安信证券 ESSENCE SECURITIES

2019 年 10 月 11 日

计算机

行业深度分析

证券研究报告

网络安全内容审查迎来黄金发展期

投资评级 领先大市-A

维持评级

首选股票 目标价 评级

行业表现

数据来源：Wind 资讯

%	1M	3M	12M
相对收益	-0.63	-3.94	-37.27
绝对收益	-1.10	-0.60	-12.06

胡又文 分析师

SAC 执业证书编号：S1450511050001

huyw@essence.com.cn

021-35082010

相关报告

计算机行业深度分析 2019-10-07

计算机板块三季报前瞻 2019-10-06

里程碑事件频发，5G 应用未来已来 2019-09-28

工信部《促进网络安全产业发展指导意见》点评 2019-09-28

网络套餐与标志性终端问世，5G 应用箭在弦上 2019-09-22

- **网络安全内容审查上升到空前高度。**近年来，网络安全形势快速变化，根据赛迪顾问《2019 中国网络安全发展白皮书》，2019 中国网络安全市场有望达到 608 亿元。根据网信办官网，多部委及企事业单位联合起草了《网络安全审查办法（征求意见稿）》并已经公开发布，网络安全内容审查上升到空前高度。该征求意见稿针对关键信息基础设施运营者采购网络产品和服务方面提出具体要求。网络安全内容审查可以分为网络安全审计产品、上网行为管理产品、开源情报分析产品和 VPN 服务产品四大细分领域。

- **网络安全审计产品。**网络安全审计过程与传统财务会计领域的审计行为类似，是一种针对已发生的网络行为及已产生的网络内容进行分析审查的行为，可细分为网络事件审计产品和网络内容审计产品。预计 2019 年国内日志安全审计产品市场规模为 11.4 亿元，并在 2021 年达到 17.8 亿元。

- **上网行为管理产品，**包括针对外网的管理和对内网的管理，针对外网的管理能够防御网络黑客和病毒入侵计算机，并进行破坏；针对内网的管理则更加关注用户在上网时的行为规范。得益于网络安全法的落地、云计算对于 IT 基础设施的重构，以及物联网设备的迅速增长，上网行为管理领域正在迎来全新的发展阶段，我们预计未来 5 年整体市场复合增长率为 25.5%。

- **开源情报分析产品。**情报分析主要针对网络空间进行舆论分析，而开源主要是指能够提供自主研发的解决方案。舆情分析作为互联网时代民意调查的主要方式，是公共安全维护的重要工具，也是企业发展方向的重要参考，市场空间巨大。从未来趋势上看，大数据+AI 将赋能开源情报分析产品。

- **VPN 服务产品。**VPN 是一种常用于连接中、大型企业或团体与团体间的私人网络的通讯方法，可以用不安全的公共网络来发送可靠、安全的消息。全球 VPN 服务市场增长迅猛，在 2016 年就达到了 156.4 亿美元，在 2022 年有望达到 357.3 亿美元。在中国市场，安全厂商加码 VPN 业务，同时与云服务厂商紧密协同，共同打造高质量安全 VPN 服务。

- **投资建议：**随着《网络安全法》、《网络安全审查办法（征求意见稿）》、《个人信息和重要数据出境安全评估办法（征求意见稿）》等一系列法律和政策文件陆续出台或公开征求意见，网络安全审查市场迎来黄金发展机遇，我们看好任子行、顺网科技、三六零、中新赛克、深信服、绿盟科技、启明星辰、拓尔思等在网络安全审查领域进行长期布局并拥有显著技术优势的领军企业。

- **风险提示：**网络安全审查行业发展进度不及预期；政策推进力度不及预期。

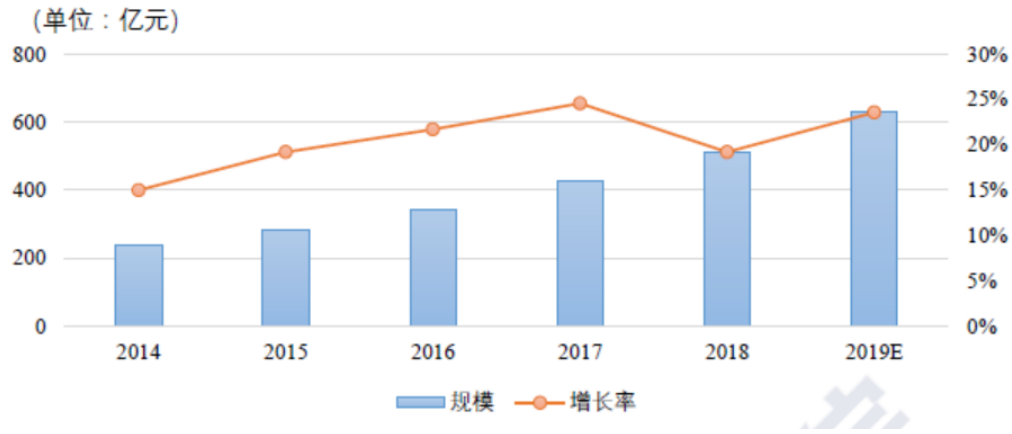
内容目录

图表目录

1. 网络安全内容审查上升到空前高度

近年来，国内外网络安全形势快速变化，根据赛迪顾问《2019 中国网络安全发展白皮书》，2019 中国网络安全市场规模有望达到 608 亿元。2019 年 5 月 13 日，国家市场监督管理总局、国家标准化管理委员会召开新闻发布会，等保 2.0 相关的《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护安全设计技术要求》等国家标准正式发布，将于 2019 年 12 月 1 日开始实施。一系列网络安全领域国家顶层规划政策的出台，在体系上进行了大升级，在标准制度上也上升到法律，标志着我国政务、公安、工农等各个领域结合云计算、移动互联、物联网和大数据等新技术新应用开展并深化网络信息建设，新兴技术的大规模渗透将从技术层面和服务层面更好地助力国内网络安全升级，国内网络安全市场将迎来快速发展。

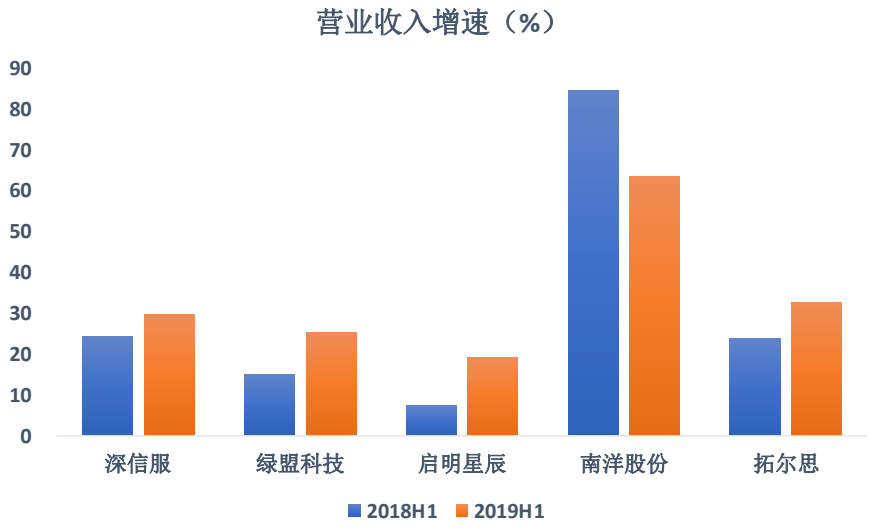
图 1：我国网络安全市场规模



数据来源：中国信息通信研究院，安信证券研究中心

我们统计了业内拥有边界安全产品的主流厂商近两年收入增速的变化情况（其中深信服、南洋股份仅参考其网络安全业务的财务数据，拓尔思主要参考其安全子公司天行网安的财务数据），从收入端的角度，2019 上半年多数公司的收入增速超过了去年同期，行业景气度上升的趋势明显。

