系统调用为根本，以规范化的数据接口和控制接口为基础，创新融合基于哈希的账号弱口令快速识别算法、基于 Rootkit 的主机安全监控、基于 Linux 的软件非法卸载防护、基于内核层的驱动级透明加解密、基于文件访问驱动过滤与沙箱的可信行为智能识别、基于语义特征与用户行为分析的数据防泄漏检测、基于大数

据的终端检测与响应等多种技术，以相对独立的模块组件嵌入到统一安全管理框架，实现对国产化平台的可信终端从操作系统行为监控、应用安全、数据安全到恶意代码防御的全方位安全管理，具备大数据采集、资产管理、行为监控、基线配置核查、补丁管理、强身份鉴别、恶意代码防御和安全审计等功能。国产化平台的可信终端成为大数据网络感知和执行安全策略的关键节点。

该系统支持多样化的国产化平台可信终端，包括四种国产 CPU（龙芯、兆芯、飞腾、申威）、四种国产操作系统（中标麒麟、银河麒麟、深度、中科方德）、四种国产数据库（达梦、金仓、神通、南通）的各类组合。

5.2.2 可信服务器安全加固与审计系统

可信服务器安全加固与审计系统针对国产化平台的可信服务器，在国产服务器操作系统的基础上，基于可信计算技术，从资产管理、身份认证、执行程序运行安全、数据安全、安全基线配置、恶意代码防御和安全审计等方面，全面提升国产操作系统的安全防护强度，保障服务器的安全。系统结构如图 4 所示。

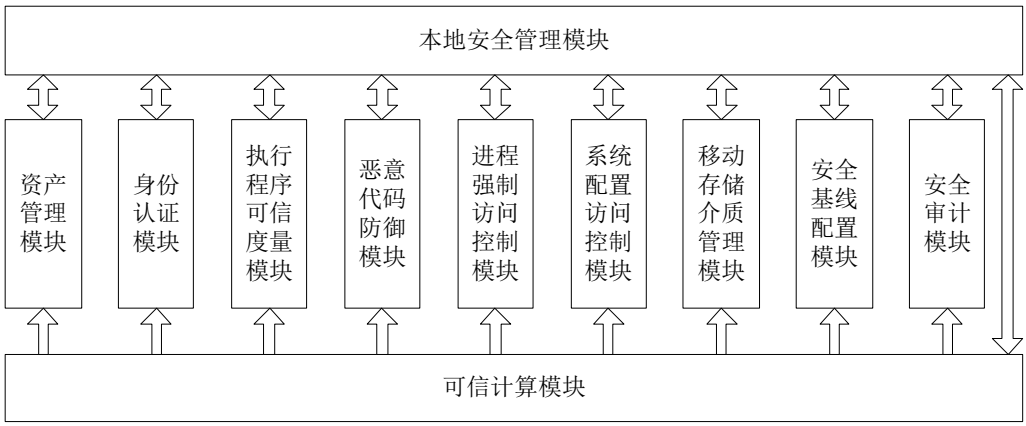

图 4 可信服务器安全加固与审计系统结构

该系统采用的关键技术包括：（1）可信计算技术，在国产操作系统底层建立一个信任根，从信任根开始到硬件平台，再到操作系统、应用进程、文件等，一级认证一级，一级信任一级，建立一条信任链，从而把这种信任扩展到整个服务器系统，提高服务器系统的安全性；（2）强制访问控制技术，基于 DTE 强制访问控制模型，通过对重要主体及客体的安全标记，控制主体对于客体的访问权限，实施强制访问控制，严格控制用户行为；（3）主动防御技术，在程序启动时进行拦截与审计，基于行为与特征，分析取证找到恶意代码行为，以保证服务器的操

作系统安全，将恶意事件控制在源头；（4）内核级安全加固技术，安全加固工作建立于操作系统内核层，既能准确全面地截获应用层的访问请求，又降低了系统安全机制被旁路的危险；（5）程序白名单，提供基于可执行程序 hash 值的白名单程序控制，禁止所有未知程序运行。

