启明星辰（002439）深度报告

拓展加密打造信息安全旗舰，引领构建开放式安全生态圈

买入（维持）

2016 年 6 月 21 日

计算机首席证券分析师郝彪
执业资格证书号码：S0600516030001
haob@dwzq.com.cn

联系人陈晨
chenchen@dwzq.com.cn

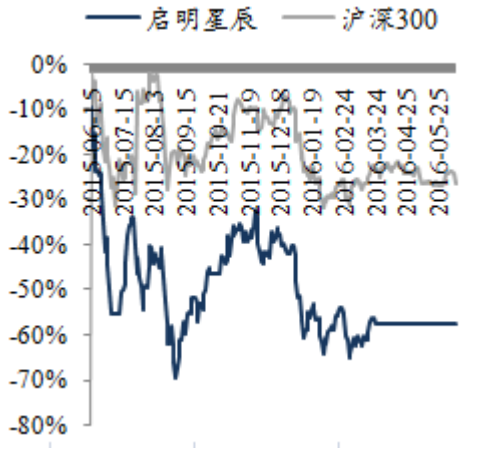
盈利预测与估值

	2015	2016E	2017E	2018E
营业收入（百万元）	1,534	2,127	2,907	3,918
同比（%）	28.3%	38.7%	36.7%	34.8%
净利润（百万元）	244.13	404.97	582.57	816.55
同比（%）	43.3%	65.9%	43.9%	40.2%
毛利率（%）	67.0%	69.0%	70.3%	71.4%
ROE（%）	14.4%	19.9%	23.0%	25.3%
每股收益（元）	0.29	0.47	0.67	0.94
P/E	80	51	35	25
P/B	12	10	8	6

投资要点

- **维持买入评级：**如考虑增发摊薄，2016-2018 年备考 EPS 分别为 0.50 元/0.71 元/0.99 元，目前股价对应 PE 分别为 47/33/24 倍。公司近五年净利润维持 44%的复合增速，在同行业中处于绝对领先地位，开放合作引领安全生态发展，应享有估值溢价。
- **网络边界不断拓展，信息安全行业迎来全新的发展空间：**万物互联和传统行业的日益触网奠定网络安全产业的长期发展逻辑，仅网络空间国防安全市场、云安全市场、物联网等行业即有望为网络安全带来过两千亿的全新增长空间。由于网络战军备竞赛升级，云、物联网（包括工业互联网、车联网、智能家居）市场的兴起，国产替代的需求等多重因素的影响，我们预计国内网络安全行业增速有望从目前的 14%左右上升到 20%。
- **收购赛博兴安拓展加密，内生外延打造信息安全旗舰：**公司以 6.3 亿元收购赛博兴安 100%股权，赛博兴安主要业务为面向军队、军工和政府部门等提供边界防护产品、安全管理与综合防护产品、数据安全产品，本次收购将完善启明星辰在网络传输加密、加密认证的深度布局。公司此前收购书生电子、合众数据、安方高科等，并通过自研使得业务从网络安全拓展到可信安全、物理安全、数据安全、应用安全等领域，拓展加密后产品形态更加完整，信息安全大航母扬帆起航。
- **发布 SOC3.0 构建开放全新的安全生态圈：**公司一方面牵手腾讯、华为等互联网和 IT 巨头打造云-网-端三位一体安全，另一方面向在安全威胁分析领域的广大安全厂商开放泰合 SOC3.0 安管平台的南向和北向数据接口，共同打造智能化大数据安管大平台。SOC 相当于安全行业的 ERP 平台，3.0 情况下开放安全分析接口，可以实现政企客户网络中全要素信息和数据的连接，并允许第三方安全分析能力以类似 App 的形式接入平台并组合应用，一方面可更加主动、智能地对企业和组织的网络安全进行管理和运营，另一方面可实现数据的跨企业整合和共享，安全业态从封闭迈向开放式发展，公司的平台属性强化。

股价走势



市场数据

收盘价(元)	23.66
一年最低价/最高价	17.00/43/96
市净率	10.3
流通 A 股市值(百万元)	13021.5

基础数据

每股净资产(元)	2.29
资产负债率(%)	30.12
总股本(百万股)	868.94
流通 A 股(百万股)	550.36

相关研究

启明星辰：SOC3.0 打造互联互通智能化大数据安全管理平台，迈出构建开放式业态第一步
2016 年 5 月 2 日

启明星辰：保守会计下仍实现快速增长，军民融合云安全前景广阔
2016 年 3 月 26 日

启明星辰：军民融合推动业务高速增长
2016 年 2 月 29 日

1. 网络安全行业迎来新的发展空间

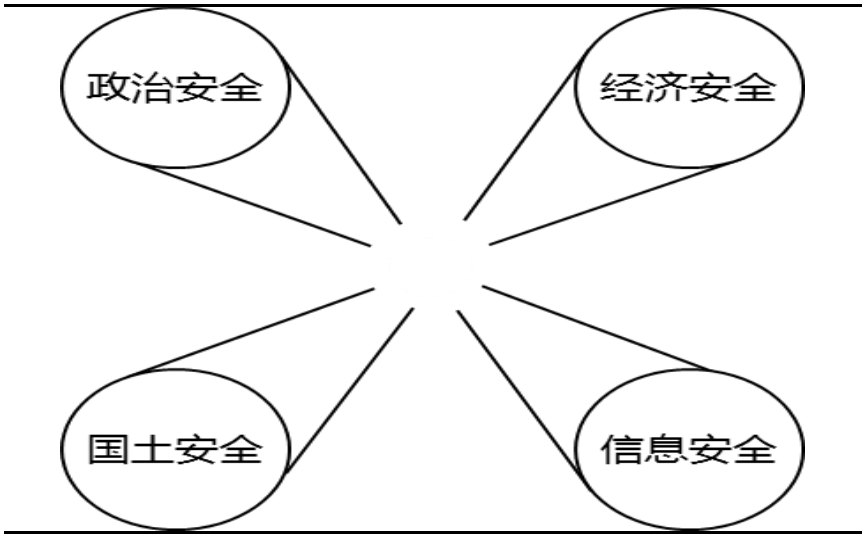
近年来，网络安全问题已经成为我国发展的一个重要议题。继 2013 年 11 月 12 日国家安全委员会正式成立之后，2014 年 2 月 27 日成立了中共中央网络安全和信息化领导小组办公室，由习近平主席亲自挂帅，将网络安全提升到国家战略高度。2015 年 6 月，《网络安全法》的草案颁布，网络安全的战略高度得到进一步的提升，而行业也正在迎接全新的发展机会。

1.1. 信息安全战略高度，市场空间指日可待

1.1.1. 战略层面关注度持续提升，年内有望推出网络安全法

信息安全正在成为国家安全的四大组成部分之一：进入 2000 年后，随着信息化的迅猛推进，网络逐渐成为了世界各国政府、商业、教育的基础设施连接的枢纽，与经济、政治、军事、文化息息相关，目前正在成为社会生活不可或缺的基础性支撑。信息网络已经独立于实体空间而衍生出一个庞大的“网域”空间，各行各业信息的电子化使得网络安全问题不再是单纯的技术问题，而是演变为复杂的社会问题，网络安全与国土安全、政治安全、经济安全一起成为国家安全的重要组成部分。

图表 1 网络安全正成为国家安全的重要组成部分之一



资料来源：互联网，东吴证券研究所

网络安全法草案彰显重大历史进步：从 2003 年国家信息化领导小组提出要“抓紧起草研究《网络安全法》”已有十多个年头，《网络安全法》草案终于于去年落地了。作为第一部网络安全法，草案宣示了国家网络安全工作的基本原则，如坚持网络安全与信息化发展并重，提出网络空间主权，强化网络安全顶层设计从上至下落实到行业规划。同时在基础设施方面扩展了保护范围，首次明确了关键信息基础设施范围，包括基础信息网络、重点行业信息系统、公共服务领域重要信息系统、军事网络、地市级以上国家机关政务网络、用户数量众多的网络服务商系统，而最后这一点包含了许多私营企业，因此草案的颁布也对他们提出了更高的要求。

信息安全正在成为国家安全的四大组成部分之一：进入 2000 年后，随着信息化的迅猛推进，网络逐渐成为了世界各国政府、商业、教育的基础设施连接的枢纽，与经济、政治、军事、文化息息相关，目前正在成为社会生活不可或缺的基础性支撑。信息网络已经独立于实体空间而衍生出一个庞大的“网域”空间，各行各业信息的电子化使得网络安全问题不再是单纯的技术问题，而是演变为复杂的社会问题，信息安全与国土安全、政治安全、经济安全一起成为国家安全的重要组成部分。

信息安全战略地位空前提高：2016 年 1 月 23 日，中共中央政治局召开会议审议通过《国家安全战略纲要》; 4 月 19 日习近平总书记主持召开了网络安全和信息化工作座谈会；此后 4 月 29 日，第三届首都网络安全日启动仪式在北京展览馆举办；5 月 5 日，由《经济参考报》牵头的国家信息安全产品（自主）生存发展之路调研座谈会在北京召开。有多位参会人士表示我国目前的信息安全现状不容乐观，并且可能会对国民经济的发展造成重大的影响；5 月 7 日，全国信息安全标准化技术委员会在京举办座谈会。针对如何维护个人信息安全，中国全国信息安全标准化技术委员会秘书长高林透露，信息数据采集的“行为准则”正在报批过程中；5 月 16 日，在贵阳召开的第十三届中国信息港论坛上，工信部网络安全管理局局长赵志国表示目前我国正积极推进《电信法》立法进程，如果顺利的话，网络安全法 2016 年内有望出台（该法律的草案已于 2015 年 6 月发布）。

图表 2 今年以来国内主要信息安全事件

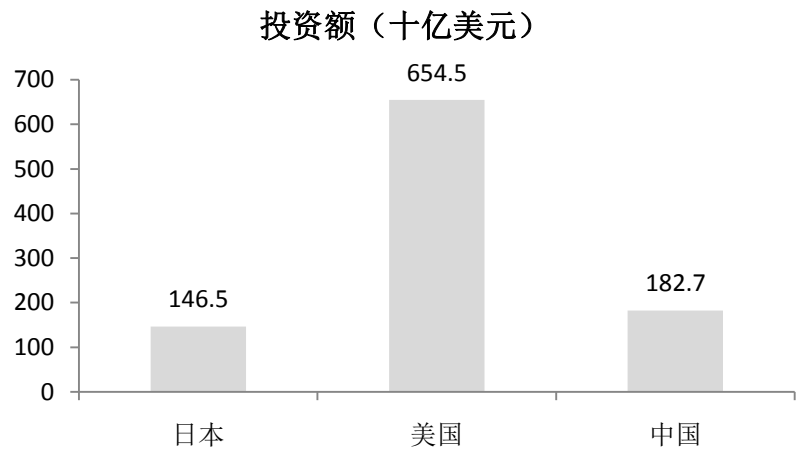
时间	政策事件
1 月 23 日	中共中央政治局召开会议审议通过《国家安全战略纲要》。
4 月 19 日	习近平总书记主持召开了网络安全和信息化工作座谈会。
5 月 5 日	由《经济参考报》牵头的国家信息安全产品（自主）生存发展之路调研座谈会在北京召开。
5 月 7 日	全国信息安全标准化技术委员会在京举办座谈会。
5 月 16 日	第十三届中国信息港论坛上，工信部发言人表示网络安全法年内有望出台。

资料来源：互联网，东吴证券研究所

1.1.2. 国内信息安全行业空间缺口巨大

国内 IT 投资总额与发达经济体存在差距：IDC 发布的研究报告《中国 IT 安全硬件、软件和服务全景图，2014-2018》显示，2013 年国内的 IT 总投资额约人民币 1827 亿美元，与美国 6545 亿美元的 IT 总投资差距仍较大，因此预计未来中国 IT 投资额将维持持续增长的趋势。