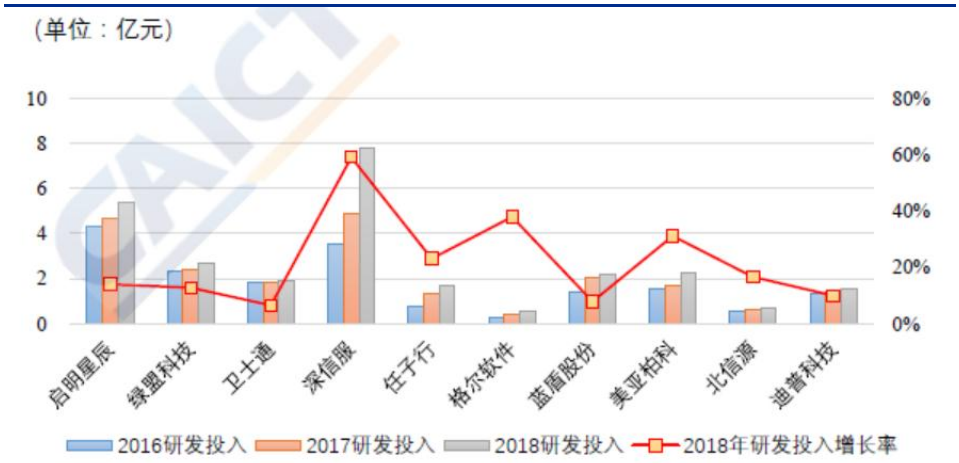
图 2：主要网络安全公司 2019H1 收入增速情况



资料来源：Wind，安信证券研究中心

在研发投入方面，企业持续加大研发投入力度。2018 年国内 10 家上市网络安全企业平均研发投入为 2.67 亿元，相较于 2017 年增长了 25.2%，为产业良好发展打下坚实基础。

图 3：网络安全上市公司研发投入持续增加



数据来源：中国信息通信研究院，安信证券研究中心

产业发展政策环境持续优化。根据网信办官网，今年 5 月中央网信办会同国家发展和改革委员会、工业和信息化部、公安部、国家安全部、商务部、财政部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局联合起草了《网络安全审查办法（征求意见稿）》并已经公开发布，网络安全内容审查上升到空前高度。

该征求意见稿针对关键信息基础设施运营者采购网络产品和服务方面提出具体要求，运营者采购网络产品和服务时，应预判产品和服务上线运行后带来的潜在安全风险，形成安全风险报告。当发生关键信息基础设施整体停止运转或主要功能不能正常运行、大量个人信息和重要数据泄露、丢失、毁损或出境、关键信息基础设施运行维护、技术支持、升级更新换代面临供应链安全威胁等严重危害关键信息基础设施安全的风险隐患时，应当向网络安全审查办公室申报网络安全审查。

表 1：近年各类网络安全相关法规汇总

相关法规	进度	相关机构
《数据安全法》	列入十三届全国人大常委会立法规划，相关研制论证工作有序开展	
《中华人民共和国密码法（草案）》	2019 年 7 月发布，公开征求意见	国家密码管理局
《关键信息基础设施安全保护条例》	列入国务院 2019 立法计划	中央网信办、工业和信息化部、公安部
《网络安全等级保护条例》	2018 年 6 月向社会公开征求意见	
《网络安全审查办法》《数据安全管理办法》《儿童个人信息网络保护规定》《网络关键设备安全检测实施办法》《个人信息出境安全评估办法》《网络安全漏洞管理规定》	2019 年 5 月以来相继完成向社会公开征求意见，进入修改完善阶段	
《云计算服务安全评估办法》	2019 年 7 月发布	国家网信办、国家发展改革委、工业和信息化部、财政部
《关于加强电力行业网络安全工作的指导意见》	2018 年 9 月发布	国家能源局
《车联网（智能网联汽车）产业发展行动计划》	2018 年 12 月发布	工业和信息化部
《加强工业互联网安全工作的指导意见	2019 年 9 月发布	工业和信息化部会同九部门
《区块链信息服务管理规定》	2019 年 1 月发布	国家互联网信息办公室
《关于开展 2019 年 IPv6 网络就绪	2019 年 4 月发布	工业和信息化部

专项行动的通知》		
《金融科技（FinTech）发展规划（2019-2021 年）	2019 年 8 月	中国人民银行
《电信法》	列入十三届全国人大常委会立法规划，相关研制论证工作有序开展	

