卫士通（002268）

密码央企龙头，重视基本面的边际变化

买入（维持）

2021 年 02 月 10 日

盈利预测与估值	2019A	2020E	2021E	2022E
营业收入（百万元）	2,104	2,410	3,165	4,162
同比（%）	8.95%	14.55%	31.33%	31.51%
归母净利润（百万元）	156	181	214	252
同比（%）	29.58%	15.93%	18.67%	17.68%
每股收益（元/股）	0.19	0.21	0.25	0.30
P/E（倍）	83	74	63	53

投资要点

- **网络安全成为电科集团四大聚焦板块之一，卫士通有望成为资源整合平台：**随着网络安全上升为国家战略，中国电科根据国家总体安全战略需要，重点打造了网络安全子集团中国网安。中国电科 2021 年度工作会议中集团董事长提出十四五聚焦电子装备、网信体系、产业基础、网络安全四大板块做强做优做大。卫士通作为中国网安旗下唯一上市公司，此前已收购了三十所旗下的三零嘉微、三零瑞通和三零盛安，为公司未来的战略整合指明发展道路。在电科集团资产证券化比例提升和重点打造网安板块的规划下，预计卫士通有望成为集团在网安领域的资源整合平台，不断扩充和完善全产业链。

- **股权激励有望激发活力，迈向发展新篇章：**公司拟以 11.42 元/股的价格向高管、核心技术人员和骨干员工合计 300 人授予 781 万股股票。对内通过长效激励机制，绑定公司核心管理和技术团队；对外释放积极信号，重塑公司在产业和资本市场的形象。通过完善中国特色现代企业制度，形成科学有效的公司治理机制，在新机制下的持续管理改善值得期待。

- **政策、新兴技术等多点需求共振，行业将迎来国产化和泛在化的机遇：**随着等保 2.0、《密码法》的正式实施，密码刚性合规需求有望爆发。短期看，密码法将在合规需求较强的党政和关键信息基础设施行业率先展开应用，加密行业迎来国产化机遇；长期来看，随着云计算、大数据、物联网等新兴领域快速发展，新技术、新模式（主动防御）、新架构（零信任）等都将推动密码泛在化应用的增长。

- **以“新四化”战略为目标，有望从密码核心企业走向综合型安全产品与服务厂商。**随着中国网安提出网络安全“新四化”战略——密码泛在化、基础国产化、攻防智能化、安全服务化，作为中国网安负责信息安全的主体单位，在子集团层面承担着更多发展网络空间安全业务的责任。公司全面加快向安全服务转型，践行“新四化”的发展思路，大力发展信创安全、云计算与数据安全、网络安全服务业务，产品从密码领域扩大到泛网安领域，业务覆盖由政务向行业拓展，有望实现业务的横纵向拓展，转型为综合型安全产品与服务厂商。根据我们测算，卫士通重点产品加密机的总市场规模为百亿量级（5 年平均替换周期，对应每年 20 亿元），而 IDC 测算，仅 2021 年网络安全市场规模就接近 80 亿美元（500 亿量级），2021-2024 年网络安全行业增速均在 20%以上，2024 市场规模将达到 179 亿美元（千亿量级），公司从加密进入泛网安领域，有望打开更大的增长空间。

- **盈利预测与投资评级：**预计 2020-2022 年 EPS 分别为 0.21、0.25、0.30 元，对应 PE 分别 74/63/53 倍，作为国内安全领域的国家队，随着中国电科对网络安全的战略地位的重视和激励机制到位，有望实现从密码龙头向综合型网络安全产品商的升级转型，维持“买入”评级。

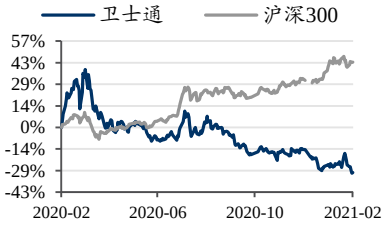
- **风险提示：**行业竞争加剧造成产品毛利率下降，应收账款持续增长等。

证券分析师 郝彪
执业证号：S0600516030001
021-60199781
haob@dwzq.com.cn

证券分析师 刘博
执业证号：S0600518070002
18811311450
liub@dwzq.com.cn

研究助理 王紫敬
021-60199781
wangzj@dwzq.com.cn

股价走势



市场数据

收盘价(元)	15.85
一年最低/最高价	15.50/31.27
市净率(倍)	3.01
流通 A 股市值(百万元)	13220.27

基础数据

每股净资产(元)	5.30
资产负债率(%)	22.01
总股本(百万股)	846.29
流通 A 股(百万股)	836.73

相关研究

1、《卫士通（002268）：营收逐季加速，密码龙头有望持续受益密码合规大时代》2020-10-28

内容目录

图表目录

1. 中国网安上市整合平台，激励机制理顺进入发展新篇章

网络安全国家队，密码产业主力军。公司成立于 1998 年，国内知名密码产品、网络安全产品、安全运维服务和行业安全解决方案综合提供商，国内最早专业从事网络信息安全的上市企业，首批商密产品研发、生产、销售资质单位，是中国电子科技集团有限公司（中国电科，CETC）旗下中国电子科技网络信息安全有限公司（中国网安，CCSC）的控股子公司，也是中国电科、中国网安在网络信息安全领域的唯一上市平台。公司始终专注于网络信息安全领域，持续为党政、军队、大型央企等客户提供专业的网络信息安全产品和服务，经过 20 余年的发展，构建了覆盖芯片、模块、平台、整机、系统、整体解决方案与安全服务的产品体系，业务横跨网络安全、主机安全、数据安全、应用安全等多个场景，并在移动互联网安全、5G、云安全、物联网安全、安全整体保障等领域进行了大量探索和创新，累计服务用户超过 10000 家，在北京奥运会、上海世博会、杭州 G20 峰会、9.3 阅兵等多个国家重大活动信息安全保障工作中发挥了重要作用。

图 1：公司主要产品

密码产品
- 金融数据密码机
- 服务器密码机
- 数字证书认证系统
- 移动终端密码软卡
- 密钥管理系统
- 商用PCI-E密码卡
- 签名验证服务器

网络安全
- 电力系统专用纵向加密认证装置
- 中华卫士网络防火墙
- 中华卫士安全隔离交换系统
- SSL VPN安全网关
- IPSec VPN安全网关

数据安全
- 网安凌云大数据脱敏平台
- 电子文件密级标志管理系统

终端安全
- 主机监控与审计系统
- 终端安全登录系统

安全应用
- 电子文档安全管理系统
- 橙讯安全即时通讯平台
- 电子公文安全交换系统

安全管理
- 安全运行监管系统

身份认证与访问安全
- 电子签章系统
- 资源信息管理服务系统
- 授权管理服务系统
- 安全应用中间件
- 身份认证应用服务系统

移动安全
- 安全保密电子记事本
- 安全无纸化会议系统
- 政务安全手机

工控安全

行业应用
- 青少年违法犯罪分析平台
- 青少年帮扶教育平台
- 涉案财物集中管理信息平台
- 检察机关大数据智能分析系统

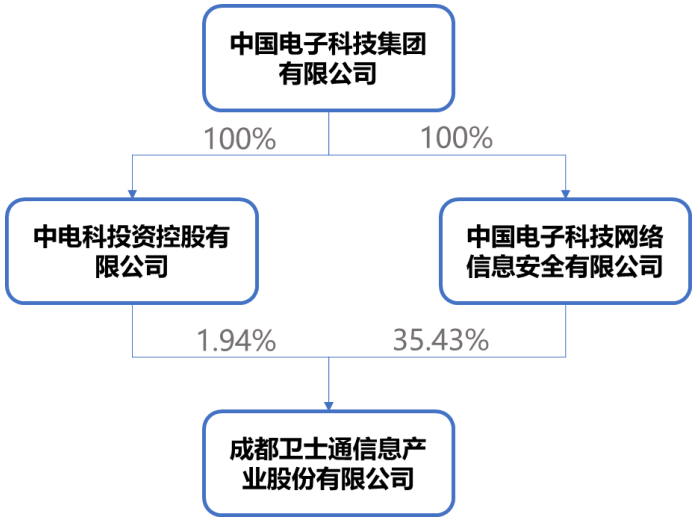
云安全
- 云密码资源池管理平台
- 网安凌云安全云监管平台
- 云服务器密码机

数据来源：公司官网，东吴证券研究所

1.1. 中国电科相继组建多个子集团，专业化整合是大势所趋

中国网安为公司控股股东，中国电科为公司实际控制人。中国网安直接持有公司 35.43%的股份，为公司的控股股东。而中国电科 100%控股中国网安，并通过全资子公司中电投资持有公司 1.94%的股份，合计持有公司 37.37%股份，为公司实际控制人。

图 2：公司股权结构（截止 2020 年 9 月 30 日）

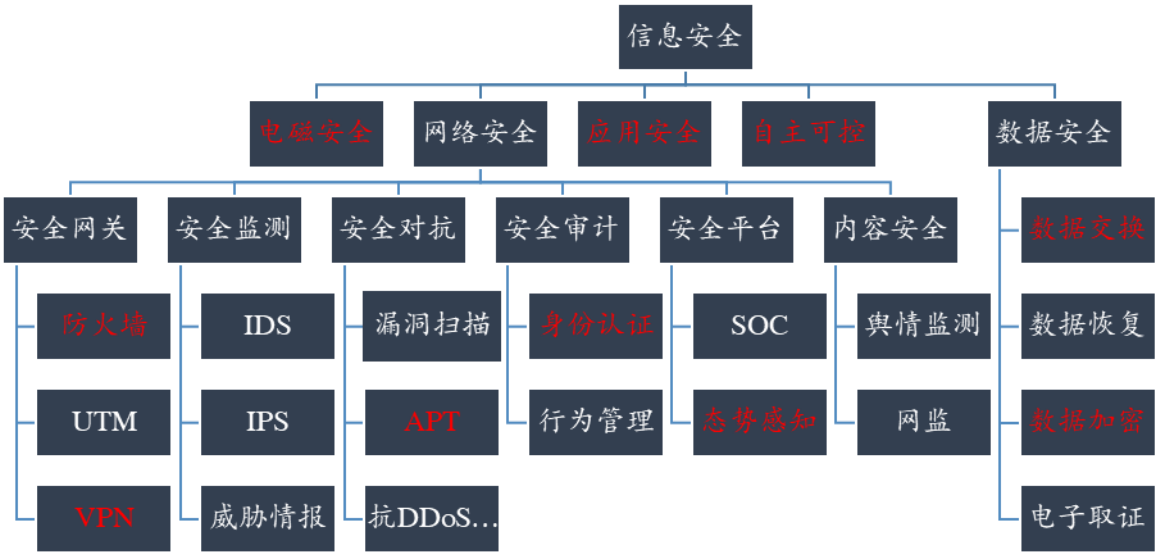


数据来源：Wind，东吴证券研究所

中国电科加快业务架构整合。2015 年 2 月，中国电科以现代企业制度为基本模式，设立董事会，开始向规范的现代企业转型。中国电科建立了母子公司、“母分公司”管控模式。基本形成以母子公司、“母分公司”体制为基本模式的“三层架构、两级经营”主营业务组织体系。“三层架构”主要是集团、子集团、科研院所/子公司的三级架构，“两级经营”主要是集团把管理权下放给各个子集团，实现子集团的自主管理。中国电科加速整合组建子集团、启动首批科研院所转制、完成公司制改制，推进混合所有制改革试点、启动发展战略委员会建设，通过内部整合打造了几大子集团和专业公司。