该系统支持中标麒麟、深度、Linux、Aix、Uinx 等市面上主流服务器操作系统，同时支持 KVM、VMware、Hyper-V 等主流虚拟化厂商，支持对虚拟化主机进行安全加固。

5.2.3 大数据共性技术支撑模块

大数据共性技术支撑模块提供大数据的采集、清洗、预处理、传输、存储、展示，以及配置、安全管理、监控等公共组件，基于开源的大数据技术和平台，针对国产化平台可信终端和其他终端的数据特点和采集需求，以及行业私有云或内网信息系统的部署和应用特点，为上层大数据安全应用提供大数据共性支撑能力。

该模块基于开源的大数据技术和平台，支持以前端大数据采集、后端大数据分析和展示为核心，通过网络和终端数据采集以及大数据分析模型，构建“数据采集、数据分析、决策支持、行动”闭环，实现基于大数据和深度学习的网络安全态势感知、威胁情报获取、业务应用性能分析、网络安全管理和安全运维管理。数据采集代理与终端安全管理代理融合，执行基于策略的数据定向采集和预处理，采集策略与大数据分析模型相关联，实现多维度、多层次的全要素数据采集。支持不同的应用需求开发不同的大数据分析模型，例如面向业务情景的数据盗取行为检测、APT 攻击检测、用户实体行为分析、异常流量分析、业务应用性能分析、面向网络舆情监测的大数据衍生处理等模型。大数据分析模型对采集的大数据进行分析，同时又指导大数据的精准采集。而且，基于搜索引擎技术的大规模数据存储与检索，以及内存索引方式，能够实现对新鲜数据的准实时查询和 TB 级硬盘数据的秒级查询。该模块的逻辑结构如图 5 所示。