数据来源：机构官网，中国信息通信研究院，安信证券研究中心

针对行业现状和市场结构，我们认为网络安全内容审查可以分为网络安全审计产品、上网行为管理产品、开源情报分析产品和 VPN 服务产品四大细分领域。

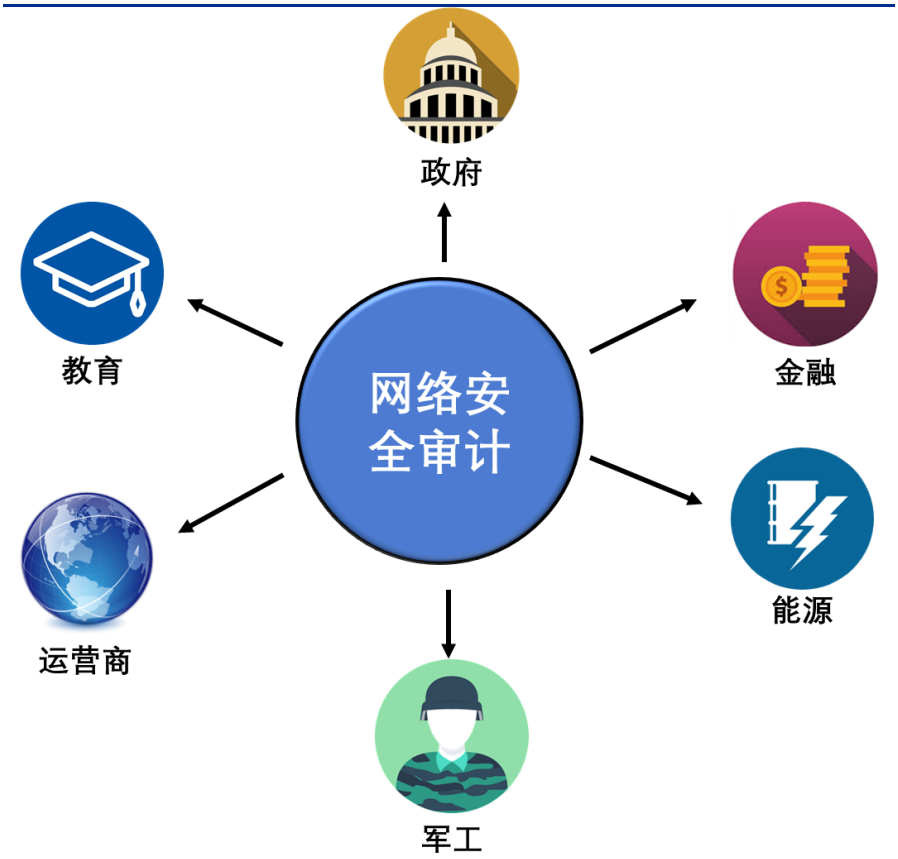
2. 网络安全审计产品

2.1. 网络安全审计产品定义及特点

网络安全审计是指按照一定的安全策略，利用记录、系统活动和用户活动等信息，检查、审查和检验操作事件的环境及活动，从而发现系统漏洞、入侵行为或改善系统性能的过程。网络安全审计过程与传统财务会计领域的审计行为类似，是一种针对已发生的网络行为及已产生的网络内容进行分析审查，从而查找安全漏洞、捕捉潜在风险的行为。

网络审计产品专注于为企业园区网络提供边界安全、内网行为管理和政策合规三大业务需求解决方案。主要面向企事业单位、教育、军工、运营商和连锁酒店商超等客户，是传统网络安全市场生态的重要建设者。其中边界安全产品主要在内外网边界构筑多重网路安全防护屏障，为内外网之间的通信提供全方位的安全保障。

图 4：网络安全审计应用领域



数据来源：安信证券研究中心整理

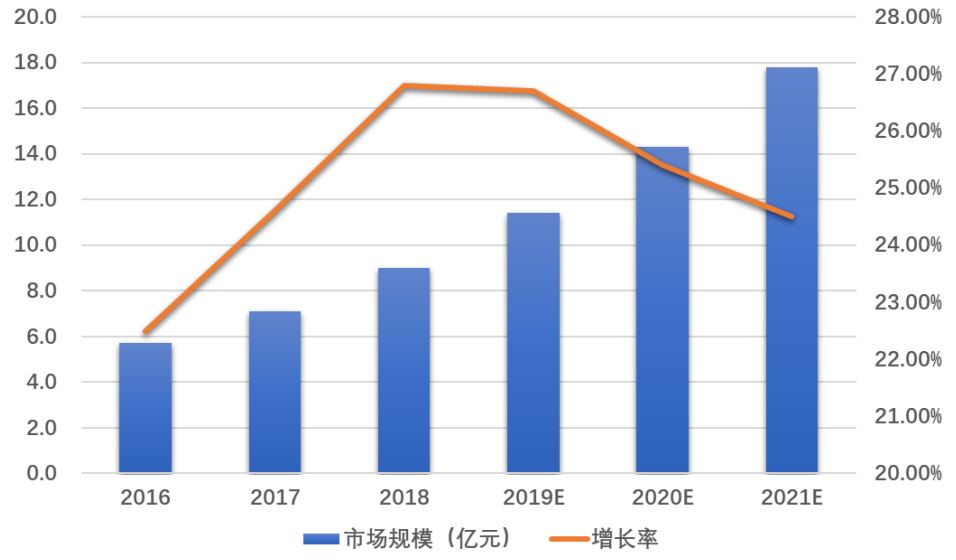
我们将网络安全审计分为网络事件审计产品和网络内容审计产品。

2.2. 网络事件审计产品

网络事件审计产品指通过对已发生事件安全日志进行审查，进而查找潜在安全漏洞、防范潜在入侵的安全类产品。在网络安全威胁日益复杂化、国际网络安全环境日趋复杂化的大背景下，以识别非法网络入侵或恶意利用网络安全漏洞为主导的预判型安全解决方案已不能完全满足政企类客户的安全需求。因而，以后验方式为主导的网络事件审计产品补充了安全体系的空白。通过整理分析已发生的用户访问、上传下载、网络服务等事件进行整合分析，网络事件审计产品能够为客户提供图形化监控、安全性判定等功能。

网络事件审计产品市场增长迅猛，2019 年有望突破 10 亿。伴随着我国网络安全扩张，网络事件审计产品表现出强劲的增长力。作为网络事件审计中的主体，日志安全审计产品市场规模在 2016-2018 期间由 5.7 亿元增长至 9.0 亿元，年复合增速达 25.66%。根据赛迪顾问预测，日志安全审计产品市场将在 2019 年突破 10 亿，达到 11.4 亿元，并在 2021 年达到 17.8 亿元。网络事件审计产品市场有望持续保持 20%以上增速，潜力巨大。

图 5：我国日志安全审计产品市场规模及增速测算



数据来源：赛迪顾问，安信证券研究中心

网络事件审计产品主要存在以下特点：

（1）可追溯：网络事件审计产品往往会对事件进行完备的系统日志记录，并对其进行持续维护。系统日志主要根据网络安全级别及强度要求，选择记录部分或全部的系统操作。通常系统日志主要包括事件发生的日期及时间、引发事件的用户 IP 地址、事件源及目的地位置、事件类型等。对于各种网络系统应采用不同的记录日志机制。日志的记录方式有 3 种：操作系统完成、应用系统完成、其他专用记录系统完成。

（2）可视化：网络事件审计产品针对安全事件进行持续分析、实时跟踪，并将结果以可视化形式展示给安全管理者。以任天行的网络安全管理系统-RAG 产品为例，其为用户提供直观丰富的统计报表，并支持合规细粒度审计，全面准确统计各类结果，可应用在各类领域。

图 6：天鉴网络安全审计与风险管理中心

数据来源：任子行，安信证券研究中心

图 7：网络安全管理系统-RAG 可视化审计

数据来源：任子行，安信证券研究中心

（3）后验性：网络事件审计产品针对的是已发生的各类网络事件，因而是一种补全型系统而非预判型系统。网络事件审计产品的核心目的在于对间谍软件、黑客远程控制等非法行为的巡查纠错。

2.3. 网络内容审计产品

网络内容审计产品指针对已产生网络内容的审查类产品，包括文本、视频、音频等各类形式的网络素材。针对面向对象的不同，可分为公司内网安全范畴的审查类产品和公网公共安全范畴的审查类产品。

公司内网安全审查类产品面向客户机构内网内容安全审查，采购对象为各大中型企业及公司。公司内网安全审查类产品将对公司内网各类数据进行分析，例如文件传输过滤与记录、邮件过滤与记录、即时通讯过滤与记录。文件传输过滤与记录通过智能识别 HTTP 网页与 FTP 协议的文件上传和文件下载，并对文件的上传和下载进行过滤与记录。邮件过滤与记录可以监控到任何一台计算机通过 Outlook 或 Foxmail 等邮件客户端软件使用 SMTP 和 POP3 收发邮件， 也可以监测到通过 Yahoo、Sohu、163、126、Hotmail、Tom、Sina、Gmail、QQmail 等 Webmail 提供商收发邮件的内容和附件。即时通讯过滤与记录支持对即时通讯协议进行阻断，及对文字聊天、语音聊天及文件传输 进行过滤与内容记录。在公司内网安全审查类产品的保护下，员工的工作效率将有效提高，公司各类机密信息将得到有效保护。

