

信息安全稀缺龙头 大数据云安全打开成长空间

——绿盟科技（300369）深度报告

2015年12月19日

强烈推荐/首次

绿盟科技 | 深度报告

报告摘要：

营收净利润增长稳定，高毛利率保障高成长性。公司是国内领先的企业级网络安全解决方案供应商。

- 主要服务于政府、电信运营商、金融、能源、互联网等领域的企业级用户，向用户提供网络及终端安全产品、Web及应用安全产品、合规及安全管理产品等信息安全产品，并提供专业安全服务。2009年到2014年营业收入的CAGR为25.31%，净利润的CAGR为30.61%，在行业内处于领先水平。

细分市场霸主地位难以撼动。

- 公司多项产品市场占有率高，在网络入侵防御系统、抗拒绝服务系统、WEB及应用防护系统、漏洞扫描产品在国内市场占有率均排名第一，在网络入侵检测系统领域排名第二，其中，在网络入侵防御市场连续5年排名第一。在云安全、大数据防护等领域积极拓展，未来成长空间逐步打开。

领先布局云安全，市场首发云安全服务平台。

- 公司在国内首发基于云的网络安全服务平台，该平台向合作伙伴、创客及行业客户提供专业的网络安全产品及服务交付能力。公司积极构建云安全生态建设，近期与华为、腾讯等大型企业的合作预示着公司云安全服务进入了新商业发展阶段。

公司盈利预测及投资评级。

- 公司是国内领先的、具有核心竞争力的企业级网络安全解决方案提供商。深耕信息安全全流程，通过并购不断完善产品线，在大数据和云安全领域逐步打开成长空间。预计公司2015年-2017年EPS分别为0.49、0.70、0.99元，对应PE分别为116.5、81.6和57.7。三家同类公司2016年平均估值为97倍，按行业平均估值水平给予公司6个月目标价68元，首次覆盖给予公司“强烈推荐”评级。

财务指标预测

指标	13A	14A	15E	16E	17E
营业收入(百万元)	623.1	702.7	1001.1	1430.7	2048.3
增长率(%)	18.18%	12.78%	42.47%	42.91%	43.16%
净利润(百万元)	110.5	144.5	176.5	250.4	354.5
增长率(%)	16.63%	30.47%	22.16%	41.83%	41.61%
净资产收益率(%)	23.65%	14.89%	12.88%	15.84%	18.86%
每股收益(元)	1.47	1.08	0.49	0.70	0.99
PE	34	46	102	72	51
PB	8.03	6.98	13.12	11.37	9.57

林阳

021-65465035

liny.ang@dxzq.net.cn

执业证书编号：

S1480510120003

杨洋

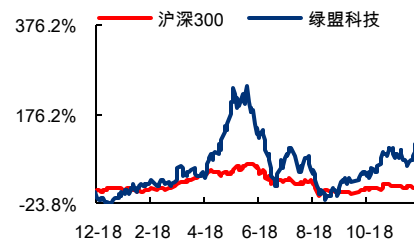
021-65465583

yang_yang@dxzq.net.cn

交易数据

52周股价区间(元)	57.1-67.44
总市值(亿元)	204.41
流通市值(亿元)	58.55
总股本/流通A股(万股)	35798/10254
流通B股/H股(万股)	/
52周日均换手率	6.99

52周股价走势图



资料来源：东兴证券研究所

相关研究报告

目录

1. 国内综合性全领域信息安全解决方案供应商	4
1.1 信息安全行业龙头，增长稳定，未来向好	4
1.2 明星产品行业领先，高技术集中带来高额利润	7
2. 国家安全战略带来行业发展确定性机遇	12
2.1 信息安全问题频发，影响蔓延全球	12
2.2 我国信息安全产业发展相对滞后，具有较大发展空间	13
2.3 三大因素驱动我国信息安全行业未来发展	15
3. 公司三大未来发展方向	17
3.1 大力发展国外业务，走国际化路线	17
3.2 并购整合完善产业链覆盖	19
3.3 领先布局云安全，市场首发云安全服务平台	19
4. 盈利预测及投资评级	23
5. 风险提示	24

表格目录

表 1 2008-2014 年公司获得的主要技术荣誉	6
表 2 公司核心客户以及公司客户范围	6
表 3 公司主要安全产品及其分类情况	9
表 4 2014 年国际影响较大的网络安全事件	12
表 5 近年来我国发生的网络安全事件	15
表 6 近年来我国出台的主要政策	16
表 7 公司国际化发展大事件	18
表 8 公司近年来主要并购和投资	19
表 9 类似公司 PE 情况	24