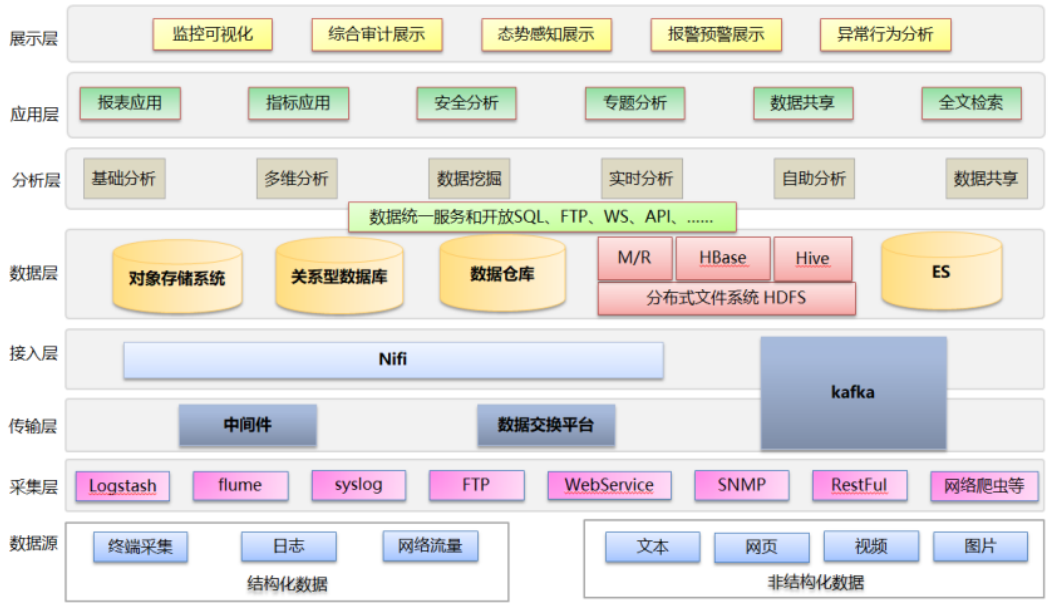

图 5 大数据共性技术支撑模块逻辑结构

该模块涉及面向终端的大数据采集与清洗、大规模数据实时检索、大数据可视化等关键技术，具体如下。面向终端的大数据采集与清洗技术以轻量级的终端异构数据采集代理，基于策略驱动的数据采集规则，通过向操作的进程注入钩子替换剪切板操作函数、向系统中注册一个硬件信息变动的消息、向操作的进程注入键盘钩子并设置回调函数、向系统中的进程注入钩子模块以及向系统中安装驱动程序截获网卡数据包，来采集终端的系统开关机数据、用户的复制粘贴数据、移动存储数据、外设插拔数据、截屏操作数据、活跃进程信息和上网行为等数据，既解决了系统信息、网络信息、文档信息、本地软件信息等终端数据的采集问题，又不多占用终端自身资源，具备良好的适用性和用户体验。清洗技术用于发现并纠正数据文件中的可识别错误，针对数据审查过程中发现的错误值、缺失值、异常值和可疑数据，进行清洗使数据变为干净可用的数据，有利于后续的分析和建模。除了去重处理和数据一致性检查之外，还运用了基于终端数据特征的冗余数据清洗和错误数据清洗，并结合终端日志采集运用基于终端的断点数据清洗。

大规模数据实时检索技术是基于搜索引擎的大规模日志行为数据存储与检索，采用内存索引方式保证对新鲜数据的近实时查询、TB 级硬盘数据的秒级查询；针对大数据特点(海量、数据异构多样性、应用需求多样性)进行设计；具备分布式并行计算、多副本机制、对等节点机制、没有单点的高可靠体系架构，与 Hadoop 无缝集成；创新的柔性多引擎机制，提供开放的二次开发接口；提供按

词索引、按字索引、字词混合索引方式，满足不同应用场景对查全和查准的不同需求；支持异步检索模式，适应大并发（高连接数）的应用场景要求，避免了同步检索模式时消耗太多线程资源的问题；多层次、多粒度的分布式 CACHE：既有单节点的检索缓存，又有合并后的整体检索缓存，大大提高了缓存的命中率，减轻高并发下的检索节点压力。

通过大数据可视化技术及时跟踪敏感数据包括文件的流程路径，出现数据泄露问题时追根溯源。

5.2.4 基于大数据的网络安全管理系统

基于大数据的网络安全管理系统用于对行业私有云或企业信息系统进行安全管理，不但支持对可信终端和可信服务器的安全管理，还支持对其他终端和网络组件的安全管理。它根据风险管理原则，基于可信终端安全管理系统、可信服务器安全加固与审计系统以及其他数据采集源的数据，利用基本的数据分析模型和大数据分析模型，从资产、威胁、脆弱性、安全措施有效性、安全事件等方面，对信息系统安全风险要素进行分析和管理；进一步地，基于各风险要素建立网络安全评价指标体系，对信息系统各部门进行安全考核，从技术和管理两方面全面提升网络安全水平。它还支持用户实体行为分析，基于用户自身的基本属性和终端/网络行为方式属性来建立基于大数据的用户画像模型，进行用户画像。该系统包括安全管理策略、用户管理、资产管理、脆弱性管理、威胁管理、安全措施管理、安全事件管理、安全综合分析、报告报表和展示等模块，具体如图 6 所示。