公网公共安全范畴的审查类产品面向公共网络内容的安全审查，采购对象为各类大型互联网平台公司和政企机关。在公共互联网环境内容日益丰富的同时，各类非法信息、非法行为充斥网络，损害公司利益并危害国家安全。针对公网公共安全内容审查需求，深信服推出了深信服网络综合审计产品（UAS）系列产品，面向政府单位设计，可帮助政府用户对访问互联网服务实行上网实名制和用户分级控制机制，规避互联网使用的法律风险、舆论风险，提供准确数据记录，定位责任人。同时，面向网吧等网络安全问题的高发地带及网络信息监管重点，顺网科技进行持续布局网络安全领域，以 3.7 亿元的对价收购国瑞信安，获得其安全审计系统、实名上网行为管理系统、互联网敏感信息管理控制系统等相关产品。在公网公共安全安全审查类产品的保护下，互联网平台内容的合法性将得到有力维护，政务类平台的运营将得到有效保障。

图 8：深信服网络综合审计(UAS)系列产品

数据来源：深信服安信证券研究中心

AI 技术加持，网络内容审计产品如虎添翼。各类文本、音频、视频等网络内容审查工程浩大，传统方法依赖人工查对，往往耗资巨大却收效甚微。自 2015 以来的人工智能技术革命为网络内容审计提供了新动力。CV 类 AI 技术帮助帮助各大云服务商及视频网站大幅削减人工成本，通过视觉类 AI 算法，传统的鉴黄、鉴恐类工作可以由机器自动实现。同时，NLP 类 AI 技术帮助各类论坛及政府网站实现文本审查的去人工化，通过语言处理类 AI 算法，各类不当言论将能够自动被机器识别，并间接起到舆情分析的作用。目前，百度、腾讯、阿里等云服务商，爱奇艺、优酷等视频厂商均在该领域进行巨大投入。安全厂商 360 旗下“快资讯”也于近日成立“信息流智能监控平台”。“信息流智能监控平台”将率先发布互联网内容安全认证体系，该项目一期内容安全生态产品将在快资讯首先落地，由人民网提供权威新闻基础数据，被认证的新闻将通过技术手段和人工手段在快资讯获得突出展示。

3. 上网行为管理产品

3.1. 上网行为管理产品定义及市场空间

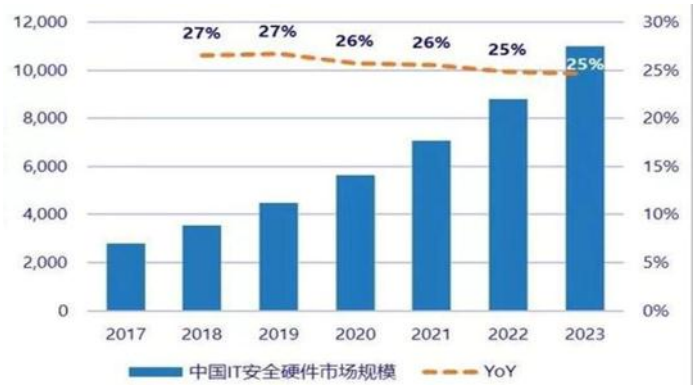
上网行为管理产品包括针对外网的管理和对内网的管理，针对外网的管理能够防御网络黑客和病毒入侵计算机，并进行破坏；针对内网的管理则更加关注用户在上网时的行为规范。为了保证局域网络内部的网络信息在用户进行上传与下载操作时相关信息的完整性、安全性等，需要通过特定的上网行为管理技术来对其所使用的网络环境进行全方位的监督与管理。如果企业在通过互联网开展工作经营时缺乏有效的管理，网络的开放性将会给业务带来各种风险，主要包括员工上网缺乏管控工作效率低下、私接无线设备使得敏感信息外泄、公司面临法律风险、带宽滥用等。上网行为管理产品基于上网行为和内容审计可为企业园区客户提供丰富的内网策略管理、行为策略管理和流量策略管理等功能。

图 9：上网行为管理需求分析

数据来源：深信服，安信证券研究中心

上网行为管理市场持续增长，深信服领跑。得益于网络安全法的落地、云计算对于 IT 基础设施的重构，以及物联网设备的迅速增长，上网行为管理领域正在迎来全新的发展阶段，2011-2015 年内容安全管理市场规模年均增速为 25.1%。2016 年我国内容安全管理市场规模约为 12.15 亿元。IDC《2019 年第二季度中国 IT 安全硬件市场跟踪报告》显示，2019 年上半年半年度 IT 安全硬件市场整体收入为 10.97 亿美元（约合 74.8 亿元人民币），较 2018 年上半年同比增长 9.48%。根据 IDC 预测，2019 年中国 IT 安全硬件市场规模将达到 44.72 亿美元；到 2023 年将达到 109.9 亿美元，未来 5 年整体市场年均复合增长率为 25.5%。在关键厂商表现上，深信服产品的市场占有率达到 25.3%，奇安信和新华三分别占据 12.8%和 6.3%的份额。

图 10：中国 IT 安全硬件市场规模预测



数据来源：IDC 中国，安信证券研究中心

图 11：2019H1 安全内容管理硬件市场关键厂商表现

数据来源：IDC 中国，安信证券研究中心

3.2. 产品主要形式——网络安全审计与风险管理平台

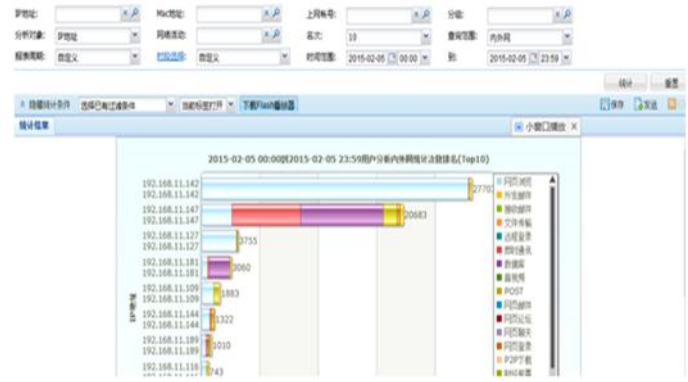
3.2.1. 平台产品介绍

通过对上网行为管理设备的数据汇聚、存储和分析，上网行为管理平台能够可视化展示用户关心的业务专题分析模型。面向校园、企事业单位等需实施内容审计与行为监控、行为管理的应用场景，上网行为管理平台帮助用户控制和管理对互联网的使用。

高质量数据管理分析平台，有效提高企业效率。通过网页访问过滤和信息收发审计，产品实现上网行为管理和合规细粒度审计，在加强上网机构内外部网络信息控制监管的同时，为避免相关信息外泄及事后的追溯取证提供了有效的技术支撑。借助网络应用控制、带宽流量管理和用户行为，产品能够详实记录网络内的各种网络活动，对网络用户的行为进行多种方式

的分组策略控制与审计，实现基于用户的细化和量化的审计与管理，过滤各类不良访问行为；产品还能实现定制化专题分析功能，经过对日志进行深度挖掘，形成丰富多样化的统计报表。产品在简单、持续、低成本地挖掘业务价值的同时，提供各类高价值的业务报表模板，为用户简化运维管理、感知网络行为风险，主动有效的保护了用户关注的信息，使管理者能更有针对性地加强网络管理，为其规范网络管理、制定正确的管理决策提供有效依据，使用户能够安全、高效、合规地利用网络，最终带来生产力的提升。

