东兴证券 DONGXING SECURITIES

信息安全解决方案提供商，成长潜力大

——蓝盾股份(300297)深度报告

2018 年 6 月 15 日

强烈推荐/首次

蓝盾股份 | 深度报告

杨若木 分析师

010-66554032 yangrm@dxzq.net.cn

执业证书编号: S1480510120014

韩宇 研究助理

010-66554131 hanyu@dxzq.net.cn

交易数据

上市以来股价区间（元）	8.12-76.00
总市值（亿元）	98.50
流通市值（亿元）	62.61
总股本/流通股（万股）	117537/74174

股价走势图

资料来源：东兴证券研究所，前复权

报告摘要：

产品+集成信息安全全方位解决方案提供商，2017 年实现营收 22.16 亿元、净利润 4.41 亿元。**增长强势，2013 年至 2017 年营收 CAGR 为 53.9%、净利润 CAGR 为 92.8%。**

安全行业大变革，具有产品能力的信息安全集成厂商迎来发展机遇。

- 安全变革趋势下，**更加要求信息安全系统的建设者具有深厚的安全研究积淀、较强的系统安全构建能力与对安全产品的深刻洞察**，产品+集成商业模式凸显特色竞争优势。
- 随着攻防态势演变，传统的依靠边界防护+终端管理+安全态势感知（SOC）三种产品堆砌的防护思路并不能保障用户的安全，**在设计系统时需要考虑系统在应用场景上的实际特点、安全产品的协同联动、系统针对未知威胁的影响能力与策略，这些都需要大量深入的安全知识**，因此在系统规划设计部署落地的阶段，**安全的能力和从业的经验将凸显其重要性**，具有安全产品生产经验的系统集成厂商竞争性将凸显。对于这些厂商来说，其系统集成业务的营收与毛利率有望出现双重增长。

从财务数据来看，（仅考虑产品线较全的综合型厂商）安全产品厂商近年毛利率一般为 65%左右，销售费用、管理费用在 25%左右，在不考虑财务费用的前提下，扣除费用因素之后还剩 10-15%；蓝盾股份近两年毛利率在 52%左右，扣除销售费用(6%)、管理费用(17%)之后还剩 29%。**由此可见采用产品+集成商业模式的蓝盾股份，在考虑费用因素的视角下，其业务盈利水平优势较为明显。**

目前产品+集成商业模式在大多数信息安全上市公司中不多见，蓝盾是具有特色的产品+集成信息安全解决方案提供商。我们预计公司零售业务板块在 2018 年的净利润约为 2.1 亿元，此业务以 25 倍估值测算，对应 52.5 亿元市值；此外安全以及安防板块贡献归母净利润约为 3.4 亿元，此业务以 35 倍估值测算，对应 119 亿元市值。**综上，分块测算加总，公司目标市值为 171.5 亿元，每股目标价为 14.59 元。**

给予“强烈推荐”评级。

风险提示：公司可转债发行存在不确定性；公司应收账款占比大。

财务指标预测

指标	2016A	2017A	2018E	2019E	2020E
营业收入（百万元）	1,573.50	2,216.48	2,723.94	3,370.44	4,196.28
净利润（百万元）	323.86	441.31	587.39	738.20	930.74
增长率（%）	165.84%	36.27%	33.10%	25.67%	26.08%
净资产收益率（%）	9.04%	10.39%	12.14%	13.38%	14.69%
每股收益(元)	0.30	0.35	0.47	0.59	0.74
PE	27.93	23.94	17.93	14.31	11.31
PB	2.76	2.47	2.18	1.91	1.66

资料来源：公司财报、东兴证券研究所。本报告股价采用前一收盘日数据。

目 录

表格目录

插图目录

1. 产品加集成特色商业模式的信息安全厂商

1.1 信息安全+安防综合解决方案提供商

1.1.1 近年业绩增长迅速

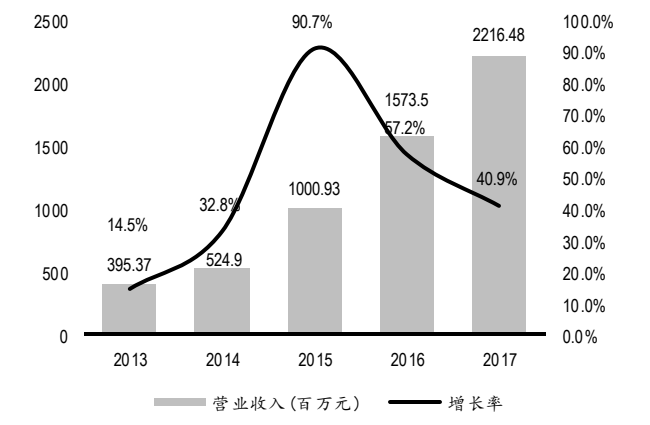
公司是采用集成+产品业务模式的信息安全、安防综合解决方案提供商，瞄准信息安全外延不断扩大的趋势，通过“自主研发+投资并购”双轮驱动的方式，持续推进“大安全”产业发展战略，并以**“技术升级”、“空间拓展”、“IT 层级突破”**三个维度为主线进行布局，构建了完整的“大安全”产业生态版图。

图 1：蓝盾大安全概念版图

资料来源：公司资料，东兴证券研究所

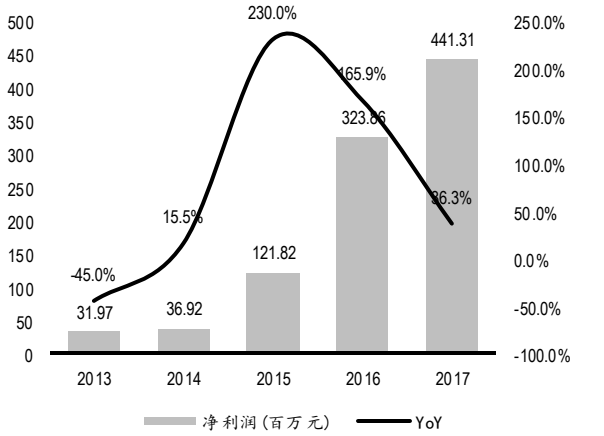
近年业绩增长迅速。公司 2017 年实现营业收入 22.16 亿元、净利润 4.41 亿元。2013-2017 年间营收 CAGR 为 53.9%，净利润 CAGR 为 92.8%。

图 2：蓝度股份近年业绩情况：营收



资料来源：公开资料，东兴证券研究所

图 3：蓝度股份安近年业绩情况：净利润

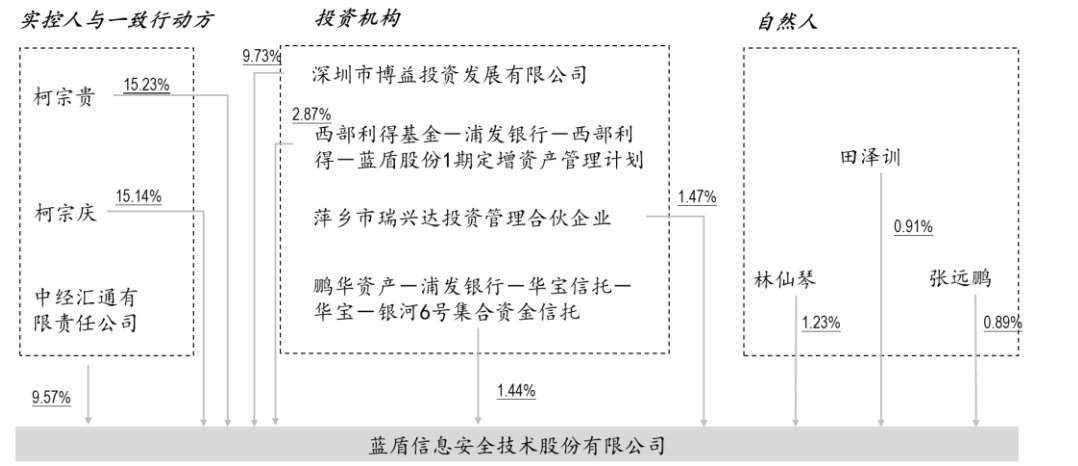


资料来源：公开资料，东兴证券研究所

1.1.2 柯宗贵、柯宗庆兄弟为实控人

公司实际控制人为柯宗贵、柯宗庆兄弟，分别控股 15.23%、15.14%；两位与中经汇通为一致行动人，中经汇通实际控制人为柯宗耀，其与柯宗贵、柯宗庆为兄弟关系。

图 4：蓝盾股份十大股东，2017



资料来源：公开资料，东兴证券研究所

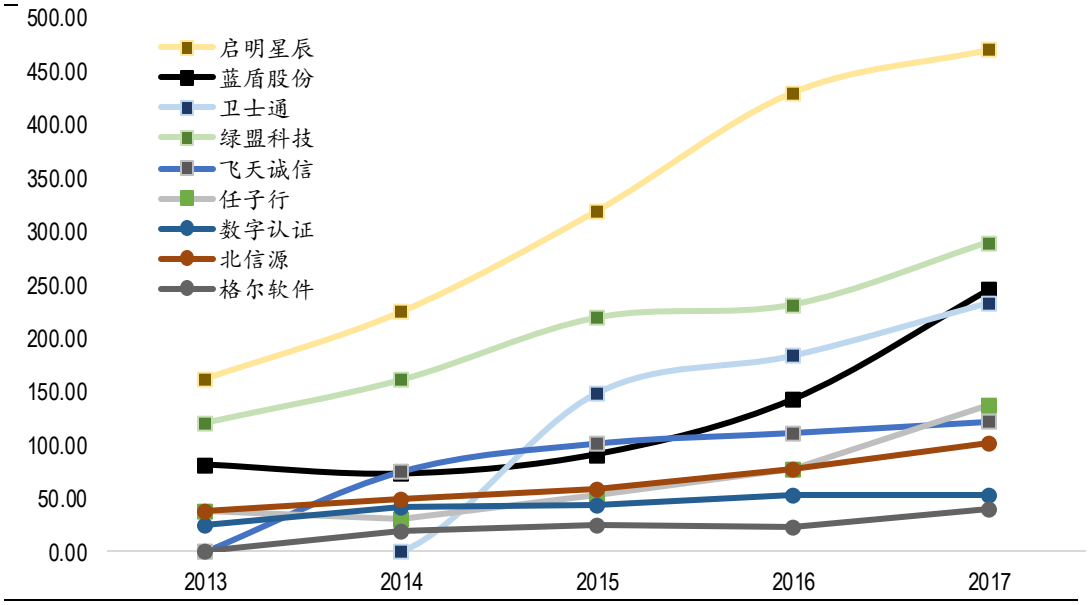
1.1.3 研发投入大、布局云安全、AI 智能防护

研发投入大。2017 年研发支出 2.45 亿元，在安全厂商中排名靠前，研发人员占比较多。**布局云安全防护、人工智能强化安全等新兴方向。**

- **云安全。**云安全方面具备一定先发优势，形成包括虚拟防火墙、虚拟 SOC、虚拟堡垒机、虚拟网页防篡改、虚拟漏扫、虚拟 WAF、虚拟上网行为审计、虚拟数据库审计的八大关键安全产品虚拟化。

- **人工智能强化安全。**1)**网关，在云端做 AI 分析。**通过云端机器学习威胁模型训练与内置在网关设备上的 AI 智能引擎联动的模式，解决了 AI 技术在网关应用的性能瓶颈。2)**SOC，人工智能攻击分析。**3)**终端安全**，在蓝盾安全卫士上利用 AI 对 **APP 进行威胁分析。**4)安全云平台，AI 能力+开放云平台，对未知文件进行检测。

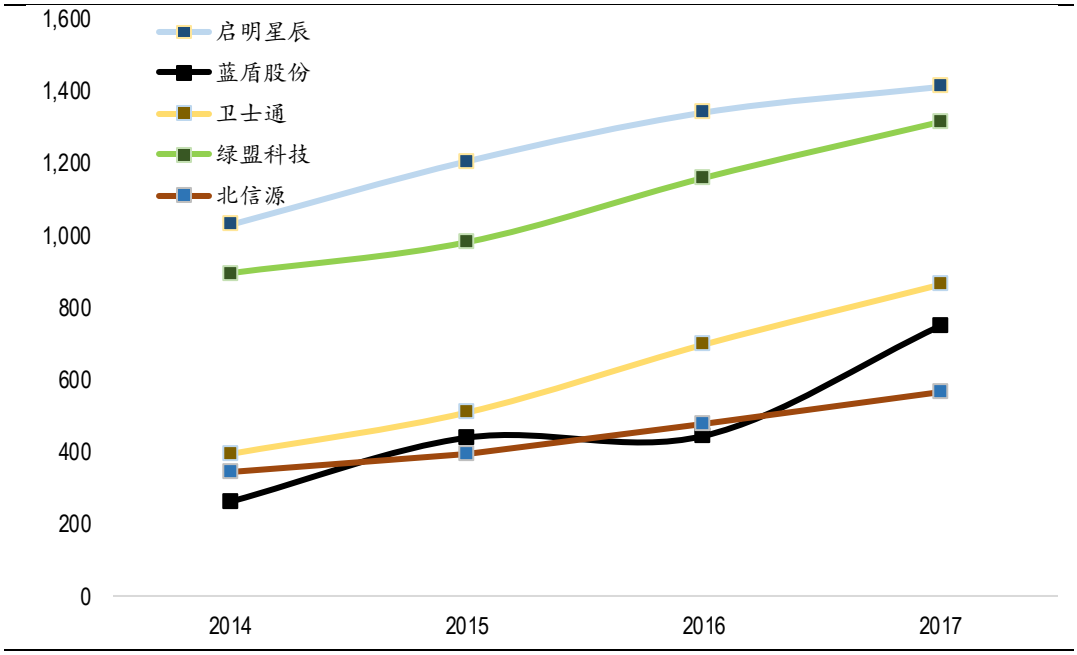
图 5：蓝盾股份研发费用（单位：百万元）以及其与信息安全标的对比



资料来源：公开资料，东兴证券研究所

蓝盾股份目前研发人员 750 人，靠近卫士通，与启明星辰、绿盟科技尚存一定差距。

图 6：蓝盾股份技术（含研发）人员以及其与信息安全标的对比

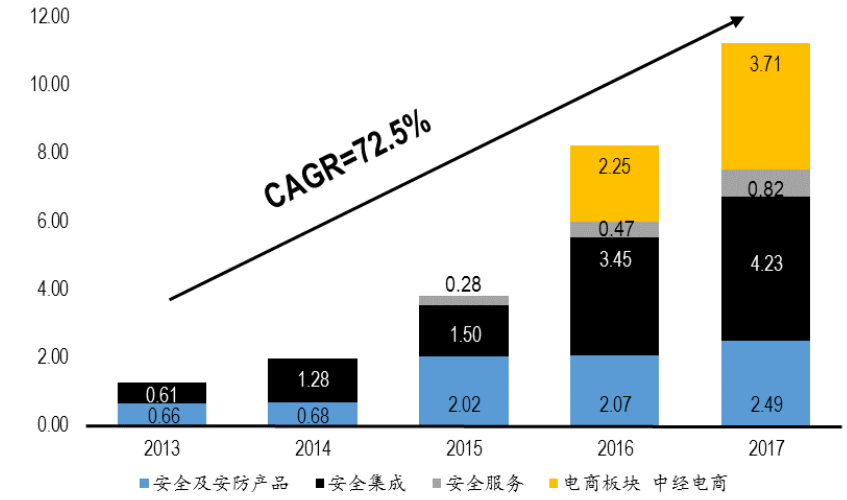


资料来源：公开资料，东兴证券研究所

1.2 安全以及安防集成+电商业务驱动公司业绩明显提升

产品+集成业务策略在近年成效凸显，集成业务模块毛利率稳步上升。近年毛利主要由安全以及安防集成、电商板块、安全以及安防服务三个板块贡献。

图 7：蓝盾股份近年各业务板块贡献毛利情况



资料来源：公开资料，东兴证券研究所

安全以及安防集成 2013 年-2017 年营收 CAGR 为 38.2%。近年伴随用户信息安全意识的增强以及网络安全法的推动，**蓝盾股份产品+服务特色解决方案商业模式竞争优势凸显，毛利率水平近年有所提升，近两年约为 40%-42%。**

安全与安防产品自 2013 年-2017 年营收 CAGR 为 57.9%，毛利率近三年在 55%-63%之间波动，自 2015 年以来，**安全产品营收的快速增长主要来自于公司在安全与安防领域的业务布局，先后并购华炜科技（信息安全物理防护领域，2017 年营收 3.00 亿元，净利润 6467 万元）、满泰科技（工控系统领域，2017 年营收 2.26 亿元，净利润 7360 万元）。**

安全以及安防服务 2015 年-2017 年营收 CAGR 为 78.3%，近年毛利率水平在 50%以上。

电商业务板块（包括公司收购的中经电商以及汇通宝）今年业绩增长稳健，2017 年实现扣除非经常损益以及借款资金使用成本（1.5 亿，来自上市公司）后净利润 1.84 亿元，CAGR 为 23.3%。

图 8：蓝度股份安全以及安防产品近年业绩情况（单位：亿元）

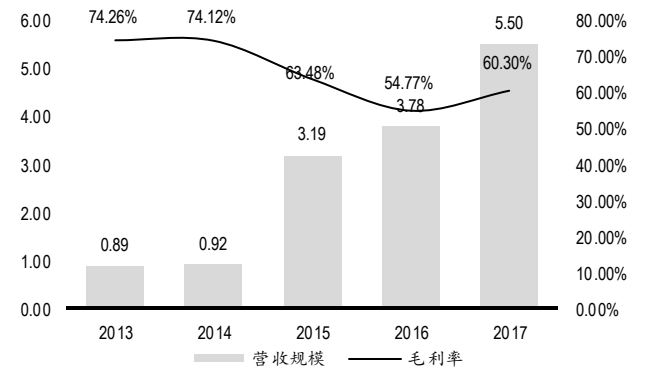
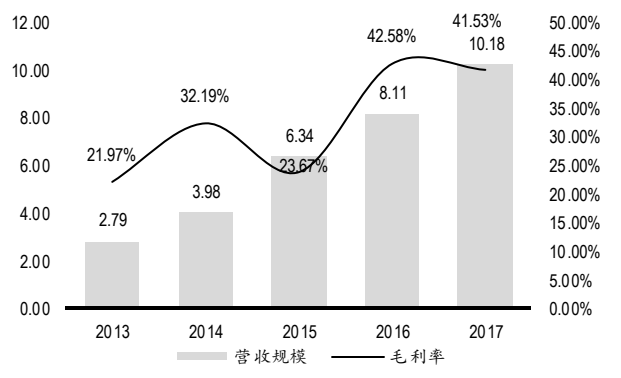
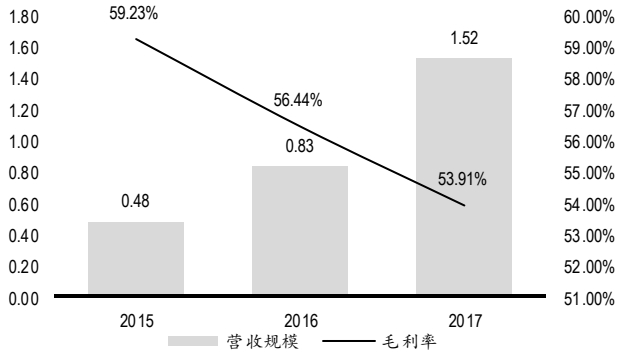