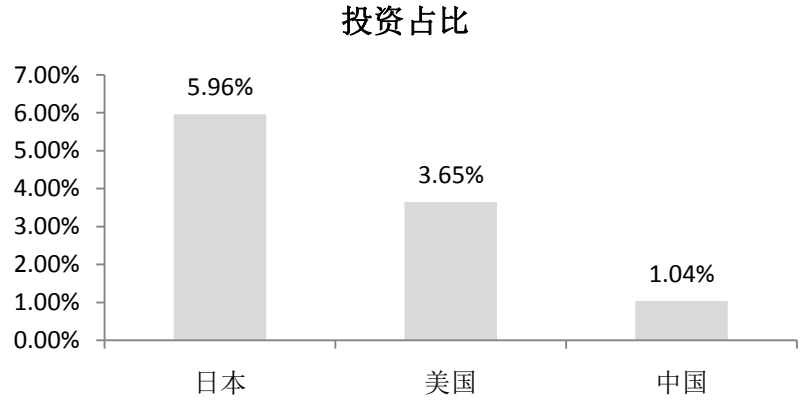
图表 3　2013 年中国与发达国家 IT 投资额比



资料来源：IDC，东吴证券研究所

国内信息安全投资占 IT 总投资之比远低于发达国家：除了 IT 总投资额的差距外，根据 IDC 的数据，2013 年中国信息安全投资总额为 19 亿美元，这一数字对比整体 IT 投资，信息安全投资占国内总 IT 投资占比仅为 1.04%，远低于日本的 5.96%及美国的 3.65%，显示中国与发达国家如日本和美国差距仍较为明显。

图表 4　2013 年中国信息安全投资比例远低于发达国家

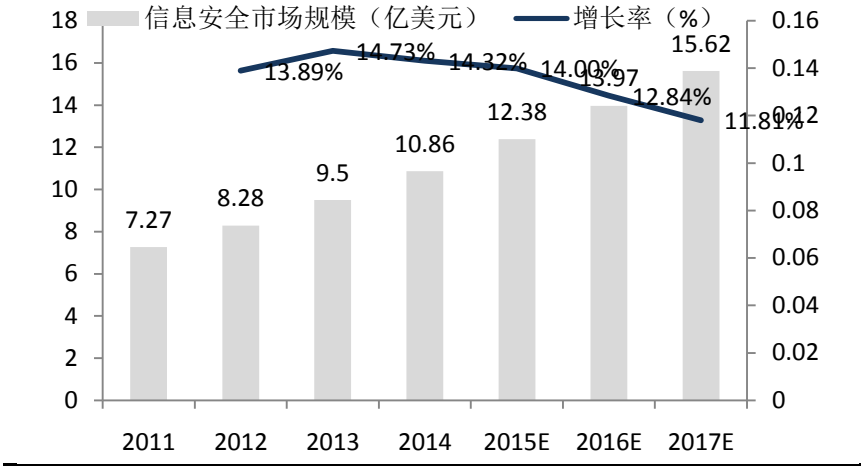


资料来源：IDC，东吴证券研究所

国内信息安全市场规模实现逐年增长：国内信息安全的市场规模在 2014 年达到 10.86 亿美元，年增长率为 14.73%，预计 2015 年市场将达到 12.38 亿美元规模，增长仍维持 14%的水平。考虑到 IT 投资总额与世界水平的差距，在信息安全的需求不断被发掘之后，将会有超过 30 倍的成长空间。以美国为例，美国目前的 IT 投资总额为 6454 亿美元，其中信息安全占比为 3.65%，即信息安全投资额为 23.87 亿美元；反观中国，仅有 1.9 亿美元左右的信息安全领域的投资额，差距为 10 倍左右。同时，我国目前在网络空间的战略部署还很薄弱，目前尚没有建立有建制的网络部队，在信息安全人才招募和网络武器研发方面也远远落后西方国家。因此，

预计未来信息安全市场的增速仍将能够维持在高位。

图表 5 中国信息安全市场规模及其增长率



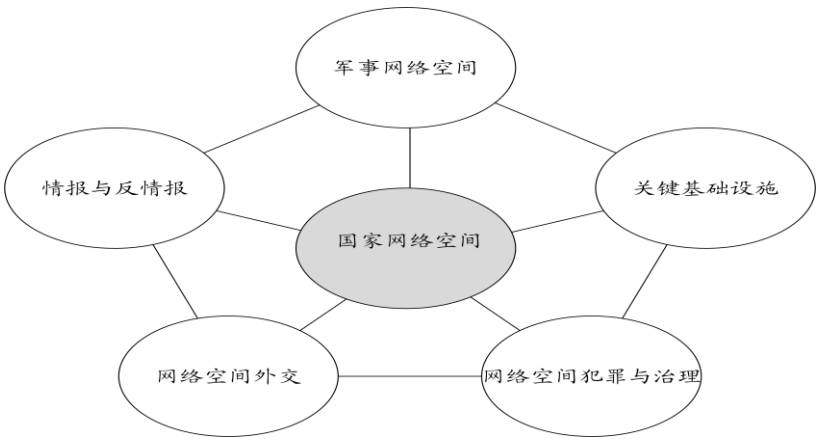
资料来源：IDC，东吴证券研究所

1.2. 全新市场需求将信息安全产业推向新高潮

1.2.1. 网络战加剧有望带来每年近千亿市场

国家网络空间安全建设带来行业本质的变化：一般来说传统的网络安全需求主要局限于企业和个人，国家网络空间安全需求的出现不仅使得网络安全含义立体化，也使得行业市场空间将从目前的一两百亿扩展到千亿以上。国家网络空间安全（NCS）在未来的国家安全中将处于比目前的军事安全更底层，战略地位更突出，其可以分为 5 个不同的领域：1、军事网络空间； 2、关键基础设施保护（CIP）与危机管理；3、情报与反情报；4、防止网络空间犯罪；5、网络空间外交与因特网治理。

图表 6 国家网络空间安全的构成

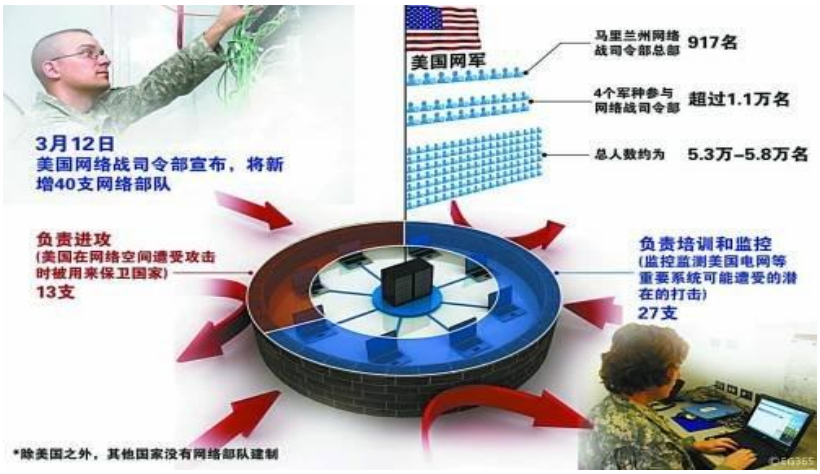


资料来源：绿盟科技，东吴证券研究所

全球网络空间军备竞赛进程进一步加快：2009 年 6 月奥巴马下令由美军战略司令部负责组建网络战司令部，以统一协调保障美军网络安全和开展网络战等与电脑网络有关的军事行动。10 月美国政府正式成立“网络作战司令部”，并计划招聘 4000 名黑客，组建特种部队。2011 年 5 月美

国发布《网络空间国际战略》提出网络战，成为世界上第一个提出网络战概念的国家，也是第一个将其应用于实战的国家。组建网络司令部，意味着美军将网络安全提升到非常重要的地位，网络战将被视为未来的战争形态之一。除了美国，目前俄罗斯、以色列、伊朗、韩国等 40 多个国家已成立了网络部队。演习上，2012 年，欧美、亚洲等国家和地区先后举办各种网络防御演习 10 余次，以提升对网络危机的评估和应对能力，以及关键信息基础设施的防御恢复能力。随着信息作为经济社会发展的战略资源越来越受到重视，脆弱的信息安全对经济安全、公共安全的威胁程度逐步加大，网络军备竞赛有愈演愈烈的态势。

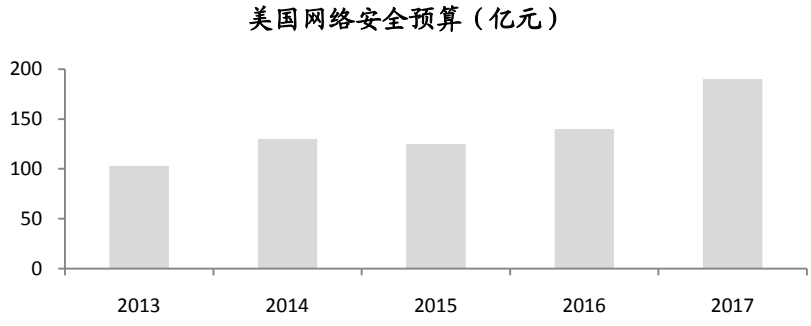
图表 7 网络空间军备竞赛展开



资料来源：互联网，东吴证券研究所

网络空间国防安全市场超千亿：以美国为例，自其 2013 年拨款 103 亿美元加强网络安全以来，美国投入网络安全的财政预算不断增长。2016 年全年预算 140 亿美元，而在今年 2 月 9 日，美国总统奥巴马提出《网络安全国家行动计划》(CNAP)，并提议在国会 2017 年财政预算中拨款 190 亿美元用于加强网络安全（一说被共和党拒绝）。考虑到目前中国市场规模及军事信息安全需求度提升，根据 IDC 的统计，2013 中国的网络安全硬件投资额仅为 19 亿美元，参考美国预算则未来具有超千亿的确定性市场。

图表 8 美国网络安全预算

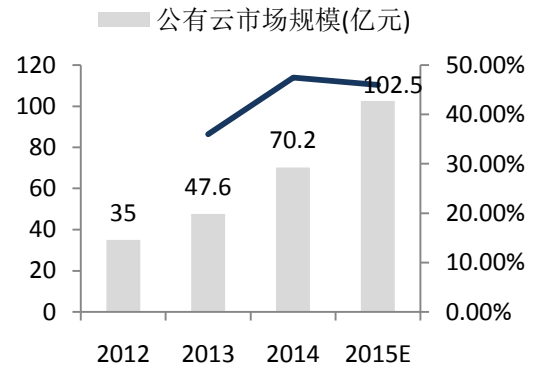


资料来源：IDC，东吴证券研究所

1.2.2. 云计算为信息安全带来千亿发展空间

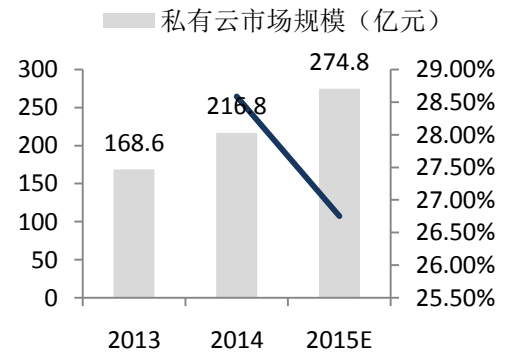
云计算高速增长迎来行业爆发：2015 年以来，国务院提出要在 2020 年让云计算成为信息化的重要形态和建设网络强国的重要支撑，并随之提出“互联网+”的指导概念，政策甫一出台便得到了积极的反馈。首先是亚马逊、阿里云等云计算大厂商交出的亮眼成绩单，其次是阿里巴巴、腾讯等互联网巨头纷纷进行云计算领域的投资布局。而从统计机构的数据来看，2015 年全球云服务市场规模已经达到了 1750 亿美元，同比实现 14.5%的增长，预计 2016 年将达到 2040 亿美元，增长率为 16.5%。而国内的云计算体量仍然较小，公有云在 2015 年突破 100 亿元人民币，私有云市场在 270 亿元以上，在全球占比约为 3%。