图 12：平台识别上网应用



数据来源：任子行，安信证券研究中心

图 13：平台针对信息泄密进行追踪分析

数据来源：深信服，安信证券研究中心

规范上网行为，实时保障网络安全态势。上网行为管理产品针对性地制定对上网行为、流量的控制策略，实现高效规范的内部网络行为管控;产品主要融合多源、异构、海量安全数据，具备快速、高性能、关联分析和深度挖掘能力以及丰富的数据展示能力，从网络宏观整体安全态势细分至网站安全、移动安全、移动资讯舆情等各个方面，满足全方位的态势感知与监管需求；可向客户提供下一代防火墙、入侵检测、入侵防御、防病毒、上网行为管理、态势感知、负载均衡、网络审计等产品，保障客户的网络高效、顺畅、安全、稳定运行。

图 14：上网行为管理需求分析

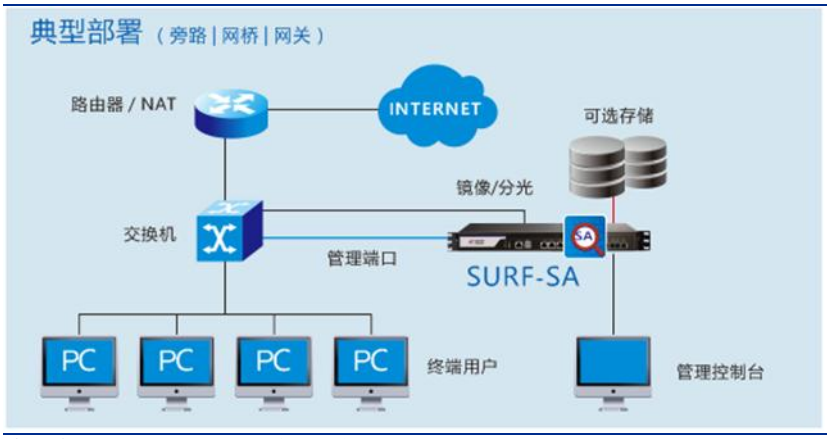
数据来源：深信服，安信证券研究中心

3.2.2. 平台技术支持

上网行为管理产品通常由管理设备和管理系统平台组成。基于硬件的高性能、高稳定性的上网行为管理和内容安全审计设备，可以根据实际情况选择以旁路监听或者透明网桥的方式工作，提供单机、分布式及其他多种部署方式。在设计上采用了先进的模块化、层次化体系结构，集成了高性能数据捕获驱动、嵌入式审计引擎 GRAM、快速的并行协议分析引擎、实时内容分析引擎，可以在基于状态的并行内容匹配、海量数据全文检索和数据挖掘等场景表现出卓越性能，集成管理、审计和认证功能，通过业务耦合和分布式数据处理技术，落实网络

安全审计监管需求，运行稳定、可靠。

图 15：上网管理平台典型部署



数据来源：任子行，安信证券研究中心

4. 开源情报分析产品

4.1. 基于网络空间舆情治理的开源解决方案

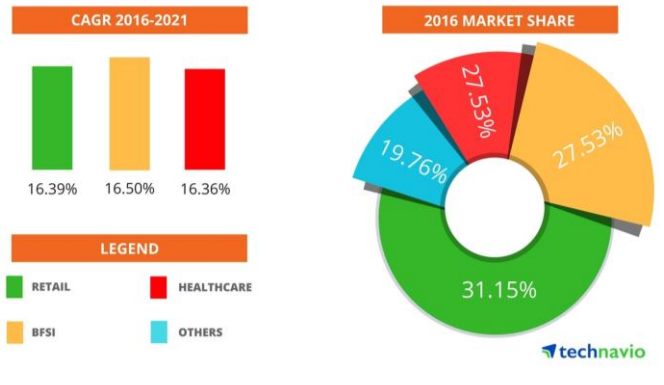
情报分析主要针对网络空间进行舆论分析，而开源主要是指能够提供自主研发的解决方案，并且这样的方案能够建立起生态圈，让开发者能够根据自己企业的情形对技术进行自主可控的转变。因此，开源情报分析的定位主要是基于网络空间安全大课题下所自主研发出的开源治理方案。

舆情分析市场空间巨大，应用场景多样化。舆情分析作为互联网时代民意调查的主要方式，是公共安全维护的重要工具，也是企业发展方向的重要参考。根据 technavio 测算，2017 年全球舆情分析市场增量空间达到 11 亿美元，预计复合增速超过 60%。同时，从市场结构来看，舆情分析的市场构成表现多样化，在零售、金融、医疗等行业均存在相应需求。

图 16：全球范围舆情分析市场空间及增速测算

数据来源：technavio，安信证券研究中心

图 17：舆情分析市场构成分析



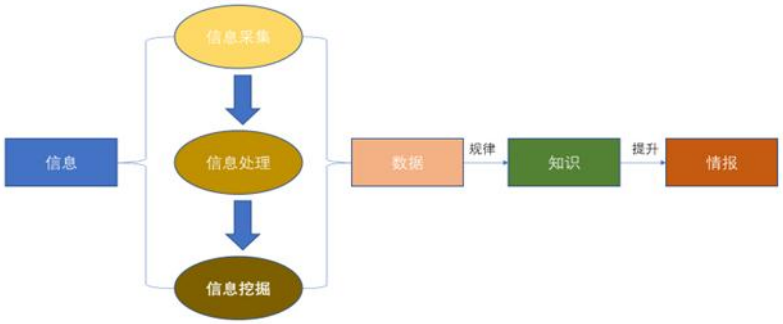
数据来源：technavio，安信证券研究中心

开源+自主研发是破解网络空间安全舆情治理命题的重要方法。如果把网络安全治理比喻成一个命题，那么破解这个命题的关键就是要能够开源，也即能够自主研发相关技术并形成生态圈，用“硬核”技术来对网络空间进行监控，判断，甚至自主判断，辅助我们进行实时、准确、有效地治理。当今世界，网络舆情可谓时时处处在发生变化，假设这样瞬息万变的舆情治理是基于“别人”的技术，基于能被“卡脖子”的技术，那么一旦技术源被切断，不仅网络空间安全公司的业务将受到影响，而购买网络安全空间治理解决方案的公司、政府部门

的命脉都会被别人拿在手里，显然这是不合理的，也非长久之计，要破此局，就必须要有真正自主研发的技术，这样的技术，不仅能给自己的公司提供安全壁垒，也能够帮助到政府部门，企业构建起自己的情报分析能力，提升相关部门的网络空间治理体系和治理能力。