图 9：蓝度股份安全系统集成近年业绩情况（单位：亿元）



资料来源：公开资料，东兴证券研究所

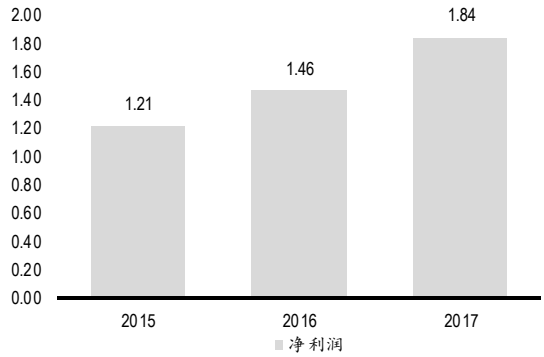
图 10：蓝盾股份安全以及安防服务近年业绩情况（单位：亿元）



资料来源：公开资料，东兴证券研究所

资料来源：公开资料，东兴证券研究所

图 11：电商业务板块业绩*情况（单位：亿元）



资料来源：公开资料，东兴证券研究所。包括中经电商与汇通宝两家公司；扣除非经常损益以及上市公司 1.5 亿元借款资金使用成本后的结果。

蓝盾股份近年并购情况以及业绩承诺：

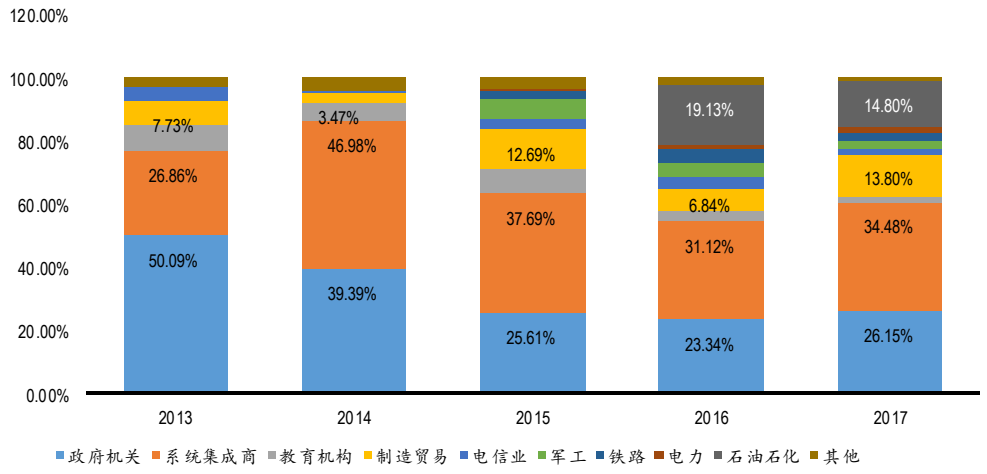
- 电磁安防方向，华炜科技，**承诺 2014-2017 年实现 2800 万元、3600 万元、4500 万元业绩。2017 年业绩承诺已达成；业绩承诺期已过。**
- 工控方向，满泰科技。承诺 2016-2019 年实现 5500 万元、7100 万元、4500 万元、业绩。2017 年实现 7360 万元净利润，达成业绩承诺。
- 零售方向，中经电商以及汇通宝。承诺两家公司累计在 2015-2018 年实现 1 亿、1.3 亿、1.69 亿、2.04 亿元净利润（扣除非经常损益以及向上市公司借款 1.5 亿的资金成本），**2017 年实际实现 1.84 亿元净利润，超额完成业绩承诺。**

2018 年 Q1 业绩强劲增长。据公司披露，**2018 年第一季度实现营收 5.31 亿元、归母净利润 6380 万元，同比增长 55.9%/12.2%。**收入水平强势上升主要来自于网络安全法实施对于行业增长的驱动以及公司自身业务的拓展。

从近年业务发展情况来看，以前业务集中在政府行业（2012 年，50.09%）、华南地区（2012 年，90.70%）的趋势有明显改变。

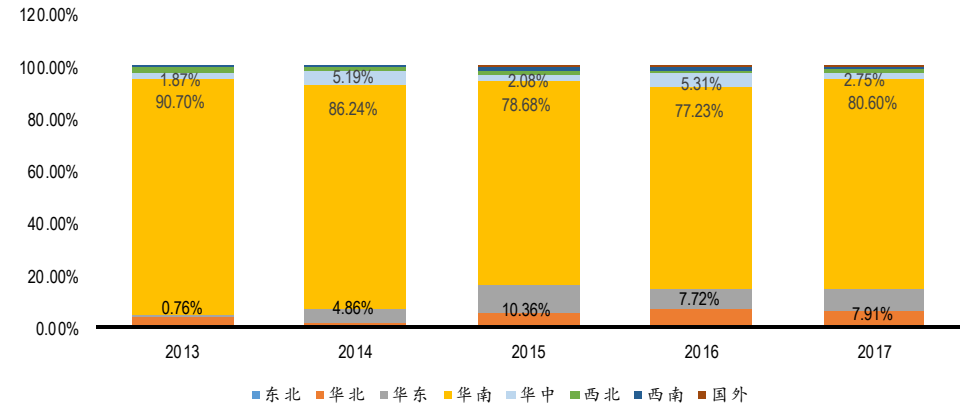
- 行业占比方面，政府机关占比从 2013 年的 50.09%下降到 2017 年的 26.15%；与此同时，系统集成商的营收占比从 26.86%上升到 34.48%。2017 年石油石化行业、制造贸易行业营收占比分别为 14.80%与 13.80%。
- 地区分布方面，华南地区营收占比从 2013 年的 90.70%下降到 2017 年的 80.60%，2017 年华东、华北、华中地区营收占比分别为 7.91%、6.17%和 2.75%。

图 12：蓝盾股份分行业营收分布



资料来源：公开资料，东兴证券研究所

图 13：蓝盾股份分地区营收分布



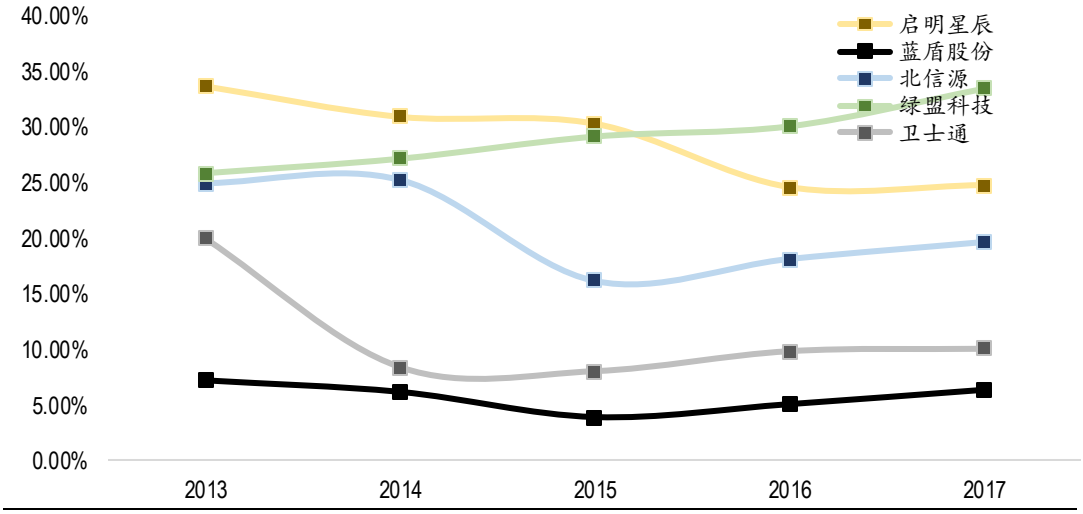
资料来源：公开资料，东兴证券研究所

1.3 信息安全产品+集成特色商业模式具有突出优势

1.3.1 信息安全厂商销售费用率高

信息安全产品厂商销售费用率非常高：即使考虑了本身行业的高毛利之后，销售费率也依然很高，具体可见信息技术行业销售费用率比毛利率图，2017 年中位数是 16.8%，启明 38.1%，绿盟 47.0%，卫士通 30.2%。

图 14：蓝盾股份销售费用率以及其与信息安全标的对比



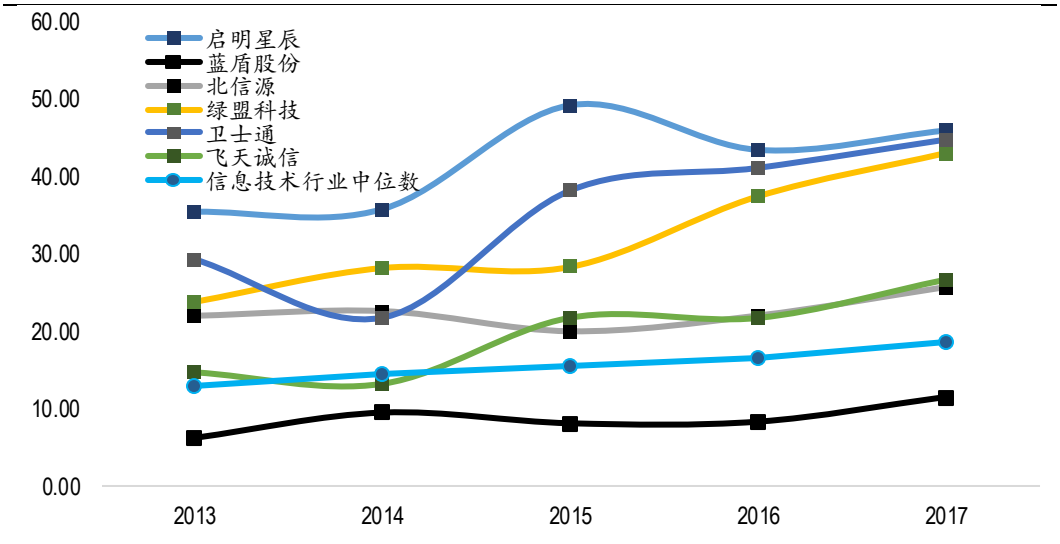
资料来源：公开资料，东兴证券研究所

原因主要包括：

1.行业竞争激烈。且对于用户而言，**信息安全的价值较难直观感受，因此各大安全产品厂商倾向于以较高的薪酬雇佣对于甲方信息系统架构、特点具有深刻了解和认识的人员进行销售，这些人员往往具有一定行业从业经验并且对技术、系统有所了解。**

从下图可以明显看到，信息安全产品企业销售人员人均薪酬较高，**启明星辰、卫士通、绿盟三个公司人均销售薪酬 45.86 万元、44.68 万元、42.93 万元，显著高于信息技术行业企业中位数 18.47 万元。**

图 15：信息安全行业销售人员人均薪酬



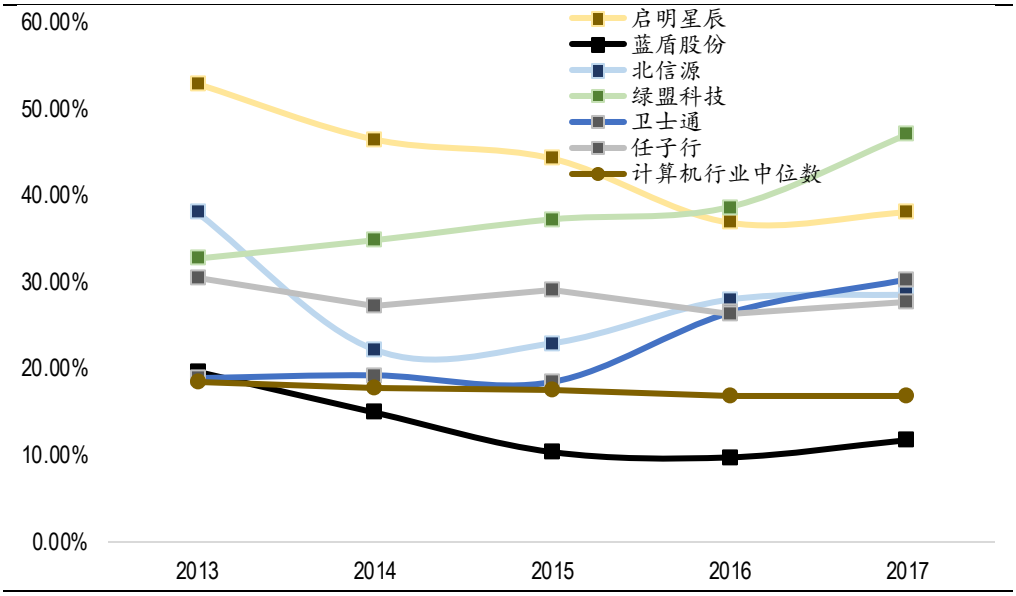
料来源：公开资料，东兴证券研究所

2.安全产品涉及到攻防且架构在用户已经成熟的信息系统上，在售前、测试、交付工作量大。和其他计算机产品不同的是，信息安全产品需要整合进用户的网络系统、业务系统当中，产品的安装调试、整合维护需要的专业性强，且安全产品紧贴 IT 产业发展实际需求，技术更新快。**在售前，需要对用户的信息系统和目前的安全态势进行**

详细的分析；在产品测试阶段，需要有我方人员参与对产品性能在客户侧进行实地验证；在产品交付环节，需要有大量的调试工作，这些对销售的专业技术能力、组织沟通协调项目管理能力提出的较高要求。

3.行业处于快速成长期，公司采取较高的激励水平促使销售开拓新市场、新客户。信息安全近年维持在 20%以上增速，是计算机板块中极少数能够兼具高成长、高毛利、高壁垒的行业。

图 16：信息安全厂商销售费用率与毛利率比值



资料来源：公开资料，东兴证券研究所

1.3.2 蓝盾股份解决方案商业模式使销售费用率明显低于其他信息安全厂商

采用安全产品+系统集成的解决方案业务模式，有效降低了销售费用率。

信息安全解决方案业务模式：以信息安全集成业务在用户信息系统构建的早期介入，**参与用户信息系统的规划设计、部署、实施、运维。**在系统集成组建中涉及到信息安全的，可以采用自己的信息安全产品（**注意包含在集成项目中的信息安全产品销售业绩是归属到集成业务板块的，并未归并到安全产品部分，依照毛利率水平测算，这部分安全产品销售的金额大约占集成整体的 30%-40%**），**从而实现了以系统集成业务带动安全产品的销售。**

产品+集成解决方案特色竞争优势在于：

- **用安全能力提升集成业务竞争优势，**在网络安全法实施大背景下，用户处于合规以及自身业务稳定运营的诉求会逐步提高对于安全价值的重视，**蓝盾是集成商里面最懂安全的厂商。**
- 用**集成业务带动安全产品销售，有效降低了安全产品的销售费用率。**一般而言，安全产品厂商的销售费用率在 20%-35%区间；参考华胜天成，系统集成厂商典型销售费用在 5%-10%之间。公司的系统集成业务为行业客户提供完整的解决方案，可以在早期参与用户信息系统的建设，从而培育用户粘性，为后续提供高附加值的信息安全产品、信息安全解决方案建设提供便利。**蓝盾股份历年销售费用率较低，控**

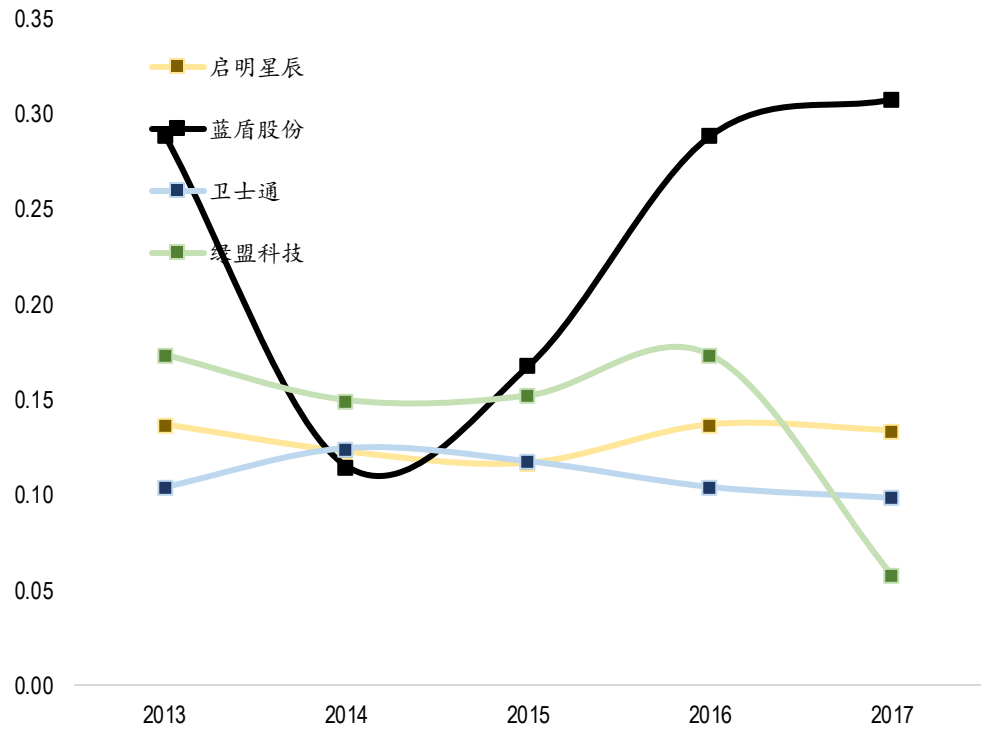
制在 3%-7%之间，显著低于启明星辰、绿盟科技等厂商。

产品+集成解决方案是蓝盾的特色优势、友商难以模仿。传统安全厂商会有相当一部分产品**通过渠道销售或者销售给系统集成商，在业务上形成相互依存的关系**，因此**不会过多涉及系统集成类业务（此部分业务利益留给合作方），也缺乏转型动力（自己产品毛利足够高），**目前看，安全 A 股二级市场上市公司中，蓝盾股份业务模式具有特色优势（卫士通也有大量集成，但是业务的重点是涉密业务，且集成毛利率较低）。