网络安全上升为国家战略，中电科组建网络安全产业子集团。公司控股股东中国网安是中国电科根据国家总体安全战略需要，以中国电科三十所、三十三所为核心，汇聚内部资源重点打造的网络安全子集团。2015 年 5 月，经国务院批准，中国网安在成都正式注册成立，**是目前国内专业从事网络安全业务经营规模最大、专业面最广、从业人数最多的企业**，深耕信息安全和物理安全，服务对象遍及党政、军队以及金融、能源、交通、电子信息等关乎国计民生的重要行业。中国网安凭借在密码保密、网络通信、信息安全及电磁防御领域的深厚积淀，拥有国内完备的网络安全资质，能力较强的网络安全研发团队以及运行有效的质量保证体系，在国家网络空间安全核心和重要领域处于国内领先地位。

图 3：信息安全产业的产品结构和中国网安的布局情况（红色）

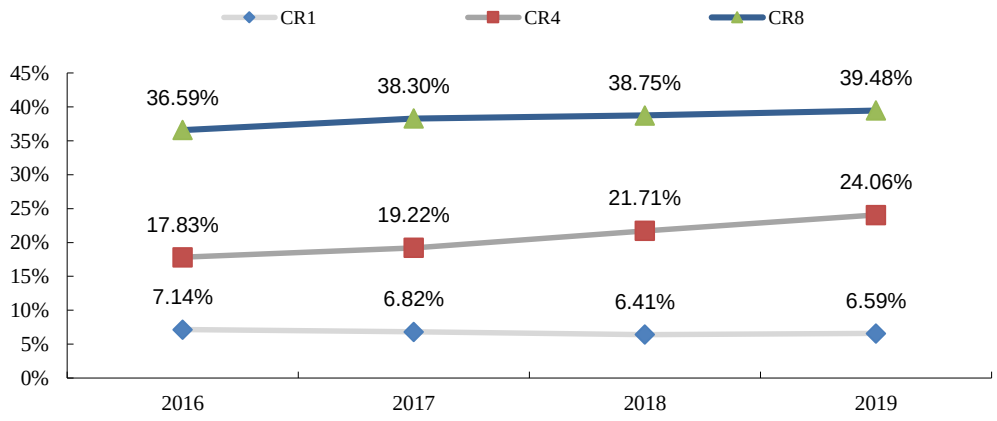


数据来源：中国网安官网，东吴证券研究所

1.2. 中国网安的整合窗口，平台价值凸显

行业龙头集中趋势明显，但竞争格局仍然分散。网络安全细分领域多，行业竞争格局分散，目前单一厂商的市场份额不超过 10%，但根据中国网络安全产业联盟的统计数据，2016-2019 年，国内网安行业 CR4 和 CR8 企业的市占率不断提升，产业正逐步往行业头部集中。目前行业内领先企业无论是技术创新力度还是产品研发能力不断提升，市场正不断的向这些具有丰富产品线和规模化服务能力的厂商汇聚，同时行业由单一产品采购逐步变为综合方案需求和安全运营能力输出，龙头公司优势将不断强化，正向反馈也带动这些厂商的竞争力越来越强，因此我们预计未来市场集中度提升的趋势仍将继续。

图 4：行业集中度持续提升，但仍然较分散



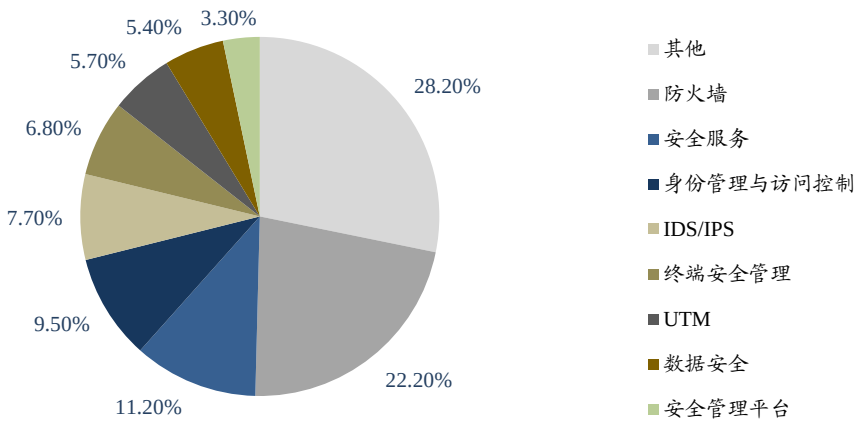
数据来源：中国网络安全产业联盟，东吴证券研究所

网络安全产业产品数量较多，并购仍是行业扩张整合主旋律。截至 2020 年 3 月安全牛统计显示，中国网络安全产业共有 16 类以及安全领域、200 类二级细分领域。网安公司往往从某一特定产品起家，各家都有自己的优势壁垒，横向拓展相对较难，此外，行业细分领域和产品数量丰富。因此，并购是行业较为主流的扩张整合方式。据 Momentum Cyber 统计，2019 年全球共完成了 188 起并购活动，较 2018 年小幅提升，处于历史最高位水平；交易额为 276 亿美元，较 2018 年大幅提高 78.06%，

图 5：中国网络安全产业全景图

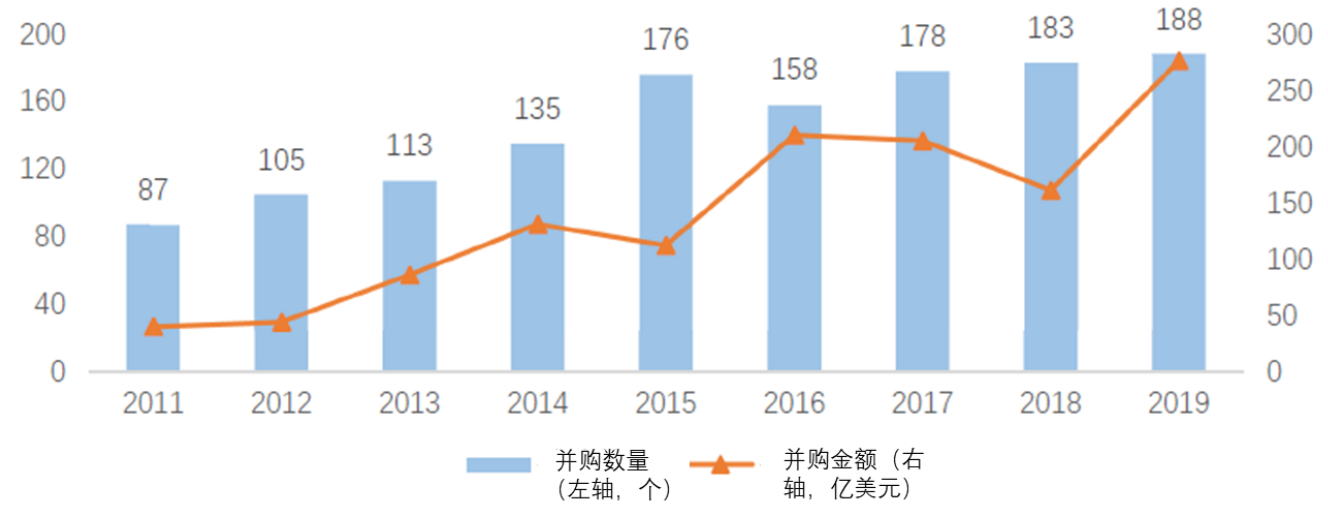
数据来源：安全牛，东吴证券研究所

图 6：网络安全产品较为分散（2017 年）



数据来源：智研咨询，东吴证券研究所

图 7：2011-2019 年全球网络安全并购活动态势



数据来源：Momentum Cyber，东吴证券研究所

卫士通是中国网安的唯一上市平台。中国网安以三十所、三十三所为核心组建而成，拥有国内最顶级的信息安全资质。卫士通作为中国电科网络信息安全板块的上市公司，2014 年 12 月通过发行股份购买资产的方式整合了三十所下属的三家公司股权及北京房产。经过 2015 年的股份无偿划转后，中国网安成为卫士通的直接股东，能够充分利用上市公司平台，开展相关业务的战略布局、资源整合和业务协同。

图 8：中国网安组织结构

数据来源：中国网安官网，东吴证券研究所

公司有望成为子集团的资源整合窗口。卫士通作为中国电科集团全资控股的中国网安旗下唯一的上市公司，未来有望成为其资产整合窗口，提升平台价值。此前卫士通已

收购了三十所旗下的三零嘉微、三零瑞通和三零盛安，为公司未来的战略整合指明发展道路。未来，在电科集团资产证券化比例提升的趋势下，结合网安公司的板块布局规划，我们预计卫士通有望进一步整合中国网安下属其他优质资产，成为资源整合平台，不断扩充和完善全产业链，快速转型综合性服务厂商。

表 1：三十所旗下信息安全企业及相关业务

公司	主营业务
三零嘉微	信息安全与通信保密系统相关芯片产品开发、测试、销售与服务
三零瑞通	安全保密手机，公众移动通信系统和专用移动通信系统的通信和网络安全服务
三零盛安	信息系统集成、涉密系统建设、信息安全产品研发、行业应用软件开发、信息安全服务及 IT 外包服务
厦门雅迅	卫星导航定位、车载终端及服务中心软硬件一体化解决方案及运营服务提供商
凯天	网络互动媒体、综合智能安方监控系统

数据来源：中国网安官网，东吴证券研究所

战略投资网安公司，有望实现内外资源的协同。2017 年 3 月，中国网安完成对深思科技的战略性投资，深思科技正式成为中国网安旗下控股公司，深思科技是国内最早研究并跟踪高级可持续攻击（APT）的网络安全公司之一，也是极少数具有国家级网络入侵检测发现和对抗能力的公司。2019 年 2 月中国电科通过产业基金（中电基金和网安基金）战略投资绿盟科技，成为其第二大股东（合计持股 13.91%）。2019 年 12 月，通过中电基金收购天融信 5.01%股份。绿盟科技和天融信作为优秀的民营网络安全公司，在安全行业深耕多年，产品体系丰富，未来在集团的推动下下，实现与卫士通的业务协同，把集团网安体系做大做强。