4.2. 提供网络内容安全解决方案的步骤

图 18：网络内容安全解决方案的步骤



数据来源：安信证券研究中心整理

从信息到情报的跨越，绝非易事。在网络空间中，我们所接触到的初始内容可以认为是信息，我们利用各种手段对信息进行采集，在采集的过程中会遇到各种各样的问题，哪些信息是我们所需要的，哪些信息是无效的，在纷繁复杂的网络信息中，必须具备甄别能力，这就是“信息处理”，然而信息处理仍然是比较浅层次的阶段，必须在甄别的基础上，进行挖掘，只有被挖掘出来的信息才能称之为“数据”，挖掘数据的手段可以是基于大数据+AI 的组合。继而在数据中总结规律，获得知识，而知识同时具备重复性和创新性的特征，运用其重复性去熟练解决已知领域的问题，运用其创新性，以解决未来可能会碰到的新问题。最后，在知识的基础上，将知识进行提炼，就可以获得情报，所获得的情报，具有高效性，准确性，动态实时性，启发性等特征，是大家争先恐后想要获取的“至宝”。基于此，开源情报分析产品对于网络空间的舆情治理能力提升以及对于政府部门进行网络空间内容分析的保障具有重要意义。

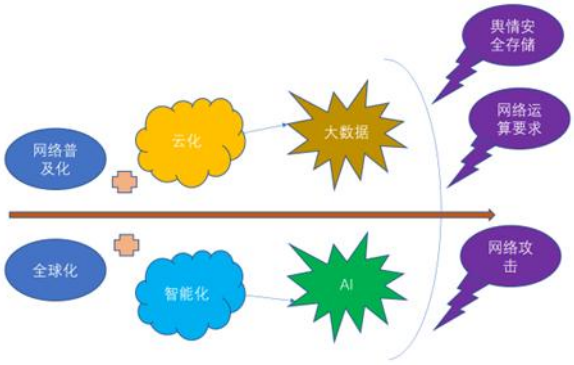
华为 SDSec 网络安全产品具有启发性意义。以华为 SDSec 网络安全产品为例，对于初始接触到的信息，进行信息采集，处理，甚至挖掘，在挖掘的过程中，我们可以清楚地看到，运用了 network devices(神经网络以及机器学习等技术)动态数据挖掘和处理手段，这与传统意义上的网络安全解决方案具有本质区别。挖掘信息之后，即得到数据，进而提炼为知识和情报，这样的流程是动态的，主动的。要获取这样高效、流畅、动态的解决方案，就必须具备自主研发的技术，只有这样的网络内容安全产品才具有足够的竞争力。华为以动态相应的思维构建了产品规划与开发的全视图，即网络安全框架，以应对更为复杂的网络安全环境。

4.3. 开源情报分析产品的发展趋势

大数据+AI 赋能开源情报分析产品。在网络普及化和全球化的过程中，交织着云化，智能化等过程，这就要求，产品具备大数据处理以及人工智能等核心要件，大数据技术保证了纷繁复杂的网络空间内容具备可处理，可分析的特质，并且这样的技术是非常高效的，网络舆情时时处处在变化，在极短的时间内，会产生大量的数据，这些亟待处理的数据，还没有上升为情报，放在终端不妥，于是，云平台、数据中心应运而生；在此基础之上，如果需要高效动态地去挖掘数据，归纳数据，提炼数据，使之成为情报，就会运用人工智能 AI 技术，例

如神经网络等基于非线性函数的处理方法，被越来越多地运用于网络舆情治理领域。大数据使得当代情报分析成为可能，而 AI 则如火箭一般起到加速推动的作用，极大地提升了产品本身的动态分析能力，其自适应学习能力将助力人们深入研究互联网信息网络机制，持续积累舆情治理业务经验。

图 19：大数据+AI 赋能开源情报分析产品



数据来源：安信证券研究中心整理

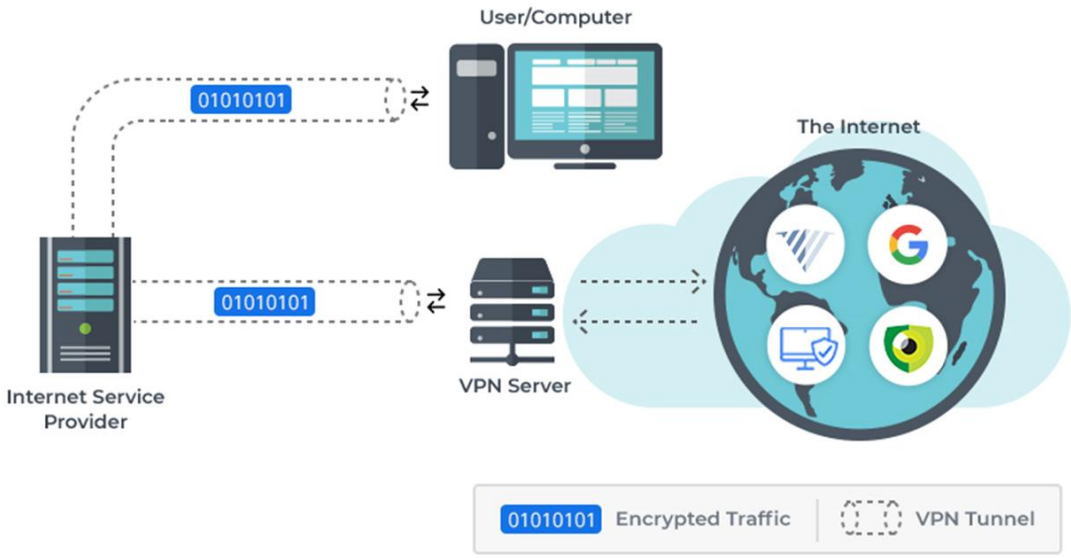
基于国家战略与发展机遇的开源情报分析解决方案。前文列举了国家出台的各项关于网络安全的政策，包括《网络安全法》、《网络安全审查办法（征求意见稿）》《个人信息和重要数据出境安全评估办法（征求意见稿）》等相关法律法规，与此同时，国家在积极与其他国家一起实践“一带一路”，在这样的法律加政治双驱动背景下，网络安全尤为重要，而网络舆情治理中所产生的情报更是重中之重。大势所趋，网络安全企业采取项目部署和产品化服务的经营模式，也是必然的，这也在客观上要求相关企业为海内外多个地区的用户提供舆情治理的解决方案。

5. VPN 服务产品

5.1. VPN 基本定义及应用场景

VPN（Virtual Private Network）即虚拟私人网络，是一种常用于连接中、大型企业或团体与团体间的私人网络的通讯方法。相比于传统的网络连接，VPN 利用隧道协议来达到保密、发送端认证、消息准确性等私人消息安全效果。VPN 最大的特点是可以用不安全的公共网络来发送可靠、安全的消息。

图 20：VPN 基本原理示意



数据来源：securityboulevard，安信证券研究中心

传统 VPN 的特点是点对点拓扑，它们不支持或连接广播域，因此 Microsoft Windows NetBIOS 等服务可能无法完全支持或像在局域网（LAN）上那样工作。设计人员已经开发出 VPN 变体，例如虚拟专用 LAN 服务（VPLS）和第 2 层隧道协议（L2TP），以克服此限制。同时，为保证 VPN 传输更强的安全性，也存在基于 IPsec、SSL 等搭建的 VPN 网络。常见的 VPN 协议包括 L2F、L2TP、PPTP、IPsec、SSL、AnyConnect 等。