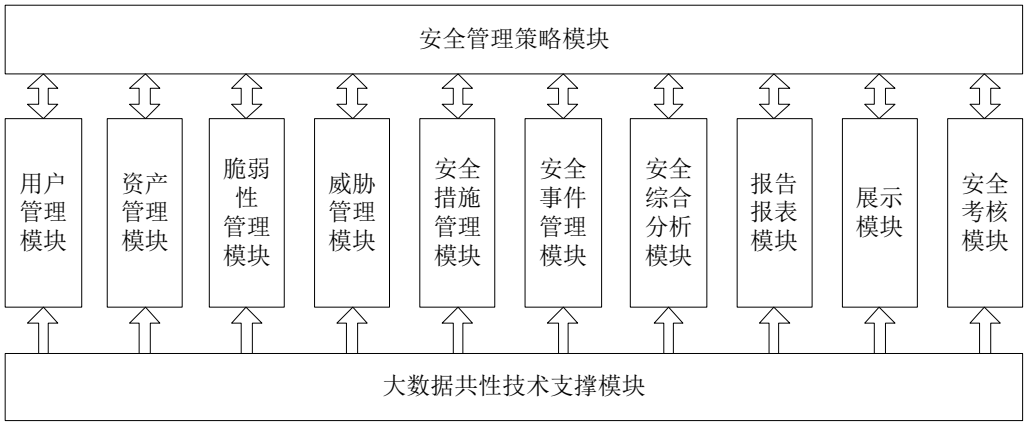

图 6 基于大数据的网络安全管理系统结构

该系统涉及精准化用户行为分析、自动关联和基于策略与执行相分离的安全

管理等关键技术，具体如下。

精准化用户行为分析技术通过机器学习对用户、实体进行分析，包括实时和离线检测方式，可得到直观的风险评级和证据分析，让安全人员能够响应异常和威胁。对用户和资产实体进行画像，建立行为基线，及时识别特权账户和普通用户的异常行为，也可以作为 APT 攻击检测的基础。实时将数据与用户、设备和应用相关联，对企业敏感数据，在网络中流动时进行全方位画像，准确监测报警异常行为。这些可疑行为按照时间序列和行为阶段进行了相互验证。以用户视角将多种数据关联和丰富起来，持续跟踪并进行风险预警；实现将数据与用户、设备和应用相关联，对企业敏感数据，在网络中流动时进行全方位画像。该技术的大数据分析模型包括业务分类模型、标签智能识别模型、终端使用效率分析模型、用户热点分析模型、用户画像、用户行为轨迹分析模型、用户行为规律分析模型等 15 大类模型体系。

自动关联技术对各类数据按照预定的流程进行流式处理，以保证各种数据处理的准确性；基于面向分布式数据流处理和批量数据处理的计算平台，提供支持流处理和批处理两种类型应用，针对数据处理与计算分析进行自动化关联；引入 CEP 规则引擎模块和类 SQL 语言，满足大数据平台在数据处理阶段的实时、高效、并发、可靠的要求；支持水平扩展，通过增加集群节点即可提高集群的并发处理能力，并具有自动容错机制。

基于策略与执行相分离的安全管理技术，采用大数据分析来驱动安全管理过程，摆脱了面向设备的管理模式，通过提高安全管理的抽象层次，来屏蔽被管理对象的物理差异，从而灵活方便地对资产设备进行集中管理；同时，在管理过程中，将策略管理和系统执行相分离，管理员只需对策略进行定义，而不必关心实现该策略的具体细节和相关设备的情况；而且，能根据需求变化的需要而动态改变管理策略，相应地改变管理行为，而无须改动管理模块的底层实现或中断管理的操作，提高了管理的可扩展性和灵活性，增加了安全管理的实时性和自动化程度。

5.2.5 基于大数据的安全态势感知系统

基于大数据的安全态势感知系统用于掌握信息系统的网络安全状态变化及

演化趋势，并融合其他安全防护措施使网络处于安全状态之中，它对能够引起安全态势发生变化的安全要素进行获取、理解、显示和预测，为信息系统主管部门、运营部门和管理员呈现信息系统的网络安全全局视图，为不同的管理角色提供不同层次的网络安全信息，从而支持正确决策行动的执行。它从网络安全防护方的视角，以网络攻防对抗双方信息的动态变化为主线，梳理和分析来自可信终端安全管理系统、可信服务器安全加固与审计系统以及信息系统中的其他数据采集源比如网络安全设备的数据，特别是以动态变化的数据为基础。可基于资产、脆弱性和安全措施有效性数据，给出信息系统整体、不同安全域和资产的安全防护能力水平；基于安全事件数据以及威胁监测与分析数据，给出已发生的、正在发生的和潜在的网络安全威胁及其攻击目标资产。该系统包括策略管理模块、安全态势要素获取、安全态势要素分析、安全态势评估与预测、决策支持和安全态势展示等六个模块，具体结构如图 7 所示。