1.3. 网络安全成为电科集团四大目标板块之一，公司有望进入发展新篇章

董事长在信息安全领域具有较高影响力。董事长卿昱作为三十所在信息安全专业领域的带头人之一，曾先后主持和参与了 20 多项项国防大中型重点科研项目，先后获得科技进步一等奖二次，部级科技进步二等奖一次，长期从事信息安全与网络安全基础理论，系统及产品的研制开发和项目管理，编写了大量军事信息系统安全防护体系技术方案和设计报告著有《云计算安全技术》，公开刊物上发表多篇论文，包括基于优化 BP 神经网络的 WSNs 路由安全评估模型，基于 PKI/PMI 的授权管理模型设计,基于 SOA 的栅格安全服务研究，信息系统的可信计算体系，基于 SOA 的 Web 安全通信模型研究等论文。

陈肇雄出任电科集团新董事长，高度重视网络安全。2020 年 5 月 19 日下午，中央组织部宣布陈肇雄同志担任中国电科集团董事长、党组书记，免去其工信部副部长、党组成员职务。陈肇雄董事长早年在中科院从事机器翻译理论研究及系统开发，是国内最早从事人工智能研究的科学家之一，并获得国家科技进步一等奖。后来先后担任中国电

子集团总经理、湖南副省长，并提出“数字湖南”战略。2015 年入职工信部担任副部长，分管信软司、信息通信发展司、**网安管理局**等部门，在多个场合强调加快网络安全高质量发展，顺应数字化转型，要持续支持网络安全关键技术手段建设，积极开展 5G、人工智能、区块链等新兴重点领域网络安全技术研发布局，构建多领域、多层次的网络安全创新技术体系，不断提升核心技术创新和保障能力。

网络安全是中国电科未来聚焦的“四大板块”之一：中国电科 2021 年度工作会议中，董事长管陈肇雄指出，2021 年电科集团要立足“军工电子主力军、网信事业国家队、国家科技创新战略力量”三大定位，聚焦“电子装备、网信体系、产业基础、网络安全”四大板块，把集团做强做优做大。网络安全已然成为 2021 年以及“十四五”期间集团重点打造的业务板块。

1.4. 通过长效股权激励绑定核心管理层利益，管理改善值得期待

10 年期长效限制性股票激励计划，绑定公司核心管理和技术团队长期利益。2020 年 12 月 28 日，公司限制性股票长期激励计划 2020 年首期限制性股票授予登记完成：1）以 11.42 元/股的授予价格向高管、核心技术人员和骨干员工合计 300 人（其中高管 5 人、其他管理人员和核心员工 295 人）授予 7806575 股股票；2）预留授予 7 名激励对象合计 152,000 股限制性股票。3）第一、二、三期股票解锁的业绩条件分别为：解锁日前一年度 ROE 分别不低于 3.6%、4.0%、4.5%；解锁日前一年度相比于 2019 年净利润平均增长率不低于 10%、13%、16%（或不低于对标企业 75 分位值）；解锁日前一年度的经济增加值完成中国电科下达的考核任务，并较上一年度△EVA 为正。4）限制性股票长期激励计划的有效期为 10 年，原则上每次授予之间需间隔两年。

2020 年 6 月 30 日，习近平总书记主持召开中央深改委第十四次会议，审议通过了《国企改革三年行动方案（2020—2022 年）》；12 月 31 日，光明日报发表文章《吹响新一轮国企改革“冲锋号”——国企改革三年行动全面实施》；2021 年 1 月 16 日，《求是》杂志刊发国务院国资委党委书记郝鹏署名文章《深入实施国企改革三年行动 推动国资国企高质量发展》，**根据《国企改革三年行动方案（2020—2022 年）》“一企一策”的要求，各中央企业国企改革三年行动实施方案和工作台账中涉及的改革任务共计 4329 项、改革举措 10729 项**：其中南方电网、中国联通、招商局集团提出加快推进数字化转型，以数字化转型催生高质量发展新动能新优势；国家能源集团、中国海油、国机集团等企业从销量、利润、成本等不同维度，提出未来 3 年经营业绩增长目标；航天科技在提出 73 条改革举措基础上，明确了 165 项标志性成果，使得实施方案更实更落地；中国一重在探索引入持股 5%以上的战略投资者作为积极股东参与公司治理的同时，进一步提出完善持股 5%以下投资者征求意见建议机制。

长期管理改善值得期待。理解公司此次 10 年期长期股权激励，**需站在战略意义的高度上**，这并不是一个孤立的激励管理层的计划，而更多体现了其背后中国网安和中国电科集团在《国企改革三年行动方案（2020—2022 年）》的指导下，抓重点、补短板、

强弱项，谋求长远发展的第一步。一方面，**对内通过长效激励机制**，绑定公司核心管理和技术团队；**对外释放积极信号**，重塑公司在产业和资本市场的形象；另一方面，**对上是国企改革三年行动方案的落实**，完善中国特色现代企业制度，形成科学有效的公司治理机制；**对下 10 年期（分 5 批次）股权激励**，基本锁定了公司未来 5-10 年的经营业绩增长目标。我们分析认为，10 年期股权激励方案的推出，是公司贯彻国家意志、落实国企改革的第一步，在新机制下的持续管理改善值得期待。

2. 政策、技术、事件带动需求多点共振，服务化转型提升行业集中度

2.1. 《密码法》正式实施，加密行业迎来国产化和泛在化新机遇

政策推动行业景气度提升。近年来随着国内外网络安全事故的频发，我国政府不断提高对网络安全的重视。2013 年以来先后设立了国家安全委员会、中央网络安全和信息化委员会。2017 年 6 月 1 日，《网络安全法》正式发布，其作为我国网络安全的基本法，使得整个行业进入合法的时代，真正做到有法可依。近两年来，与《网络安全法》相配套的等保 2.0、《密码法》等也都陆续发布或者在立法阶段，法律将渗透在网络安全的各个分支和各个行业，提高政府、企业在网络安全方面的投入，必将推动整个行业往更为规范和成熟的方向发展。与此同时，合规需求和攻防需求也将带动整个行业进入新的加速成长阶段。

表 2：近年来网络安全相关的政策密集发布

时间	事件	内容
2020 年 7 月	全国人大发布《数据安全法（草案）》	确立数据分级分类管理以及风险评估、监测预警和应急处置等数据安全管理各项基本制度；明确开展数据活动的组织、个人的数据安全保护义务，落实数据安全保护责任；坚持安全与发展并重，规定支持促进数据安全与发展的措施；建立保障政务数据安全和推动政务数据开放的制度措施。
2020 年 4 月	国家互联网信息办公室等 12 部门正式发布了《网络安全审查办法》	于今年 6 月 1 日起实施。网络安全审查重点评估关键信息基础设施运营者采购网络产品和服务可能带来的国家安全风险，包括金融、电信、交通、能源等 10 多个行业的网络系统。
2020 年 1 月	全国人大通过的《密码法》正式施行	规定使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估，并对涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可，于 2020 年 1 月 1 日正式实施。

数据来源：网信办官网，东吴证券研究所

等保 2.0 强化国产化商用密码应用要求。2019 年 5 月 13 日等保 2.0 国家标准正式发布，并于 2019 年 12 月 1 日开始实施。等保 2.0 对新的应用场景做了更明确的安全要求。利好数字签名和身份认证（CA）：相比等保 1.0，等保 2.0 增强了安全防护力度，增加对身份识别和加密需求，目前的动态口令已不足以支撑，更高安全等级的数字加密身份认证方式需求必将快速增长。

表 3：等保 2.0 中涉及加密的政策变化

	等保 1.0	等保 2.0
通信传输	a）应采用校验码技术保证通信过程中数据的完整性； b）在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；应对通信过程中的整个报文或者会话过程进行加密。	a) 应采用校验码技术或者密码技术保证通信过程中数据的完整性； b) 应采用密码技术保证通信过程中敏感信息字段或整个报文的保密性。
身份鉴别	a) 应对登录操作系统和数据库的用户进行身份标识和鉴别； b) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换； c) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施 d) 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听； e) 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性； f) 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换； b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； c) 当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听； d) 应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现。
数据保密性	a) 应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性； b) 应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。	a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
数据完整	a) 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施； b) 应能够检测到系统管理数据、鉴别信息和重要业	a) 应采用校验码技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

性	务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。	b) 应采用校验码技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

数据来源：卫士通官网，东吴证券研究所

《密码法》有望加速国产密码替代和泛在化应用。作为我国密码领域的综合性、基础性法律，《密码法》于 2020 年 1 月 1 日起正式实施，有望长期推动密码在网络安全与信息化发展中发挥更大作用，更加深入、泛在地保障我国网络空间各个领域的权益。《密码法》规定使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估，并对涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可，密码将迎来国产机遇。短期密码法将在合规需求较为强的党政和关键信息基础设施行业率先展开应用，未来随着云计算、大数据、物联网等行业的快速发展，加密将逐步在视频安防、工控、车联网、数字或欧比等新兴行业实现泛在化应用，打开新市场空间。

密码工作经费纳入政府预算，密码成为刚性合规需求。《密码法》第十一条规定县级以上人民政府应当将密码工作纳入本级国民经济和社会发展规划，所需经费列入本级财政预算。从立法层面，要求政务机关把对密码产品的采购列入到预算，把信息化和网络安全同步规划、同步建设、同步运营，通过政府采购规定可以进一步拉动产业。从实施手段上，强化财政预算中纳入密码工作所需经费，主张采购有效密码产品，以增大政府对密码产品采购和安全防护实施。从责任上，尤其是关键信息基础设施领域，运营者违规使用商密可能被处以罚款；违反密码法视后果可能追究刑事或者民事责任。

市县级潜在市场规模大，密码法将加速渗透。根据国家采招网的招标数据，我们发现受政策影响，以政府机构和军工集团为主的单位，正不断加快 PKI/PMI 国密算法升级改造的步伐。通过搜集公开招标信息数据，加密算法国产替代环节，我们测算出仅政府机构和军工集团领域的国产替代空间接近 129 亿元。未来，考虑到芯片等硬件级别替换和银行金融领域渗透，我们认为整体国产替代市场空间有望超过 200 亿元。目前 PKI 体系建设在部委、省级有了较好的覆盖，而市场空间更大的市县级目前渗透率还较低，此次密码法将密码工作所需经费纳入县级以上政府财政预算后，我们预计 PKI 建设向市县级渗透的速度有望加快。