图表 9 国内公有云市场规模及增速



资料来源：中国信息通信研究院，东吴证券研究所

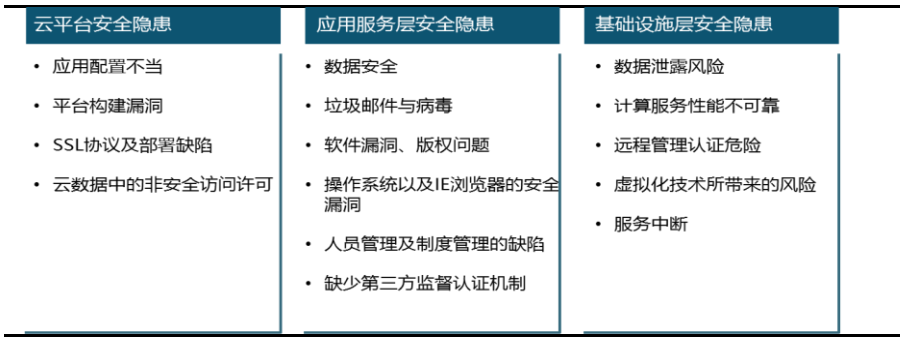
图表 10 国内私有云市场规模及增速



资料来源：中国信息通信研究院，东吴证券研究所

云计算的虚拟化架构带来更大的安全隐患：云计算将原先在企业内部封闭的 IT 系统内部较为稳定的运营模式转移为在云端的虚拟化架构下的业务处理，使得原先相对封闭可控的风险点出现了开放性的变化。因为在云计算架构下，对外接口呈现多样性，导致攻击行为难以被监控，风险点分布更广，风险点更难被隔离。同时由于客户的广泛性及信息的多样化，一旦云端服务器遭到黑客入侵，或服务器和云端系统供应商在系统中留有后门，企业信息将完全暴露，危害极大。常见的安全隐患主要来自云平台、应用服务层及基础设施层。

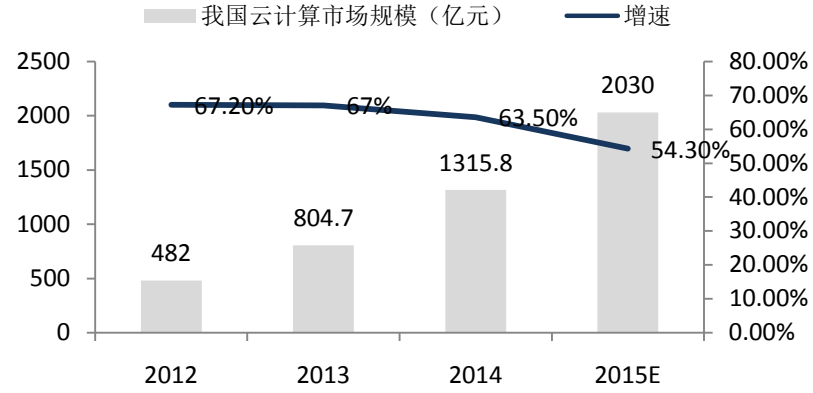
图表 11 云计算带来更大的安全隐患



资料来源：互联网，东吴证券研究所

云计算将带来更多的防护投入：赛迪顾问预测 2015 年云计算市场整体规模可达到 2030.0 亿元（相较中国信息通信研究院的统计，我们预计赛迪的统计口径包含了设备和集成），同比增长 54.3%。2012-2015 年，我国云计算市场保持高速增长态势，年均复合增长率高达 61.5%。从技术角度看，云计算带来了超出传统 IT 架构的风险，而与此同时，由于云计算目前的细分领域主要集中于制造业、政府等对国民经济具有举足轻重的影响的行业中，因此客户对于安全性的要求将高于以往。这一切决定了云计算时代安全防护的投入将会多于以往。

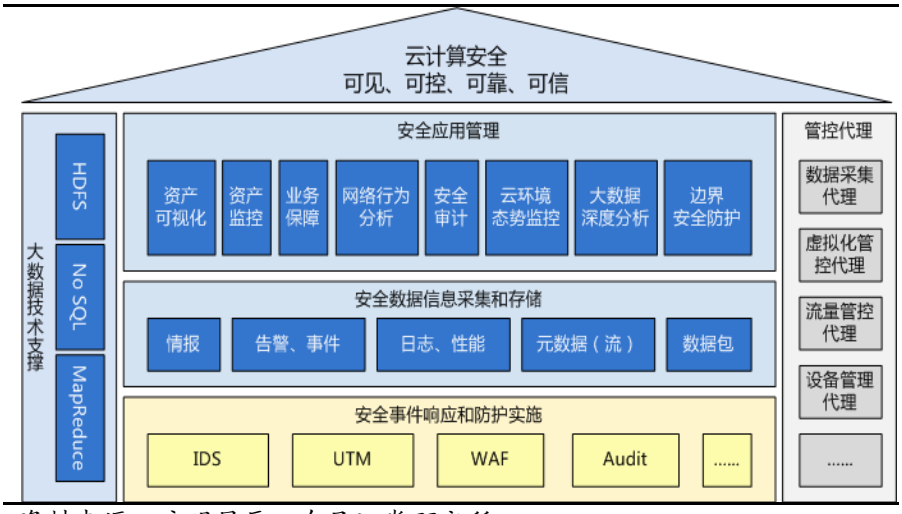
图表 12 我国云计算市场规模及增速



资料来源：赛迪智库，东吴证券研究所

私有云安全为第三方安全提供商主要应用场景：国内许多大型企业采用私有云，而中小企业托管则采用公有云，私有云和共有云都面临着严峻的安全问题，但是公有云的托管多由大型云平台公司进行统一的安全管理，采用第三方安全服务比例较低。相比而言，建设于企业内部或外部的私有云在维护上会更加倾向于选择专业的第三方安全服务商为其提供安全防护，包括平台安全、运维权限、虚拟机之间的间隔、安全防护机制资源冲突等。

图表 13 云控安全解决方案

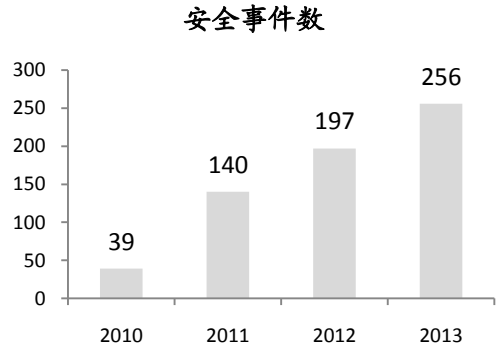


资料来源：启明星辰，东吴证券研究所

1.2.3. 物联网带来巨大的信息安全市场需求

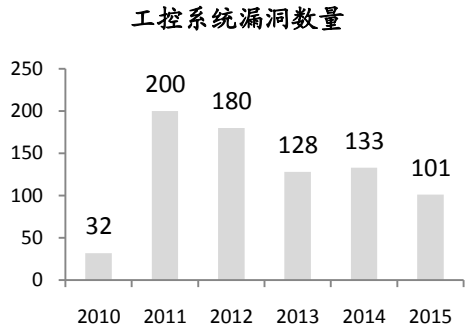
工控系统存在大量安全漏洞：工控系统由于计算资源有限，为了保证实时性和可用性，系统在设计时往往无法过多考虑信息安全的需求，从关键芯片到文件系统、进程调度、内存分配等都可能存在安全漏洞。据 ICS-CERT 统计，工控安全事件数量呈明显的递增趋势。2010-2013 年 4 年间共发生 632 件安全事件。这些工控安全事件大多分布在能源、关键制造业、市政、交通等涉及国计民生的重要行业。2010 年后，国家逐步加强了对工业控制系统漏洞数量的检测，整体上保持平稳趋势，但仍然存在大量的系统漏洞。

图表 14 ICS-CERT 统计的工控安全事件数



资料来源：绿盟科技，东吴证券研究所

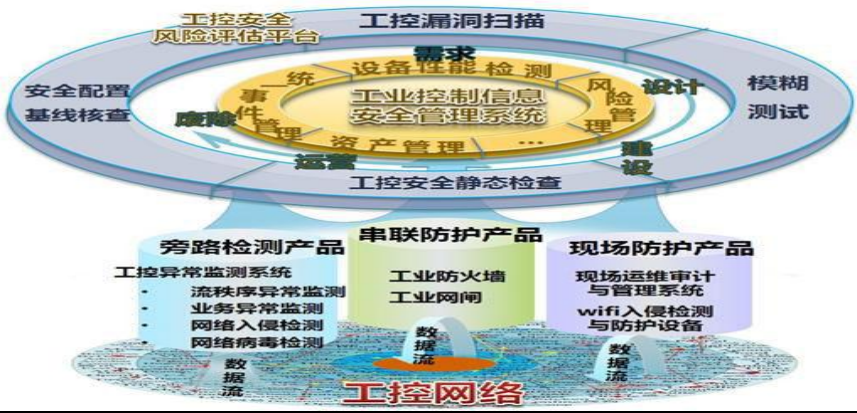
图表 15 工控系统漏洞数量



资料来源：国家信息安全漏洞共享平台，东吴证券研究所

工控系统的安全问题产可能生重大影响：工控系统一般应用在工业设备、军事设施、能源网络、水力分配，汽车交通、甚至公共和私人建筑中，因此，对它们的潜在威胁会产生深远影响。工业病毒对控制系统的影响已不再仅仅是影响计算机和网络设备运行，它们可以导致控制系统拒绝服务，可以修改控制程序从而控制或破坏工业生产，可以向操作人员发出虚假信息，以使操作员采取错误动作，其结果可能是造成生产瘫痪而导致重大经济损失，甚至于造成人员伤亡、环境破坏等重大事故。

图表 16 工控安全平台及检测防护产品



资料来源：启明星辰，东吴证券研究所

车联网快速发展带来安全漏洞：伴随车联网的发展的是随之而来的安全问题。早在 2011 年，就有来自加州大学和华盛顿大学的计算机专家的研究报告指出，汽车的安全驾驶存在巨大隐患。而近年来，随着国内车联网的进一步发展，安全漏洞问题越来越显得严重。这主要有几个原因：一是车联网会在车主不知情的情况下采集车主信息，造成大量隐私暴露问题；二是联网之后，车辆的网络入口之多足以让黑客入侵操纵从而威胁驾驶安全；三是车辆联网定位信息会被利用进行非法追踪。

物联网带来信息安全巨大的市场空间：根据 IT 三大定律之一的麦特卡夫定律，如果智能终端的连接数量达到 N 的话，网络的价值为 N 的平方，因此可以预期，未来社会生产力的进一步提高需要大量增加智能终端的连接数量以形成工业互联网。所谓工业互联网是全球工业系统与高级计算、分析、传感技术以及互联网的高度融合。工业互联网通过对智能设备产生的海量数据的分析和利用，能带来网络优化、机器自主学习、智能决策等益处，达到降低成本、节省能源、提高生产率的目的。根据 GE 的测算，在中国未来 15 年，如果燃气发电机组能耗降低百分之一，就意味着节约价值 80 亿美元的燃料；在铁路运输领域，如果效率提高百分之一，则意味着节约 20 亿美元的燃料成本。工业互联网仅仅 1%效率的提升将带来行业效率的成倍增长。根据思科的统计，目前 99.4%的物理对象尚未连接到互联网，由于工业互联网上的智能设备目前基本没有信息安全的防护，未来新增的将为信息安全带来巨大的市场增量。

2. 自研外延共同完善产品布局

2.1. 外延收购，打造综合性解决方案服务商

2.1.1. 收购赛博兴安，拓展军工加密和物联网安全

作价 6.3 亿收购赛博兴安：2016 年 6 月 2 日，公司发布公告称拟作价 63,706.50 万元收购赛博兴安 100%股权。其中，以发行股份方式支付交易对价的金额为 38,610.00 万元；以现金方式支付交易对价的金额为 25,096.50 万元。赛博兴安 2014、2015 年净利润分别为 982.59 万元和 3018.27 万元，2015 年收入 9216 万。承诺业绩 2016-2018 年分别为 3874.00、5036.20、6547.06 万元，承诺期合计承诺净利润数为 15,457.26 万元。