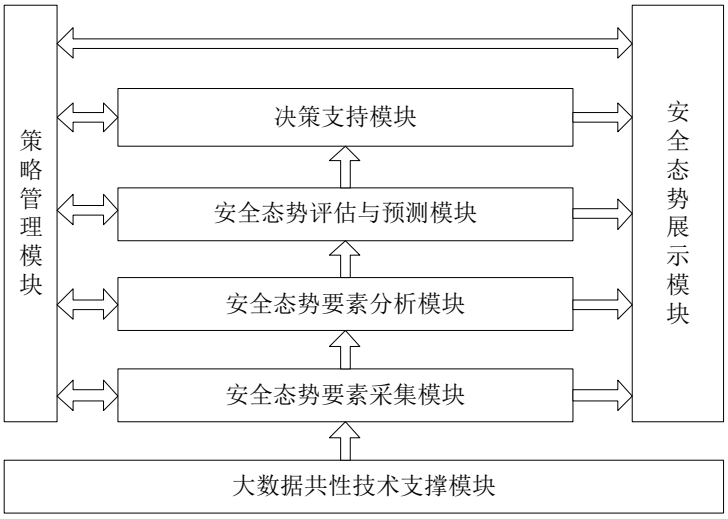

图 7 基于大数据的安全态势感知系统结构

该系统涉及恶意代码分析、网络攻击行为检测分析、终端检测与响应等关键技术，其支撑是各种基于大数据的安全分析模型，例如面向业务情景的数据盗取行为检测、APT 攻击检测、DDoS 攻击检测、勒索软件检测分析、挖矿木马检测分析等模型。

终端检测与响应技术是大数据态势感知的基本技术，其前端基于可信终端安全管理系统、可信服务器安全加固与审计系统和其他数据采集源，进行大数据采集，执行安全态势感知系统下发的安全策略；后端基于各数据采集源的数据，执

行基于大数据的安全分析，发现潜在安全威胁，并生成响应的安全策略。随着安全威胁的日趋严峻，单点的终端处于资源占用和计算能力因素，不足以应对日益复杂的网络攻击行为，汇聚各终端数据至管理端（云端）进行大数据安全分析成为必然选择，同时利用深度学习手段辅助进行攻击检测。

面向业务情景的数据盗取行为检测技术区别于传统基于安全信息和安全事件管理的异常分析，是借助机器学习算法的一种用户与实体行为分析技术，而非基于业务系统或内网的特定事件或特定流量信息（该信息包括用户登录信息、管理员设定的阈值、从设备、应用和主机发起的数据访问等）。它摒弃预先配置的关联规则，利用机器学习，使用聚类、函数回归等方法，通过对海量用户行为数据进行分析，建立用户行为模型，并用其指导、分析终端的用户行为数据，检测并发现违反用户行为模型的异常数据，再进一步结合终端用户的使用环境和业主情景，做出综合判断。基于终端采集的数据，它能够面向不同的行业网环境和用户情景，创建行为检测基线，重点解决内网数据盗取、内部威胁检测、内部系统是否被攻击等安全问题。

5.2.6 基于大数据的应用性能分析系统

基于大数据的应用性能分析系统以分析信息系统内资产和应用系统的使用性能和效率为目标，给出资产与应用的效能分析数据和报告，并对异常使用和访问进行预警。基于终端进行统计分析，可分析应用的活跃度，包括应用网站访问TOP榜单、应用访问区域TOP榜单、IP访问TOP榜单和设备访问应用次数榜单等。基于网络会话进行统计分析，从源IP的角度和目标IP的角度进行，分别提供针对IP和端口的访问次数榜单，提供对跨区域访问重点应用服务器的行为的分析和发现功能。基于应用访问进行分析，提供应用覆盖分析、应用访问次数分析、访问对象分析、热点对象分析、应用访问离散度分析、高频访问分析、跨用户角色访问分析、跨区域访问分析和业务应用关联分析等。综合风险评估，可提供根据终端行为数据对人员和设备数据泄露风险的评估。对异常行为进行预警，包括违规进程报警、网络会话报警、PKI违规使用报警、红名单与热点库预警、下班时间访问应用次数预警、网络会话次数与端口数预警。该系统包括策略管理、终端分析、应用分析、流量分析、安全分析、监控预警、性能展示和报告报表等模