1.3.3 从毛利减管理、销售费用率视角看，蓝盾股份优势突出

从财务数据来看，（仅考虑产品线较全的综合型厂商）安全产品厂商近年毛利率一般为 65%左右，销售费用、管理费用也在 25%左右，**在不考虑财务费用的前提下，扣除费用因素之后还剩 10-15%**；蓝盾股份近两年毛利率在 52%左右，**扣除销售费用(6%)、管理费用(17%)之后还剩 29%。由此可见采用产品+集成商业模式的蓝盾股份，在考虑费用因素的视角下，其业务盈利水平优势较为明显。**

图 17：蓝盾股份与安全厂商比较分析：毛利率减管理/销售费用率



资料来源：公开资料，东兴证券研究所

2. 大变革拉开序幕，信息安全集成商迎来机遇

2.1 严峻的网络威胁态势催生信息安全产业加速变革

2.1.1 异常严峻的全球网络安全态势引起各国政府高度关注

从棱镜门到邮件门，全球网络安全高危事件不断引发社会高度关注。网络空间不太平，大规模敏感数据泄露、网络服务中断、政府机构内部网络遭遇入侵等事件频频引发社会各界的高度关注，

网络空间安全形势严峻。近年以来，我国政府和企业不断重视并加强信息安全保障，但网络空间安全形势依然严峻，重大安全事件仍然频发，呈现一些典型特征：

- **APT(advanced persistent threat，高危可持续)攻击频发，重点威胁国家级重要信息系统和关键基础设施。**例如于 2015 年 5 月被 360 公司"天眼实验室"发布报告曝光的专门攻击中国政府的境外黑客组织"海莲花"。2016 年德国核电站、叙利亚政府、乌克兰电网、希腊银行等都遭到了黑客攻击。
- **随着生产生活对于信息技术依赖提升，信息安全事件带来的社会影响日趋显著。**近期，Wannacry 勒索病毒大规模爆发，全球超过 150 个国家遭受攻击，其中包括快递巨头 FedEx、英国医疗系统、俄罗斯电信企业以及我国高校与能源企业，部分程度上扰乱了正常的生产生活秩序。
- **网络黑产发展迅速，规模惊人。**例如 2016 年的以徐玉玉因数据泄露遭电信诈骗为典型的多起电信诈骗事件。我国网络黑产发展速度极快，**已经呈现跨平台、跨行业的集团犯罪趋势**。据 360，黑产从业人员早已越过 150 万大关，黑产市场规模已经达到千亿级别，给人民的生活和工作带来很大的不利影响。
- **网络攻击方式不断创新和升级。**2015 年 9 月的苹果 Xcode 开发链被污染事件并没有采用传统恶意代码传播的方式，而是利用非官方供应链（工具链）进行污染，导致苹果应用商店超过 3000 个应用被感染，微信、铁路 12306、滴滴出行、高德地图、网易云音乐乃至部分银行手机应用都受到了影响。全新的网络攻击形态，已经引起云平台运营者和主管部门的高度重视。

整体信息安全行业保持高速增长。"十三五"规划将"国家网络空间安全"列为重大信息工程。受益于政府政策的大力支持，信息安全行业的发展有个很好的契机。据推测，"十三五"期间，信息安全行业将呈现快速增长趋势，增长速度将近 30%。另一方面，网民数量规模的快速增加，对信息安全的需求也会增加，从而更加支持行业的高速发展。

2.1.2 信息安全已上升到国家战略安全层面

高层引领，国家级部署动作频出，信息安全已上升到国家战略安全层面。网络安全的严峻态势使得各国制定新的政策，以尽可能地减少信息安全威胁。我国于 2016 年 11 月 7 日发布了《中华人民共和国网络安全法》，其他国家也纷纷采取措施，如美国已成立军事化的网络攻击组织。

表 1：2015-2017 年各国信息安全政策颁布

时间	介绍
2017.7.1	我国网络安全法正式实施。
2016.11.7	中国全国人民代表大会常务委员会发布《中华人民共和国网络安全法》。
2016.3.25	美国海军陆战队成立新网络安全部门，开展网络空间防御行动。

2016.2.9	奥巴马公布《网络安全国家行动计划》，将从提升网络基础设施水平、加强专业人才队伍建设、增进与企业的合作等五个方面入手，全面提高美国在数字空间的安全。
2015.12.28	美国国会通过了《2015 网络安全信息分享法案》。
2015.6	第十二届全国人大常委会第十五次会议初次审议了《中华人民共和国网络安全法（草案）》。

资料来源：互联网资料、东兴证券研究所

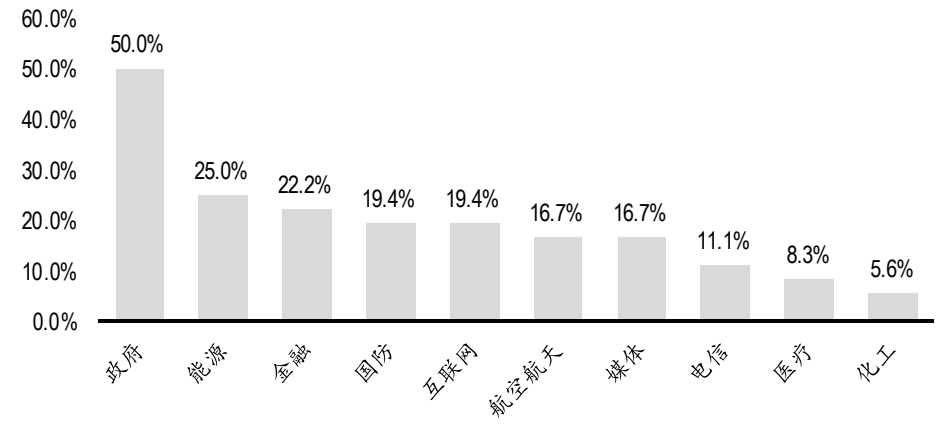
2.1.3 传统的壁垒式防护体系在先进的攻击手法面前不堪一击

当前，我国安全市场上占据主导地位的仍然是以防火墙/VPN、IDS/IPS、终端防护管理、SOC 等产品，但是面对新的信息安全威胁仍然采用之前的“堡垒式”防护体系的安全保护思路已经难以适应时代，信息安全正在带来日益严峻的挑战，包括：

- **高度组织化的黑客攻击行为**。目前已经有了成熟、完整且庞大的黑色产业链，与传统意义上黑客出于兴趣或名声从事攻击行为不同，现在很多造成巨大威胁的组织团体以窃取有价值的数据或商业机密为主要目的，甚至背后有政府的支持。**高度组织化的攻击往往具有目标明确、技巧高超、难于发现与追踪的特点，使得受攻击者在难以察觉的前提下泄露大量核心机要，带来的损失难以估量。**
- **APT 攻击显著增长**。近年网络攻击大量的利用了 0-day/1-day 漏洞的（业界一般将已经公布但尚无官方补丁漏洞叫 0-day 漏洞，已有官方补丁但是其公布时间较短、用户尚未广泛应用补丁进行安全防范的漏洞叫作 1-day 漏洞）。**对于这些基于高级别漏洞的攻击，传统的全面化解决方案试图通过多种安全产品搭建“堡垒式”保护罩的思路显得不堪一击。**

我国是 APT 攻击的重点受害国。据 360，截至 2016 年底，已累计有超过 36 个组织对我国境内目标发起 APT 攻击，重点关注大学、企业、政府以及事业单位等。

图 18：2017 全球 APT 组织关注领域情况



资料来源：360，东兴证券研究所

2.2 专精化防护+安全产品协同联动是新方向

全面化防护的思路是以完整的结构来抵御攻击。但面对层出不穷的新的攻击手法与高度组织化的黑客行为，**全面化防护思路应该向专精化转变。**

- **防护思路从全面化向专精化的转变。**全面化防护思路更像是构建堡垒，力求以看上去完整的结构来抵御攻击，**但是新的攻击手法涌现与高度组织化的黑客行为，使得构建纯净的内部网络的愿望成为“乌托邦”似的幻想。**安全从业者不得不面对并接收这样一个事实：**内网并不安全，攻击或许已经发生。因而，对于数据等核心业务资产的保护就成了现阶段的当务之急，**数据库安全防护、数据防泄漏、文档加密是专精化安全时代安全产品的代表。

- **安全产品高度协同化的趋势。**应对新兴威胁的另一个重要手段就是协同，通过防火墙、终端、IPS/IDS 之间高度的信息共享，通过大数据分析手段、结合威胁情报，发现可能存在的安全隐患。

- **自适应安全。**概念由 Gartner 提出，自适应安全强调检测、响应和预测的能力；安全策略贯穿防护、检测响应和预测四个阶段。

专精化防护聚焦信息系统内部重要的数据以及核心业务，其涵盖的概念包括：

- **数据安全。**对于以文档形式存储的数据，采用 DLP(data leakage prevention，数据防泄漏)或文档加密的方式防护；对于在数据储存的数据，采用响应的数据库审计与防护方案。

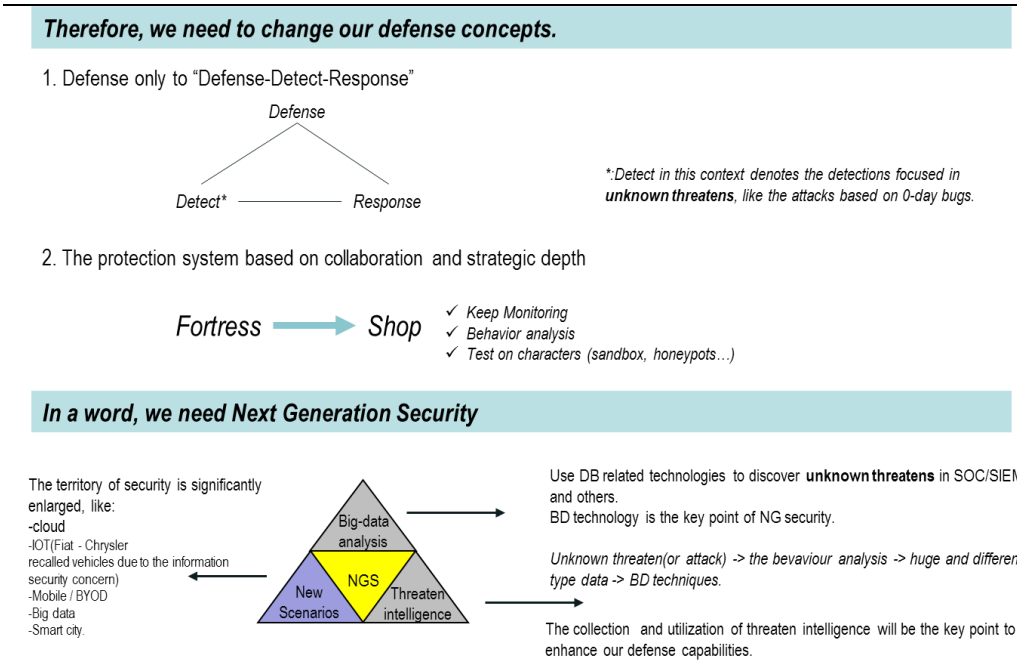
- **核心业务安全。**具体包括金融反欺诈、网页安全防护等。

安全产品协同联动是防范 APT 攻击的重要抓手。参考《中国大数据安全分析市场白皮书》(2016 版，亦由作者撰写)：

- **攻击手法的不断演进，结合利用鱼叉、水坑、0-day 漏洞、n-day 漏洞、社会工程学等未知威胁进行的攻击层出不穷。**面对这种组织更加精细、策划更加周密的网络攻击，**传统的点对点防御理念和堡垒式安全防御体系的应对能力日益不足，**难以及时发现并有效抵御此类攻击，缺乏快速响应机制和数据分析能力使得传统防御手段开始漏洞百出。例如，在网关安全上，对于攻击数据流加解密缺乏有效的检测与防御方法；在终端安全上，对于基于 0day 漏洞、高度定制化的恶意应用缺乏有效的查杀手段。

- 产品协同联动+大数据安全分析是解决之道。面对复杂的网络安全局面，业界的安全防护思路从以防为主，开始逐步向防御、检测、响应三者并重转变；**安全防御体系从传统的点对点、端到端的堡垒型防护思路向全方位、立体化、协同防御的纵深防护思路转变。**在这种背景下，利用大数据技术对海量数据进行实时的处理分析，以快速检测和发现未知威胁，就成为了安全防护理念转型的核心与关键。目前这一理念得到了业界的高度关注，相关的产品也应运而生。现阶段已有的大数据安全分析产品主要包括两种，一种是融入大数据技术进行威胁态势感知和未知攻击发现的大数据安全管理平台(BD SOC)；另外一种是聚焦未知攻击检测的未知威胁感知系统。

图 19：安全新态势下的防御理念变革



资料来源：东兴证券研究所

2.3 看好具有产品背景的信息安全厂商发展机遇

安全变革趋势下，更加要求信息安全系统的建设者具有深厚的安全研究积淀、较强的系统安全构建能力与对安全产品的深刻洞察，产品+集成商业模式凸显特色竞争优势。

攻防态势变革+专精化防护大趋势下，信息安全解决方案提供商会有更多的机会。随着攻防态势演变，传统的依靠边界防护+终端管理+安全态势感知（SOC）三种产品堆砌的防护思路并不能保障用户的安全，在设计系统时需要考虑系统在应用场景上的实际特点、安全产品的协同联动、系统针对未知威胁的影响能力与策略，这些都需要大量深入的安全知识，因此在系统规划设计部署落地的阶段，安全的能力和从业的经验将凸显其重要性，具有安全产品生产经验的系统集成厂商竞争性将凸显。对于这些厂商来说，其系统集成业务的营收与毛利率有望出现双重增长。

目前产品+集成商业模式在大多数信息安全上市公司中不多见，比如启明星辰、绿盟等安全产品厂商并不会大量做信息安全集成的业务，因为会损害到其已有的渠道商与集成商的利益。**蓝盾是具有特色的产品+集成信息安全解决方案提供商。**

3. 网络安全法实施，对行业构成实质性利好

3.1 强调网络运营者保护义务、明确处罚措施，提振信息安全市场整体增速

从法律责任层面明确信息安全保护义务，意味着我国网络安全建设迈向新高度。我国政府于 2016 年 11 月 7 日表决通过了《中华人民共和国网络安全法》，并自 2017 年 6 月 1 日起施行。此法明确指出："要加强党政机关以及重点领域网站的安全防护，建立政府、行业与企业网络安全信息有序共享机制；建立实施网络安全审查制度，对关键信息基础设施中使用的重要信息技术产品和服务开展安全审查；健全信息安全等级保护制度。"**《网络安全法》进一步从法律层面界定了公民和法人的行为边界和细节，为网络的健康和可持续发展奠定了基础。**

安全法明确网络运营者的保护义务：产品、服务提供者具有维护信息安全的义务，包括反病毒、放攻击、数据安全、应急响应等。利好整个安全行业。从安全法中规定的运营者保护责任来看，对于安全运维、应急响应等安全服务业务来说构成实质性利好。

安全法首次提出，网络运营者不履行安全义务将有可能被暂停服务，直接抓到互联网服务提供商的命门，目前大量网络运营商在安全系统构建层面存在不足，导致数据库遭到非法复制（俗称拖库攻击）的恶性安全事件频发。互联网公司的安全产品需求将逐步启动。

表 2：网络安全法中规定运营者的保护义务以及法律责任

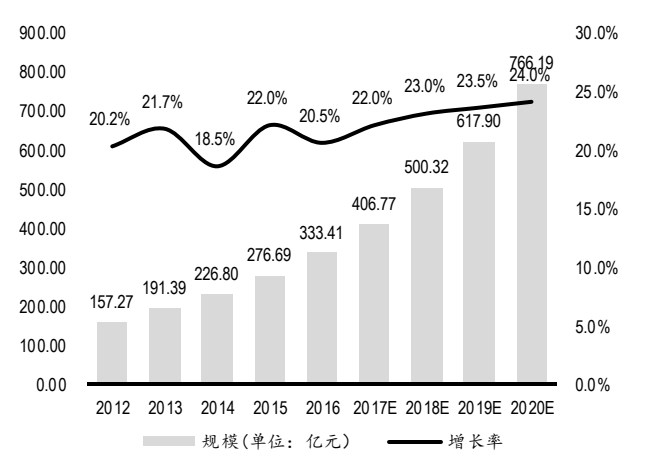
条款序号	解读	条款内容
第二十一条	部署基本的安全系统，利好行业整体，鉴于大量用户安全防护水平较为基础，	保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；（二）**采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施**；（三）采取监测、记录网络运行状态、网络安全事件的技术措施
第二十二条	利好安全运维服务。	发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。**网络产品、服务的提供者应当为其产品、服务持续提供安全维护**；在规定或者当事人约定的期限内，不得终止提供安全维护。
第二十五条	利好信息安全服务中应急响应部分，	网络运营者应当制定网络安全事件应急预案，**及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案**，采取相应的补救措施，并按照规定向有关主管部门报告。
第四十二条	网络运营者对用户安全有保护义务，之前大量出现用户信息泄露的事件，网络安全法实施后会促使响应公司加强信息安全整体**防护建设以及专精化防护领域，重点包括数据库安全等。**	网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，**防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失**的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。
第六十四条	情节严重暂停业务，对于互联网公司来说处罚**措施非常严重，会促使相关行业公司加大安全投入。**	网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；**情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。**