表 2：主流 VPN 协议梳理

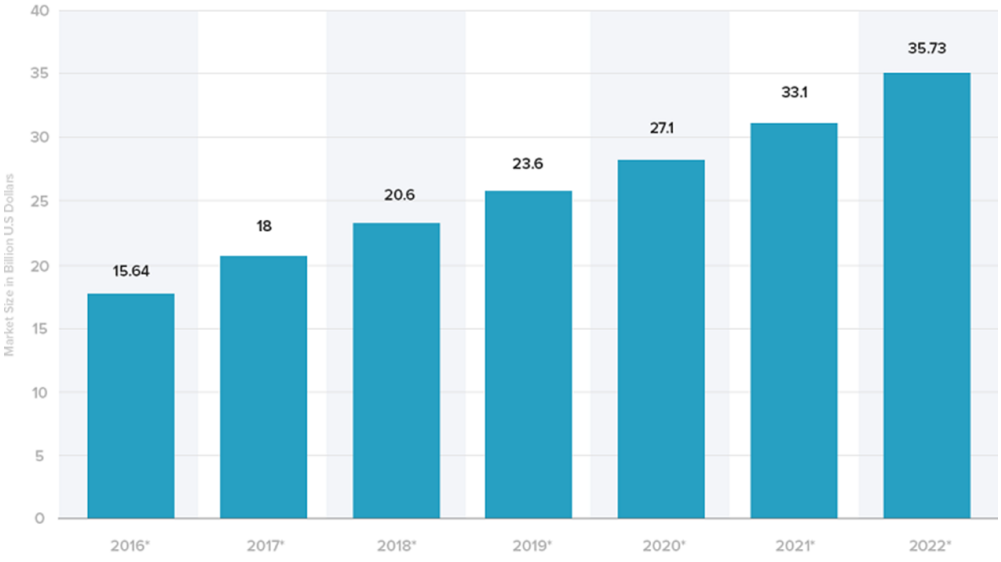
协议名称	主要特点
L2F	由思科系统公司开发的，L2F 协议本身并不提供加密或保密，而是依赖于协议被传输以提供保密。L2F 是专为隧道点对点协议（PPP）通信。
L2TP	L2TP 协议自身不提供加密与可靠性验证的功能，可以和安全协议搭配使用，从而实现数据的加密传输，常与 IPsec 搭配
PPTP	最早由微软等厂商主导开发，PPTP 使用传输控制协议（TCP）创建控制通道来发送控制命令，但因为它的加密方式容易被破解，微软已经不再建议使用这个协议。
IPsec	IPsec 是一个协议包，透过对 IP 协议的分组进行加密和认证来保护 IP 协议的网络传输协议族
SSL	SSL 协议主要由 SSL 握手协议和 SSL 记录协议组成，它们共同为应用访问连接提供认证、加密和防篡改功能。SSLVPN 是解决远程用户访问公司敏感数据最简单最安全的解决技术。
AnyConnect	AnyConnect 由思科系统公司开发，主要作用是方便员工在任何设备上安全地办公

数据来源：思科等，安信证券研究中心整理

5.2. VPN 服务市场空间

全球 VPN 服务市场增长迅猛，企业需求旺盛。在各大跨国企业全球办公的大背景下，VPN 作为大型公司全球各部门交流的重要工具，存在旺盛的市场需求。根据 Orbis Research Statista 两家公司的测算，全球 VPN 服务市场在 2016 年就达到了 156.4 亿美元，在 2022 年有望达到 357.3 亿美元，年复合增长率将达到 14.76%。各大 VPN 服务提供商的竞争也将日趋激烈。

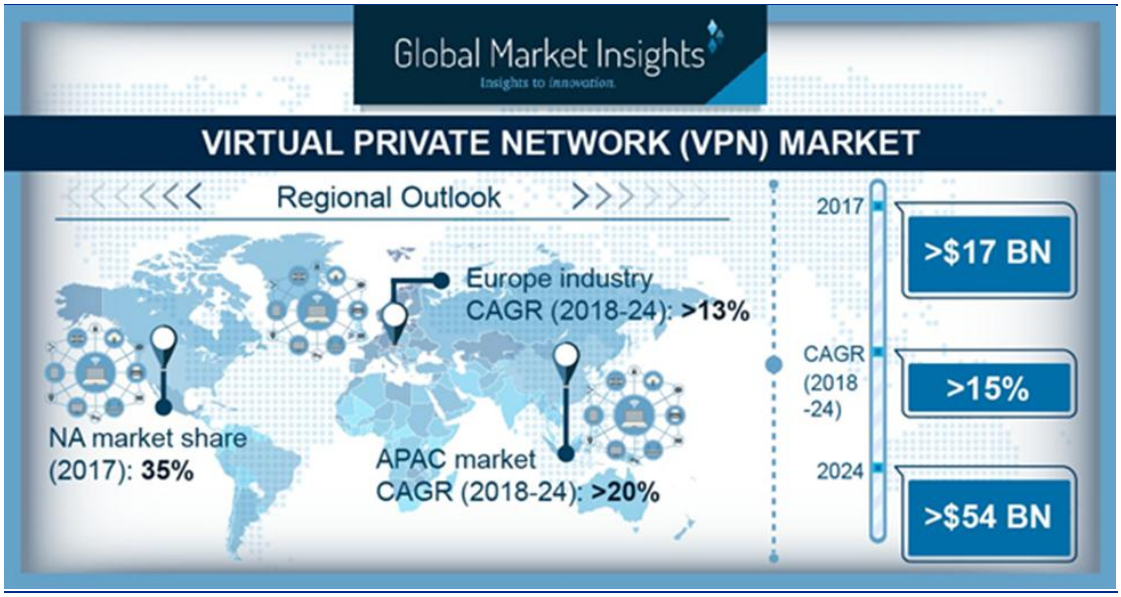
图 21：2016-2022 全球 VPN 服务市场规模测算（单位：十亿美元）



数据来源：Orbis Research Statista，安信证券研究中心

亚太地区 VPN 服务市场充满活力，发展潜力巨大。从地域上看，VPN 市场的分布及增长速度存在地域差异。根据 Global Market Insights 测算，北美地区的 VPN 市场达 35%，超过全球市场的 1/3。从 VPN 市场增长速度上看，亚太地区表现得较为强劲，2018 年复合增速超过 20%，远高于欧洲地区的 13%，同时也高于全球平均的约 15%。这一表现可以部分归因于由亚太地区经济高速增长所带来的各类跨国业务所产生的需求，中国作为亚太地区的经济增长引擎，将存在更为旺盛的 VPN 服务需求。

图 22：2018 年全球 VPN 服务市场占比及增速分地区测算



数据来源：Global Market Insights，安信证券研究中心

5.3. 我国 VPN 服务产品发展情况

安全厂商加码 VPN 业务，产品多样化。VPN 业务作为网络安全领域的延伸之一，受到了安全厂商的广泛重视。例如，深信服推出了 VPN(SJW78)系列产品，为政府单位量身打造，助力政府单位实现异地网络安全互连、保证资源共享，提升行政办公业务平台的扩展性，实现

随时随地移动办公与第三方接入。除此之外，任子行和山石网科等尝试将 VPN 服务植入自己已有的产品中。任子行的网络安全管理系统 RAG 产品为用户提供基于 IPsec VPN 和 PPTP VPN、L2TP VPN 多种方式的免费 VPN 服务，山石网科在自身下一代防火墙产品中内置 VPN 加速芯片，可显著提升 IPSec/SSL VPN 性能，支持大规模网络环境中 VPN 部署。