图 9：PKI 国产算法替代空间测算

政府端				
	数量	重点部门	国产算法升级改造项目金额(万)	市场空间(亿元)
国家部委	64	——	300	1.92
省级	31	10	250	7.75
地市级	334	10	120	40.08
区县级	2850	5	50	71.25
军工端				
	数量	国产算法升级改造项目金额(万)		市场空间(亿元)
主要军工集团	22	300		0.66
直属单位/专业化公司/科研院所	566	120		6.79
合计				128.5

数据来源：国务院官网、各公司官网、中国采招网，东吴证券研究所测算

金融数据密码机国产潮来临。密码机主要有金融数据密码机和服务器密码机两大类，可广泛应用在金融、电力、社保、公交、卫生等行业，在金融领域前者需求更大，在银行、银联、第三方支付等金融机构广泛使用。此前国务院发布《金融领域密码应用指导意见》，要求我国各金融机构要逐步采用国产密码算法，建立以国产密码为主要支撑的金融信息安全保障体系。目前各金融机构正不断推进国密算法改造工作。国密的加密机核心不仅在于算法标准，更在于密码算法芯片的国产化、密码机需要的通用芯片的国产化，预计金融数据密码机在《密码法》推动下有望加速迎来国产潮。

仅金融市场市场空间超 100 亿。根据统计招标信息，目前一台密码机价格在五、六万元左右。根据银保监统计的金融机构数量，结合不同类型金融机构对保密机的需求，我们预计金融行业的加密机需求在 20 万台左右，市场空间 100 亿元左右。若叠加银联、券商、第三方支付等，行业空间则更大。

图 10：加密机市场空间测算

类型	总行/总公司/法人/省级数量（个）	密码机数量（台）	一级分行/分公司/市级数量（个）	密码机数量（台）
银行（包含政策性&国有&股份制&其他商业银行）	1678	86300	1973	78315
农村合作银行&信用社	53	1590	452	6690
其他金融机构	2167	29453	217	2365
		117343		87370
合计（台）		204713		

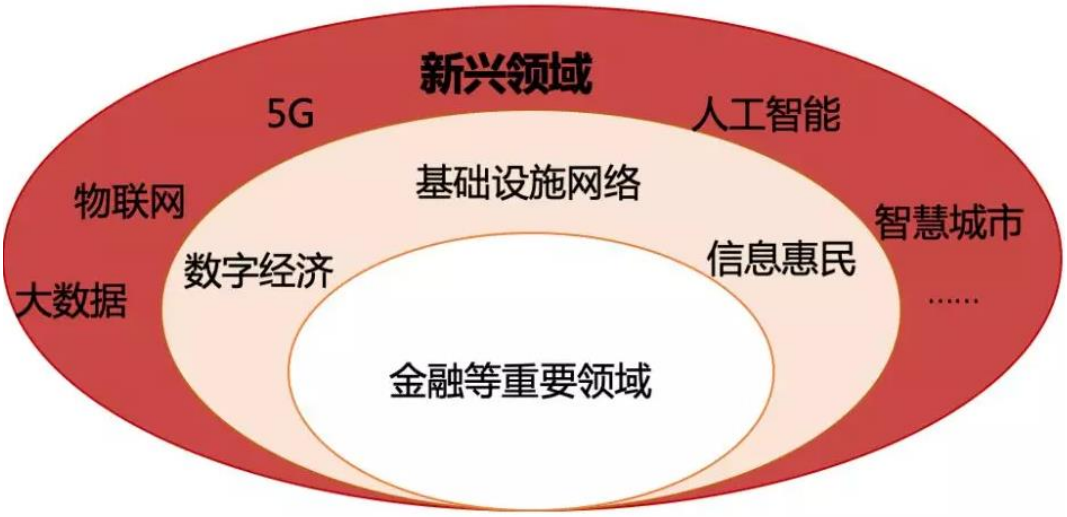
数据来源：银保监会网站，东吴证券研究所测算

2.2. 技术：5G、云计算、大数据等新技术的出现，对网安提出更高要求

新技术的应用给安全市场带来新的需求。在传统网络安全防护时代，由于网络环境

（互联网、隔离或非隔离内网）、用户终端（PC 为主）、政企应用（OA、CRM、ERP 为主）等相对简单，针对信息化的安全防护更加注重网络边界的保护，产品主要以针对边界防护隔离的硬件产品和针对主机及应用系统的软件形态的产品为主。随着云计算、大数据等新兴技术的广泛应用，用户终端（PC 向移动终端、IoT 终端、工业主机等泛终端形态扩展）、网络环境（云、端带来新边界）、应用和数据（类型和复杂度增加）的变化等对安全防护带来了新的需求，围绕上层的身份、数据、应用和行为等需要构建新的防御体系，新的产品细分赛道不断涌现。

图 11：网络安全领域正在迅速扩张



数据来源：卫士通官网，东吴证券研究所

客户的安全建设需求从被动防御向主动防御阶段转变。近年来，网络攻击由过去黑客炫技的个人行为，发展成有组织的犯罪或者攻击行为，呈现手段专业化、目的商业化、源头国际化及载体移动化的趋势。传统的以安全硬件为核心的被动防御体系无法抵御当前的网络攻击，整个行业正在由被动防护向主动防御模式转变。

以安全大数据为核心的态势感知体系是主动防御体系的安全大脑。随着互联网的迅猛发展，网络安全态势感知应运而生，其工作原理是对网络环境中引起网络态势发生变化的安全要素信息进行获取、理解，进而评估网络安全的状况，预测其发展趋势，并以可视化的方式展现给用户，帮助用户实现相应的安全决策与行动，从而实现积极主动的动态安全防御。被动防御时代以边界防护为主，防火墙是最重要的产品，主动防御时代安全大脑是防御体系中最核心的组成部分，而态势感知充当的就是安全大脑的角色。

图 12：态势感知是主动防御的安全大脑

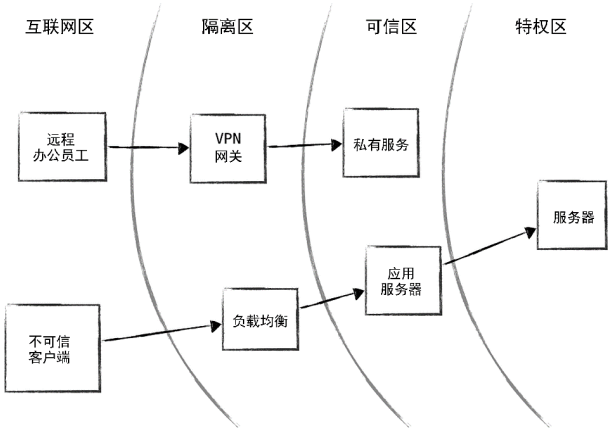
数据来源：环球网，东吴证券研究所

网络态势感知成为国家重点推进工程。2016 年 4 月 19 日，习近平总书记在网信工作座谈会上发表讲话，第一次提到“全天候全方位感知网络安全态势”，国家把态势感知的建设放到了十分重要的位置。2016 年 12 月 15 日，国务院发布的十三五国家信息化规划中，将“健全网络安全保障体系”作为十大任务之一，明确提出要“全天候全方位感知网络安全态势”。在 2017 年的 2.17 国家安全工作座谈会中，习近平总书记强调“要筑牢网络安全防线，提高网络安全保障水平，强化关键信息基础设施防护，加大核心技术研发力度和市场化引导，加强网络安全预警监测，确保大数据安全，实现全天候全方位感知和有效防护”。这充分表明，党中央和国务院均将态势感知作为国家重点工程推进。

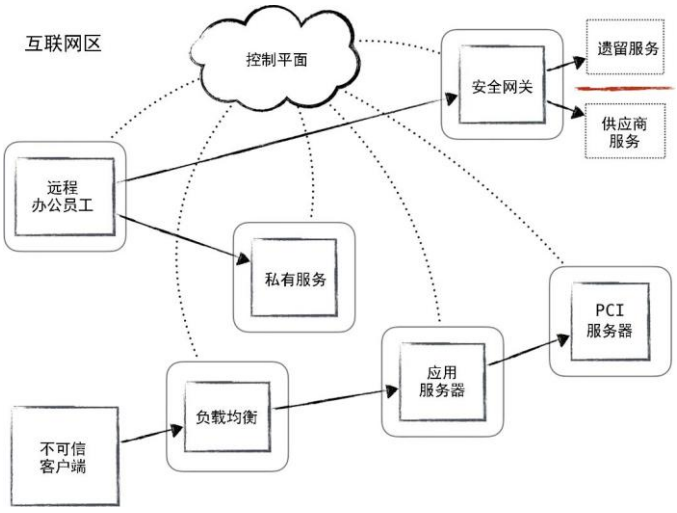
零信任安全架构正逐步取代传统基于网络边界的安全架构。传统的安全架构通过边界防护设备划分出企业内网和外网，并以此构建企业安全体系，内网用户默认享有较高的网络权限，而外网用户接入内网都需要通过 VPN。随着云计算、大数据、物联网、移动互联网等技术的兴起，带来日趋开放和复杂的网络边界，灵活的移动办公，内网边界也日趋复杂与模糊，让基于边界的安全防护逐渐失效，来自企业外部的欺诈和内部的信息泄露造成的损失逐年剧增，一种基于“零信任框架模型”的网络安全架构由此诞生。零信任体系对外部公共网络和本地网络的设备在默认情况下都不会授予任何特权，用户无论在哪里，无论什么时间，只有使用通过受控设备、通过身份认证，且符合“访问控制引擎”中的策略要求，通过专用访问代理才能访问特定的公司内部资源。