块，如图 8 所示。

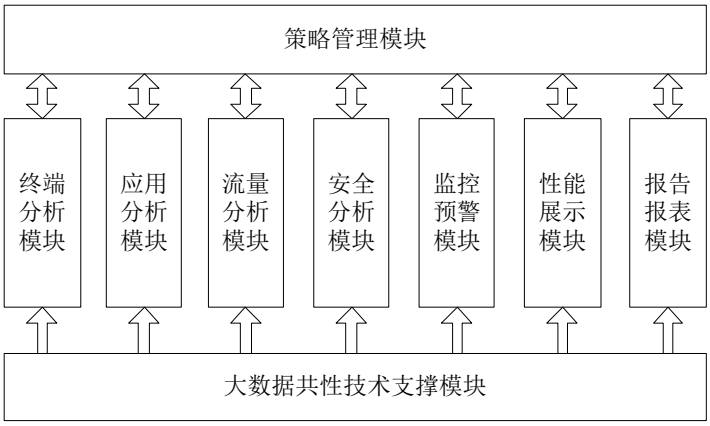

图 8 基于大数据的应用性能分析系统结构

该系统涉及支持面向网情监测的大数据衍生处理等关键技术。支持面向网情监测的大数据衍生处理技术支持自然语言智能处理，采用以词典为基础，规则与统计相结合的分词技术，通过“最长关键词优先法”有效解决切分歧义。综合利用基于概率分析的语言模型方法实现自动分词；通过预分析监测专业关键词表及全文语义理解，在不需要人工干预的情况下实现对检测对象的自动分类处理；基于相似性算法的自动聚类，自动对海量的无类别文档进行归类处理，实现对检测对象的自动聚类；基于文档“指纹”的文本查重，支持海量数据的信息查重，并支持对话题的情感分析。此外，还利用面向互联网的专题跟踪，实时查看该舆情专题相关的时间变化曲线（接日、星期、月进行选择）、媒体分布、地区分布、媒体类型分布、作者分布（便于发现舆论领袖），并可以自动生成专题报告，支持舆情处置专家库的构建。

5.2.7 基于大数据的安全运维管理系统

基于大数据的安全运维管理系统用于对信息系统内的安全设备、网络设备、服务器和终端主机，以及操作系统与应用系统的性能和可用性进行集中化实时监控，并在此基础上，作为安全服务平台，提供安全检测、威胁情报、应急处置和安全防护配置等安全服务，完成“安全基线+安全服务”双轮驱动保障网络安全的拼图。该系统主要利用 IT 资产的性能与可用性数据，进行全方位细粒度的监控，对监控指标设置告警阈值，对各种性能监控指标进行对比分析，全面监控资产的使用性能和安全状态。在事件分析方面，提供实时监视与审计视图，管理员

可以根据内置或者自定义的实时监视策略，从日志的任意维度实时观测安全事件的走向，进行事件行为分析和来源定位，并进行安全事件的情境关联。引入考核管理，通过量化性和行为性的指标体系，来评价各部门的网络安全状况、运维水平与安全规章执行情况。同时，建立预案库、模板库、策略库、案例库、漏洞库、事件库等支撑安全运维的知识库。利用大数据展示功能，结合地理信息、机房信息展示信息系统运维状态。