图表 17 公司收购交易方案

序号	交易对方	对价总额（万元）	现金对价（万元）	股份对价（万元）	发行股份数量（股）
1	王晓辉	28223.910	9407.970	18815.94	9384508
2	李大鹏	16940.395	5613.465	11226.93	5599466
3	蒋涛	8667.945	2889.315	5778.63	2882109
4	文芳	4182.750	1394.250	2788.50	1390773
5	星源壹号	5791.500	5791.500	0	0
合计		63706.500	25096.500	38610.000	19256856

资料来源：公司公告，东吴证券研究所

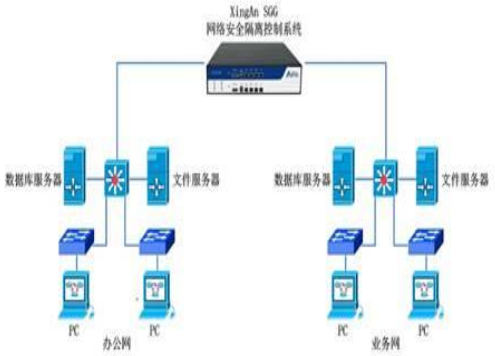
通过收购获得加密资质，清除发展障碍：赛博兴安的具体业务领域主要包括网络传输加密、加密认证及数据安全、军队军工行业安全管控、不同安全域间网络互联等。赛博兴安在通信系统加密架构设计、通信协议适配、国产化 CPU/FPGA 应用、高速密码算法实现等方面有突出技术优势，具备快速满足用户定制化安全保密需求的能力。其加密资质将极大加强启明的技术竞争力，并帮助启明突破加密门槛，进一步深入加密领域，为扫清发展障碍。

收购将巩固启明星辰在军工信息安全的龙头地位：赛博兴安在军工行业具有很大的影响力，客户都是军队、军工、政府、能源等行业中的大客户。通过收购，启明星辰拓展了全新的军工行业渠道，弥补了原先的渠道空白。

赛博兴安四大核心技术拓展物联网安全：（1）兴安网络处理平台：产品可以快速定制，性能稳定，具有自主可控的底层协议栈，能够屏蔽通用操作系统的处理，规避各种系统漏洞；（2）线速硬件加解密处理平台：满足视频流和实时消息数据低延迟、高性能的加解密需求，防止恶意篡改；（3）物理级网络安全隔离体系：满足多种环境下的需求，实现硬件阻断连接，黑客无法绕过器件，保证数据交换的安全性；（4）网络安全数据分析平台：增加关联分析，提升全网综合管控性能。赛博兴安的主要产品包括：边界防护产品、安全管理与综合防护产品、数据安全产品

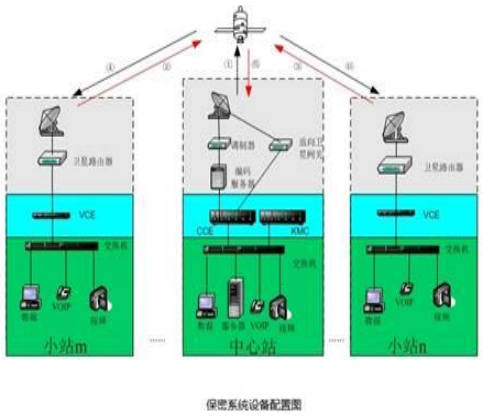
以及安全集成与服务，属于广义物联网领域，为启明在物联网领域的业务布局打下坚实基础。

图表 18 边界防护类（医院案例）



资料来源：公司公告，东吴证券研究所

图表 19 数据安全与加密（卫星通信）



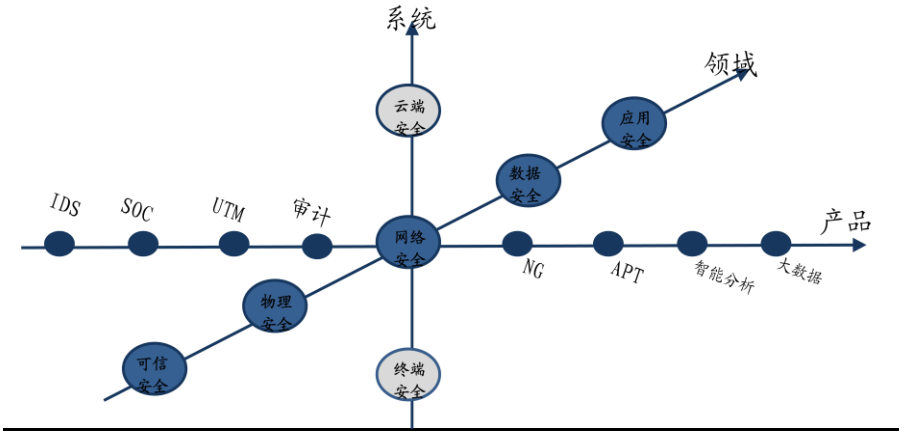
资料来源：公司公告，东吴证券研究所

配套融资与员工持股计划彰显公司发展信心：公司拟向启明星辰第二期员工持股计划、中植投资发展（北京）有限公司、北京中海盈创投资管理中心（有限合伙）、天津七龙投资管理合伙企业（有限合伙）发行股份募集配套资金，配套资金总额不超过 26,435.00 万元，不超过本次交易拟购买资产交易价格的 100%，拟用于支付本次交易的现金对价和中介机构费用。

2.1.2. 外延收购夯实市场龙头地位

清晰的发展脉络扩张业务版图：在系统方面，启明星辰由原来的网络安全逐步拓展到云端安全和终端安全；而在广义信息安全领域方面，启明星辰目前已经通过外延布局从原先的狭义信息安全即网络安全发展成为如今包括可信安全、物理安全、网络安全、数据安全和应用安全的广义信息安全领域的公司；产品也从原先的 IDS 逐步扩张到包括 UTM、审计、APT、SOC、大数据等产品形态。

图表 20 启明清晰的发展脉络



资料来源：东吴证券研究所

控股收购逐步扩大规模：启明于 2011 年全资收购网御星云在安全网关领域巩固市场地位，并利用技术协同性在 IPS 技术领域超越天融信和华为，在硬件安全领域成为本土规模最大的一家。2014 年公司收购书生电子 75%股权，主要填补了公司在数据加密领域产品的空白。同年收购合众信息 51%的股权，并已于 2015 年完成剩余 49%股权的收购，实现全资控股，增强了公司在数据安全领域的实力。2015 年，公司还实施了对安方高科 100%股权的收购，重点在于对电磁防护领域业务的深入。

图表 21 公司重要收购标的布局

时间	标的	股权比例	标的主营业务
2011	网御星云	100%	防火墙、UTM 等网络产品
2014	书生电子	75%	数据安全、安全文档软件
2014	合众数据	100%（2015 年完成剩余 49%）	大数据分析及数据安全
2015	安方高科	100%	电磁防护

资料来源：公司公告，东吴证券研究所

客户协同效应逐步凸显：收购整合之后，公司在各个细分子行业的客户实现了互相补充。目前公司在政府、电信、金融、能源、交通、军队、军工、制造等行业是企业级用户的首选品牌，在政府和军队拥有 80%的市场占有率，为世界五百强中 60%的中国企业客户提供安全产品及服务，对政策性银行、国有控股商业银行、全国性股份制商业银行实现 90%的覆盖率，为中国移动、中国电信、中国联通三大运营商提供安全产品、安全服务和解决方案。

图表 22 启明星辰代表客户

客户类别	说明	典型代表
金融	200 多家金融行业用户	人民银行、银监会、保监会、外汇管理局、工行、交行、招行
电信	涵盖三大运营商集团总公司及 70 多家省级分公司	中国电信集团、中移动集团、联通、网通集团、北京电信、四川移动
政府	涵盖中央、国务院直属 100 多个国家级部、委、办、局	全国人大、发改委、财政部、公安部、信息产业部、工商总局、国家信息中心
军队	拥有 80%的市占率	总参、总装、总后、二炮、中航工业第一集团、兵器集团、航天科技集团
能源交通		国家电网、中石油、中石化、西南航空、深圳航空、民航总局
教育		中科院、北大软件学院、博士后基金会、哈工大、北邮

资料来源：公司公告，东吴证券研究所

技术领先稳固信息安全领域龙头地位：截止到 2015 年年末，公司已经在系统漏洞挖掘与分析、恶意代码检测与对抗等上百项安全产品、管理与服务技术方面形成拥有完全自主知识产权的核心技术积累。在此基础上形成了较为全面的安全产品线和安全服务模式。此外，公司还是国家认

定的企业级技术中心、国家规划布局内重点软件企业，拥有最高级别的涉及国家秘密的计算机信息系统集成资质，并获得国家火炬计划软件产业优秀企业、中国电子政务 IT100 强等荣誉。公司拥有我国规模最大的国家级网络安全研究基地，创造了百余项专利和软件著作权，参与制订国家及行业网络安全标准，填补了我国信息安全科研领域的多项空白。完成包括国家发改委产业化示范工程，国家科技部 863 计划、国家科技支撑计划、核高基重大专项等国家级科研项目近百项。启明在 IDS 领域国内份额连续 10 多年第一，在合并网御星云后，在 IPS 领域的市场份额位列第二仅次于绿盟，成为国内首批有权查看微软 Windows 系统源代码的企业，其“黑客入侵检测与预警系统”获得国家优秀火炬计划称号，在针对黑客攻防方面积累了较多的技术和良好的口碑。

图表 23 启明核心技术居于市场龙头地位

资料来源：启明星辰，东吴证券研究所

2.1.3. 细分领域持续深耕，打造综合性解决方案服务商

收购网御星云，合作开发安全网关产品：2013 年 5 月，网御星云和启明星辰联合发布了下一代安全网关产品，这个产品是启明收购网御后两家公司首次联合发布新产品，均为自主研发。产品包括下一代防火墙（NGFW）和下一代统一威胁管理（NGUTM），除了支持 Gartner 所定义的深度入侵防御、应用可视化等下一代防火墙的标准特性外，还具备对用户业务建模和识别、双引擎过滤病毒查杀、基于云沙箱技术的未知威胁防护、BYOD 移动安全管控等功能。从市场角度考察，根据 IDC 的统计，2014 年启明星辰入侵检测和入侵防御的市场份额分别位居第一位和第二位，VPN 排名由第三上升至第二(份额 15.7%)；网御星云 UTM 市场占有率持续保持第一，防火墙排名大幅提升，由第五位上升至第三位。

收购书生电子，布局可信安全：公司于 2014 年收购数据安全厂商书生电子 51%的股权，并于随后再次收购 24%的股权，现在持有总股权共计 75%。根据收购公告显示，书生电子成立于 1998 年。自成立以来，公司就专注于数据安全领域，在安全文档软件方面有多项国际领先的技术及专利，

为重要行业用户提供安全数字签名、电子印章、电子公文等软件产品，在该市场领域处于领先位置，客户群遍及政府、金融、大企业等，拥有国家有关部门颁发的涉密和商密资质，曾获国家火炬计划重点高新技术企业、国家自主创新产品、2013 中国软件和信息技术服务业最有价值品牌、中国电子信息产业标准化领军企业、中关村 20 年突出贡献奖、电子政务 IT 百强等荣誉。收购书生电子帮助启明星辰在原有产品框架上增加覆盖，技术协同性高，并在客户渠道运营及管理方面获得丰富经验。目前书生电子主要产品包括电子公文传输系统及电子印章系统等，客户以政府部门居多。

图表 24 书生电子主要应用安全产品

电子公文传输系统	公文传输系统利用计算机网络技术、版面处理与控制技术、安全技术等，实现部门与部门之间，单位与单位之间红头文件的起草、制作、分发、接收、阅读、打印、转发和归档等功能。
书生电子印章系统	集合书生公司两大自主核心技术—SEP 技术、电子印章技术而开发的一款极具应用针对性的电子文档安全产品。