插图目录

图 1 2009-2014 年公司营业收入和净利润情况	4
图 2 2009-2014 年公司营业收入和毛利情况	5
图 3 2009-2014 年公司营业收入和研发费用情况	5
图 4 2009-2014 年公司主营业务及其营收占比情况	8
图 5 2009-2014 年公司主营业务与其毛利率情况	8

图 6 网络入侵防御系统（IPS）/网络入侵检测系统（IDS）示意图	10
图 7 2014 年 1-12 月网络安全事件发生次数情况.....	11
图 8 2014 年我国与欧美等发达国家信息安全投入占比情况.....	14
图 9 2012-2017 年信息安全产品市场规模及增长率情况	14
图 10 2012-2017 年信息安全服务市场规模及增长率情况	15
图 11 2010-2014 年公司海外营收及毛利率情况.....	18
图 12 绿盟科技云安全体系架构简介.....	20
图 13 绿盟云产品服务体系.....	20
图 14 绿盟云产品服务体系.....	21
图 15 公司云安全体系架构简介.....	21
图 16 腾讯云构架体系.....	22

1. 国内综合性全领域信息安全解决方案供应商

1.1 信息安全行业龙头，增长稳定，未来向好

公司是国内领先的企业级网络安全解决方案供应商。成立于2000年4月，总部位于北京。在国内外设有30多个分支机构，主要服务于政府、电信运营商、金融、能源、互联网等领域的企业级用户，向用户提供网络及终端安全产品、Web及应用安全产品、合规及安全管理产品等信息安全产品，并提供专业安全服务。

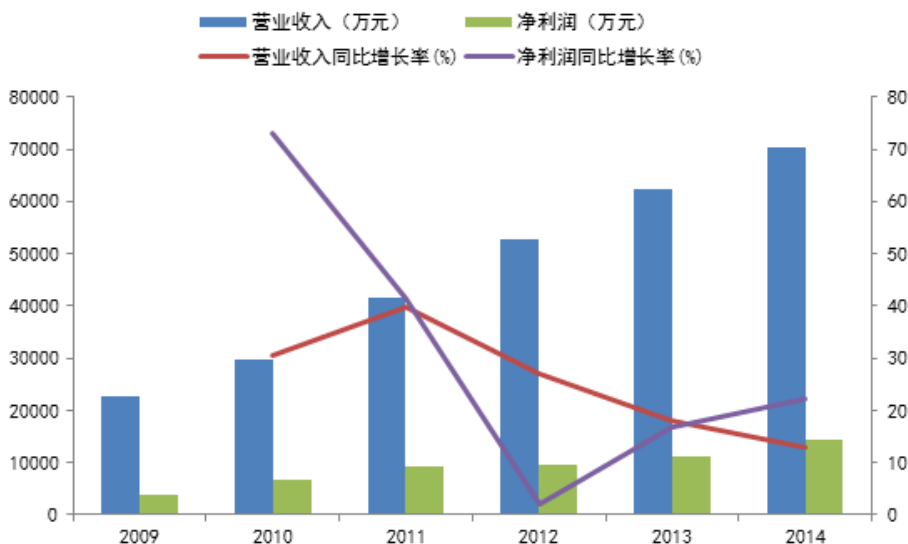
1.1.1 营收净利润增长趋于理性，高毛利率保障高成长性

近年来，公司的营业收入和净利润由早期的爆发性增长逐渐趋于理性，主要原因：

行业发展初期，市场空间广阔：公司是较早一批进入行业的先行者之一，早期的市场空间异常广阔，客户对于产品的质量和性能要求不高，使得早进入行业的公司可以迅速打开市场，占领高地。所以公司早期增长迅速。