在安全服务方面，提供基于大数据平台的安全检测与评估，一是对目标信息系统进行远程安全检测与评估，二是对用户提交的可疑样本文件进行安全性分析，发现潜在的恶意代码或攻击样本。同时，对发现或上报的安全事件，启动应急处置程序，借助系统提供的大数据技术和平台支撑，远程或本地分析解决问题。具有威胁情报获取能力，基于安全事件分析、安全检测和实时监控，以及第三方威胁情报，形成威胁情报信息，向管理员和用户反馈。而且，能够根据运维安全状况，依据事先配置的安全策略，自动对安全防护设备进行策略配置或策略配置建议，确保网络处于安全状态。

该系统由实时监控、安全检测与评估、安全事件分析、应急处置与通报、安全防护配置、威胁情报、运维展示、知识库、考核管理和运维报告等模块组成，如图 9 所示。

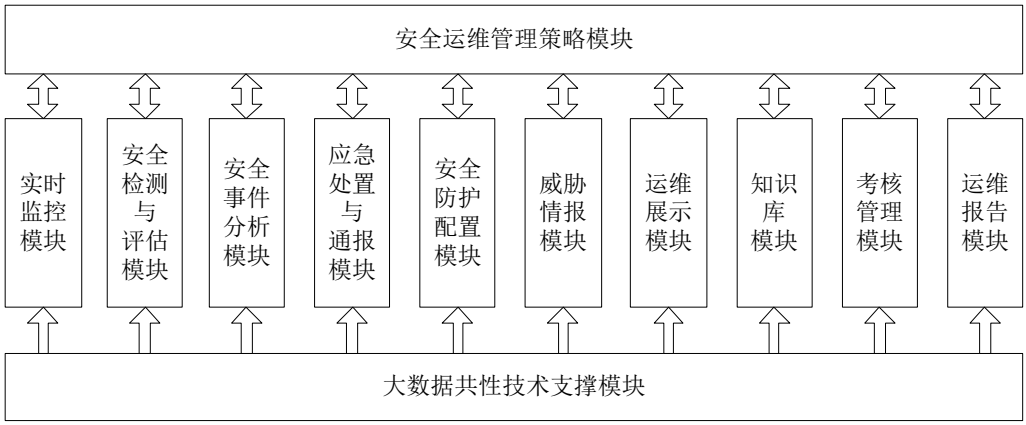

图 9 基于大数据的安全运维管理系统结构

该系统涉及情景关联和基于地理信息与机房机架信息的网络拓扑描绘等关键技术。情境关联分析技术包括基于资产的情境关联、基于弱点的情境关联、基于网络告警的情境关联和基于拓扑的情境关联等，可以将事件中的 IP 地址与资产名称、资产价值、资产类型（包括自定义类型）、自定义资产标签进行关联；

将安全事件与该事件所针对的目标资产当前具有的漏洞信息进行关联，包括端口关联和漏洞编号关联；将安全事件与该事件所针对的目标资产（或发起的源资产）当前发生的告警信息以及当前的网络告警信息进行关联；根据网络故障沿网络拓扑水平传播的特性，通过对大量网络告警事件在拓扑空间中的分布，以及传播时间上的顺序，自动进行网络根本故障源（Root Cause）诊断。

基于地理信息与机房机架信息的网络拓扑描绘技术，将实际地理信息、IP地址信息与网络拓扑结构相结合，展示IT资产之间的物理与逻辑拓扑连接关系，并可自动进行多种拓扑布局。通过网络拓扑图，管理人员可以对全网的资产进行可视化的监控。可动态更新网络拓扑，实时显示资产的运行状态和安全状态，方便地链接到其他功能模块。提供机房机架视图，将客户资产设备根据实际机架摆放可视化地展示出设备的物理摆放，管理员透过机架视图可以清楚地知道每个资产的位置，机架视图也具备动态更新能力，能够实时地显示资产的运行状态和安全状态。

5.3 项目投资概算

大数据驱动的可信终端安全管理平台项目，总投资金额拟不超过23,400万元，资金的投入主要包括研发场地装修改造及软硬件购置费、研发及辅助人员薪酬、市场营销推广费及其他铺底费用等，项目建设期1年3个月，预计2020年12月31日前完成，投资估算情况如下：