资料来源：公司网站，东吴证券研究所

合众数据助力公司数据安全发展：公司于 2014 年收购合众数据 51%股权，并已于 2015 年实现了对剩余 49%股权的收购，现在合众数据为公司全资控股子公司。根据收购公告显示，合众信息是专注于大数据处理技术和安全数据交换产品研发与销售的专业信息安全厂商，是“国家 863”信息安全等级保护技术联盟的发起单位，是 2013-2014 国家规划布局内重点软件企业，也是浙江省信息产业厅最早认定的“双软”企业之一，浙江省信息安全产业技术创新联盟的理事长单位。公司设计、研发了具有自主知识产权的系列信息安全产品，包括网闸、安全数据交换系统、单向光闸、视频网闸等。在利润贡献方面，合众数据 2015 年-2017 年净利润（扣除非经常性损益后）分别不低于 2,500 万元、3,125 万元、3,610 万元，承诺期合计承诺净利润数为 9,235 万元。2015 年公司研发投入增加，预计 2016 年开始业绩会有比较优秀的表现。

图表 25 合众数据主要解决方案

资料来源：公司网站，东吴证券研究所

安方高科聚焦电磁空间安全新领域：电磁信息安全防护需求起源于电磁泄露，电磁泄露是指信息设备在工作时产生的电磁波能以电磁辐射方式向空间传播，同时通过地线、电源线、信号线以传导发射方式传播的现象。这些电磁信号如被截取，经过提取就会造成信息失密。我国的电磁信息安全防护技术的研发起步较晚，初期参与厂商较少；1999 年开始，国家保密局颁布了一系列国家保密标准，规范了电磁信息安全防护行业的发展。尤其是 2006 年之后，电磁信息安全防护的产品化工作才开始迅速发展。安方高科的主营业务分为电磁屏蔽工程和电磁屏蔽产品两大类。客户集中在各级党政机关、国防、武警、公安、检察院、法院、军工、科研单位等领域。技术方面公司处于领先地位，截止 2014 年末，安方高科共拥有 45 项专利，其中 6 项发明专利；安方高科产品质量过硬，现有 6 大系列 50 余款产品，获得多项质量体系认证；业务资质齐全，具有为军队系统和党政机关服务的资质；工程施工经验丰富，最近三年签署电磁屏蔽工程合同数 472 份，建造电磁屏蔽室 472 个，合计面积 28,802 平方米。安方高科 2015 年度、2016 年度和 2017 年度经审计的扣除非经常性损益后归属于母公司所有者的净利润分别不低于 1,850 万元、2,150 万元和 2,360 万元，承诺期合计承诺净利润数为 6,360 万元。

图表 26 安方高科承建国家天文台电磁屏蔽室项目现场

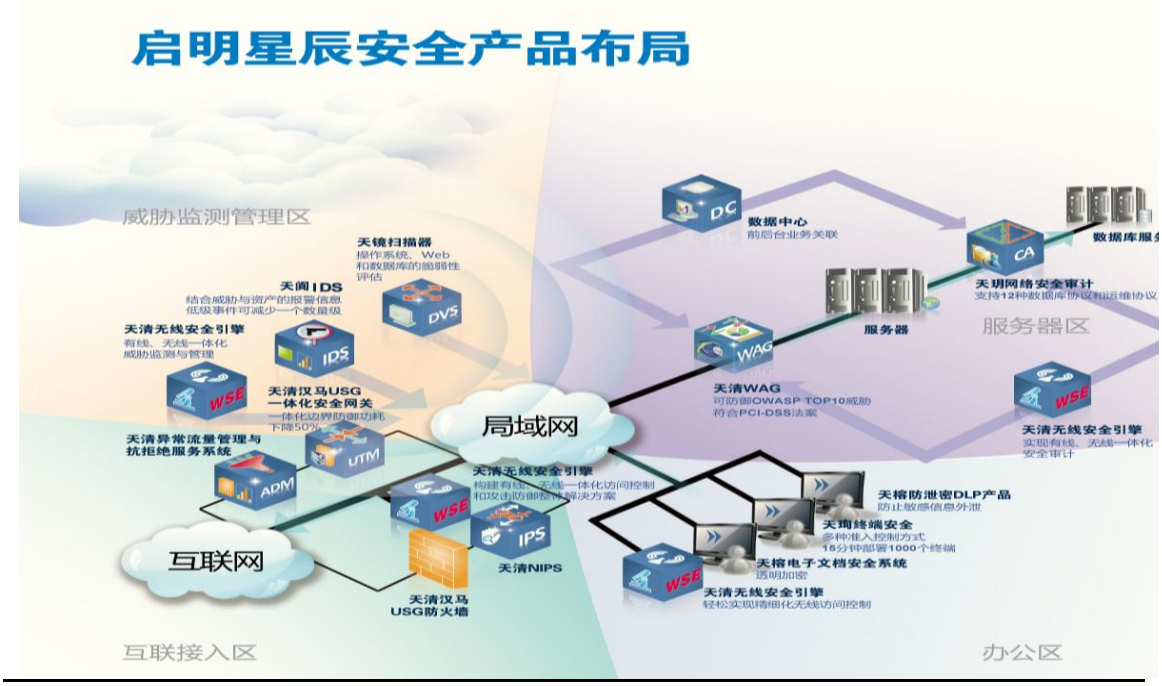
资料来源：互联网，东吴证券研究所

2.2. 完善产品布局，巩固行业龙头地位

2.2.1. 拥有行业最全面的网络安全产品线

公司完善产品布局之路逐步深入：启明成立于 1996 年，是国内最具实力的、拥有完全自主知识产权的网络安全产品、可信安全管理平台、安全服务与解决方案的综合提供商。在产品方面，公司拥有完善的专业安全产品线，横跨防火墙/UTM、入侵检测管理、网络审计、终端管理、加密认证等技术领域，共有百余个产品型号，并根据客户需求不断增加。

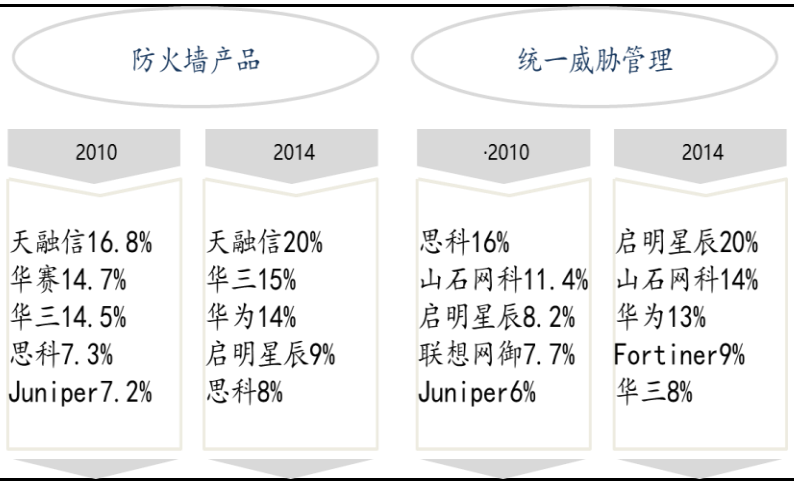
图表 27 启明星辰信息安全全方位解决方案



资料来源：互联网，东吴证券研究所

公司产品市占率逐步提升，位居市场前列：公司在业务逐步布局与整合后市场实现比较大的扩张。其中统一威胁管理（UTM）、入侵检测与防御（IDS/IPS）、安全管理平台（SOC）均取得市场占有率第一的成绩，同时在安全性审计、安全专业服务方面保持市场领先地位，其它还包括防火墙（FW）、Web 应用防火墙、漏洞扫描、互联网行为管控、终端安全、数据防泄密、无线安全引擎、应用交付、网闸、数据安全交换、大数据处理等多个产品类型；在营销方面，公司在全国各省市自治区设立了三十多家分支机构，拥有覆盖全国的渠道和售后服务体系。

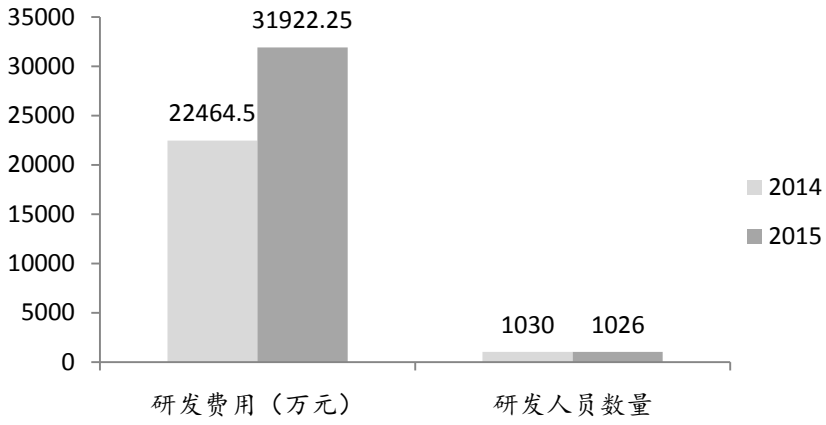
图表 28 公司产品市占率逐步提升



资料来源：IDC，东吴证券研究所

整合效果显著，研发项目密集：2015 年，公司在外延收购领域布局继续深入，在研研发项目共有 11 个，研发投入费用相比 2014 年同比增长 42.10%，研发人员同比增长 17.09%，彰显公司收购后产品研发整合能力。2015 年在研项目主要包括：新一代防火墙 NGFW 产品研发项目、新一代 VPN 产品研发项目、工控防火墙产品研发项目、泰合新一代信息安全运营中心系统研发项目、针对云计算环境审计产品新型号研发项目、FlowEye 产品新型号研发项目、文件访问控制管理系统 FCM 研发项目、合众大数据基础平台研发项目、电动插刀式屏蔽门研发项目、移动式低漫射计算机研发项目等。

图表 29 公司研发费用金额及研发人员数量变化



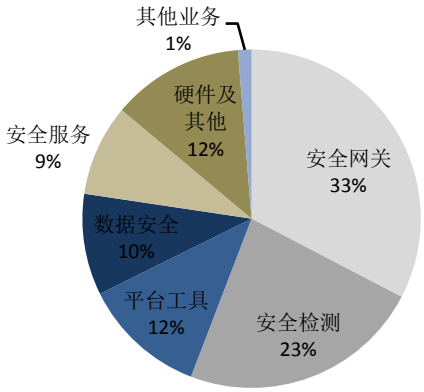
资料来源：赛迪智库，东吴证券研究所

2.2.2. 主打产品持续盈利，公司内生增长可期

网关和检测产品仍然是公司产品重点，平台工具和数据安全产品占比逐步提升：2015 年，公司经营和规模继续发展和壮大。从产品分项来看，最主要的业务收入来源仍然是安全网关和安全检测产品，两者收入合计目前仍占比超过 50%。但同时可以看到的是，安全网关和安全检测收入占比相比 2014 年有所下降，这主要是由于平台工具和数据安全产品收入的逐步提升。而这两项产品收入的提升正体现出公司在外延并购的公司业务方面所获得整合性