资料来源：公开资料、东兴证券研究所

网络安全法要求政府、行业和重点企业持续加强自身的信息安全建设，**从基础设施安全和个人信息安全两个方面进行重点保护，标志着我国网络安全和信息保护进入全新阶段。**

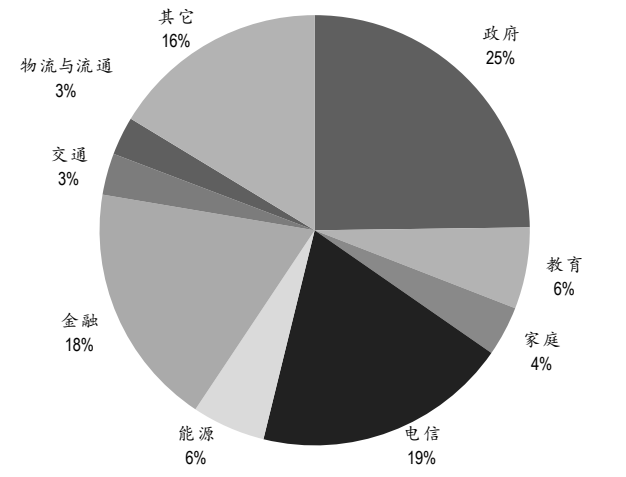
我国安全行业市场增速有望进一步提升。目前我国信息安全产业规模约 418 亿元，**总体看，安全占 IT 总投入比重还是显著偏小、行业成长空间大**——信息安全投入占我国 IT 总投入约 2%、与美国等发达国家 10%的投入占比相去甚远。**受到网络安全法的强势驱动，我们预计行业增速将进一步提升**，市场规模至 2020 年可达 766 亿元，2017-2020 年 CAGR 为 23.5%。

图 20：我国信息安全市场规模及预测，2012-2020



资料来源：CCID，东兴证券研究所

图 21：我国信息安全市场行业分布



资料来源：CCID，东兴证券研究所，2015 年数据

3.2 强化个人信息安全保护，利好数据安全

网络安全法中对个人信息的定义：**“是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等”。**

3.2.1 个人信息泄漏事件频发、我国数据安全形势很严峻

近年拖用户数据泄露事件频发，我国过亿用户数据遭遇泄露，涉及到大量知名互联网企业，数据安全形势严峻。

表 3：2015-2017 年数据泄露事件

事件	关键词	事件描述
1	网易邮箱，过亿	2015 年 10 月 19 日，乌云漏洞报告平台发现网易用户数据库泄露，**影响到网易 163、126 邮箱过亿数据**，泄露信息包括用户名、MD5 密码、密码及密保信息、登录 IP 以及用户生日等。
2	伟易达集团，500 万	2015 年 11 月 27 日，全球最大的婴幼儿及学前电子学习产品企业伟易达集团（VTech）被爆发生信息泄露事件。黑客入侵 VTech 的客户资料，当中**有大约 500 万个家长和超过 20 万个小童的资料**，包括姓名、电邮地址、密码和个人住址。
3	OpenSSL，水牢漏洞	2016 年 3 月 2 日，OpenSSL 发现水牢漏洞（DROWN 漏洞），其会影响部分使用 HTTPS 的服务及网站。利用该漏洞，攻击者可以**监听加密流量，读取诸如密码、信用卡账号、商业机密和金融数据等加密信息。**经国外相关机构初步探测识别，目前全球有大约 400 万网站和服务易受此漏洞的影响，我国十余万家网站受到威胁。
4	Verizon，150 万	2016 年 3 月 30 日，美国最大的电信运营商 Verizon 公司客户数据在地下网络市场被人出售。**遭受黑客盗窃的 150 万条客户信息中包括一些财富 500 强企业。**Verizon 公司代表已经确认了在其网站发生

		的数据泄露事件，目前泄露数据的漏洞都已经修复了。
5	土耳其，5000 万	2016 年 4 月 3 日，土耳其爆发重大数据泄露事件，近 5000 万土耳其公民个人信息牵涉其中，这些个人信息规模达 6.6G，包括姓名、身份证号、父母名字、住址等等一连串敏感信息，同时为了证明这些被盗取数据的真实性，黑客**特地公布了土耳其现任总统埃尔多安与总理达式特奥卢的个人信息为例证**，并且对该泄密数据库的编程水平大肆嘲讽。
6	Ramnit，网页恶意代码	2016 年 4 月 22 日，据国家互联网应急中心（CNCERT）通报，一段名为“"Ramnit”的网页恶意代码被挂载在境内近 600 个党政机关、企事业单位网站上，一旦用户访问网站有可能受到挂马攻击，对网站访问用户的 PC 主机构成安全威胁。
7	MySpace，3.6 亿	2016 年 5 月 22 日，有新闻曝光了 **1.17 亿条 LinkedIn（领英）数据被泄露**的消息，而最新的消息是社交网站 MySpace 也遭到了数据泄露，而泄露的数据比领英还要多。该黑客宣称已经拿到了 3 亿 6000 万 MySpace 用户的电子邮件地址以及密码。目前 LeakedSource 表示：“在这 3 亿 6000 万泄露的信息中，有 111341258 个账户绑定了用户名，其中有 68493651 个账户有二次验证密码，如果想要查看泄露记录可以每天支付美元或每年支付 265 美元，就可以查看 16 亿被攻击或被泄露的数据记录。”目前 MySpace 官方没有正面回复这一情况。
8	MongoDB；5800 万	2016 年 10 月 17 日，知名数据库及数据存储服务提供商 MBS 遭到黑客攻击。**其 MongoDB 数据库由于缺乏有效的安全保护措施，5800 万商业用户的重要信息泄露**，包括名称、IP 地址、邮件账号、职业、车辆数据、出生日期等信息。
9	Equifax；1.43 亿	作为美国四大信用报告机构之一。Equifax 在 9 月份透露，网络犯罪分子已经渗透到他们的网络中。**漏洞泄露了一亿四千三百万美国人的数据，基本上包括了美国的每一个成年人。泄露的信息包括姓名、社会保险号码、生日、地址，在某些情况下还包括驾照号码。**
10	雅虎；30 亿	2017 年 10 月，**雅虎宣布公司在 2013 年黑客入侵事件中共有 30 亿名用户的账号信息被窃取，这一数字在 2016 年 12 月的初步报告中还只是 10 亿**。此次事件中，遭到泄露的雅虎用户账号信息包括用户姓名、电子邮件地址、电话号码、出生日期、密码，以及一些安全问题和答案。对此，雅虎和调查方曾表示，“得到国家资助的黑客”发动了这次攻击，但并未指明具体是哪个国家。其实，在改起事件中失窃账户数量的多少不是最重要的，用户隐私才是最大的受害方，而雅虎也因账户被盗事件面临至少 41 个联邦或地方法庭的诉讼。

资料来源：互联网资料，东兴证券研究所

网络安全法明确了网络运营者对于个人信息的妥善保管义务，以及处罚措施，对于出现重大问题的情况，可以暂停业务。

表 4：网络安全法中规定的涉及个人信息的内容

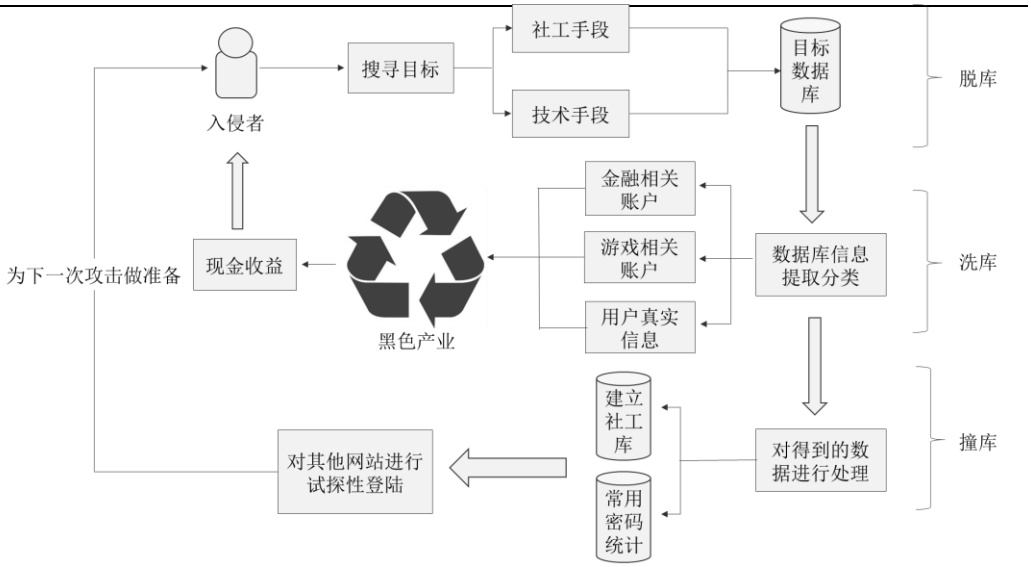
条款序号	解读	条款内容
第二十二条	明确个人信息应当由网络运维这保护。	网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。
第四十一条	规定了个人信息的应当如何被搜集、使用，**保护个人信息不被肆意搜集和滥用**。	网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。
第四十二条	**防止泄露，涉及到 DLP、数据库安全，防止损毁丢失，涉及到灾备。及时采取补救措施，涉及到安全应急响应服务。对个人信息的脱敏处理要求，促使 DLP 转型升级。**	网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。**但是，经过处理无法识别特定个人且不能复原的除外**。网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，**防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，**应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。
第四十三条	涉及到安全应急响应以及安全运维服务。	第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。
第四十四条	针对利用个人信息搞黑产的	**任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售**

	犯罪行为。	**或者非法向他人提供个人信息。**
第四十五条	**对网络运营者违规后果和非法使用个人信息犯罪惩处措施做规定。**	依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。
第六十四条		第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，**并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。** 违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法**所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。**

资料来源：公开、东兴证券研究所

目前网络安全态势严峻、数据泄露频发的事实，**已经实质上形成了围绕个人信息盗用的黑色产业链，黑客通过盗取数据库（拖库）以及利用已经泄露的数据对大量互联网服务提供商进行“测试”**(撞库，因为极少有用户可以做到不同网站均应用不同密码)，可以极大的**增强所盗取数据的效用。**

图 22：针对数据库的攻击示意图



资料来源：互联网资料，东兴证券研究所

3.2.2 看好数据安全细分领域

直接利好数据安全细分领域。数据安全主要包括数据库防护和数据防泄漏两个部分。目前我国数据安全业务较为凸显的厂商有启明星辰、亿赛通（绿盟子公司）、明朝万达等：

表 5：数据安全领域主要市场参与者、产品以及核心竞争优势

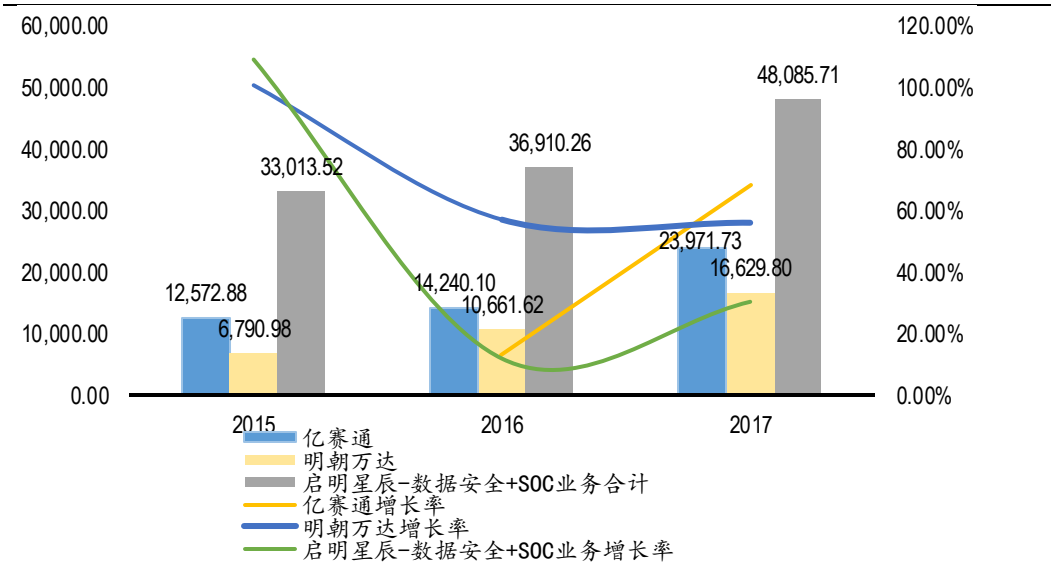
公司名称	覆盖领域	介绍	核心竞争优势
亿赛通	DLP/数据加密	主要产品方向是文档安全管理系统和数据泄露防护领域,包括数据资产安全、文档安全、移动安全、终端安全、网络安全、咨询服务和文档加密等。**该公司已于 2014 年被神州绿盟收购。**	在数据安全领域积淀较深；**被绿盟科技收购，借力后者品牌以及渠道优势强势拓展政企市场**
北信源	DLP/数据	北信源数据泄露智能防护系统是针对大数据时代而推出的数据泄露	北信源是终端安全行业领头羊，

	加密	防护全新体系架构，**该系统以数据智能识别为核心**，对企业内数据实行精准分类分级，知晓数据分布和风险，进而保护数据资产。	业务能力以及渠道优势独树一帜。**因此在数据安全领域具有强大的市场推广能力。**
启明星辰	数据库安全	数据库安全行业龙头，进入行业较早。对业务人员访问数据库的行为进行记录分析，发现异常情况并进行报警、阻断等处置。	启明是安全行业龙头，产品线布局全，大单承揽能力强，有利于其推广数据安全产品。
明朝万达	DLP/数据加密	强调数据安全全生命周期管控，覆盖数据产生、存储、交换、使用等全生命周期重要环节，实现对服务器、数据库、PC 终端、移动终端以及网络通信的全 IT 架构下数据安全的协同联动管理。	公安、金融领域数据安全解决经验丰富。
Symantac	DLP	赛门铁克是美国的一家信息安全企业,为企业、个人用户和服务供应商提供广泛的内容和网络安全软件及硬件的解决方案产品包括防火墙、VPN、IDS、病毒防护、内容过滤。	**在终端以及数据保护层面技术积淀深厚**，品牌大。
McAfee	DLP	Macfee 是美国一家专业安全技术公司，最畅销的产品是杀毒软件,此外也包括数据保护和加密、数据库安全、电子邮件和 Web 安全、终端保护、移动安全和网络安全等产品。	**在杀毒领域良好的品牌影响力**以及技术积累。
IBM	数据库安全	IBM **数据安全产品 InfoSphere Guardium 提供的一组集成模块，使用一个统一的控制台和后端数据存储，管理整个数据库的安全与合规周期**。通过 Guardium，既能实时保护数据库，**又能自动化所有合规审计流程。这套方案不仅在解决问题方面表现卓越**。	具有显著的技术实力以及品牌影响力；**支持数据库种类多，开销少，对分布式数据库支持好。**
Oracle	数据库安全	基于 Oracle 全面的数据库安全解决方案的**纵深防御体系包括对企业核心数据库从阻止与记录、审计与监测、访问控制到加密与屏蔽的四层防护壁垒，而数据牢牢地置于四层保护的核心**。	**数据库行业地位无可置疑**；产品功能强
优炫软件	DB Sec/DLP	USOS 在**操作系统的安全功能之上提供了一个安全保护层。通过截取系统调用实现对文件系统的访问控制，以加强操作系统安全性。**	**在 OS 层面的底层技术方向积淀深厚，近年业务快速稳定增长**

资料来源：公开资料、赛迪顾问、51CTO、东兴证券研究所

目前几家数据安全大厂近年业绩增长较快，亿赛通 2017 年营收达到 2.39 亿，2015-2017 年 CAGR 为 38.1%；明朝万达 2017 年营收为 1.66 亿元，近三年 CAGR 为 56.5%；启明星辰数据安全以及平台（主要包括数据安全、SOC）2017 年营收为 4.81 亿元，根据我们的判断，其中数据安全业务占约 2.3 亿左右。

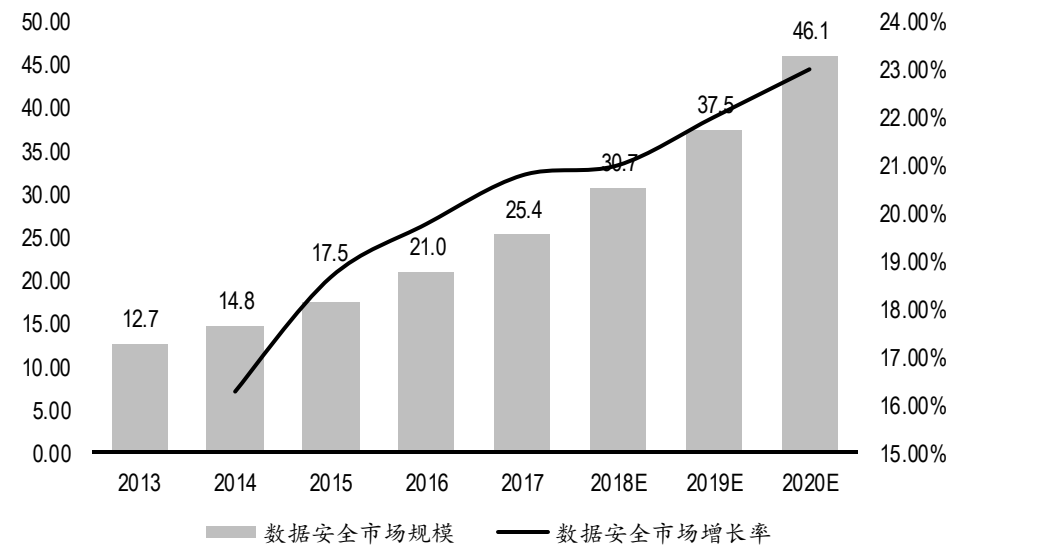
图 23：部分数据安全厂商近年业务规模（单位：万元）



资料来源：公开资料，东兴证券研究所

我们判断伴随网络安全法的强势驱动以及我国信息安全防护建设逐步深化，数据安全市场将保持高速增长态势，预计今后三年 CAGR 不低于 21%的增速，2020 年达到逾 46 亿的市场规模。