序号	项目	投资金额（万元）	投资占比（%）
1	**固定资产及无形资产投入**	**1,100**	**4.70%**
1.1	研发场地装修改造费	500	2.14%
1.2	项目硬件及软件设备购置费	600	2.56%
2	**研发及技术支持人员费用**	**10,000**	**42.74%**
2.1	研发及测试人员综合薪酬	7,000	29.91%
2.2	技术支持人员综合薪酬	3,000	12.82%
3	**第三方合作研发**	**1,500**	**6.41%**
4	**营销推广费**	**8,800**	**37.61%**
4.1	营销人员综合薪酬	2,800	11.97%
4.2	市场推广及运维费	6,000	25.64%

5	**项目其他铺底费用**	**2,000**	**8.55%**
合计		**23,400**	**100.00%**

具体费用明细如下：

（1）研发场地装修改造费

本项目研发场地装修改造费 500 万元，主要包括研发场地建设、装修、专线运营等费用。

（2）项目硬件及软件设备购置费

本项目设备购置投资共 600 万元，用于购置国产化计算机、服务器、网络设备、测试和样机设备、办公设备以及应用软件等；构建产品研发、测试和实验的基础设施环境等。

（3）研发及技术支持人员费用

本项目研发及技术辅助人员费用投资共 10,000 万元，用于国产化平台研发及测试人员薪酬、技术支持人员薪酬。

（4）第三方合作研发

本项目第三方合作研发投资共 1,500 万元，用于同第三方机构共同开展领域内关键技术联合攻关和前沿技术研究与开发。

（5）营销推广费

本项目市场营销投资共 8,800 万元，用于销售人员薪酬、市场推广活动以及运营维护费用等。

（6）项目其他铺底费用

本项目其他费用投资共 2,000 万元，用于知识产权申请费、差旅费、会议费、其他租赁费等。

6．项目效益分析

通过本项目的实施，公司提供的产品和服务能够紧贴国产化替代进程，为可信终端的推广应用保驾护航，为政府、军队军工、金融和能源等行业部门构建国产化平台之上的信息系统或私有云打造整体的网络安全解决方案。一方面，有助于公司提高现有客户的粘性，帮助他们从“Windows+Intel”平台平滑过渡到基于可信计算的国产化平台；另一方面，能够基于领先的技术和产品大幅拓展新增

客户，扩大公司用户群体，形成长期稳定的营业收入和营业利润，有效提升公司的核心竞争力和行业影响力，促进公司快速增长和良好发展。而且，本项目能够为重点行业打造基于大数据的网络安全管理、网络安全态势感知、应用性能分析和安全运维管理的样板工程，重点面向政府、军工和金融等涉及国家安全的重点行业，针对企业级信息系统或私有云的各种典型应用场景，提供大数据驱动的“安全基线+安全服务”一体之两翼的网络安全解决方案与产品，融合网络安全与业务应用，打造符合国家标准要求的网络安全防护与运维体系，形成样板工程和最佳实践，有效抵御持续变化的网络安全威胁。

7. 项目实施的风险

本项目会紧跟国产化替代进程的步伐，但国产化替代进程仍可能因政策、技术和应用因素而放缓，国产 CPU、操作系统或应用软件等国产平台的整个生态系统的所有因素出现的问题，都可能会影响到产品的市场推广和表现，达不到预期的目标。为此,公司将会与各国产化平台厂商进一步加强战略合作，在人才、技术和市场等方面增进合作，打造以可信终端整机厂商为核心的“底层平台+操作系统+安全+应用”的国产化平台生态体系，共同拓展客户资源和市场，来加快国产化替代进程，推进大数据安全解决方案。

8. 投资项目结论

本项目实施符合国家安可与大数据发展战略与相关产业政策，符合公司战略布局，有利于提升公司的研发能力和行业地位，增强公司综合实力，形成公司盈利新的增长极，本项目具有良好的发展前景，具备了实施项目所需的各项基本条件，未来发展空间广阔，具备较好的可行性。

北京北信源软件股份有限公司

2019 年 10 月 14 日