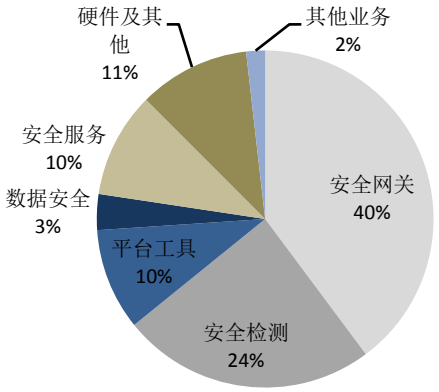
的成功，未来内生增长可期。

图表 30 2015 年产品收入构成



资料来源：公司公告，东吴证券研究所

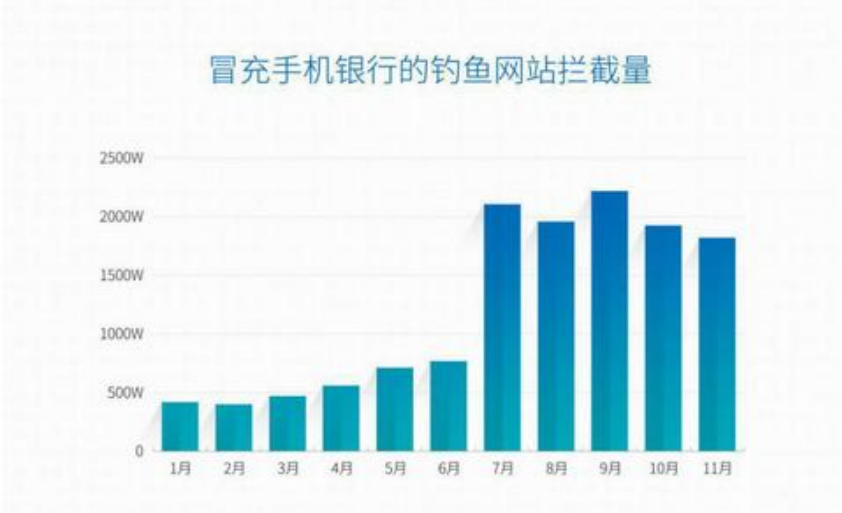
图表 31 2014 年产品收入构成



资料来源：公司公告，东吴证券研究所

Web 应用攻击成主流威胁，Web 防火墙前景向好：目前，Web 网站一直都是黑客重点攻击的目标，根据腾讯发布的《2015 年互联网安全报告》数据显示，2015 年全年腾讯网址安全云共检测出恶意网址 3.87 亿条，虚假博彩网址 1.08 亿条、木马网址 0.93 亿条。由于 Web 应用攻击规模的进一步扩大，市场对 Web 防火墙的需求日益强烈，而在目前的情形下，Web 攻击容易和短信诈骗、电话诈骗相结合出现，危害极大，无论是对单位还是对政府来说，Web 防火墙的采购必不可少，因此前景看好。

图表 32 腾讯互联网安全报告的钓鱼网站拦截数量



资料来源：腾讯报告，东吴证券研究所

启明继续领跑 ADP：目前中国数据库安全审计与防护市场正处于高增长期，启明星辰的数据库安全解决方案是以安全审计与防护为主，包含事前事中事后三个部分。事前实施数据库扫描，漏洞检查等预防措施;事中利用数据库防火墙进行实时的访问控制与攻击防护;事后进行数据库的审计。这样的三部分组成了比较完整的数据库解决方案。根据 Frost&Sulivan 的调研，在目前国内数据库安全与审计市场启明星辰以 9.5%的份额占据了市场第一的位置。

目前中国数据库安全市场正处于高增长期，预计启明 2013 年市场份额将会进一步扩大至接近 11%，并持续保持市场领先地位。

2.2.3. 持续推出新产品，研发收获显著

2015 年推出多项新产品打开新空间：公司在安全技术领域的研究成就可喜，在 2015 年获得了公安部首批信息安全等级保护安全建设服务机构能力评估合格证书。同时，公司在云安全领域获得显著突破，获得了工信部首届云帆奖中两个关于云计算安全解决方案的重量级奖项；被《互联网周刊》评选为 2014 年云服务商综合能力排行榜首位。在产品方面，公司也在云安全方面布局深远，推出了如泰合安全运维管理平台解决方案、CloudSOC 云安全管理平台等多项产品。

工控防火墙产品将成为公司新的业务增长点：工控防火墙项目是为应对新的市场需求而进行的新产品研发工作。 2015 年历时 9 个月发布了国内唯一取得工控三级最高资质的工业防火墙新品。随着工控业务在国内信息安全行业的发展，本产品将成为公司新的业务增长点。

针对云计算环境审计产品新型号试点： 新型号产品支持云计算环境、大数据平台，支持 APT 联动、 WAF 联动，围绕功能/界面、客户关系上进行了竞争力的提升，一方面弥补传统网络审计的缺项，另一方面坚持走行业化道路，结合行业特点形成行业审计产品。目前已在多个行业进行试点，形成了一定的行业影响力。

文件访问控制管理系统 FCM 提高文件安全管理能力：2015 年研发新品，该产品支持第三方数字证书、着重文件的传输过程加密和文件落地加密，可以提高用户文件的安全管理能力，后续有望成为新的业绩增长点。

电动插刀式屏蔽门样机通过测试，2016 年有望放量：电磁插刀屏蔽门具有低阻力、高性能、美观等优点，是公司收购的安方高科所在的电磁安全防护领域的重要产品之一。公司于 2015 年开展了电动插刀式屏蔽门开发项目。项目研发样机已于 2015 年 8 月通过赫安辐源实验室测试，测试数据表明该产品性能达到了 BMB3-1999 C 级要求，开门阻力小于 10kg，满足了项目研发技术指标。电磁插刀屏蔽门的研发成功，将为 2016 年销量提升奠定基础。

3. 打造全新的云安全生态圈

3.1. 牵手巨头，打造云-管-端三位一体安全

3.1.1. 云管端安全三位一体安全成为趋势，启明一马当先

互联网时代安全问题愈加严峻：互联网时代，无论是企业用户还是企业用户，都习惯将自己的数据储存在云端，而获取数据则需要通过网络进行。而根据腾讯安全发布的互联网安全报告，大多数网民认为目前互联网较安全，而事实上恰恰相反与传统认知相反，2015 年腾讯电脑管家反病毒实验室新发现的电脑病毒数为 1.45 亿个，较 2014 年相比增加了 5%，而相比 2013 年则增加了有 41%之多；而 2015 年病毒感染机器数量达到 48.26 亿次，流氓软件感染量为 3.70 亿次，盗号木马感染量达 0.80 亿次。随着互联网在用户中的逐步普及，电脑病毒数量直线上升，导致感染病毒机器也迅速增多，平均一台电脑中毒数十次。

图表 33 腾讯互联网安全报告电脑病毒数量

资料来源：腾讯互联网安全报告，东吴证券研究所

云管端安全产业链的打造将整合安全服务行业：互联网的未来是连接一切，而安全正是连接一切的基石。在过去，无论是企业终端安全，还是用户终端安全，不同领域内的安全厂商虽均有推出自己主打的安全产品，但国内的企业终端安全服务市场分散，行业整合度不高，企业终端安全产品在安全防护上大多是孤军奋战，不同厂商之间难以形成产品联动，鲜有及时联动的完整的企业终端安全解决方案；近两年频繁发生的企业网络遭受攻击、用户数据泄露事件，引发安全厂商对企业终端安全问题的关注。

参与国家标准制定，奠定未来云安全领域领头羊地位：由于云计算如火如荼的发展，很多企业已经把自己的业务数据和管理系统架构在云端，这使得原先相对封闭可控的风险点出现了开放性的变化。而随着技术和终端的迅速发展，网络攻击也变得更加频繁化和多样性，云安全问题也时有发生，对此启明通过支持典型客户的云计算系统建设项目，不断创新云计算系统安全解决方案的应用与实践。同时还与业内同行密切合作，广泛参与云安全的技术讨论、标准制定以及国家有关云安全的科研项目，积累云计算安全领域方面的技术储备和宝贵经验，以解决用户在云计算应用建设过程中的安全问题并满

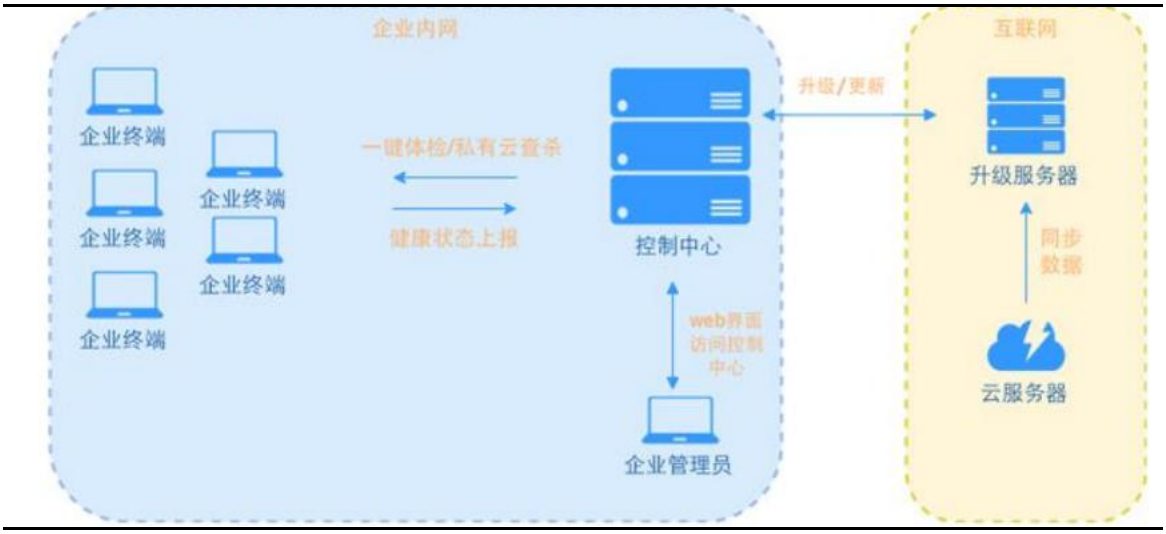
足未来云计算产业的发展需求。

3.1.2. 合作腾讯与华为，深度布局云安全

腾讯在云安全领域布局已久，双方强强联手：近年来，腾讯积极的致力于推动互联网安全开放平台的建设，积极开展产业链协同模式，整合了旗下四大联盟——天下无贼反信息诈骗联盟、移动支付安全联合守护计划、腾讯安全 Wi-Fi 联盟、移动电子市场联盟，并以开放的姿态与警方、银行、金融公司、安全厂商、运营商等产业链各方联手呼吁联盟成员共同输出各自核心优势，发挥产业链联动作用。而启明与腾讯的合作其实也由来已久，双方都是中国信息安全漏洞信息共享知识库 CNVD 工作委员会/技术合作单位、中国反网络病毒联盟 ANVA 的成员单位，在网络安全领域具备合作共识。作为两大领军企业，终端安全防护与产品经验的优势互补将会达到强强联合 1+1>2 的效果。

与腾讯合作聚焦终端安全：2015 年 6 月 1 日，第二届国家网络安全宣传周在中华世纪坛正式举行。期间，启明与腾讯联合召开新闻发布会，宣布达成战略合作，并面向企业市场推出全面的终端安全解决方案——云子可信网络防病毒系统，建立企业安全服务战略联盟，为“互联网＋”国家战略落地提供终端安全服务。发布会上，浪潮、国药集团等企业当即签订了相关合作意向。云子可信网络防病毒系统为用户提供全方位端到端的解决方案，为终端安全，网络安全领航护驾，主动发起威胁检测并自主构建能够有效抵御已知病毒、未知恶意代码和 APT 攻击，并修复漏洞的终端安全防御体系。云子可信网络防病毒系统由控制中心和企业终端两部分组成，其中控制中心是云子可信的管理平台，部署在服务器端，采用 B/S 架构，可以随时随地的通过浏览器访问；企业终端执行最终的杀毒扫描、漏洞修复等安全操作，并向安全控制中心发送相应的安全报告；云服务器主要用于更新病毒库，主防以及补丁库。

图表 34 云子可信网络防病毒系统由控制中心和企业终端两部分组成



资料来源：云子可信用户手册，东吴证券研究所

深度参与华为构建网络安全：2015 年 5 月，在 HNC 大会上，华为推出了敏捷网络 3.0 架构，在物联网时代正式开启了敏捷物联时代。作为敏捷网络开

放生态系统的一员，启明星辰应邀参加了此次大会，参加了主题演讲，展示了与华为联合创新的两个案例，并在展台上进行了情景演示。在与华为名为“全网安全协防解决方案”的联合创新案例中，启辰的泰合下一代 SOC 安全管理平台与华为 SDN 网络控制器进行了敏捷联动。通过泰合下一代 SOC，采集网络中分散的安全要素信息，通过基于规则和基于行为的分析引擎进行综合分析研判，识别隐匿的威胁和攻击行为。在识别出攻击行为后，泰合下一代 SOC 通过华为的敏捷网络接口向华为 SDN 控制器发出指挥命令，并由 SDN 控制器对网络中相关敏捷设备派发控制指令，调整工作姿态，阻断网络攻击。通过该方案，结合了启明星辰下一代 SOC 在基于最新技术的综合威胁分析方面的优势，以及敏捷网络的智能控制能力，形成了一个安全管理的闭环。