图 23：任子行的网络安全管理系统 RAG

数据来源：F2M 溯源新采购，安信证券研究中心

图 24：山石网科下一代防火墙

数据来源：系统集成网，安信证券研究中心

与云服务厂商紧密协同，共同打造高质量安全 VPN 服务。云服务厂商作为 VPN 通信实现的重要载体，是 VPN 业务推广的门户之一。安全厂商的安全类 VPN 硬件产品搭载于国产云服务厂商，可以在完成国产自主化的同时实现高度安全性。目前，华为云已与深信服、山石网科展开合作，推出了绑定指定厂商 VPN 服务的云服务产品，分别售价为 4000 元/月和 2500 元/月。随着华为生态伙伴计划的持续推进、国内 BAT 等其他云服务厂商的业务拓展，云上安全 VPN 业务存在巨大的市场空间。

图 25：华为云与山石网科、深信服等在安全 VPN 领域共同打造产品

数据来源：华为云，安信证券研究中心

6. 投资建议

近年来，随着中国越来越重视网络安全，《网络安全法》《网络安全审查办法（征求意见稿）》《个人信息和重要数据出境安全评估办法（征求意见稿）》等一系列法律和政策文件陆续出台或公开征求意见，对网络安全审查和数据离境审核等进行了规定，网络安全审查市场迎来黄金发展机遇，我们看好任子行、顺网科技、三六零、中新赛克、深信服、绿盟科技、启明

星辰、拓尔思等在网络安全审查领域进行长期布局并拥有显著技术优势的领军企业。

表 3：网安审查相关上市公司及业务布局

上市公司	网安审查相关业务布局
任子行	国内领先的“网络空间数据治理专家”，旗下拥有警务大数据、网络审计、舆情治理、移动应用监管等一系列网络空间信息治理的产品族
顺网科技	公司持续布局网络安全领域，此前以 3.7 亿元的对价收购国内网安安全提供商国瑞信安，并将原顺网本级和子公司国瑞信安的安全业务进行全面整合，成立安全事业部，继续发力网络安全领域。同时，公司与腾讯游戏杭州联合宣布达成网吧游戏安全领域的战略合作，并共同成立网吧安全技术联合实验室。
三六零	公司旗下“快资讯”新成立“信息流智能监控平台”，联合人民网等新闻媒体及各行业专家学者共建互联网内容安全生态联盟。通过“媒体内容力、智慧化平台能力、行业专业力”三方融合，升维互联网内容安全性，遴选优质、真实、值得信赖的信息
启明星辰	网络安全一线厂商，上网行为管理、网络审计、VPN 等产品在 IDC 的分类排名中位居前列
绿盟科技	拥有针对内容、行为和流量的安全审计产品，以及上网行为管理等产品
中新赛克	网络内容安全领导厂商，拥有整合时空信息，社会管理等数据资源，构建业务流程可视化、数据全方位立体分析的网络内容安全大数据分析平台
南洋股份	子公司天融信的网络审计、上网行为管理、VPN 等产品的市场排名靠前
深信服	上网行为管理、VPN 等产品领跑企业级市场，得到广泛应用
东方通	子公司微智信业在互联网不良信息监控、互联网反诈骗、违规恶意链接监测等领域的市场排名靠前
拓尔思	网络舆情监测分析领导厂商
卫士通	旗下拥有 VPN 系列产品，应用于央企和中央部委客户

数据来源：公司官网、IDC、安全牛、数说安全、安信证券研究中心

7. 风险提示

网络安全审查行业发展进度不及预期；政策推进力度不及预期。

■ 行业评级体系

收益评级:

领先大市 — 未来 6 个月的投资收益率领先沪深 300 指数 10%以上;

同步大市 — 未来 6 个月的投资收益率与沪深 300 指数的变动幅度相差-10%至 10%;

落后大市 — 未来 6 个月的投资收益率落后沪深 300 指数 10%以上;

风险评级:

A — 正常风险，未来 6 个月投资收益率的波动小于等于沪深 300 指数波动;

B — 较高风险，未来 6 个月投资收益率的波动大于沪深 300 指数波动;

■ 分析师声明

胡又文声明，本人具有中国证券业协会授予的证券投资咨询执业资格，勤勉尽责、诚实守信。本人对本报告的内容和观点负责，保证信息来源合法合规、研究方法专业审慎、研究观点独立公正、分析结论具有合理依据，特此声明。

■ 本公司具备证券投资咨询业务资格的说明

安信证券股份有限公司（以下简称“本公司”）经中国证券监督管理委员会核准，取得证券投资咨询业务许可。本公司及其投资咨询人员可以为证券投资人或客户提供证券投资分析、预测或者建议等直接或间接的有偿咨询服务。发布证券研究报告，是证券投资咨询业务的一种基本形式，本公司可以对证券及证券相关产品的价值、市场走势或者相关影响因素进行分析，形成证券估值、投资评级等投资分析意见，制作证券研究报告，并向本公司的客户发布。

■ 免责声明

■ 销售联系人

上海联系人	朱贤	021-35082852	zhuxian@essence.com.cn
	李栋	021-35082821	lidong1@essence.com.cn
	侯海霞	021-35082870	houhx@essence.com.cn
	潘艳	021-35082957	panyan@essence.com.cn
	刘恭懿	021-35082961	liugy@essence.com.cn
	孟昊琳	021-35082963	menghl@essence.com.cn
	苏梦	021-35082790	sumeng@essence.com.cn
	孙红	18221132911	sunhong1@essence.com.cn
	秦紫涵	021-35082799	qinzh1@essence.com.cn
	王银银	021-35082985	wangyy4@essence.com.cn
	陈盈怡	021-35082737	chenyy6@essence.com.cn
北京联系人	温鹏	010-83321350	wenpeng@essence.com.cn
	姜东亚	010-83321351	jiangdy@essence.com.cn
	张莹	010-83321366	zhangying1@essence.com.cn
	李倩	010-83321355	liqian1@essence.com.cn
	姜雪	010-59113596	jiangxue1@essence.com.cn
	王帅	010-83321351	wangshuai1@essence.com.cn
	曹琰	15810388900	caoyan1@essence.com.cn
	夏坤	15210845461	xiakun@essence.com.cn
	袁进	010-83321345	yuanjin@essence.com.cn
深圳联系人	胡珍	0755-82528441	huzhen@essence.com.cn
	范洪群	0755-23991945	fanhq@essence.com.cn
	聂欣	0755-23919631	niexin1@essence.com.cn
	杨萍	13723434033	yangping1@essence.com.cn
	巢莫雯	0755-23947871	chaomw@essence.com.cn
	黄秋琪	0755-23987069	huangqq@essence.com.cn
	王红彦	0755-82714067	wanghy8@essence.com.cn
	黎欢	0755-23984253	lihuan@essence.com.cn

安信证券研究中心

深圳市

地　址： 深圳市福田区深南大道 2008 号中国凤凰大厦 1 栋 7 层

邮　编： 518026

上海市

地　址： 上海市虹口区东大名路638号国投大厦3层

邮　编： 200080

北京市

地　址： 北京市西城区阜成门北大街 2 号楼国投金融大厦 15 层

邮　编： 100034