图 13：传统的网络安全架构

图 14：零信任架构



数据来源：《零信任网络》，东吴证券研究所

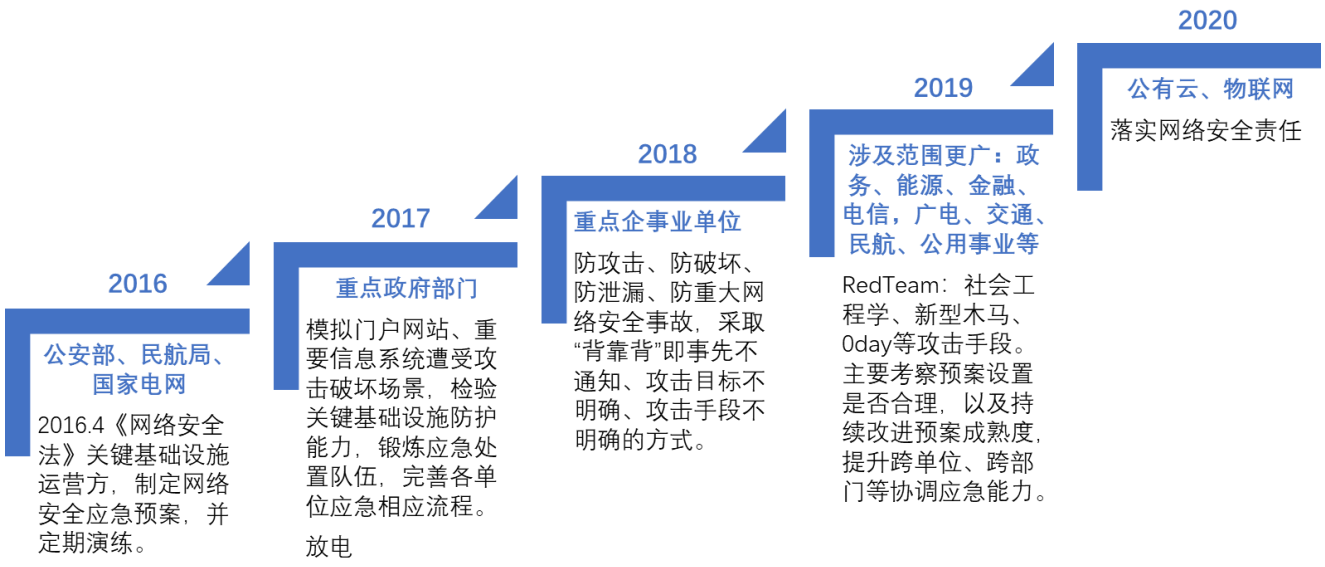


数据来源：《零信任网络》，东吴证券研究所

零信任的核心思想是身份控制：网络边界内外的任何访问主体（人/设备/应用），在未经过验证前都不予信任，需要基于持续的验证和授权建立动态访问信任，其本质是以身份为中心进行访问控制。

建设需求由等保合规进阶实战化演习。网络安全的本质不是被动防御，是主动防御对抗。《网络安全法》规定关键信息基础设施的运营者应制定网络安全事件应急预案，并定期进行演练，自此实战攻防演练成为网络安全建设的重要一环。网络安全实战攻防演练专项行动已成为一年一度的惯例，同时所涉及的单位和规模持续扩大。攻防实战演练已成为检验参演单位网络安全综合防御水平的“试金石”和提升网络攻击应对能力的“磨刀石”。在攻防实战演习的带动下，机构对网络安全的需求也从被动构建向业务保障刚需升级。

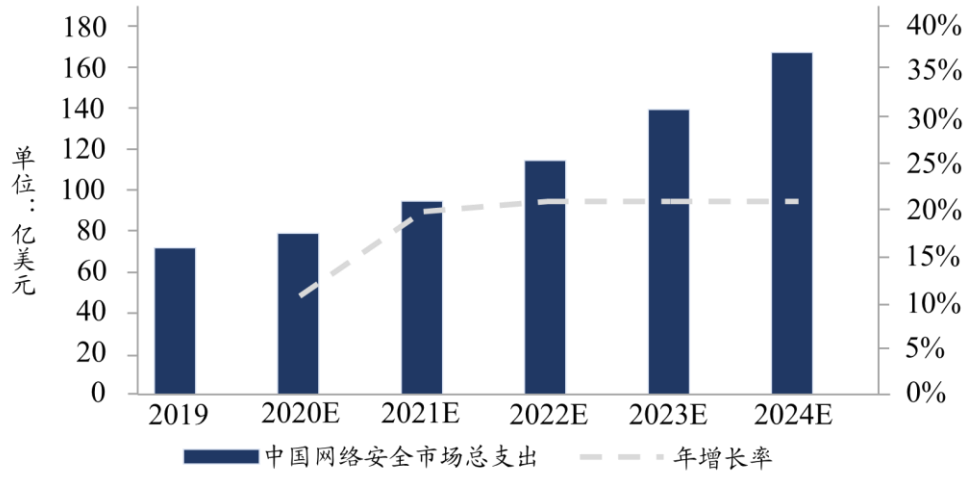
图 15：攻防实战演习范围不断扩大



数据来源：人人云图，东吴证券研究所

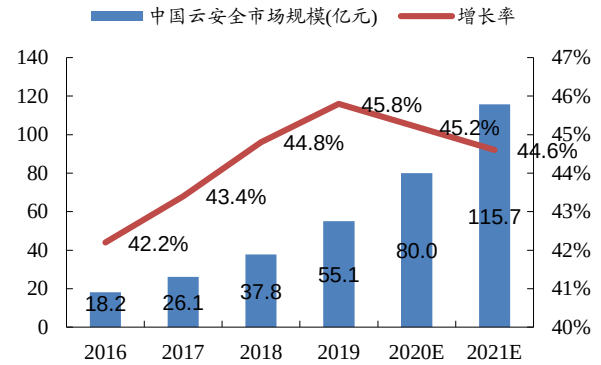
新兴安全领域增速高于行业整体增速，呈加速发展态势。在政策和数字化经济转型的驱动下，我国网络安全行业仍将继续保持较快的增长。根据 IDC 预测，2020 年中国网络安全市场总体支出将达到 78.9 亿美元，较 2019 年同比增长 11.0%，到 2024 将增长至 179.0 亿美元，2020-2024 年 CAGR 为 18.7%。而根据赛迪咨询的预测，2020 年云安全、大数据、物联网安全、工控安全等新兴安全领域的市场规模分别为 80.0、51.5、195.1、168.7 亿元，同比增速分别为 45.2%、35.2%、51.4%、34.8%，高于网络安全市场的总体增速；2020 年将达到 495.3 亿元，同比增速为 42.7%，各增速均高于行业增速。

图 16：2019-2024 年中国 IT 安全支支出规模预测



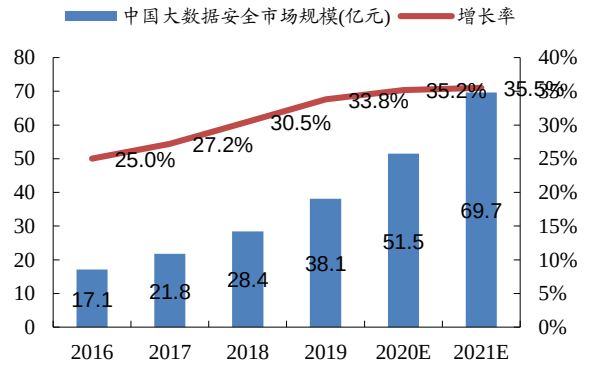
数据来源：IDC，东吴证券研究所

图 17：2016-2021 年中国云安全市场规模及增速



数据来源：赛迪咨询，东吴证券研究所

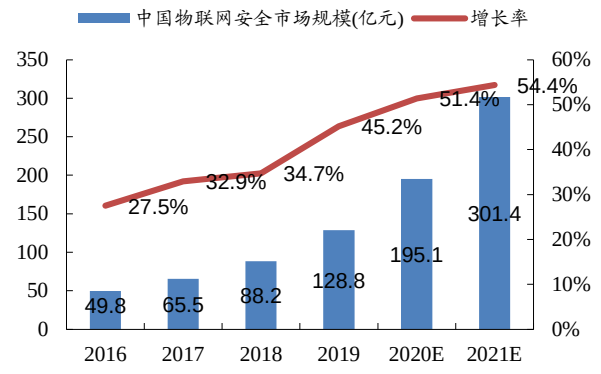
图 18：2016-2021 年中国大数据安全市场规模及增速



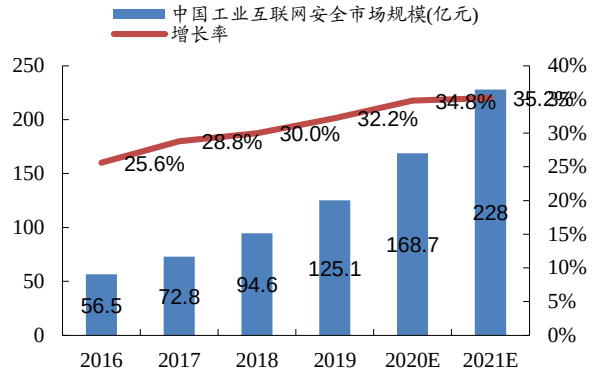
数据来源：赛迪咨询，东吴证券研究所

图 19：2016-2021 年中国物联网安全市场规模及增速

图 20：2016-2021 年中国工业互联网安全市场规模及增速



数据来源：赛迪咨询，东吴证券研究所



数据来源：赛迪咨询，东吴证券研究所

2.3. 事件：网安关乎社会稳定和居民隐私，案件频发加速推动需求释放

根据国家互联网应急中心（CNCERT）发布的《2019 年中国互联网网络安全报告》，2019 年我国互联网安全威胁包括分布式拒绝服务攻击（DDoS 攻击）、高级持续性威胁攻击（APT 攻击）、漏洞威胁、数据安全隐患、移动互联网恶意程序、网络黑灰色产业链（黑灰产）、工业控制系统安全威胁等呈现出许多新的特点，带来新的风险与挑战：1）党政机关、关键信息基础设施等重要单位 DDoS 攻击呈现高发频发态势，攻击组织性和目的性更加凸显。2）APT 攻击逐步向各重要行业领域渗透，在重大活动和敏感时期更加猖獗。3）事件型漏洞和高危零日漏洞数量上升，信息系统面临的漏洞威胁形势更加严峻。4）数据安全防护意识依然薄弱，大规模数据泄露事件频发。5）“灰色”应用程序大量出现，针对重要行业安全威胁更加明显。6）恶意注册、网络赌博、勒索病毒、挖矿病毒等黑茶依然活跃，高强度技术对抗更加激烈。7）工业控制系统产品安全问题依然突出，新技术应用带来新安全隐患更加严峻。

表 4：2019 年以来发生的部分信息安全事件

时间	信息安全事件
2019.1	HackenProof 的网络安全人员 Bob Diachenko 在推特上爆料称，一个包含 2.02 亿中国求职者简历信息的数据库泄露，包括个人全名家庭住址，手机号码，电子邮件，婚姻状况，子女数量，政治关系，身高，体重，驾驶执照，识字水平，薪水期望、教育背景、过去的工作经验等等。
2019.1	澳大利亚维多利亚州政府 3 万多名公务员工作数据被盗，不法分子可能会利用盗窃的邮件、电话号码等信息对政府公务员进行网络钓鱼攻击、垃圾邮件攻击等
2019.2	2019 年 2 月，北京字节跳动公司向海淀警方报案，其公司旗下抖音 APP，遭人拿千万级外部账号密码恶意撞库攻击，其中上百万账号密码与外部已泄露密码吻合。
2019.3	华硕超百万用户可能感染恶意后门。俄罗斯卡巴斯基实验室发现了一项新型的复杂 APT 攻击行动，该行动可能通过一个后门应用程序感染了超过一百万的华硕用户。
2019.5	易到用车服务器遭攻击，黑客勒索巨额比特币，App 也无法正常使用。易到用车官方发布微博称：“2019 年 5 月 26 日凌晨，易到用车服务器遭到连续攻击，因此给用户使用带来严重的影响。攻击者索要巨额的比特币相要挟，攻击导致易到核心数据被加密，服务器宕机。