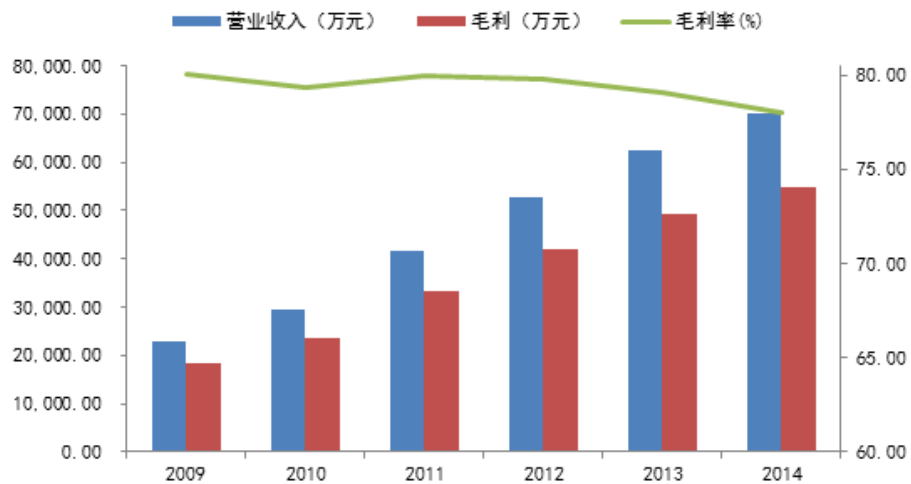
高技术壁垒和客户粘性限制公司持续做大：公司所处行业具有极高的技术壁垒，技术壁垒的打破需要时间与资源的不断累积，我国信息安全类公司起步较晚，时间与资源相对于国外公司均不占优势，所以当用户对产品的质量与性能有较高要求的时候，国内公司往往难以满足。且行业的客户粘性极大，用户对现有厂商产品的依赖性强，不会轻易用同类产品替代，或替代的成本极高，缺乏不可抗力时难以实现。

图 1 2009-2014 年公司营业收入和净利润情况



资料来源：WIND，东兴证券研究所

公司在2010年到2011年期间，营收和净利润迎来爆发性增长，但在后面的几年间增长逐步放缓，2009年到2014年营业收入的CAGR为25.31%，净利润的CAGR为30.61%，在行业内处于领先水平。近年来营收和利润的稳步增长的背后靠的是长期稳定的高毛利率。

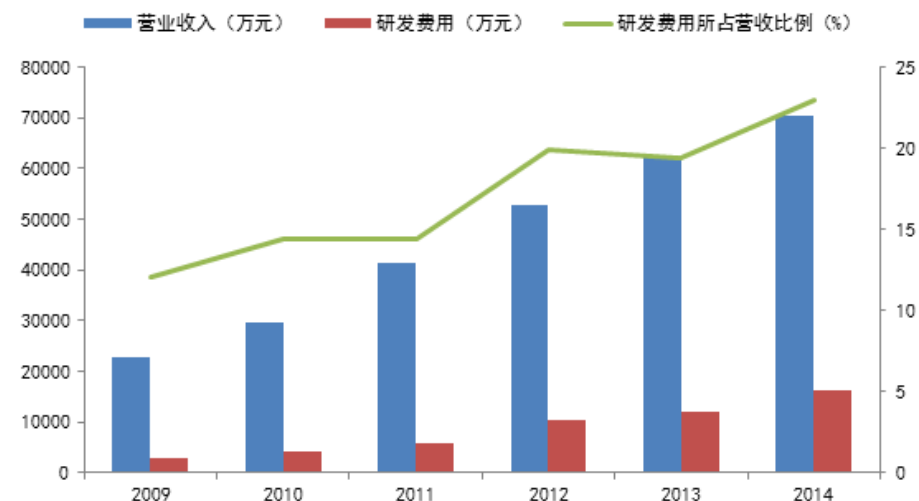
图 2 2009-2014 年公司营业收入和毛利情况


资料来源：WIND，东兴证券研究所

公司长期保持 80% 左右的毛利率，这是公司盈利能力与未来高成长性的必要保证。

1.1.2 研发投入不断加大造就技术领先

公司的研发费用占比从 2009 年的 12.06% 增长到了 2014 年的 22.91%，且在这些年期间一直保持增长。在科技型企业中研发投入占比超 10% 已属难得，达到 20% 以上更说明了公司深耕技术研发的决心，可见公司对于自主技术的重视程度之高。

图 3 2009-2014 年公司营业收入和研发费用情况


资料来源：WIND，东兴证券研究所

正是因为长期以来在研发上的不懈投入，公司取得了一系列的技术荣誉，真正做到业界技术领先。公司建立并维护的全球最大的中文漏洞库已经成为业界广泛参考的标准，并承担了多项国家级重点科研项目。远程安全评估系统产品“极光”获英国西海岸实验室的 Checkmark 认证，入侵防御系统通过 NSSLab 测试并获得最高级别的推荐认证。