图表 35 腾讯互联网安全报告电脑病毒数量

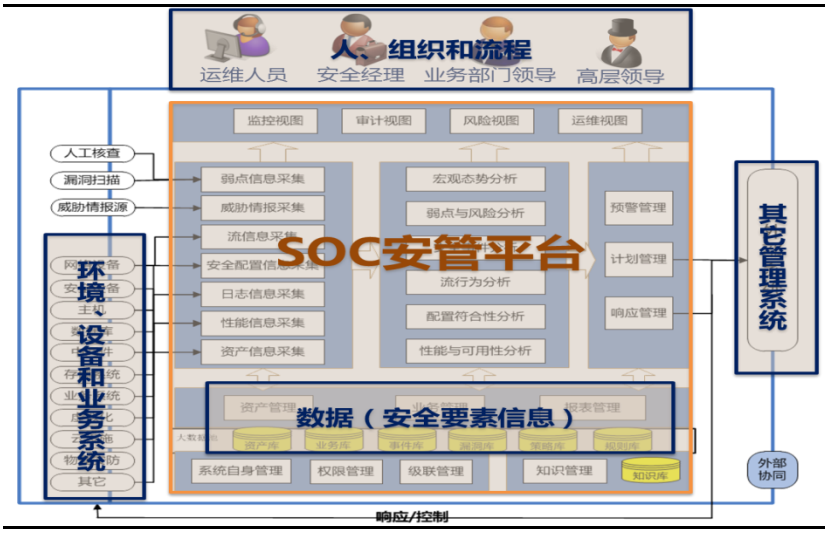
资料来源：公开资料，东吴证券研究所

3.2. 开放第三方接口，构建开放式安全新业态

3.2.1. SOC3.0 时代的全新安管平台构建连接

现有 SOC 安管平台的连接能力还需增强：SOC 安管平台的传统定义为以资产为核心，以安全事件管理为关键流程，采用安全域划分的思想，建立一套实时的资产风险模型，协助管理员进行全局性的事件分析、合规分析、风险分析、态势感知、预警管理和应急响应处理的集中安全管理系统。而面对客户需要更好的知己知彼、更强的态势感知能力等新的诉求，需要以数据为核心重构现有安管平台的整体架构。

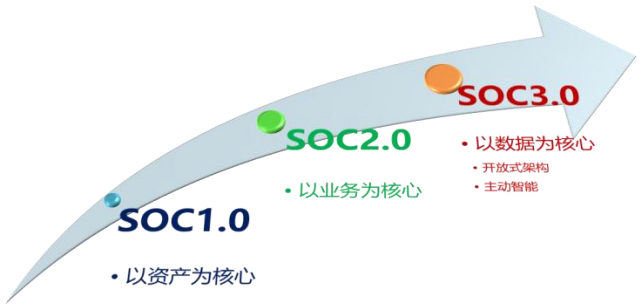
图表 36 传统 SOC 安管平台构成



资料来源：公开资料，东吴证券研究所

SOC3.0 打造互通共享的智能化大数据安全管理平台，构建从封闭到开放的安全业态：公司在 4.29 号的第三届首都网络安全日发布“泰合安全威胁分析合作计划”，向在安全威胁分析领域的广大安全厂商开放泰合 SOC3.0 安管平台的南向和北向数据接口，共同打造智能化大数据安管大平台。SOC 相当于安全行业的 ERP 平台，3.0 情况下开放安全分析接口，可以实现政企客户网络中全要素信息和数据的连接，并允许第三方安全分析能力以类似 App 的形式接入平台并组合应用，一方面可以更加主动、智能地对企业和组织的网络安全进行管理和运营，另一方面可以实现数据的跨企业整合和共享，安全业态从封闭迈向开放式发展，公司的平台属性强化。

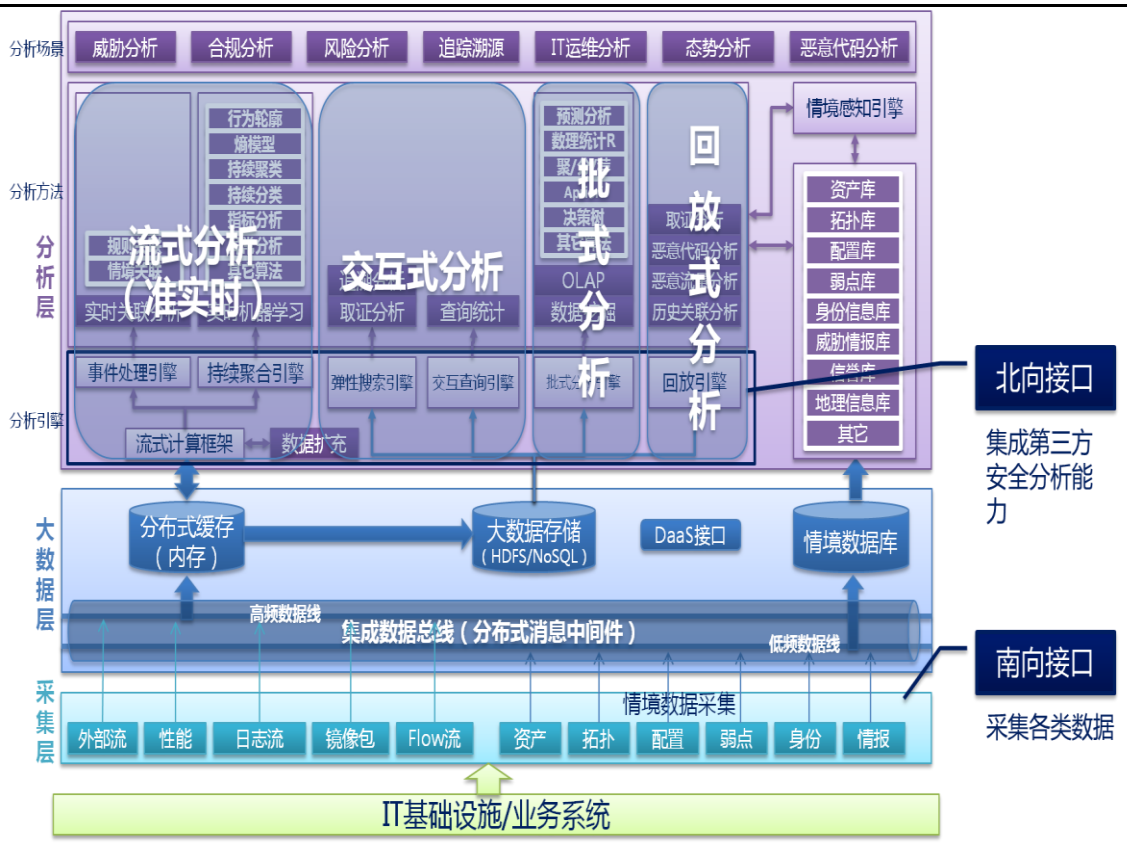
图表 37 传统 SOC 迈向 SOC3.0 时代



资料来源：公开资料，东吴证券研究所

构建基于 SOC3.0 开放架构的全新泰合安管平台：SOC3.0 以大数据分析架构为支撑，以业务安全为导向，构建起以数据为核心的开放式安全管理平台，强调更加主动、智能地对企业和组织的网络安全进行管理和运营。

图表 38 基于 SOC3.0 开放架构的全新泰合安管平台



资料来源：云子可信用户手册，东吴证券研究所

3.2.2. 联合合作伙伴打造全新泰合计划

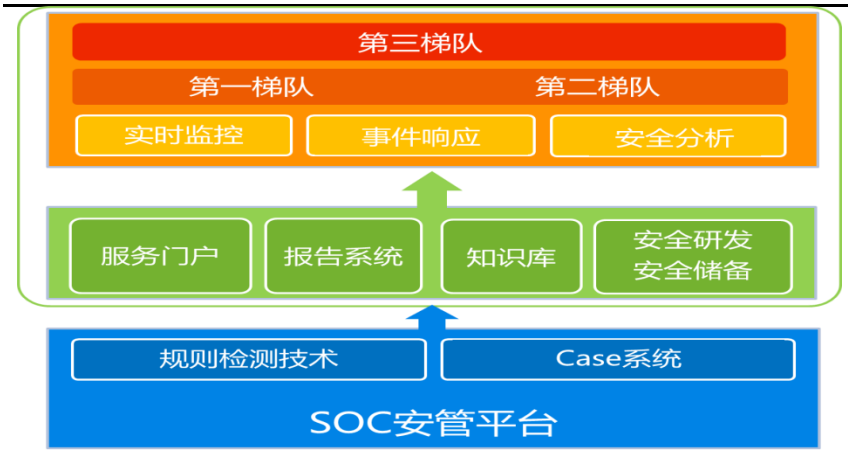
联合合作伙伴构建泰合团计划：“泰合团计划”的合作伙伴目前包括烽火台威胁情报联盟、诺恒信息、天际友盟和微步在线。其中，烽火台威胁情报联盟是国内首个安全威胁情报联盟，诺恒信息具有丰富的基于 SOC 进行安全运维的能力和资深的安全分析师团队，而天际友盟和微步在线则是目前国内最专业的两家独立威胁情报服务提供商。

图表 39“泰合团计划”合作伙伴

资料来源：公开资料，东吴证券研究所

应用场景 1 泰合 SOC+安全分析师：基于泰合 SOC 构建一套服务平台，并用自己的安全分析师为客户提供现场/远程/云安全事件分析服务。

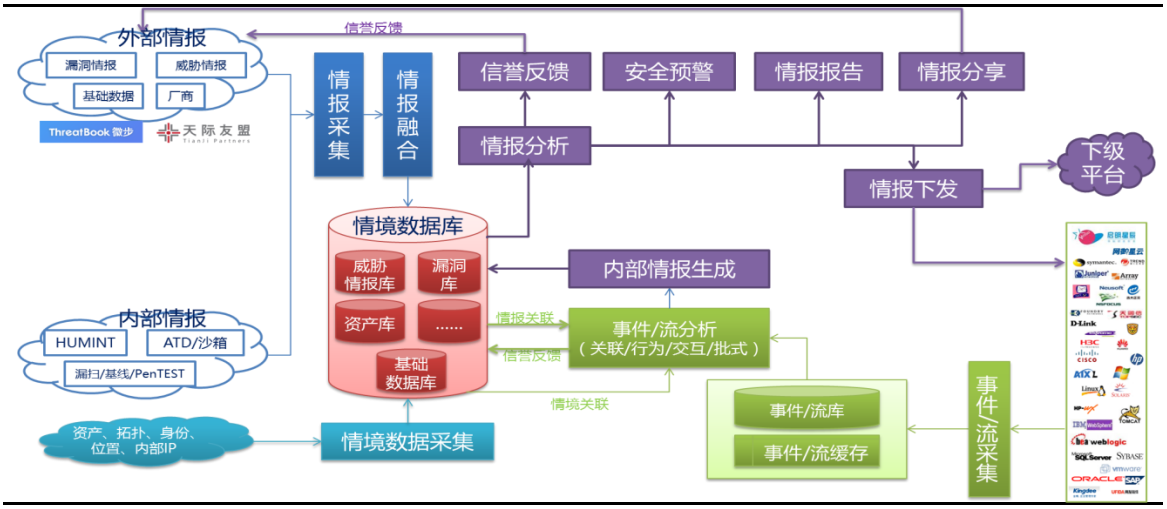
图表 40 典型应用场景 1：泰合 SOC+安全分析师



资料来源：公开资料，东吴证券研究所

应用场景 2 泰合 SOC+威胁情报:SOC/SIEM 是承载机读威胁情报的最优选择，同时 SOC 需要借助威胁情报来提升自身的价值，因此 SOC+威胁情报的场景是最优选择。泰合 SOC 目前聚焦在将外部威胁情报在政企端落地。