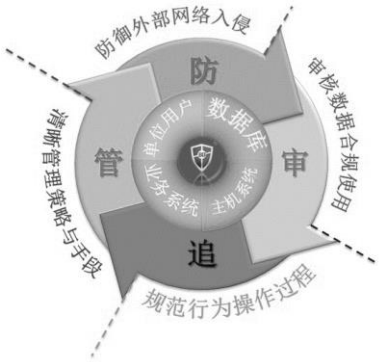
图 24：数据安全市场规模以及预测（单位：亿元），2013-2020



资料来源：CCID，东兴证券研究所

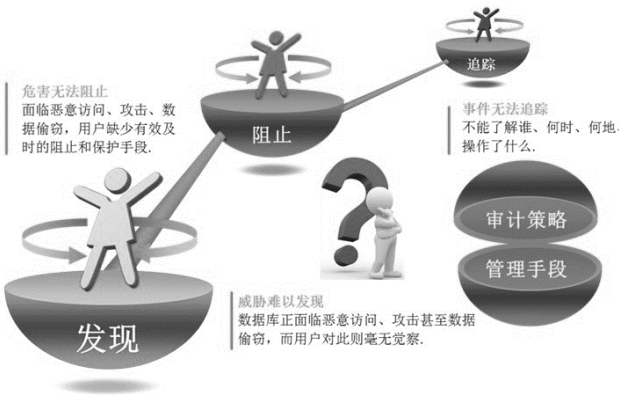
蓝盾提出了数据安全解决方案，以事前防御、事中审计、全面管理为指导思想。针对用户终端、数据库、主机、业务系统对象，对危害数据安全的行为进行阻断、分析记录、审计。

图 25：蓝盾数据安全解决方案-防护思路



资料来源：CCID，东兴证券研究所

图 26：蓝盾数据安全解决方案-防护策略



资料来源：CCID，东兴证券研究所，2015 年数据

3.3 强调关键基础施设施，推进工控安全市场启动

3.3.1 重点利好工控

网络安全法提出“关键基础设施”概念：“公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，**以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生**、公共利益的关键信息基础设施”。

从上文定义来看，关键基础设施可以分为几类：

- 第一类：基础 IT 设施。包括上文的公共通信和信息服务。
- 第二类：政务设施。包括上文的公共服务、电子政务。
- 第三类：金融。
- 第四类：能源、交通、水利。

我们判断对于关键基础设施信息安全的强调重点利好工控安全。从目前的行业发展来看，电信、政务、金融的信息安全细分市场已经规模初显，**但是面向能源、交通、水利领域工业控制系统的安全防护市场仍处于萌芽阶段，网络安全法以法规形式强调了对于关键基础设施的检测评估、人员教育、应急演练、容灾备份义务，会对工控安全领域形成实质性利好：**

表 6：网络安全法中关于关键基础设施的内容

条款序号	解读	条款内容
第三十一条	明确关键基础设施的核心属性：遭到破坏损害公众利益。	国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，**以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设**施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。
第三十二条	关键基础设施涉及到的各行业有望出现信息安全规划	按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。
第三十四条	目前信息安全行业人才较为短缺，利好信息安全培训教育；利好灾备；利好应急演练和安全服务。	除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；**（二）定期对从业人员进行网络安全教育、技术培训和技能考核；（三）对重要系统和数据库进行容灾备份；**（四）制定网络安全事件应急预案，并定期进行演练；（五）法律、行政法规规定的其他义务。
第三十八条	利好信息安全测评和风险评估，“自行或者委托”，考虑到安全行业加速变革的现状，会有相当一部分自身 IT 能力有限的机构选择委托第三方评估。	关键信息基础设施的运营者**应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，**并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。
第三十九条	明确了有关部门在安全检测评估、应急处置方面的义务。	国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：（一）**对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；**（二）**定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；**（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

资料来源：公开资料、东兴证券研究所

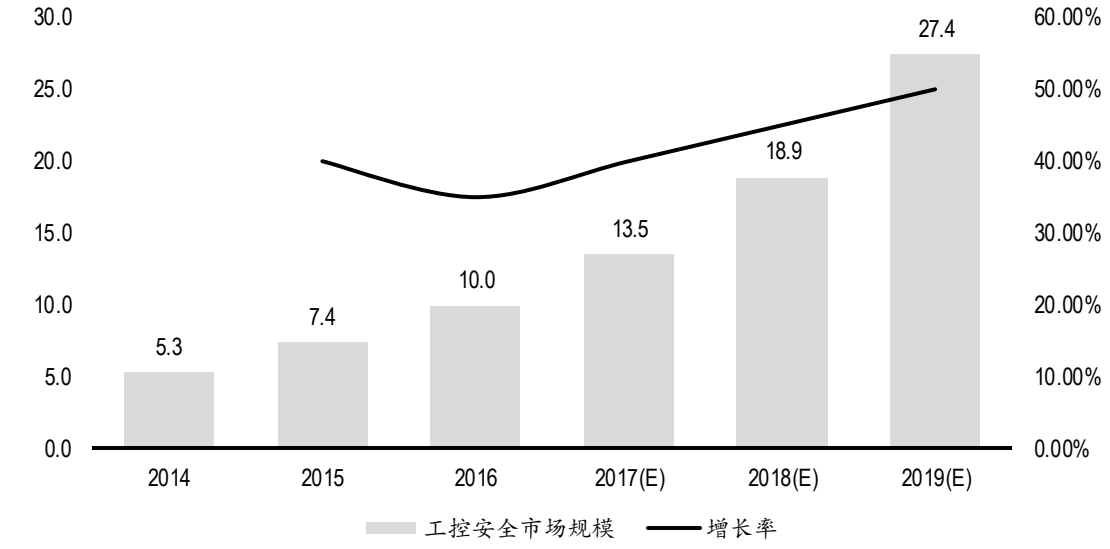
我们认为 2017 年网络安全法的实施**将带动重要关键基础设施防护的建设，工控安全市场将迅速启动，**关键驱动因素包括：

- 发电、输配电、制造、市政等行业的企事业单位维护信息安全意识增强，加大在工控安全方向的投入力度。
- 行业相关安全标准的不断出台以及完善，对于工控系统信息安全体系的构建提出明确、实操性强的指导。

- 工控安全领域自身的发展，网闸、工控防火墙、状态感知等系统的日趋完善将促进产品的部署与普及。

我们由此对我国工控安全市场增速持乐观预期，**预计至 2020 年，工控安全市场将达到 27.4 亿元，2016-2019 年 CAGR 为 39%。**

图 27：我国工控安全市场规模以及预测（单位：亿元），2014-2019



资料来源：东兴证券研究所

3.3.2 满泰科技推出工控安全解决方案

2016 年 12 月，蓝盾并购水务工控设备厂商满泰科技，**满泰科技主要面向水利场景提供自动化解决方案，应用场景包括水电站、泵闸站、水库、大坝等。**

表 7：满泰科技主要解决方案概要

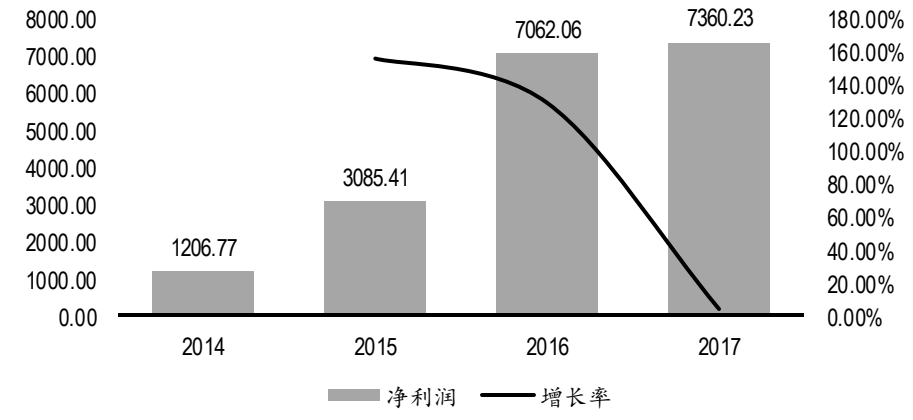
业务线	产品类别	概述
水利水电自动化	满泰水电站监控系统	专门针对水电站需求开发的新一代计算机监控系统，可自动调节电站库区容量、发电负荷及泄洪流量。
	满泰水电站（群）优化调度系统	主要服务对象是水电站及水库，用于水库管理和梯级电站之间的综合水资源调度。
	满泰水电站自动发电控制与自动电压控制系统	保证发电出力与负载平衡，针对电压变化控制调节发电机励磁，保证向电网输送合格的电压和满足系统需求的无功。
	满泰水库综合自动化系统	包括水库闸门控制系统、电力自动化系统、水情自动测报系统、大坝安全监测系统、视频监控系统等综合解决方案。
	满泰泵闸站（群）综合自动化系统	将某一河道流域内所有闸站及泵站的监控集中在一个控制平台中，实现泵站群、闸站群的远程集中统一调度。
	满泰电力远动通讯系统	适用于与电力调度相关场合的通讯，也可当作各种电力规约转换器使用。
智慧水务	满泰“智慧水务”综合解决方案	包括污水处理、城市管网监控、优化供水调度、自来水管道监测、集中供水监控、水源井监控、蓄水池水位监控等综合解决方案。
	满泰污水处理厂（自来水厂）综合自动化系统	对污水处理厂、自来水厂进行监视、测量、控制及保护，以实现污水处理厂、自来水厂的全集成综合自动化控制。
	满泰农村饮水安全工程解决方案	包括农村供水实时信息接收处理、自动控制、水质在线监测、实时视频监控、实时险情监测预警、农村供水信息综合分析和决策支持、信息发布等功能的综合解决方案。
	满泰水情测报系统	专用于江河流域及水电站群、水库洪水预报、防洪调度及水资源合理利用

		等水情测报工程。
	满泰水质水量在线监测系统	集水样预处理、水质自动分析、数据采集、远程监控、信息共享、水资源管理于一体的综合性在线自动检测系统。
	满泰山洪灾害预警系统	通过接收水雨情监测站采集的水雨情数据，进行分析处理，实现水雨情实时监测，提高对山洪灾害快速、全面、准确的预报预警能力，并为指挥调度提供有力的技术保障。
	满泰三防调度决策指挥系统	城市防灾减灾决策支持和调度指挥。
	满泰地面坍塌防治管理系统	对地面隐患点进行探测排查，将数据集成到 GIS 系统中进行管理与应用，为预防地陷事件提供手段和信息来源。
	满泰管网 GIS 巡检系统	基于高精度北斗和移动互联网技术，为市政部门提供整体的管网巡查及综合运营服务，实现排水管网的动态管理。
	满泰船闸收费系统	利用计算机收费并且出示票据来代替人工收费。
海绵城市	满泰城市防洪排涝系统	用于城市防洪排涝、排水管理工程，实现城市汛情监测和城市排涝、排水的监控和管理。
	满泰社区抗汛管理系统	通过采集社区河道及易涝危险区水雨量、视频等信息，通过网络传送到抗汛监测预警平台，提供社区汛情预警信息并采取应对措施，防范和遏制社区内涝事故发生。
系统集成服务	智能建筑系统集成	搭建建筑主体内的建筑智能化综合管理系统，包括综合布线、楼宇自控、电话交换机、机房工程、监控系统、防盗报警、公共广播、门禁系统、楼宇对讲、一卡通、消防系统、多媒体显示系统、远程会议系统等子系统。
	计算机网络系统集成	通过结构化的综合布线系统和计算机网络技术，将各个分离的设备、功能和信息等集成到相互关联的、统一和协调的系统之中，使资源达到充分共享，实现集中、高效、便利的管理。
	安防系统集成	搭建组织机构内的安全防范管理平台，包括门禁系统、楼宇对讲系统、监控系统、防盗报警、一卡通、停车管理、消防系统、多媒体显示系统、远程会议系统等子系统，既可作为一个独立的系统集成项目，也可作为一个子系统包含在智能建筑系统集成中。
	应用系统集成	深入到用户具体业务应用层面，为用户提供一个全面的行业信息化整体解决方案。

资料来源：公开资料、东兴证券研究所

满泰科技近年业务成长迅速，2017 年实现净利润 7360.23 万元，2014-2017 年 CAGR 为 82.7%。

图 28：满泰科技近年净利润情况（单位：万元）



资料来源：公开资料，东兴证券研究所

政策驱动水文监测系统建设完善+水利信息化系统建设深入，水务自动化市场行业前景看好。《水利改革发展“十三五”规划》明确指出，要加强水文监测服务能力建设，充实调整各类水文测站，优化完善水文站网布局和功能，加强水土保持监测网络、重

要水功能区和主要省界断面水质水量监测体系建设。加强水文监测中心建设，提高水文技术装备整体水平，**提升水文巡测、水质分析和水文信息处理服务能力。要推进水利信息化建设，完成水资源监控管理系统建设，建立覆盖城镇和规模以上工业用水户、大中型灌区的取水计量设施和在线实时监测体系。**加快**推进国家防汛抗旱指挥系统、山洪灾害监测预警系统、大型水库大坝安全监测监督平台、覆盖大中小微水利工程管理信息系统和水利数据中心等应用系统建设，提高水利综合决策和管理能力。**

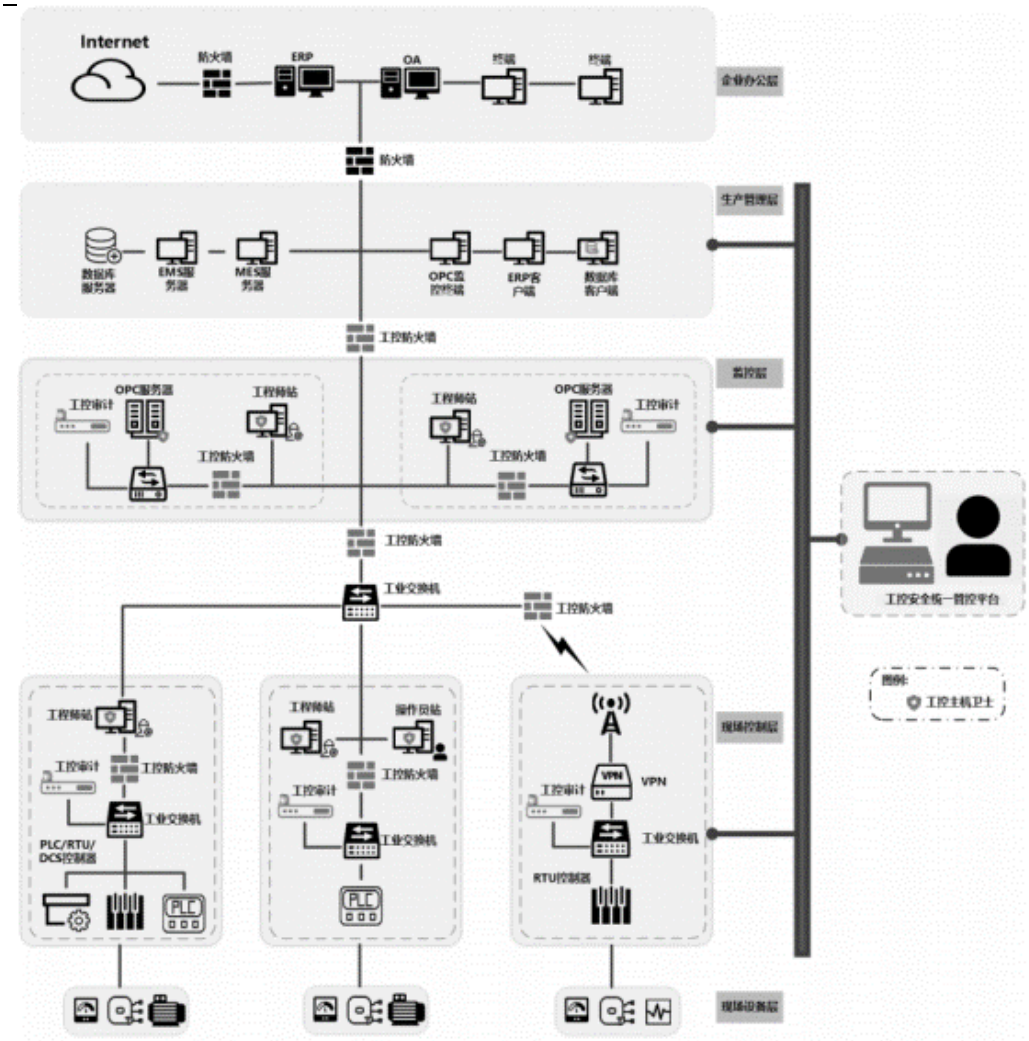
满泰在近期推出了工控安全解决方案，**主要策略是通过防火墙+终端+审计+SOC 安全实现工控系统的全面防护。**