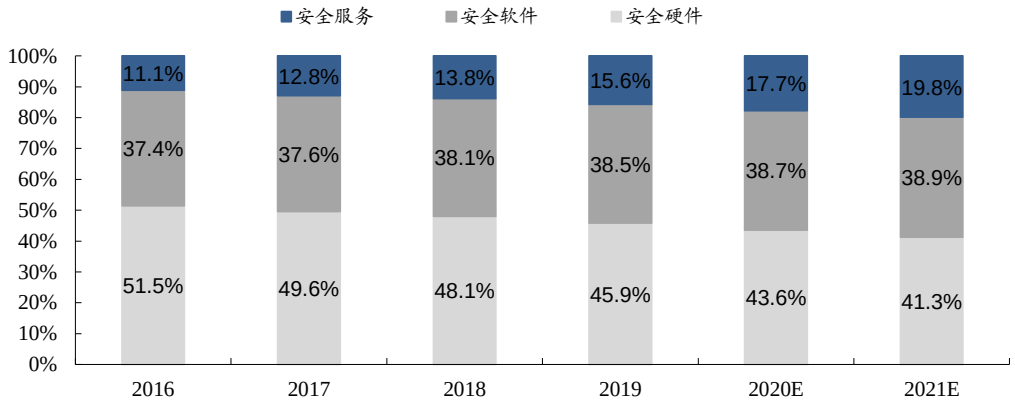
2019.7	美国第一资本银行金融公司顾客个人基本信息被窃取，被窃取数据包括 2005 年至 2019 年初信用卡申请者的基本个人信息（主要为信用评分、支付历史以及部分交易数据）、大约 14 万个美国用户的社会安全号码以及 8 万个关联银行账号。俄罗斯联邦安全局服务器遭到黑客入侵，7.5TB 数据被盗，包括俄罗斯有关社交网络用户登录信息等重要数据。
2019.8	据腾讯安全御见威胁情报中心消息，湖北、山东等地的医疗、电力系统均遭到勒索病毒攻击，攻击者会留下勒索说明文档，要求联系指定邮箱购买解密工具。

数据来源：国家保密局官网、东吴证券研究所

2.4. 行业服务化转型，头部集中趋势不变

网络信息安全市场持续向服务化转型，安全市场结构进一步优化。在网络信息安全产业发展过程中，大多数是由合规需求驱动的，而近年来的灾难性攻击表明网络风险是重大威胁，网络威胁正向多样化和复杂化的方向演化，传统的单一安全产品的模式已经很难满足客户的安全防护需求。企业开始把安全视为一项重要的商业风险，以风险评估、安全管理咨询、安全应急响应、安全托管服务等为主的安全服务越来越受到用户的青睐。随着虚拟化及云理念渗透，云化产品快速发展，安全服务的价值得到认可，威胁监测、威胁情报等新兴模式逐步试点应用，行业盈利模式将由软硬件产品销售向服务模式逐步转变。赛迪咨询数据显示，2016 年以来，中国安全服务的支出占比提升了 6 个多点。

图 21：安全服务占比逐年提升



数据来源：赛迪咨询，东吴证券研究所

3. 围绕“新四化战略”，有望从密码核心厂商走向综合型网安龙头

3.1. 加密是网络安全核心环节，卫士通全产业链布局

密码是网络安全的基础支撑，作用在于保护用户的数据安全。网络安全从层次角度来看，可以大体上分为物理安全、逻辑安全、系统安全和联网安全。从防护的区域来讲，可以分为边界安全与主机安全。过去的网路安全发展过程中，边界安全得以不断加强，

但主机安全的发展却有所落后。主机安全的主要功能是保证主机在数据存储的保密性，它包括硬件、固件、系统软件的自身安全以及一系列安全软件和技术。密码是信息安全的核心，密码最主要的功能是实现机密性，同时还具有认证鉴别、完整性和抗抵赖等功能。密码技术在数据保护、身份认证、系统加固等领域将发挥更大的作用。

国家信息安全三个等级，商用密码市场空间最大。我们国家将信息安全划分为三个等级：核密、普密和商密。其中核密最高，普密次之，商密最低。核密一般指国家党政领导人及绝密单位的安全级别，此领域不存在任何商务行为。普密是指国家党政军机关的信息安全级别，此领域安全设备由国家指定的五家研究机构负责研制工作，商密用于保护企业级的商业秘密，技术上不一定比普密低，但商密产品的管理程度不如普密，应用产品多，应用面广（如 VPN）。

表 5：国内加密等级及说明

信息安全等级	安全程度	内容描述	资质情况
核密	最高	国家党政领导人及绝密单位的安全级别。	无商业行为。
普密	次之	国家党政军机关的信息安全级别。普密可用于保护一定范围的国家安全信息，对国家秘密保护的强度包括它的手段和技术。因保护国家秘密信息的时候所采用的密码必须是普密级以上的，普密设备从管理上要求对普密产品、设备的管理非常严格，应用面较小。	国家指定五家研究机构负责研制：电子工业集团 30 研究所（卫士通）、原邮电部数据通信研究所（数据所）、总参 56 所（江南所）、中船 722 所、空三所。
商密	最低	用于保护企业级的商业秘密，技术上不一定比普密低，但商密产品的管理程度低于普密，应用产品多，应用面广（如 VPN）。	卫士通(国内唯一一家同时拥有涉密，商密领域最高级别资质信息安全企业)、立思辰、蓝盾股份等。

数据来源：卫士通官网，东吴证券研究所

商用密码产业链完整，销售额达百亿以上。目前，商用密码产品已经形成了从芯片、办卡、整机到软件、系统和密码服务的完整产业链，而且密码产品更加实用。根据北京市密码管理局局长介绍，截至 2016 年底，北京市商用密码产品销售额达到 70 亿元，占全国商用密码产品总销售额的 60%，处于领先地位[1]。以此推算，全国商用密码产品的销售额为 120 亿元左右。未来商用密码市场在信息安全产业中占比有望提升，增速获得进一步提高。

表 6：商用密码产品按照功能分类

类别	解释	典型产品
密码算法类	构成密码应用基础的能提供密码运算功能的产品	密码算法实现软件、密码算法

[1] http://bj.people.com.cn/n2/2017/0212/c82839-29702880.html

		芯片等产品
数据加解密类	提供数据加解密功能的产品	加密机、加密卡、智能密码钥匙等产品
认证鉴别类	提供身份认证、密码鉴别功能的产品	动态口令系统、身份认证系统等产品
证书管理类	提供数字证书的产生、分发、管理功能的产品	数字证书管理系统等产品
密钥管理类	提供密钥的产生、分发、更新、归档和恢复等功能的产品	密钥管理系统等产品
密码防伪类	提供密码防伪验证功能的产品	电子印章系统、支付密码器、数字水印等产品
综合类	提供上述两种或两种以上功能的产品	电子商务安全平台等产品

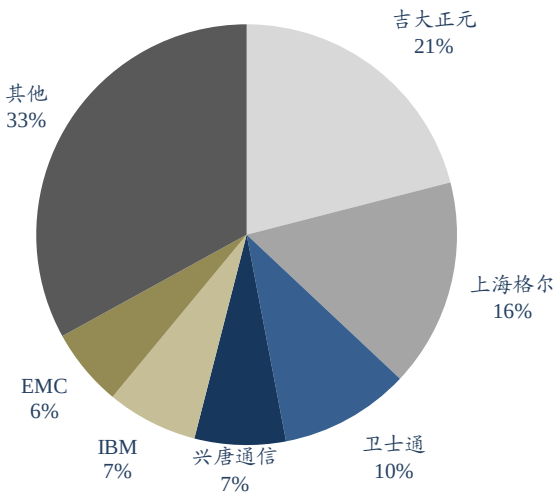
数据来源：中孚信息招股说明书，东吴证券研究所

密码产品起家，目前已实现密码全产业链布局。密码产品是卫士通公司一直以来的核心产品，2015 年，卫士通收购了三零盛安、三零瑞通和三零嘉微，目前拥有从密码芯片、密码模块、密码整机和密码系统的全系列、全产业链的密码产品。密码芯片有嵌入式安全 SE IP、高速可编程安全芯片、超低功耗安全芯片、移动终端安全芯片和物理噪声源芯片等；密码模块有 TF 密码卡、PCI-E 密码卡、软件密码模块等；密码机有金融数据密码机、服务器密码机、签名验签服务器等；密码系统有密钥管理系统、证书管理系统、密码应用中间件、LTE 加密系统、PDT 加密系统、加密卫星通信系统等。

密码技术行业领先。目前我国的商用密码是不公开的，商用密码算法由商用密码科研定点单位或者国家密码主管部门组织专家设计，算法经国家密码主管部门审查批准后，方可使用。卫士通依托中国电科三十所，在密码领域具有多年的技术积累和丰富经验，并一直积极开展大量和密码相关的理论研究。同时承担了大量国密局算法研制任务，如分组算法，轻量级分组密码算法，轻量级序列密码算法的设计、分析、评估等；实现了 SM1、SM2、SM3、SM4、SM9 等国家商用密码的自主软/硬件开发，在国内加密认证类产品市场长期保持领先

国内商密领域最高级别资质信息安全企业。密码产品生产单位需要使用密码算法时，需要向国家主管部门申请，经批准后从密码主管部门或者密码算法授权管理部门获取密码算法载体或者购买密码芯片。卫士通凭借着 20 多年的技术及品牌积淀，成为国内首批商密产品研发、生产、销售资质单位，占据着国内密码机第一、信息加密/身份认证市场份额第三的地位，通过产业链的不断延伸，业务布局不断拓展，产品类型和服务领域不断扩大。同时，公司作为密码行业标准化技术委员会首批成员单位之一，参与过多项商用密码技术的专项研究项目。

图 22：2016 年我国信息加密/身份认证市场品牌结构



数据来源：Wind，东吴证券研究所

龙芯最新 3 系 4000 处理器集成卫士通安全 SE。龙芯 3A4000/3B4000 使用了龙芯最新研制的新一代处理器核 GS464V，相比上一代 GS464e 微架构，进一步优化了流水线，提升了运行频率，同时加强了对虚拟化、向量支持、加解密、安全机制等方面的支持。相比上一代四核处理器龙芯 3A3000，芯片整体实测性能提升一倍左右。值得重视的是，3A4000/3B4000 采用新的安全方案，将卫士通高性能嵌入式安全 SE 直接置入芯内，能够为用户提供高性能的密码算法服务能力、可信计算服务能力和硬件级安全防护能力，可广泛应用于高安全等级的自主安全终端、可信计算终端和各型安全设备中，安全核心模块的算法可重构能力又为系统厂商提供了平台化的安全解决方案，从而构建安全可信的信息系统生态。相对传统的在芯片外附加安全模块的方案更加安全和经济。