绿盟科技云安全运营服务获得国际上最权威、最严格、也是最被广泛接受和应用的信
息安全标准 ISO27001 管理体系认证，成为国内首家通过该项认证的可管理安全服务
(MSS)和安全即服务(SECaaS)提供商。公司建立了完善的专业安全服务体系(NSPS)，
具备国内最高级安全服务资质，连续多年被评为“值得信赖的安全服务品牌”。

表 1 2008-2014 年公司获得的主要技术荣誉

时间	主要荣誉简介
2008	“极光：远程评估系统获得英国西海岸实验室 Checkmark 认证
2009	网络入侵防护系统获得由中国信息安全测评中心颁发的国家信息安全测评信息技术产品安全测评证书（EAL3 级）
2009	网络入侵检测系统 V5.6 获得由中国信息安全测评中心认证的首批“信息技术产品自主原创测评证书”产品
2010	入侵防御产品 NIPS 获得美国 NSS Labs 最高级别推荐认证
2011	公司获得由中国网络管理技术大会颁发的年度技术品牌创新奖
2012	公司获得年度中国信息安全最具影响力企业
2014	漏洞评估产品入选 Gartner 全球市场指南报告
2014	Web 应用防火墙入选 Gartner 魔力象限，通过第三方国际独立测评机构 ICSA Labs 的 WAF 产品认证
2014	安全审计系统堡垒机（SAS-H）、WEB 应用漏洞扫描系统（WVSS）获得 2014 中国 IT 运维管理最值得推荐奖
2014	可管理安全服务（MSS）获得 Best Managed Security Service（最佳可管理安全服务）金奖和 Business Expansion of the Year（年度业务拓展）银奖两项国际奖项
2014	云安全运营服务业务获得 ISO27001 管理体系的认证，成为国内首家通过 ISO27001 认证的可管理安全服务（简称：MSS）和安全即服务（简称：SECaaS）提供商

资料来源：招股说明书，公司年报，东兴证券研究所

2014 年公司继续加大研发投入，投入金额再创新高，合计为 161,012,174.73 元，占营业收入的比例为 22.91%。2014 年内公司取得计算机软件著作权证书 19 项，取得国内发明专利 17 项，日本发明专利 6 项，并先后发布多款新产品和对老产品进行升级，包括：升级版网络入侵防护系统、新一代威胁防御整体解决方案、工控漏洞扫描系统、高性能流量清洗产品、数据库审计系统等，其中公司工控漏洞扫描系统为国内首款工业控制系统漏洞扫描产品。

1.1.3 优质而稳定的客户群体，长期深耕带来丰富的行业经验

公司通过多年努力逐步发展形成了以政府、电信运营商、金融、能源和互联网等领域优质客户为主体的客户群体，并保持了长期稳定的合作关系。

表 2 公司核心客户以及公司客户范围

客户领域	公司客户/公司客户范围
政府	全国人大信息中心、财政部、组织部、人力资源社会保障部、国土资源部、教育部、科学技术部、环境保护部、商务部、公安部、民政部、国家海关总署、国家税务总局、国家工商总局、国家质检总局、国家知识产权局、国务院新闻办、中国科学院、新华社、中国银监会、最高人民法院等

电信运营商	中国移动集团及 31 家省公司、中国电信集团及 28 家省公司、中国联通集团及 21 家省公司
金融	中国人民银行、中国工商银行、中国建设银行、中国银行、中国农业银行、交通银行、招商银行、华夏银行、中国人保、中国平安、中信证券、银河证券、中国证券登记结算中心等
能源	国家电网、南方电网、中国石油、中国石化、中海油等
互联网	中央人民政府门户网站、人民网、新华网、腾讯、网易、263 等

资料来源：招股说明书，东兴证券研究所

同时，行业经验的积累对于信息安全厂商至关重要，公司通过与上述核心客户的密切合作，积累了丰富的信息安全项目实施经验，同时也帮助公司不断完善信息安全产品的性能，做到动态把握主要领域客户对于信息安全的技术需求及发展趋势。

公司核心优质客户稳定有保障，对公司长期发展大有助益：

信息安全业务本身具有束缚力：信息安全业务本身会涉及到客户较多的核心数据和机密信息，所以客户不会冒着巨大的风险随意更换合作的公司，这就使得二者之间的合作会逐渐加深。特别是对于绿盟这种业务覆盖面比较广公司，可以满足客户对于信息安全各方面的需求。所有公司的核心客户粘性极大，可以长期稳定为公司贡献业绩。