表 8：满泰科技工控防护体系构成

产品名称	概要	特点
工控审计系统	以旁路部署方式，通过对工控网络中数据分析，建立工控网络安全通信模型，**实现对工控网络“无损”实时监控，**检测网络中的攻击和异常，并为工控网络安全事件调查提供数据依据。实时分析工控网络流量并深度解析工控协议，实现网络流量**可视化、指令级的工控协议通信审计**、异常控制操作和网络攻击等关键事件告警。提高工控网络安全事件感知、响应、溯源能力。	**智能异常检测**。通过对 Modbus、S7、OPC、Ethernet/IP 等工控协议的深度解析（DPI）**以及机器学习技术，建立多维度的网络通信安全模型**，实现对设备、网络、协议、行为等异常的智能监控，从而实时高效发现网络攻击、误操作等各类安全威胁。**全面安全审计。除多维度网络会话（IP、MAC、协议、时间等）审计外，我方工控审计系统还支持重要的操作审计，如工程师站组态变更、指令变更、PLC 下装等，同时提供对触发告警报文的记录功能，便于对安全事件分析取证。**
工控墙	**工控协议深度包解析技术不仅对二层三层网络协议进行解析，更进一步解析到工控网络包的应用层**，对 OPC、Modbus、DNP3、IEC104、S7、Profinet 等进行深度分析，防止应用层协议被篡改或破坏。	**采用学习、测试、防护三种工作模式，避免部署过程中错误配置导致的异常阻断，提高生产网络的可靠性**，此外在硬件层面采用冗余电源，接口 bypass 设计，进一步提高系统可靠性。通过对 Modbus TCP、S7、OPC、Ethernet/IP 等多种工控协议识别以及深度解析，**实现指令级的控制，如操作命令码、地址范围、参数范围等，有效防御来自内外部的安全威胁。**
主机卫士	**应用“白名单”机制，轻量级的软件设计提高工控网络适应性以及工控主机的软硬件兼容性**，同时支持主机加固，有效防御已知与未知的病毒、木马等恶意软件威胁，**实现工控主机的启动、加载、运行的全生命周期的安全保护。在工程师站、操作员站、OPC 服务器部署工控主机卫士终端防护软件，实现软件白名单管理、**移动存储介质管理、系统加固等，此外配合安全 U 盘使用，在各主机系统上进行数据交换，进一步降低病毒、恶意软件的感染风险。	区别于传统防病毒软件，采用应用白名单防护机制，从而实现工控软件广泛兼容，避免发生工控应用的误杀。**无需频繁升级，符合工控网络与互联网隔离的特性。软件资源占用低，内存占用小于 20M，CPU 占用小于 5%，**支持对老旧低配置工控主机的安全防护。支持从操作系统、注册表、内存空间完整性、本地安全策略方面进行主机加固，防止系统被恶意破坏。
工控安全统一管控平台	工控安全统一管控平台是针对工控网络安全产品统一管理的软硬件一体化系统。**通过对分散在工控网络中的安全设备集中管理，实现统一配置、整网监控、综合展示，**提高对安全设备以及安全事件的掌控能力的同时降低安全运维成本。	全面记录工控网络的**主机安全日志、网络攻击日志、网络审计日志等，并进行关联分析**，为网络安全事件分析和调查取证提供必要的数据依据。**提供整网安全设备、工控设备、网络设备等资产的拓扑展现，并支持流量、会话、协议、攻击、异常事件等多维度的报表**，帮助用户实现覆盖终端、网络、边界的全可视化纵深安全管理

资料来源：互联网资料、东兴证券研究所

图 29：满泰科技工控防护体系示意图



资料来源：互联网资料、东兴证券研究所

3.3.3 看好此类具有工控基因厂商开展工控安全业务的潜力

工控安全行业属性特殊，和互联网信息安全相比，至少存在以下几点不同：

- 和传统计算机网络使用被广泛接收的 TCP/IP 等协议不同，工控系统存在着大量的工控协议。**要进行工控防护需要先了解并吃透这些协议，在此基础上搞清楚工控系统的传输架构与业务逻辑，需要大量设计自动控制和与部署场景相关的专业知识。**
- 对工控系统的攻防手法与传统信息安全场景有根本性差异，已有相当一部分的攻击都是围绕改变系统的某些参数并躲避监控展开的，这与传统网络攻击存在差异，**理解并深刻认识工控场景下的信息安全攻防很重要。**
- 和传统网络安全存在根本性差异的一点在于，**工控系统特别强调业务的连续性，以电厂为例，停机造成的损失可能数以百万计**。传统的网络安全设备厂商因设备的安装调试等原因造成的短时间断网完全可以接受。

我们判断工控安全领域，具有工控安全基因的厂商会更好的主导市场，**因其对工控系统及其业务逻辑有深刻认识，且能够深刻领会工控系统维护正常平稳运行为首要任务的逻辑。看好蓝盾利用原有销售渠道向用户提供水务领域工控安全解决方案的能力。**

3.4 强调监测预警，利好 SOC

3.4.1 态势感知法规化，SOC 产品线重点受益

网络安全法将态势感知法规化，明确了单位在感知网络安全态势方面的责任：

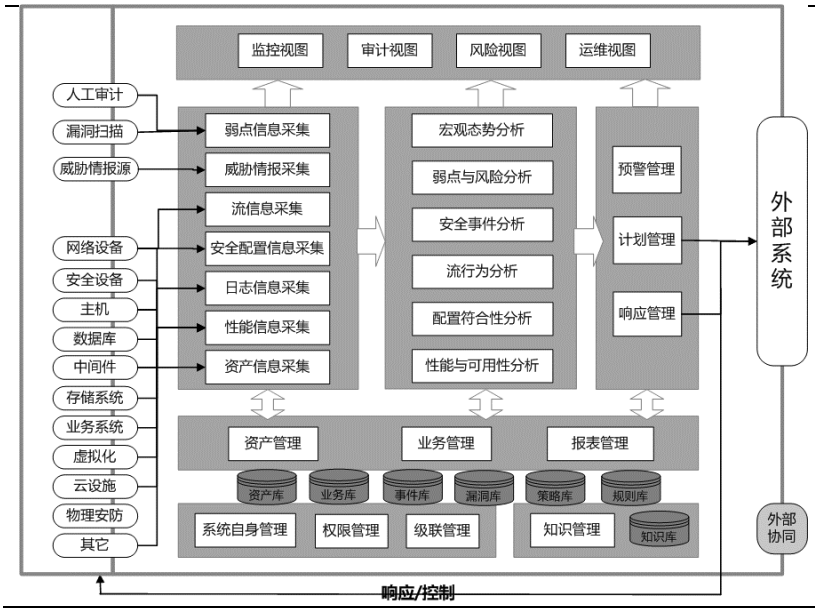
表 9：网络安全法中关于关键基础设施的内容

条款序号	解读	条款内容
第五十一条	监测预警制度化。	国家建立网络安全监测预警和信息通报制度。**国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报**工作，按照规定统一发布网络安全监测预警信息。
第五十二条	建立行业监测预警制度。	**负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，**并按照规定报送网络安全监测预警信息
第五十三条	利好应急响应领域。	国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。**负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。网络安全事件应急预案应当按照事件发生后的危害程度**、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。
第五十四条	对于网络风险的监测、分析评估主要依靠 SOC，利好 SOC。	"网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和

资料来源：公开资料、东兴证券研究所

强调对于信息安全态势的监控，包括安全信息的搜集分析与通报等，利好 SOC 产品线。SOC 是信息安全系统的最顶端的管控中心，负责安全态势感知、威胁发现与预警，与整个信息安全安防体系的边界防护、终端防护、检测产品进行数据交互，**SOC 对于网络整体安全形势有最为敏锐的感知。**

图 30：SOC 运作模式

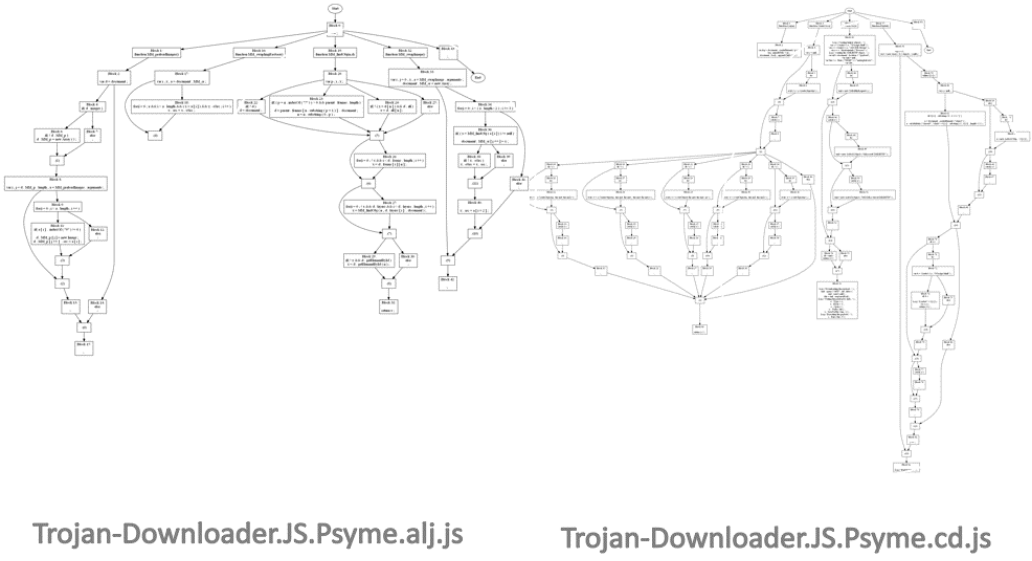


资料来源：公开资料，东兴证券研究所

3.4.2 蓝盾推出深层次溯源的新一代 SOC

蓝盾下一代 SOC 强调溯源，**通过对木马蠕虫的文件进行深度分析，**了解恶意软件族谱这以及供给来源，为管理层决策提供依据。实施的手段是对软件基因进行识别和分析，**“软件基因”是软件体上具有功能或携带信息的二进制片段**，它支撑着软件的基本构造，存储着软件生命周期的全部信息，**是程序编制者的语义实现、编译器、基础库和系统环境互相依赖、影响、制约的结果，**如同生物的基因。

图 31：蓝盾恶意软件溯源功能示意图



资料来源：公司资料，东兴证券研究所

利用基金检测技术，可以用来进行未知威胁和未公开漏洞的挖掘，海量数据中发现有用的、可理解的数据模式,，动构建检测模型。

4. 可转债发行获批，建设西北中心充实研发能力

5 月 7 日，蓝盾股份公开发行可转换债券的申请获得证监会批准。

4.1 十亿募资强化研发，聚焦移动安全、态势感知、云安全三大前沿领域

据《公开发行可转换公司债券募集资金投资项目可行性分析报告（二次修订稿）》，蓝盾股份此举拟加强在西北地区的业务布局，拟总募资 5.38 亿元，除补充流动资金 1.61 亿元之外，**准备筹建研发与产业化基地，总投资 10.22 亿元、募集 3.77 亿元。**

研发以及产业基地主要包括：**基地基建建设、一站式安全云计算体系研发项目建设、网络综合态势预警平台研发项目建设和企业移动信息化安全管理体系研发项目建设。项目概算如下：**

表 10：蓝盾股份建设项目概算

序号	项目名称	金额（万元）
基地基建建设		
一	**建安工程费用**	**61198.56**
1	土建工程	37822.88
2	装修工程	21042.40
3	其他工程	2333.28
二	**工程建设其他费用**	**6838.82**
三	**预备费**	**2041.12**
一站式安全云计算体系研发项目建设(16134.00 万元)		
一	机房建设	1882.00
二	网络安全	2785.00
三	计算建设	5046.00
四	软件建设	6421.00
网络综合态势预警平台研发项目建设(11032.00 万元)		
一	情报共享平台	6230.00
二	态势感知与评估平台	1968.00
三	态势预警管控平台	984.00
四	研发平台	1850.00
企业移动信息化安全管理体系研发项目建设(5000.25 万元)		
一	服务运营平台	2500.50
二	服务容灾中心	999.75
三	研发平台	1500.00
合计		102244.75

资料来源：公开资料，东兴证券研究所

除基建外，可以看出企业规划资金主要覆盖涉及专精化防护的三个领域：云安全（1.6 亿）、态势感知（1.1 亿元）、移动安全（5000 万元）。

云计算主要包括：**融合云计算**。涵盖基础设施和运营管理平台。**安全资源池**。涵盖安全产品和对外部威胁情报等安全信息的调用。**SaaS 服务体系构建**，包括漏扫、运维、防护、人工服务等。

图 32：一站式安全云计算体系项目架构图

资料来源：公开资料，东兴证券研究所

网络综合态势预警平台，建设内容涉及平台构建、态势感知、预警管控三个层面。包括大数据平台（云模式）、数据采集、流量分析、用户与实体行为分析、网络安全威胁分析、业务安全监控、网站监测、数据安全管理、网络安全态势可视化、网络安全威胁通报与预警、安全运维管理等模块组成。

图 33：网络综合态势预警平台建设内容

建设内容	内容描述
全网架构设计	融合云计算、大数据、流量采集、SIEM、机器学习算法、网站监测、数据泄露监测、数据安全管理、用户与实体行为分析、大数据可视化、ITIL运维管理等技术，基于全网从安全事件统一管理、安全运维统一执行过渡到可扩展的大型分布式高性能实时监控分析全网网络安全要素的平台进行整体架构搭建和设计。
平台多功能研发	研发工作主要是所有子系统大数据平台（云模式）、数据采集系统、流量分析系统、用户与实体行为分析系统、网络安全威胁分析系统、业务安全监控系统、网站监测系统、数据泄露检测系统、数据安全管理系统、网络安全态势可视化系统、网络安全威胁通报与预警系统、安全运维管理系统的研发，以及系统之间的协同工作开发。
性能优化和升级	基于大数据分行列存式存储技术和ES多级索引技术，设计可便捷横向扩展的平台组件集群，提高数据流高速处理能力和大并发流量下的数据捕获效率，达到高性能、高扩展的目的。
产品灵活性和安全标准设计	基于国家标准的监控审计体系各级安全要求设计以及基于WEB服务的个性化模块组合和兼容性设计。

资料来源：公开资料，东兴证券研究所

企业移动信息化安全管理体系研发，包括安全能力建设（PaaS 与 SaaS）与客户端解决方案建设两个方面。安全能力建设包括基础设施、服务运营平台、应用安全管理平台、设备监测平台、安全分析平台等。客户端解决方案包括监测平台、管控平台、身份验证、客户端等。

图 34：企业移动信息化安全管理体系概要

资料来源：公开资料，东兴证券研究所

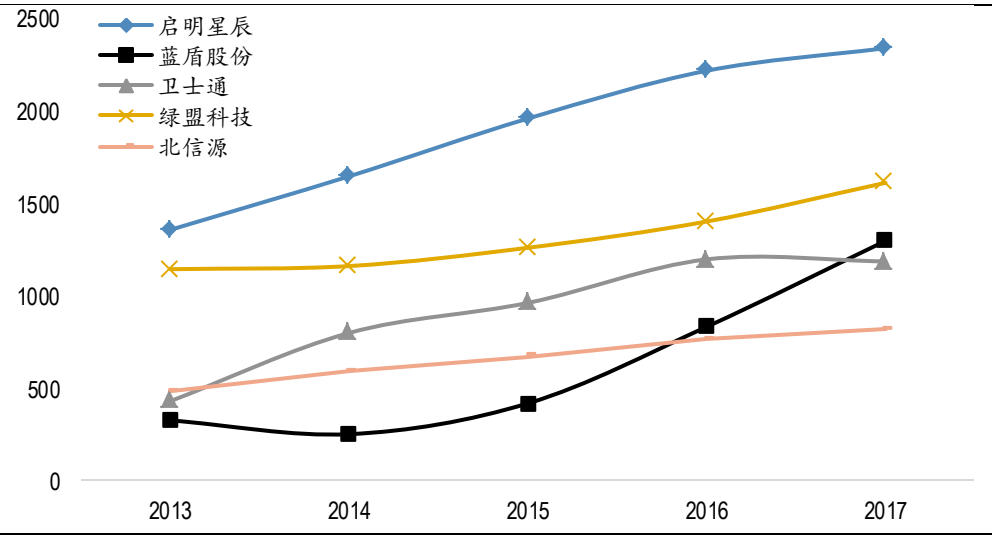
项目实施的重要意义主要体现吸纳优质人才、布局新兴领域、开拓西部市场三个层面。一、布局专精化防护等新安全重点方向，具体如上所示。**二、吸引西安地区优秀毕业人才，**西安地区有西安交大、西北工业大学。三、沣西新城是信息技术产业聚集地，目前已经有了全国人口数据（备份）中心、国家林业数据备份中心等十大部委的数据中心，未来拟建国家政务资源后台处理与备份中心、国家级大数据处理中心。

4.2 补短板：和安全产品巨头比，人才是蓝盾弱项，布局西部研发基地有望改善之

4.2.1 蓝盾高学历人员相对薄弱，是短板

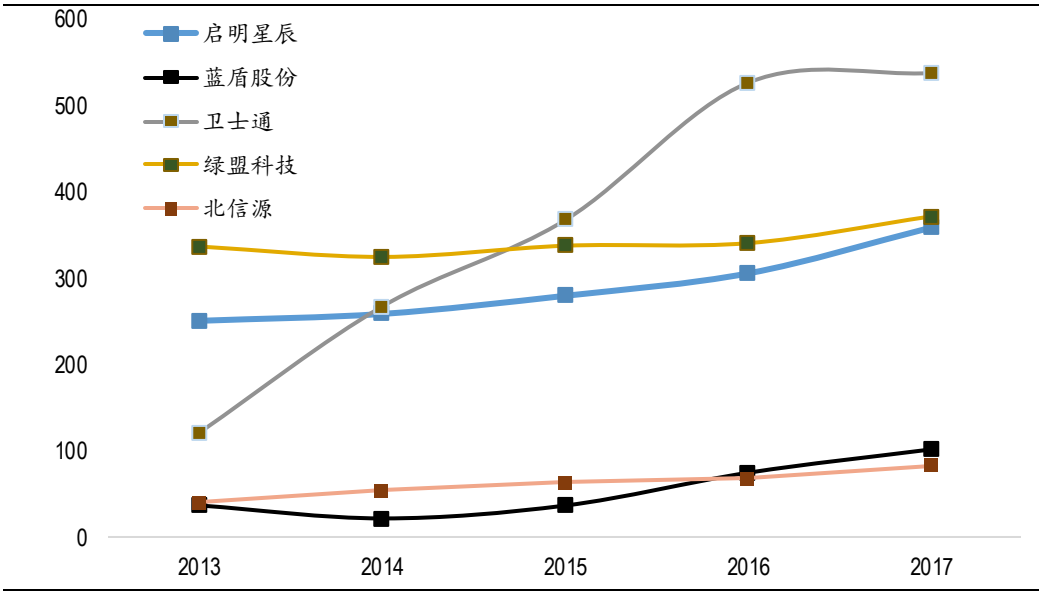
在安全厂商中，蓝盾高学历背景人才少，是蓝盾股份的短板。2017 年蓝盾股份本科学历员工人数为 1298 人，少于启明星辰、绿盟科技，略高于卫士通。2017 年蓝盾硕士以上学历员工人数为 102 人，显著少于卫士通（538 人）、启明星辰（359 人）、绿盟科技（372 人），可以看出，**高学历背景人才少是蓝盾的短板，这将制约蓝盾在安全攻防深入挖掘、人工智能算法探究方面的技术能力。**