3.2. “新四化”战略，有望在横纵向打开新的增长空间

密码产品起家，目前业务范围已覆盖安全产品、安全服务和安全集成。公司从核心的密码技术应用持续拓展，经过 20 余年的耕耘，目前业务范围从早期的密码产品已覆盖安全产品、安全服务和安全集成。

中国网安发布新战略，提出网络空间安全“新四化”。中国网安提出了网络安全“新四化”战略——密码泛在化、基础国产化、攻防智能化、安全服务化。公司作为中国网安负责信息安全的主体单位，在子集团层面承担着更多发展网络空间安全业务的责任。公司面对网络安全产业发展环境新形势，全面加快向安全服务转型，积极践行“新四化”的发展思路，大力发展信创安全、云计算与数据安全、网络安全服务业务，业务覆盖由政务向行业拓展。

以合作促进密码泛在化应用。公司与视联动力（视联网领域）和安天（威胁检测分析）签署战略合作协议。卫士通以密码技术为基础，通过与合作伙伴的协同，可以实现在不同领域的深耕，实现密码技术的泛在化应用。

积极打造态势感知和检测预警解决方案。结合网络安全监管需求，通过多维采集、纵向汇聚和横向共享属地关键信息基础设施的安全数据，进行基于大数据分析的安全威胁检测和通报预警、响应处置，为监管机构提供完整的网络安全态势感知和监测预警解决方案，帮助用户实现业务管理灵活方便、业务创新能力提升。同时，卫士通已经发布基于鲲鹏生态的国产化态势感知产品，该产品依托华为 TaiShan 服务器，在这之上搭载卫士通自主创新的安全态势感知平台。

图 23：中国网安的网络安全态势感知平台产品

数据来源：中国网安官网、东吴证券研究所

中标政务数据安全项目，未来政务大数据安全运营有望扮演重要角色。2020 年 1 月，卫士通中标国家公共数据开放网站（一期）工程数据标识和分类分级保护、安全审计等系统定制开发及安全标准编制项目，金额 261 万元。随着政务信息共享交换平台业务的不断发展，数据共享交换的数据安全成为关注重点。本次招标项目中，卫士通提出了以数据标识和分类分级保护系统为核心的体系化的数据安全共享交换解决方案，实现共享交换全过程数据“身份化”以及精准管控和安全保护。目前，该系统也在党、政、军及关键基础行业展开应用。借助本次试点项目，公司将有望在未来的政务大数据安全运营中扮演重要角色。

实现加密技术和云计算的结合与应用。随着信息化的加速，云计算正在全国不断普及，而伴随云云计算而来的安全和监管问题愈发凸显。公司依托在云计算和加密领域的长期积累，自主研发了包括云密码资源池管理平台、网安凌云安全云管理平台、云服务器密码机等云安全产品，以硬件设备虚拟化和软件产品云部署作为产品云化的有效途径，全面推动公司产品云化，积极支持安全服务转型，云密码机实现了和主流云平台的对接，能够更好地助力用户在云端的各类安全需求。

图 24：网安领域安全云管理平台

数据来源：公司官网，东吴证券研究所

安全应用橙讯安全即时通讯平台入选中国电科国家信息化产品库。2020 年 9 月，卫士通橙讯作为唯一一款软件类产品加入国家信息化产品库，未来将配合中国电科国际业务云平台的实施完善。中国电科的国际业务云平台是电科国际化经营体系建设重要工具，在国家“一带一路”倡议的引领下，越来越多的央企走出国门对外进行投资建设，卫士通橙讯作为一款以“安全”+“沟通”+“协作”为主打的平台型产品，能提供七大安全保障和一整套密码支撑体系，全面提升跨境沟通及文件传递的安全性和可靠性，为政企用户跨地域乃至跨国业务的安全、高效、有序开展提供有力保障。

3.3. 研发投入占比接近 12%，信创业务稳步推进

2016-2019 年，公司研发人员数量分别为 698、864、871、853 人，占比员工总数分别为 33.37%、41.38%、41.92%、41.39%；研发投入金额分别为 1.84、2.33、2.41、2.47 亿元，占比营收总额分别为 10.20%、10.90%、12.46%、11.73%，技术创新能力持续提升。

图 25：2016-2019 年公司研发人员数量及占比（人）

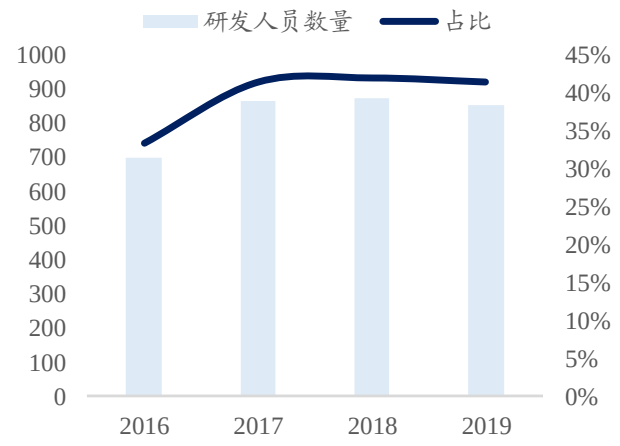
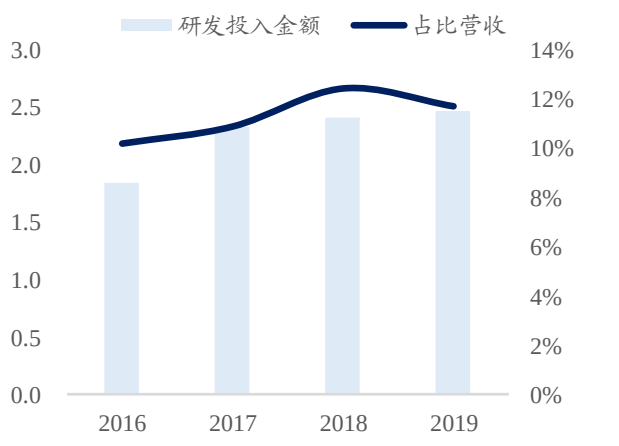


图 26：2016-2019 年公司研发投入金额及占比（亿元）



数据来源：Wind、东吴证券研究所

数据来源：Wind、东吴证券研究所

信创业务稳步推进，加密业务有望放量。积极推进基础国产化战略应用于电子政务、企业网络和互联网的产品，全面开展与鲲鹏、龙芯、飞腾、兆芯、海光、申威等处理器的适配工作，与人大金仓（数据库）、万里红、华安保进行战略合作，携手共同打造国产生态体系。公司在基础领域有密码机、数字证书认证系统，在应用领域有身份认证服务系统、电子签章、电子公文交换系统、电子公文处理系统等众多重磅产品和方案，有望率先受益于基础信息创新的大规模放量。

在信创产品研制方面，加强基础共性平台的研究，SJJ1940-G IPSec VPN 安全网关等 7 款产品获得国密局商密资质，安全隔离与单向导入系统、防火墙 2 款产品通过公安部测评，3 款交换机通过工信部资质测评，信任服务基础设施通过相关机构资质测评，终端安全登录系统等产品实现了专用机全平台的适配。

在商密产品研制方面，积极推动密码泛在化战略，金融数据密码机等 18 款产品获得商密资质；加强密码能力的整合，启动高性能商密芯片、密码管理服务平台的设计工作；云安全服务平台完成立项和方案评审；完成嵌入式安全 SE IP，以及采用该款 SE 的系列安全产品的发布，嵌入式安全 SE IP 降低了产品成本，提升了产品性能和可靠性，加速推动了公司国产化大生态建设，并通过和龙芯的合作，开拓出新的安全应用领域；云密码产品与银联、华为、平安、京东等企业对接成功，增强了公司在云安全领域的产品竞争力；身份认证系统实现了互联网+政务服务信任体系产品的市场突破，安全视频加密和视联网密码应用方案实现了公司产品在物联网市场的突破，软件密码模块成功进入 Win10 政府版生产版本。

3.4. 辐射全国的市场营销网络，积极拓展新的客户领域

公司建立了行业和区域相结合的矩阵式营销服务支撑体系，通过华北、华东、华南、西部、四川 5 大区域营销中心及下设的 20 余个办事处，配合政府、行业等行业营销部门与整体保障、移动互联网、卫士云三大事业部，建立了辐射全国的营销服务网络，为用户提供专业的网络信息安全整体解决方案、7x24 小时的日常维护、驻场、应急保障等服务，为公司全国化业务布局提供强力支撑。在客户拓展方面，公司加强传统市场布局力度，巩固核心优势：1）在党政业务领域，积极争取全国新系统建设项目，实现重大行业用户突破，为积极探索布局面向党政领域云密码服务打下坚实的基础；2）在商密领域，不断完善金融、电力、政务云、安全移动办公等行业解决方案，在泛金融领域积极进行市场开拓；3）积极开拓新市场，打造业务新动能，深度参与安全运营服务、安全移动办公等新业务工作，取得一定进展；4）大力推进安全服务平台的设计研发工作；5）面向电子政务云的安全服务业务以及面向重点央企的整体保障服务业务有序推进，均取得一定成绩。

3.5. 产品业务占比逐年下降但毛利率高，集成服务业务毛利低、增速快

1）**单机和系统产品**：公司能为电子政务网用户、企业用户和互联网用户提供密码产品、网络安全、数据安全、终端安全、安全应用、安全管理、身份认证与访问安全、云安全、移动安全和行业应用类安全产品。

2）**安全集成与服务**：1）安全集成业务是公司依托雄厚的技术支持和强大的营销网络为各层次用户提供的系统集成及全生命周期安全支持与服务，包括项目规划、整体解决方案设计、工程建设、用户培训及安全服务等。2）安全运营服务包括云密码服务、云认证服务、企业微信加密服务、网站安全防护和 SaaS/PaaS/IaaS 服务；监测预警服务包括安全态势感知与监测预警服务、高级威胁监测服务、互联网舆情监测服务和安全事件分析服务等；风险评估服务包括系统架构评估、渗透测试和安全加固等。

表 7：公司 2017-2020Q3 的收入、利润、毛利率、净利率和 ROE 情况（亿元、%）

	2017	2018	2019	2020Q3
收入	21.37	19.31	21.04	9.80
收入增速	18.79%	-9.64%	8.96%	-6.04%
归母净利润	1.69	1.20	1.56	-0.94
净利润增速	8.33%	-28.99%	30.00%	46.88%
毛利率	35.30	35.01	32.54	35.73
净利率	8.29	6.45	7.56	-9.91
ROE	5.84	2.76	3.48	-2.09