图表 41 基于 SOC3.0 开放架构的全新泰合安管平台



资料来源：云子可信用户手册，东吴证券研究所

未来 SOC 发展趋势：①在战略和战术上集成威胁情报②通过高级分析将安全智能落地③尽可能地安全自动化④主动的威胁捕猎与调查⑤部署自适应安全架构。

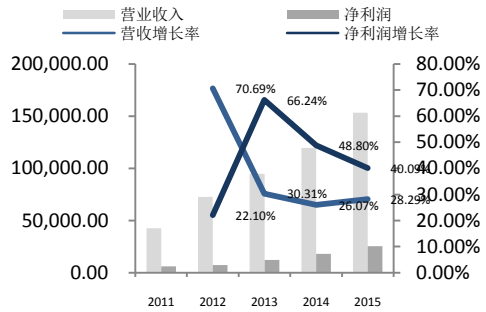
4. 财务数据与估值

4.1.1. 公司业绩稳步提升，未来业绩有支撑

公司营收稳步提升，净利润增长显著：2011 年以来，近 5 年公司收入保持稳步提高，复合增速达到 37%之高，净利润复合增速达到 42%。仅看 2015 年的数据，公司的营收增长率为 26%，净利润增长率 40%仍然维持在高位。2012 年之后，人员保持平稳，因此公司的费用率保持平稳。2015 年公司发布多项新产品，并在云安全、工控安全等领域布局深远，后续业绩逐步兑现，会为公司带来进一步的收入提升和利润提升空间。作为信息安全行业的龙头企业，

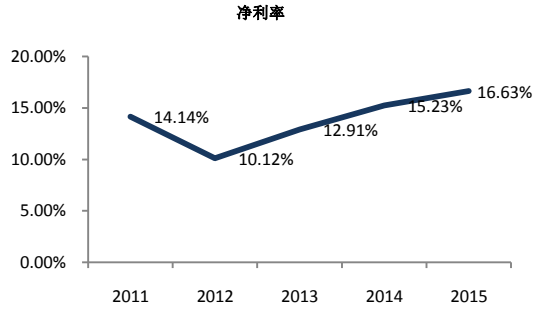
启明未来几年的增速值得期待。

图表 42 公司营收及净利润增速



资料来源：公司公告，东吴证券研究所

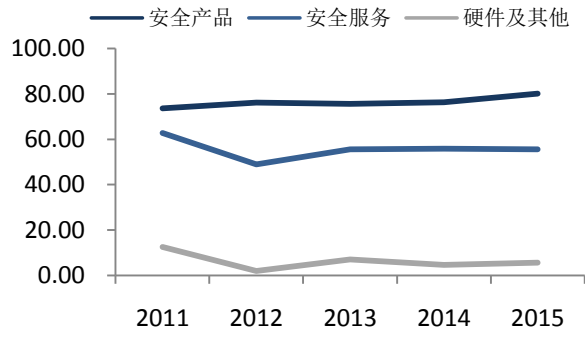
图表 43 净利率变动



资料来源：公司公告，东吴证券研究所

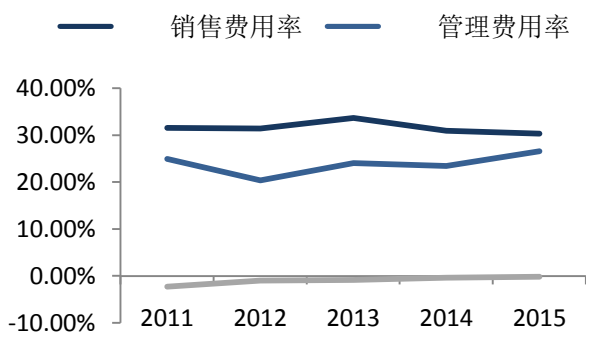
公司毛利率稳中有升，期间费用率稳中有降：公司主要分三项业务，包括安全产品、安全服务、硬件及其他。其中安全产品包括安全网关、安全检测、平台工具和数据安全四种细分领域的产品。在三大项业务中，公司传统主业安全产品的毛利率最高，维持在 75%-80%之间，硬件的毛利率较低，维持在 10%以下。近年来，毛利率稳重有升，同时公司团队及经营较为稳定，因此费用率稳中有降，因此未来预计净利率有望获得进一步提升。

图表 44 公司各项业务毛利率



资料来源：公司公告，东吴证券研究所

图表 45 期间费用率变动



资料来源：公司公告，东吴证券研究所

并购战略力保收入稳健增长，一季报亏损规模持续缩小：书生电子和合众数据业务并表，公司营收延续自上市以来的增长态势，一季度连续第三年减亏。亏损主要由于并表企业一季度亏损，应收账款及存货大幅增加相应的资产减值准备损失 892.38 万元，以及投资收益大幅减少 271.69%；公司预计 16 年上半年业绩同比下滑 54.63-94.33%，在 100 万-800 万之间。但剔除投资收益下降的因素，我们预计内生业绩增速在 40%左右，预收款同比大增 117.83%，表明订单充裕，后续业绩有保障。

4.1.2. 海内外公司对比

海外公司先例，云安全仍是重点发展方向：PANW（paloalto）目前已经推出其专属的云安全服务，其提供的云安全服务从最小的组织到最大的企业、公有或私有云都予以覆盖。业务方向主要以预防监控为重点。统一安全平台可

以部署在客户的整个网络中，可随着客户的业务需求的增长而不断扩展。全球范围内关联的威胁情报和近乎实时的自动安全更新可在整个网络、端点和云之间创建一致的保护，以免受整个攻击生命周期的威胁，立即阻止已知威胁。同样做安全防御的另一家公司 Fireeye 针对目前网络 WEB 攻击频发的局面，利用统一防御措施抵制网络攻击。重点在对网络、电子邮件、端点等内容进行分析和监控，同时获取动态威胁情报以方便客户制定相应的防御措施。

图表 46 Fireeye 业务结构

资料来源：Fireeye 网站，东吴证券研究所

信息安全企业的收购 PE 多在 40 倍以上：2006 年以来发生 10 多起网络设备企业收购信息安全企业的案例，并且收购价格均不菲，典型的例子如：

2010 年 Intel 以 77 亿美元收购美国最大的信息安全公司之一 McAfee，当年收购 PE 为 41.7 倍；

2010 年 HP 以 15 亿美元收购安全软件厂商 ArcSight，按照 ArcSight 当年 2264.6 万的净利润算，收购 PE 高达 66 倍；

2010 年同样是 HP 以 9.45 亿美元收购网络与安全技术提供商 Radware。Radware10-11 年的净利润分别为 963.4 万、2133.7 万，即使按照 11 年净利润算，收购 PE 也达到 44.3 倍；

2011 年华为宣布以 5.3 亿美元收购赛门铁克持有的华赛 49%的股份，在收购之前华赛已经连年亏损，从 08 年到 10 年，赛门铁克因为持有 49%的股份导致亏损 1.23 亿美元。

公司净利润增速居前，同行业中估值相对便宜：与可比信息安全行业的公司包括卫士通、榕基软件、美亚柏科、蓝盾股份、任子行、北信源和绿盟科技等相比，公司的三年净利润复合增速居前为 44%，并在未来具有业绩支撑，同时估值只有 82 倍，在 8 个可比公司中处于第二低位。仅绿盟科技的估值 63 倍低于公司估值，但考虑到公司的增速及技术水平已大幅度超越绿盟科技，因此公司估值处于相对低位。

图表 47 信息安全行业可比公司

代码	公司	总市值(亿元)	市盈率(TTM)	11 年净利润	13 年净利润	15 年净利润	五年复合净利润增速
002439	启明星辰	205.59	82.65	0.60	1.22	2.55	43.6%
002268	卫士通	130.97	95.72	0.90	0.36	1.63	16.0%
002474	榕基软件	75.04	524.24	1.19	0.63	0.15	-40.4%
300188	美亚柏科	120.30	90.22	0.62	0.63	1.52	25.1%
300297	蓝盾股份	134.46	104.02	0.52	0.32	1.22	23.8%
300311	任子行	86.34	122.59	0.39	0.22	0.57	10.0%
300352	北信源	86.82	122.59	0.45	0.68	0.71	12.1%
300369	绿盟科技	130.86	63.60	0.93	1.11	1.93	20.0%

资料来源：Wind 资讯，东吴证券研究所

	2015	2016E	2017E	2018E
流动资产	**1954.8**	**2475.9**	**3392.2**	**4617.7**
现金	795.9	805.3	1122.5	1572.4
应收款项	711.4	932.4	1274.2	1717.5
存货	185.7	206.5	268.9	348.3
其他	261.8	531.7	726.7	979.5
非流动资产	**872.9**	**855.2**	**802.8**	**742.7**
长期股权投资	77.1	77.1	77.1	77.1
固定资产	172.9	160.2	112.7	57.6
无形资产	147.9	143.0	138.0	133.1
其他	475.0	475.0	475.0	475.0
资产总计	**2827.6**	**3331.1**	**4195.0**	**5360.4**
流动负债	**972.0**	**1131.3**	**1500.0**	**1971.4**
短期借款	0.0	0.0	0.0	0.0
应付账款	262.0	327.0	425.7	551.4
其他	710.0	804.3	1074.3	1420.0
非流动负债	**56.1**	**56.1**	**56.1**	**56.1**
长期借款	0.0	0.0	0.0	0.0
其他	56.1	56.1	56.1	56.1
负债总计	**1028.1**	**1187.4**	**1556.1**	**2027.5**
少数股东权益	108.0	108.0	108.0	108.0
归属母公司股东权益	1691.6	2035.8	2531.0	3225.0
负债和股东权益总计	**2827.6**	**3331.1**	**4195.0**	**5360.4**

现金流量表（百万元）	**2015**	**2016E**	**2017E**	**2018E**
经营活动现金流	417.1	80.1	412.6	578.0
投资活动现金流	194.0	-10.0	-8.0	-5.6
筹资活动现金流	-77.4	-60.7	-87.4	-122.5
现金净增加额	533.6	9.4	317.2	449.9
企业自由现金流	619.4	-97.2	199.6	324.7

利润表（百万元）	**2015**	**2016E**	**2017E**	**2018E**
营业收入	**1534.0**	**2127.0**	**2906.7**	**3918.0**
营业成本	483.3	628.2	817.8	1059.3
营业税金及附加	22.3	31.9	45.1	62.7
营业费用	465.0	638.1	872.0	1175.4
管理费用	467.5	526.0	702.5	925.7
财务费用	-1.9	-2.8	-3.4	-4.7
投资净收益	21.0	15.0	13.0	10.0
其他	32.7	-25.1	-30.1	-35.1
营业利润	**151.5**	**295.5**	**455.6**	**674.6**
营业外净收支	145.2	170.0	214.0	264.0
利润总额	**296.7**	**465.5**	**669.6**	**938.6**
所得税费用	41.6	60.5	87.1	122.0
少数股东损益	11.0	0.0	0.0	0.0
归属母公司净利润	**244.1**	**405.0**	**582.6**	**816.5**
EBIT	156.0	307.7	474.2	699.8
EBITDA	242.1	332.8	499.7	725.5

重要财务与估值指标	**2015**	**2016E**	**2017E**	**2018E**
摊薄每股收益(元)	0.29	0.47	0.67	0.94
每股净资产(元)	2.04	2.34	2.91	3.71
发行在外股份(百万股)	830.2	868.9	868.9	868.9
ROIC(%)	8.1%	15.3%	22.3%	29.5%
ROE(%)	14.4%	19.9%	23.0%	25.3%
毛利率(%)	67.0%	69.0%	70.3%	71.4%
EBIT Margin(%)	10.2%	14.5%	16.3%	17.9%
销售净利率(%)	15.9%	19.0%	20.0%	20.8%
资产负债率(%)	36.4%	35.6%	37.1%	37.8%
收入增长率(%)	28.3%	38.7%	36.7%	34.8%
净利润增长率(%)	43.3%	65.9%	43.9%	40.2%

资料来源：Wind 资讯，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。

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 个月行业指数涨跌幅相对大盘在 5%以上；

中性：预期未来 6 个月行业指数涨跌幅相对大盘介于-5%与 5%之间；

减持：预期未来 6 个月行业指数涨跌幅相对大盘在-5%以下。

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.gsjq.com.cn