图 35：蓝盾股份本科学历人员构成以及其与信息安全标的对比



资料来源：公开资料，东兴证券研究所

图 36：蓝盾股份硕士以上学历人员构成以及其与信息安全标的对比



资料来源：公开资料，东兴证券研究所

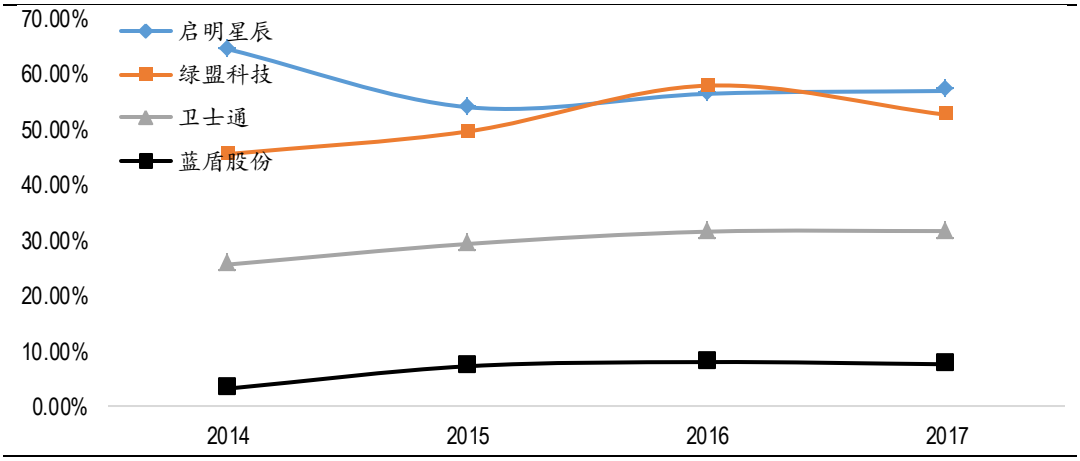
4.2.2 此举有望有效补短板

项目建设地点在陕西省西咸新区沣西新城，**周围有西安交通大学、西安电子科技大学、西北工业大学等理工科 985 院校**，高素质 IT 人才较多，有望进一步充实公司的人员力量。

4.3 建立北方区域运营销售中心，进一步强化业务向非华南地区拓展

目前广州蓝盾在“三北”地区营收占比明显偏少，与公司地理位置存在一定关系，**公司建立产业化基地有利于其在北方地区的营销本地化、服务本地化，推动其在北方地区的业务开展。**

图 37：蓝盾股份在三北地区业务占比以及其和其他信息安全标的的对比



资料来源：公开资料，东兴证券研究所

5. 收购中经电商，介入零售市场

5.1 油品预付卡销售领军企业

5.1.1 做终端客户和合作商户中介商

2016 年 4 月，蓝盾股份完成对中经电商和汇通宝 100%股权的交割。合计对价为 11 亿元，其中现金支付占比 15%、股份支付占比 85%。**2017 年，中经电商为蓝盾股份贡献扣非净利润 1.84 亿元。**

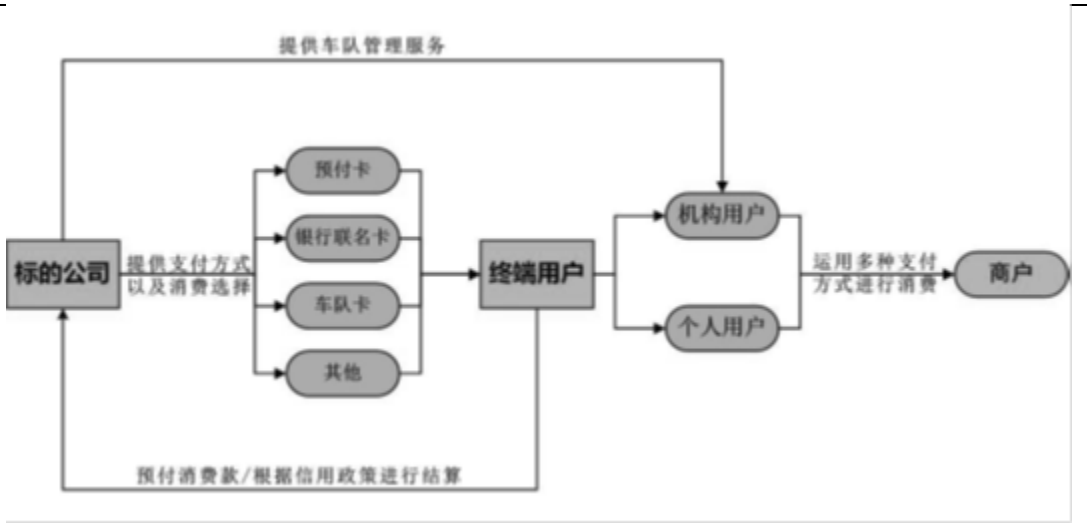
中经电商是以预付卡销售为业务核心的零售新业态公司。据相应公开资料披露，**主要通过预付的形式使线下合作商户实现预销售来获取市场份额**，并通过标的公司的电子商务网络及平台以及用户管理系统实现线下合作商户更有效率的营销与终端用户管理，线**下合作商户因此会根据业务推广金额或商品数量按一定的结算标准支付给标的公司相应的服务费用。**

对于合作商户而言，中经电商可以提供预付款，帮其提前锁定部分收入；对于终端客户而言，中经电商可以提供一定折扣（电子加油券-九八折，翼汇通-九五折）。中经电商相当于做了用户（包含个人以及车队等机构用户）、合作商户（目前以加油站为主，目标商户还包括零售、餐饮、居民服务业等行业）之间的一个中介商。

图 38：中经电商业务模式-对商户

资料来源：公开资料，东兴证券研究所。标的公司指中经电商，下同。

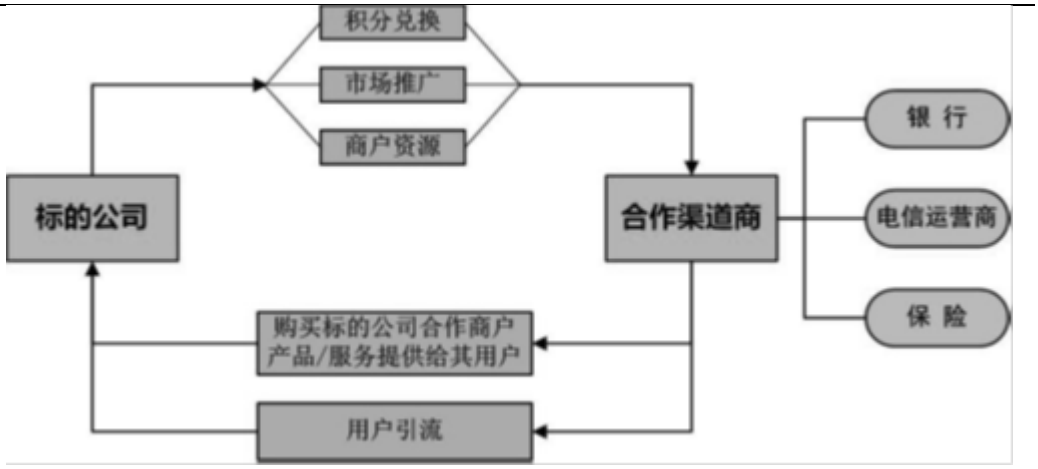
图 39：中经电商业务模式-对用户



资料来源：公开资料，东兴证券研究所

此外，公司充分认识到电信运营商与银行等金融机构在接触终端用户方面的强的能力，因此**开拓了和渠道商合作的模式**。目前渠道合作方**已经包括中国移动、联通、电信，建、农、工等银行，中国平安、阳光保险等险企。**公司可以为合作渠道商提供积分兑换、客户管理活动。

图 40：中经电商业务模式-对渠道商



资料来源：公开资料，东兴证券研究所

5.1.2 交易金额与用户数目增长态势显著

中经电商介入市场较早，发现并证实了加油领域“消费卡折扣销售+商户返佣”的业务模式，实现了用户数、交易金额的快速增长，是行业先行者，目前业务主要包括油品、非油品两大部分：

- **油品商户贡献了大多数的交易金额、但非油品商户增长迅猛。**2016 年油品合作客户 31.36 亿元，非油品 4.89 亿元；2017 年油品合作商户 35.26 亿元、增长 12.4%，非油品 8.91 亿元、增长 82.0%。
- **从合作商户端个数来看，非油品商户增长迅猛。**2016 年油品合作客户 3288 家，非

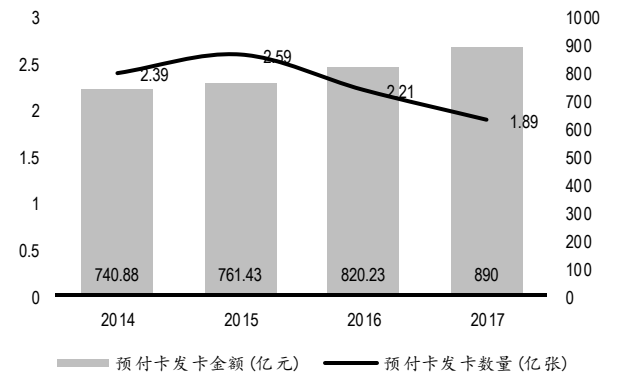
油品 4564 家；2017 年油品合作商户 4720 家、增长 43.6%，非油品 11470 家、增长 115.3%。

- 从用户构成来看，2016 年个人用户 9723148 个，机构用户 13336 家；2017 年个人用户 12226548 个、增长 25.8%，机构用户 13777 家、增长 3.31%。**个人用户在较大的基数上保持了较为显著的增长。**
- 从用户消费情况来看，2016 年个人用户消费 18.97 亿元，机构用户消费 17.29 亿元；2017 年个人用户消费 27.60 亿元、增长 45.4%，机构用户消费 16.56 亿元、同比略有下滑。**个人用户消费金额增长非常显著，且人均消费水平有所上升（2016 年，195.1 元/2017 年，225.8 元）。**

5.2 预付卡市场繁荣发展，中经汇通成长空间大

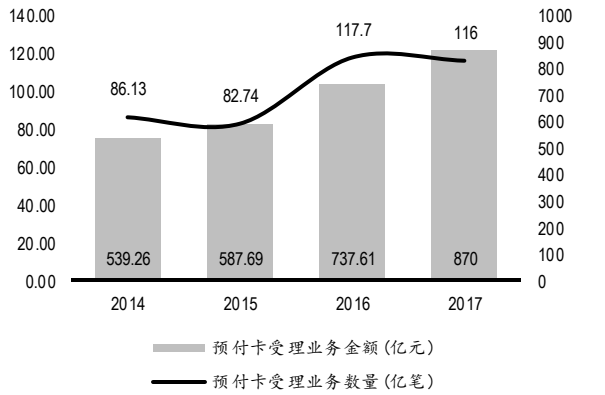
伴随消费升级以及新业态的不断涌现，我国预付卡支付市场繁荣发展，2017 年预付卡交易金额达到 870 亿元，2014-2017 年 CAGR 为 17.3%:

图 41：我国预付卡发卡情况，2014-2017



资料来源：中国支付清算协会，东兴证券研究所

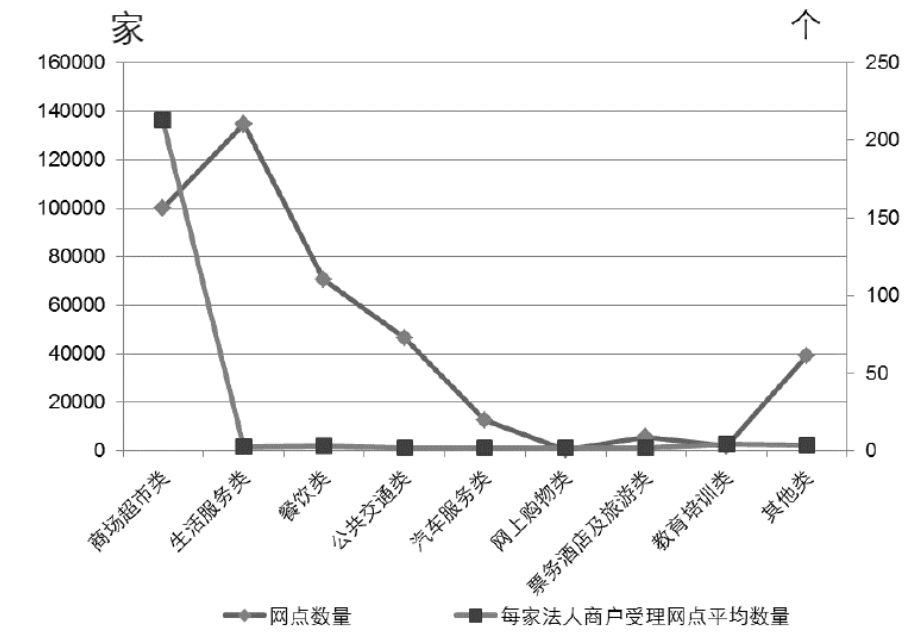
图 42：我国预付卡业务受理情况，2014-2017



资料来源：中国支付清算协会，东兴证券研究所，2015 年数据

2016 年数据显示，已有的很多支付网点以消费为场景、汽车类预付卡相对而言网点数目较少：

图 43：预付卡机构网点数量分类情况，2016

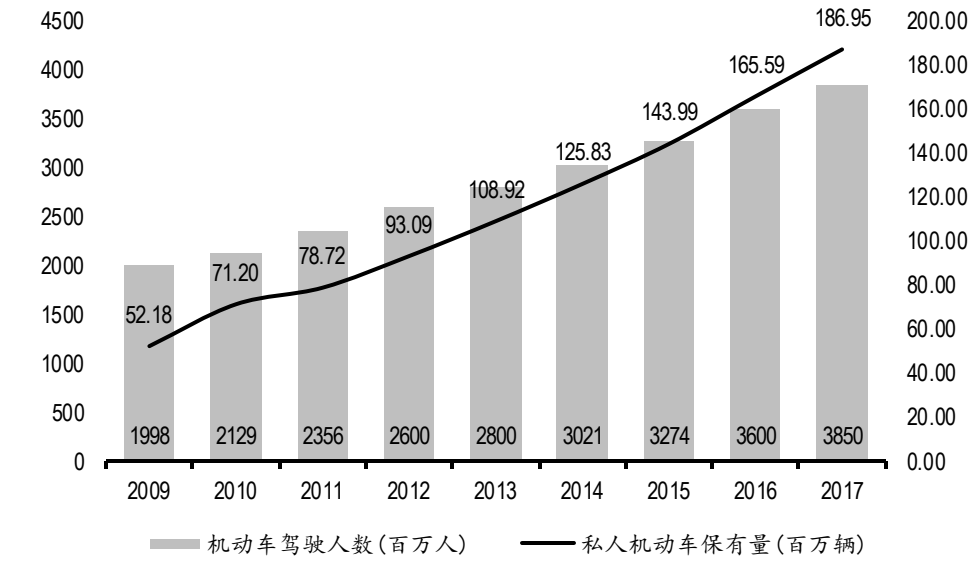


资料来源：中国支付清算协会，东兴证券研究所

中经电商切入市场早，交易金额高。假设中经电商 2017 年所有商户交易金额均通过预付卡完成，其 44 亿收入规模远高于行业平均水平（870 亿元/116 家，平均每家 7.5 亿元）。

从应用行业来看，中经电商传统优势领域为加油服务领域，我国机动车保有量和驾驶员数目保持稳步提升，中经电商仍有较大成长空间：在 2009 年至 2017 年间，我国机动车驾驶人数从 2.00 亿人增加到 3.85 亿人，CAGR 为 17.8%，与此同时，私人机动车保有量从 5218 万辆增长到 1.87 亿量，CAGR 为 37.6%。我们判断，伴随经济发展、人均可支配收入提升以及城镇化进程的推进，机动车保有量、驾驶员数目稳步提升的态势将持续，这为中经电商业务的持续开展提供了较强的基础。

图 44：我国机动车驾驶员数目和机动车保有量



资料来源：Wind，东兴证券研究所

6. 营收预测与估值

6.1 营收预测

6.1.1 安全以及安防集成：行业变革推动，集成业务有望高速增长

安全以及安防集成以信息安全系统集成为主，推算后者占整体约 90%或更多。参考我们前面的分析，**有望于目前整体日趋复杂化的安全形势以及安全行业整体高增长：**

- **安全法实施明确网络运营者的保护义务**：产品、服务提供者具有维护信息安全的义务，包括反病毒、放攻击、数据安全、应急响应等。利好整个安全行业。受到网络安全法的强势驱动，**预计信息安全行业市场规模至 2020 年可达 766 亿元，2017-2020 年 CAGR 为 23.5%。**
- 安全形势大变革，传统的依靠边界防护+终端管理+安全态势感知（SOC）三种产品堆砌的防护思路并不能保障用户的安全，**具有信息安全产品能力的信息安全集成厂商将拥有更多机会**，通过在系统架构、方案实施、运维监控、应急响应等维度的全方位介入将有效提升用户的系统安全和水平。

基于以上两点原因，判断蓝盾安全以及安防集成业务将维持强势增长态势，保守看，我们预计其未来的数年间 CAGR 不低于 25%。

6.1.2 安全以及安防产品：集成业务带动，保持稳步增长

蓝盾安全+安防板块的信息安全、电磁防护、水务检测三种业务：

- **安全产品，**受到系统集成业务的带动作用，**预计增速不低于行业平均水平，参考值 25%。**
- **电磁防护产品，2017 年营收 2.16 亿元，2015-2017 年 CAGR 为 23.1%，**华炜科技主要下游应用场景军事领域与高铁。军事领域，我们参考每年军费增长水平，认为其将继续保持稳定增长。高铁领域，根据《中长期铁路网规划》，我国高速铁路高速建设将持续，2020 年、2025 年高铁里程分别达到 3 万公里、3.8 万公里，2016 年、**2017 年高铁里程为 2.2 万公里、2.5 万公里，预计高铁列车生产制造行业仍将持续景气**；华炜科技 2014-2017 年 CAGR 为 16.6%，**预计其未来数年间复合增速在 15%左右。**
- 水务检测，受到行业十三五规划中对于水文监测+水利信息化业务的驱动，**预计其近年稳步增长的态势可基本维持，预计 20%+。**