数据来源：Wind、东吴证券研究所

表 8：公司 2017-2020H1 分业务的收入和毛利率情况（亿元、%）

分业务	2017	2018	2019	2020H1
安全集成与服务收入	10.45	10.08	12.40	2.73
集成和服务收入增速	22.80%	-3.54%	23.02%	-28.91%
单机和系统产品收入	10.93	9.23	8.64	1.61
产品收入增速	20.51%	-15.55%	-6.39%	-29.39%
分业务毛利率				
安全集成与服务	15.49	12.40	16.02	18.18
单机和系统产品	54.24	59.72	56.26	61.52

数据来源：Wind、东吴证券研究所

4. 盈利预测与估值

收入估算:

1）**短期:** 根据我们在图 9 和图 10 中的测算，《密码法》出台后，密码工作经费纳入政府预算，密码成为刚性合规需求，仅政府机构和军工集团领域的国产替代空间接近 129 亿元（详细测算过程请见图 9），按照平均 5 年的替换周期，对应每年约 26 亿元的市场空间。同时，考虑到金融机构密码机国产替代进程正在加速，我们测算金融行业的加密机总需求在 20 万台左右，市场空间 100 亿元左右（详细测算过程请见图 10），按照平均 5 年的替换周期，对应每年 20 亿元的市场空间。政府机构、军工集团、金融领域加总后，短期对应每年市场空间为 46 亿元左右，考虑到公司作为我国密码领域的国家队，股东背景实力雄厚，预计单机和系统产品业务 2020-2022 年收入同比增长 2.39%、25.00%、25.00%，对应收入 8.85 亿元、11.06 亿元、13.82 亿元。预计安全集成与服务业务 2020-2022 年收入同比增长 23.02%、35%、35%，对应收入 15.25 亿元、20.59 亿元、27.80 亿元。

2）**长期:** 根据 IDC 预测，2024 年中国网络安全市场总体支出将达到 179 亿美元，对应 1152 亿人民币，公司在技术、资质、团队等核心竞争优势明显，目前正在积极从加密领域龙头转型为综合型安全产品与服务厂商。作为信息安全国家队，央企股东背景体现国家意志，从加密进入泛网安领域，有望打开更大的增长空间。

图 27：营收拆分与预测（单位：亿元）

	2016	2017	2018	2019	2019H1	2020H1	2020	2021	2022
营业总收入	17.99	21.37	19.31	21.04	6.12	4.33	24.10	31.65	41.62
yoy		18.79%	-9.64%	8.96%		-29.25%	14.55%	31.33%	31.51%
安全集成与服务	8.51	10.45	10.08	12.40	3.84	2.73	15.25	20.59	27.80
yoy		22.80%	-3.54%	23.02%		-28.91%	23.02%	35.00%	35.00%
单机和系统产品	9.07	10.93	9.23	8.64	2.28	1.61	8.85	11.06	13.82
yoy		20.51%	-15.55%	-6.39%		-29.39%	2.39%	25.00%	25.00%
其他主营业务	0.41								
营业成本	11.65	13.83	12.55	14.19	4.36	2.85	15.89	21.10	28.07
安全集成与服务	7.31	8.83	8.83	10.41	3.34	2.23	12.48	16.85	22.75
单机和系统产品	4.01	5.00	3.72	3.78	1.02	0.62	3.40	4.26	5.32
其他主营业务	0.33								
毛利	6.34	7.54	6.76	6.85	1.76	1.48	8.22	10.55	13.56
安全集成与服务	1.21	1.62	1.25	1.99	0.50	0.50	2.77	3.74	5.05
单机和系统产品	5.06	5.93	5.51	4.86	1.26	0.99	5.44	6.80	8.50
其他主营业务	0.07								
毛利率(%)	35.25	35.30	35.01	32.54	28.79	34.24	34.09	33.32	32.57
安全集成与服务	14.17	15.49	12.40	16.02	13.08	18.18	18.18	18.18	18.18
单机和系统产品	55.80	54.24	59.72	56.26	55.25	61.52	61.52	61.52	61.52
其他主营业务	18.24								

数据来源：Wind，东吴证券研究所

盈利预测：2020-2022 年公司营收分别为 24.10、31.65、41.62 亿元，增速分别为 14.55%、31.33%、31.51%；归母净利润分别为 1.81、2.14、2.52 亿元，增速分别为 15.93%、18.67%、17.68%，EPS 分别为 0.21、0.25、0.30 元，对应 PE 分别为 74、63、53 倍。

估值及投资建议：公司作为国内信息安全领域的国家队，深耕密码技术，并围绕加密实现全产业链布局。随着中国电科对网络安全的战略地位的重视，全面加快向安全服务转型，公司作为电科集团旗下唯一的信息安全平台，未来有望持续获得集团的资源对接和大力扶持；同时根据我们紧密跟踪行业和公司的情况，在《密码法》等政策加速落地的情况下，行业景气度逐渐抬升，我们判断无论是行业还是公司，基本面均发生了极为明显的边际变化，强烈建议关注，给予“买入”评级。

表 9：公司与 A 股部分信息安全行业标的的估值比较（截止 2021 年 2 月 9 日）

公司	净利润（亿元）			PE		
	2020 E	2021E	2022 E	2020 E	2021 E	2022 E
卫士通	1.81	2.14	2.52	74	63	53
中孚信息	2.24	3.36	4.41	36	24	18
格尔软件	1.04	1.54	2.04	33	22	17

数据来源：中孚信息盈利预测来自于 Wind 一致预期，东吴证券研究所

5. 风险提示

1）商业密码放管服推行后，行业竞争加剧造成产品价格和毛利率持续下降；商业密码推广不达预期;

2）疫情影响使得下游金融、工业、能源行业的盈利能力下降、需求释放不达预期;

3）党政机关国产替代和自主化的进程不达预期，在采购过程中订单释放和盈利水平不达预期;

4）应收账款持续增长带来了形成坏账的风险。

卫士通三大财务预测表

资产负债表（百万元）	2019A	2020E	2021E	2022E
流动资产	4,090	4,442	4,845	6,080
现金	1,500	1,341	506	666
应收账款	1,520	2,194	2,683	3,731
存货	291	381	511	676
其他流动资产	780	525	1,144	1,007
非流动资产	1,867	2,030	2,515	3,121
长期股权投资	29	29	29	29
固定资产	310	583	927	1,322
在建工程	1,177	1,056	1,184	1,384
无形资产	195	206	220	230
其他非流动资产	156	156	155	155
资产总计	5,957	6,471	7,360	9,200
流动负债	1,315	1,652	2,342	3,943
短期借款	0	0	112	1,070
应付账款	957	1,281	1,692	2,261
其他流动负债	358	372	538	612
非流动负债	39	48	57	65
长期借款	0	9	18	26
其他非流动负债	39	39	39	39
负债合计	1,354	1,701	2,400	4,008
少数股东权益	52	55	59	64
归属母公司股东权益	4,551	4,715	4,901	5,128
负债和股东权益	5,957	6,471	7,360	9,200

现金流量表（百万元）	2019A	2020E	2021E	2022E
经营活动现金流	-98	61	-359	-47
投资活动现金流	-84	-225	-579	-741
筹资活动现金流	-262	5	104	947
现金净增加额	-443	-159	-834	160
折旧和摊销	55	62	94	135
资本开支	84	163	485	606
营运资本变动	-337	-174	-661	-433

利润表（百万元）	2019A	2020E	2021E	2022E
营业收入	2,104	2,410	3,165	4,162
减:营业成本	1,419	1,588	2,110	2,806
营业税金及附加	13	12	16	21
营业费用	249	289	380	500
管理费用	141	381	501	659
财务费用	-29	-11	-11	-6
资产减值损失	-8	0	0	0
加:投资净收益	-3	0	0	0
其他收益	0	0	0	0
营业利润	148	190	225	265
加:营业外净收支	5	0	0	0
利润总额	153	190	225	265
减:所得税费用	-6	6	7	8
少数股东损益	3	3	4	5
归属母公司净利润	156	180	214	252
EBIT	108	147	202	285
EBITDA	163	209	296	419

重要财务与估值指标	2019A	2020E	2021E	2022E
每股收益(元)	0.19	0.21	0.25	0.30
每股净资产(元)	5.38	5.58	5.80	6.07
发行在外股份(百万股)	838	846	846	846
ROIC(%)	2.4%	3.0%	3.8%	4.4%
ROE(%)	3.5%	3.9%	4.4%	4.9%
毛利率(%)	32.5%	34.1%	33.3%	32.6%
销售净利率(%)	7.4%	7.5%	6.8%	6.1%
资产负债率(%)	22.7%	26.2%	32.5%	43.5%
收入增长率(%)	8.9%	14.55%	31.33%	31.51%
净利润增长率(%)	29.6%	15.93%	18.67%	17.68%
P/E	85	74	63	53
P/B	2.95	2.84	2.73	2.61
EV/EBITDA	73.76	58.10	44.36	33.27

数据来源：贝格数据，东吴证券研究所

免责声明

东吴证券股份有限公司经中国证券监督管理委员会批准，已具备证券投资咨询业务资格。

本研究报告仅供东吴证券股份有限公司（以下简称“本公司”）的客户使用。本公司不会因接收人收到本报告而视其为客户。在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议，本公司不对任何人因使用本报告中的内容所导致的损失负任何责任。在法律许可的情况下，东吴证券及其所属关联机构可能会持有报告中提到的公司所发行的证券并进行交易，还可能为这些公司提供投资银行服务或其他服务。

市场有风险，投资需谨慎。本报告是基于本公司分析师认为可靠且已公开的信息，本公司力求但不保证这些信息的准确性和完整性，也不保证文中观点或陈述不会发生任何变更，在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。

东吴证券投资评级标准:

公司投资评级:

买入：预期未来 6 个月个股涨跌幅相对大盘在 15%以上;

增持：预期未来 6 个月个股涨跌幅相对大盘介于 5%与 15%之间;

中性：预期未来 6 个月个股涨跌幅相对大盘介于-5%与 5%之间;

减持：预期未来 6 个月个股涨跌幅相对大盘介于-15%与-5%之间;

卖出：预期未来 6 个月个股涨跌幅相对大盘在-15%以下。

行业投资评级:

增持： 预期未来 6 个月内，行业指数相对强于大盘 5%以上;

中性： 预期未来 6 个月内，行业指数相对大盘-5%与 5%;

减持： 预期未来 6 个月内，行业指数相对弱于大盘 5%以上。

东吴证券研究所
苏州工业园区星阳街 5 号
邮政编码：215021
传真：（0512）62938527
公司网址： http://www.dwzq.com.cN