由上，我们预计其未来的数年间 CAGR 不低于 20%。

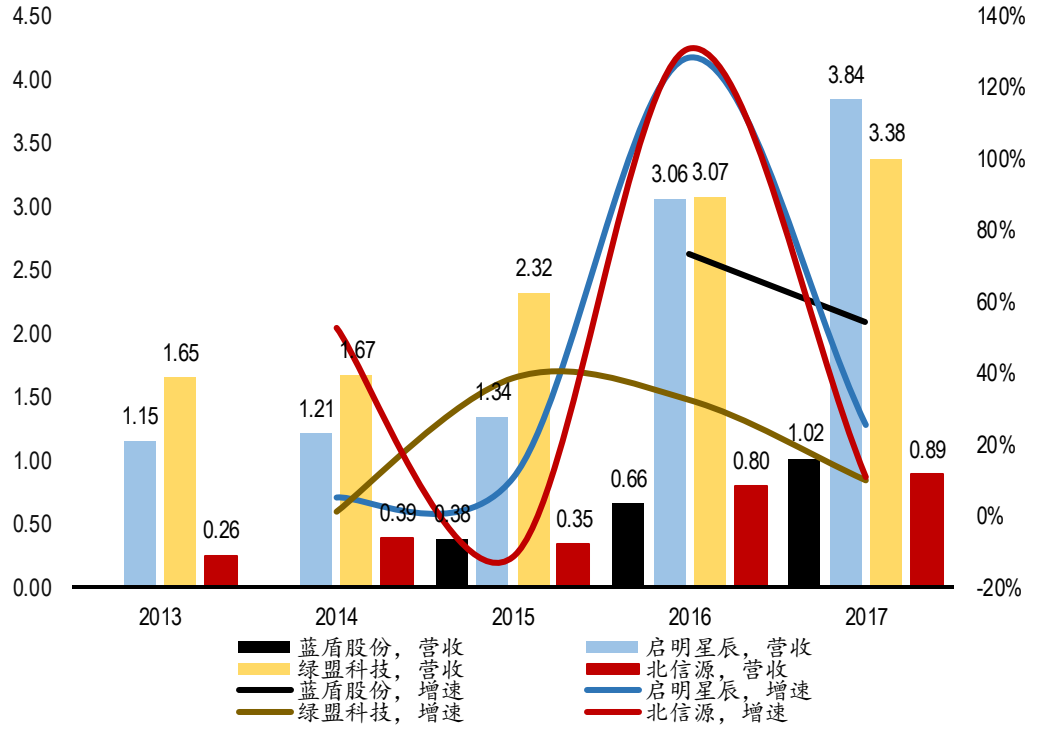
6.1.3 安全以及安防服务：近年信息安全服务整体增速较高，30%+增速可期

蓝盾的安全以及安防服务以信息安全为主，**2017 年信息安全服务规模为 1.02 亿元，2015-2017 年 CAGR 为 63.2%。**此外包含约三成的安防服务，2017 年业务规模 5002 万，对于这部分的分析可以参考上节。

近年安全服务业务增速强势，**是信息安全领域硬件、软件、服务三大划分中增速最快的领域**，主要原因包括：

- **近年信息安全形势经历深刻变革**，行业用户在应对钓鱼等新型攻击策略、加密病毒等新病毒形式、APT 等新威胁类型时，需要专业人员进行培训、指导、系统规划与应急响应，促进安全服务类业务快速增长。
- **网络安全法以及响应行业信息安全政策出台，**强化了行业用户就维护信息系统安全的认知，**促进人员培训业务快速启动。**

图 45：部分信息安全厂商安全服务*业务营收规模（单位：亿元）与增速



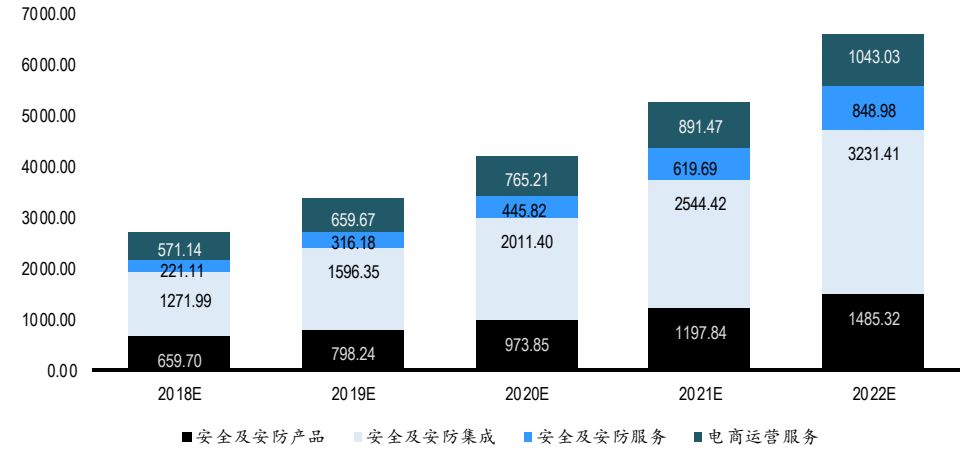
资料来源：公开资料，东兴证券研究所。

蓝盾特色是信息安全综合解决方案提供商，提供信息系统以及安全系统的构建部署，用户黏性好，因此我们判断其安全服务业务不会低于行业整体增速水平，近年强势增长的态势可以持续，**我们预计未来 3 年内复合增速不会低于 40%。**

6.1.4 零售：稳步增长可期

我国预付卡支付市场繁荣发展，2017 年预付卡交易金额达到 870 亿元，2014-2017 年 CAGR 为 17.3%。**中经汇通布局汽车服务领域，切入行业较早，2017 年商户交易金额 44 亿元，远高于有统计的企业平均水平。“消费卡折扣销售+商户返佣”商业模式独特，汽车服务领域市场空间大。**我们看好蓝盾电商的业务持续成长前景，其在 2016-2017 年营收规模为 3.01 亿元、4.97 亿元。**保守看，其未来三年业增速不低于 15%。**

图 46：蓝盾股份分版块营收预测（单位：百万元）



资料来源：公开资料，东兴证券研究所

综上，我们预计公司在 2018-2020 年的营收分别为 27.24 亿元、33.70 亿元、41.96 亿元，测算可得净利润为 5.87 亿元、7.38 亿元、9.31 亿元。对应 eps 为 0.47 元、0.59 元、0.74 元。

6.2 估值水平

我们预计公司零售业务板块在 2018 年的净利润约为 2.1 亿元，此业务以 25 倍估值测算，对应 52.5 亿元市值；此外安全以及安防板块贡献归母净利润约为 3.4 亿元，此业务以 35 倍估值测算，对应 119 亿元市值。**综上，分块测算加总，公司目标市值为 171.5 亿元，每股目标价为 14.59 元。**

7. 投资评级

公司是产品+集成信息安全全方位解决方案提供商，2017 年实现营收 22.16 亿元、净利润 4.41 亿元。增长强势，2013 年至 2017 年营收 CAGR 为 53.85%、净利润 CAGR 为 92.75%。

业务规模增长快：安全以及安防产品自 2013 年-2017 年营收 CAGR 为 57.9%，毛利率近三年在 55%-63%之间波动。安全以及安防集成 2013 年-2017 年营收 CAGR 为 38.2%，毛利率水平近年有所提升，近两年约为 40%-42%。安全以及安防服务 2015 年-2017 年营收 CAGR 为 78.3%，毛利率水平近年在 50%以上。

安全行业大变革，具有产品能力的信息安全集成厂商迎来发展机遇。

- 安全变革趋势下，更加要求信息安全系统的建设者具有深厚的安全研究积淀、较强的系统安全构建能力与对安全产品的深刻洞察，产品+集成商业模式凸显特色竞争优势。
- 随着攻防态势演变，传统的依靠边界防护+终端管理+安全态势感知（SOC）三种产品堆砌的防护思路并不能保障用户的安全，安全架构在设计系统时需要考虑系统在应用场景上的实际特点、安全产品的协同联动、系统针对未知威胁的影响能力与策略，这些都需要大量深入的安全知识，因此在系统规划设计部署落地的阶段，安全的能力和从业的经验将凸显其重要性，具有安全产品生产经验的系统集成厂商竞争性将凸显。对于这些厂商来说，其系统集成业务的营收与毛利率有望出现双重增长。

目前产品+集成商业模式在大多数信息安全上市公司中不多见，蓝盾是具有特色的产品+集成信息安全解决方案提供商。我们预计公司零售业务板块在 2018 年的净利润约为 2.1 亿元，此业务以 25 倍估值测算，对应 52.5 亿元市值；此外安全以及安防板块贡献归母净利润约为 3.4 亿元，此业务以 35 倍估值测算，对应 119 亿元市值。综上，**分块测算加总，公司目标市值应为 171.5 亿元，每股目标价为 14.59 元。**

给予“强烈推荐”评级。

风险提示：信息安全领域近年受到信息技术业界高度关注，存在行业竞争加剧、影响公司盈利能力的风险。

8. 风险提示

公司可转债发行存在不确定性；公司应收账款占比大。

表 11：公司盈利预测

资产负债				单位:百万元		利润表				单位:百万元	
	2016A	2017A	2018E	2019E	2020E		2016A	2017A	2018E	2019E	2020E
流动资产合计	3990.61	4996.39	5647.07	6530.37	7619.47	**营业收入**	1573.50	2216.48	2723.94	3370.44	4196.28
货币资金	2093.27	1666.73	2042.96	2527.83	3147.21	**营业成本**	749.02	1009.05	1251.20	1563.01	1961.48
应收账款	1018.36	1897.92	2089.60	2400.86	2759.20	营业税金及附加	17.14	24.68	29.96	37.07	46.16
其他应收款	28.20	34.18	42.00	51.97	64.70	营业费用	80.21	141.49	177.06	215.71	264.37
预付款项	710.11	1113.47	1113.47	1113.47	1113.47	管理费用	291.49	385.84	490.31	606.68	755.33
存货	121.67	220.76	274.24	342.58	429.91	财务费用	69.06	120.65	69.40	56.59	43.69
其他流动资产	6.05	47.26	47.26	47.26	47.26	资产减值损失	35.95	100.89	110.00	120.00	130.00
非流动资产合	2311.13	3292.59	3140.29	2978.73	2814.23	公允价值变动收	0.00	0.00	0.00	0.00	0.00
长期股权投资	2.36	14.26	14.26	14.26	14.26	投资净收益	0.43	0.34	0.00	0.00	0.00
固定资产	550.83	642.99	683.04	709.59	729.39	**营业利润**	331.07	521.12	683.01	858.37	1082.26
无形资产	202.00	407.18	366.46	329.81	296.83	营业外收入	47.47	0.14	0.00	0.00	0.00
其他非流动资	416.35	272.34	272.34	272.34	272.34	营业外支出	5.33	6.50	0.00	0.00	0.00
资产总计	6301.74	8288.98	8787.36	9509.10	10433.71	**利润总额**	373.21	514.76	683.01	858.37	1082.26
流动负债合计	1722.76	3006.18	2924.20	2976.57	3057.50	所得税	49.35	73.45	95.62	120.17	151.52
短期借款	725.00	1282.07	1112.95	998.72	866.78	**净利润**	323.86	441.31	587.39	738.20	930.74
应付账款	224.56	347.51	668.45	835.03	1047.91	少数股东损益	0.96	27.50	38.00	50.00	60.00
预收款项	460.65	823.45	823.45	823.45	823.45	归属母公司净利	322.89	413.81	549.39	688.20	870.74
一年内到期的非流动负债	22.95	145.16	145.16	145.16	145.16	EBITDA	515.56	790.54	903.08	1075.06	1289.13
非流动负债合	974.98	1193.61	1193.61	1193.61	1193.61	**EPS（元）**	0.30	0.35	0.47	0.59	0.74
长期借款	539.64	766.54	766.54	766.54	766.54						
应付债券	298.94	299.44	299.44	299.44	299.44	**主要财务比率**	2016A	2017A	2018E	2019E	2020E
负债合计	2697.75	4199.79	4117.81	4170.17	4251.11	**成长能力**					
少数股东权益	32.35	106.23	144.23	194.23	254.23	营业收入增长	57.21%	40.86%	22.90%	23.73%	24.50%
实收资本（或股本）	1175.46	1175.37	1175.37	1175.37	1175.37	营业利润增长	195.63%	57.41%	31.06%	25.67%	26.08%
资本公积	1876.01	1895.41	1895.41	1895.41	1895.41	归母净利润增长	32.76%	25.27%	32.76%	25.27%	26.53%
未分配利润	551.04	927.54	1367.05	1917.61	2614.21	**获利能力**					
归属母公司股东权益合计	3571.64	3982.96	4525.32	5144.70	5928.37	毛利率(%)	52.40%	54.48%	54.07%	53.63%	53.26%
负债和所有者	6301.74	8288.98	8787.36	9509.10	10433.71	净利率(%)	20.58%	19.91%	21.56%	21.90%	22.18%
现金流量				单位:百万元		总资产净利率	5.12%	4.99%	6.25%	7.24%	8.35%
	2016A	2017A	2018E	2019E	2020E	ROE(%)	9.04%	10.39%	12.14%	13.38%	14.69%
经营活动现金	343.20	25.35	758.72	844.51	1012.09	**偿债能力**					
净利润	323.86	441.31	587.39	738.20	930.74	资产负债率(%)	42.81%	50.67%	46.86%	43.85%	40.74%
折旧摊销	115.43	148.77	109.95	123.45	130.20	流动比率	2.32	1.66	1.93	2.19	2.49
财务费用	69.06	120.65	69.40	56.59	43.69	速动比率	2.25	1.59	1.84	2.08	2.35
应付帐款的变	0.00	0.00	(191.67)	(311.26)	(358.34)	**营运能力**					
预收帐款的变	0.00	0.00	0.00	0.00	0.00	总资产周转率	0.37	0.30	0.32	0.37	0.42
投资活动现金	(703.10)	(1178.61)	(110.00)	(120.00)	(130.00)	应收账款周转率	1.94	1.52	1.37	1.50	1.63
公允价值变动	0.00	0.00	0.00	0.00	0.00	应付账款周转率	7.54	7.75	5.36	4.48	4.46
长期股权投资	0.00	0.00	0.00	0.00	0.00	**每股指标（元）**					
投资收益	0.43	0.34	0.00	0.00	0.00	每股收益(最新摊	0.30	0.35	0.47	0.59	0.74
筹资活动现金	1907.52	678.53	(272.49)	(239.64)	(262.71)	每股净现金流(最	1.32	(0.40)	0.32	0.41	0.53
应付债券增加	0.00	0.00	0.00	0.00	0.00	每股净资产(最新	3.04	3.39	3.85	4.38	5.04
长期借款增加	0.00	0.00	0.00	0.00	0.00						
普通股增加	204.77	(0.09)	0.00	0.00	0.00						
资本公积增加	1865.85	19.40	0.00	0.00	0.00						
现金净增加额	1547.61	(474.72)	376.23	484.87	619.38						

分析师简介

杨若木

基础化工行业小组组长，9 年证券行业研究经验，擅长从宏观经济背景下，把握化工行业的发展脉络，对周期性行业的业绩波动有比较准确判断，重点关注具有成长性的新材料及精细化工领域。曾获得卖方分析师"水晶球奖"第三名，"今日投资"化工行业最佳选股分析师第一名，金融界《慧眼识券商》最受关注化工行业分析师，《证券通》化工行业金牌分析师。

研究助理简介

韩宇：北京航空航天大学通信与信息系统专业学术硕士，并拥有 2 年市场咨询研究经验。2016 年进入东兴证券研究所，关注 TMT 领域。

分析师承诺

负责本研究报告全部或部分内容的每一位证券分析师，在此申明，本报告的观点、逻辑和论据均为分析师本人研究成果，引用的相关信息和文字均已注明出处。本报告依据公开的信息来源，力求清晰、准确地反映分析师本人的研究观点。本人薪酬的任何部分过去不曾与、现在不与，未来也将不会与本报告中的具体推荐或观点直接或间接相关。

风险提示

本证券研究报告所载的信息、观点、结论等内容仅供投资者决策参考。在任何情况下，本公司证券研究报告均不构成对任何机构和个人的投资建议，市场有风险，投资者在决定投资前，务必要审慎。投资者应自主作出投资决策，自行承担投资风险

免责声明

本研究报告由东兴证券股份有限公司研究所撰写，东兴证券股份有限公司是具有合法证券投资咨询业务资格的机构。本研究报告中所引用信息均来源于公开资料，我公司对这些信息的准确性和完整性不作任何保证，也不保证所包含的信息和建议不会发生任何变更。我们已力求报告内容的客观、公正，但文中的观点、结论和建议仅供参考，报告中的信息或意见并不构成所述证券的买卖出价或征价，投资者据此做出的任何投资决策与本公司和作者无关。

我公司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头寸并进行交易，也可能为这些公司提供或者争取提供投资银行、财务顾问或者金融产品等相关服务。本报告版权仅为我公司所有，未经书面许可，任何机构和个人不得以任何形式翻版、复制和发布。如引用、刊发，需注明出处为东兴证券研究所，且不得对本报告进行有悖原意的引用、删节和修改。

本研究报告仅供东兴证券股份有限公司客户和经本公司授权刊载机构的客户使用，未经授权私自刊载研究报告的机构以及其阅读和使用者应慎重使用报告、防止被误导，本公司不承担由于非授权机构私自刊发和非授权客户使用该报告所产生的相关风险和责任。

行业评级体系

公司投资评级（以沪深 300 指数为基准指数）：

以报告日后的 6 个月内，公司股价相对于同期市场基准指数的表现为标准定义：

强烈推荐：相对强于市场基准指数收益率 15%以上；

推荐：相对强于市场基准指数收益率 5%～15%之间；

中性：相对于市场基准指数收益率介于-5%～+5%之间；

回避：相对弱于市场基准指数收益率 5%以上。

行业投资评级（以沪深 300 指数为基准指数）：

以报告日后的 6 个月内，行业指数相对于同期市场基准指数的表现为标准定义：

看好：相对强于市场基准指数收益率 5%以上；

中性：相对于市场基准指数收益率介于-5%～+5%之间；

看淡：相对弱于市场基准指数收益率 5%以上。