核心客户因素更加看重公司实力：公司的核心客户主要来自政府、电信运营商、金融、能源和互联网等领域，这些核心客户对于控制成本的要求比较少，而对公司的行业经验以及产品的成熟度稳定性要求较高，这点恰恰和绿盟的实际情况相契合。

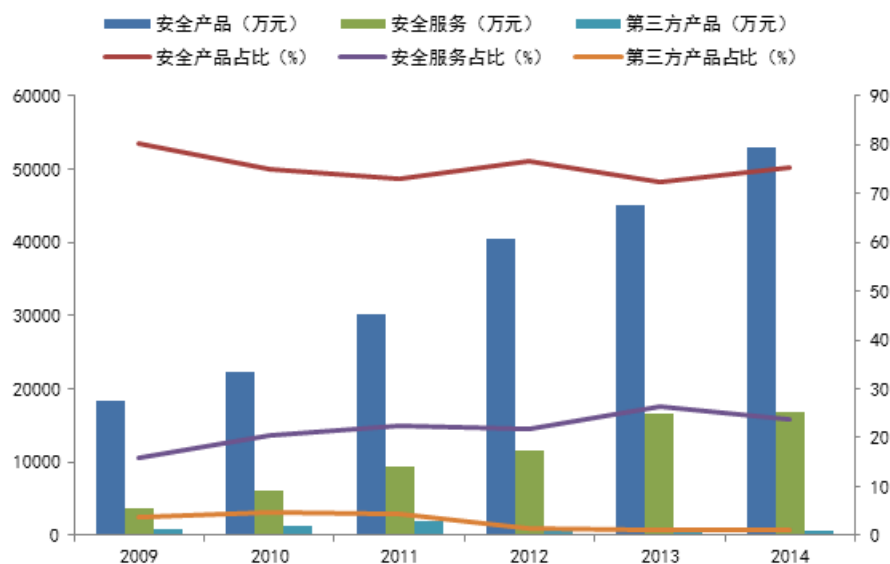
渠道带来的上下游拓展空间广阔：核心客户所涉行业都相对宽泛，有着比较复杂的上下游供求网络。长期合作带来的渠道优势可以帮助公司快速进去核心客户涉及的上下游行业，完成产品与业务的扩张与拓展。

1.2 明星产品行业领先，高技术集中带来高额利润

1.2.1 追求高毛利率驱动主营构成不断优化

从公司的主营构成上来看，公司收入主要来自于三块业务，包括：安全产品，安全服务与第三方产品。历年来三块业务所占的比重上，安全产品占据绝对优势，维持在 75% 左右，随着公司产品应用的越来越广泛，与之相对应的安全服务所占比重呈现逐年上升的趋势，约占 24%。而第三方产品则逐年递减，由原来的 4% 左右下降到不到 1%。

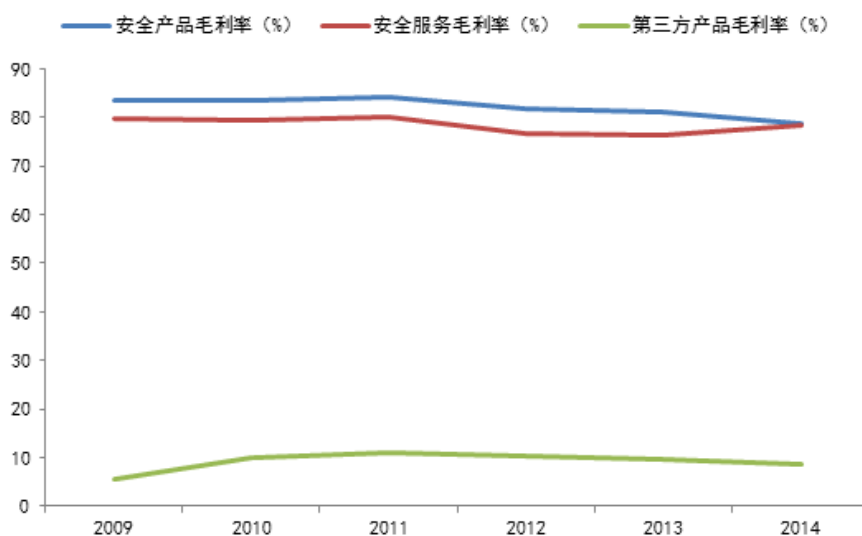
图 4 2009-2014 年公司主营业务及其营收占比情况



资料来源：WIND，东兴证券研究所

公司主营构成的改变基本符合行业整体的发展过程：初期国内公司基础差技术落后，只能依靠代销第三方产品，赚取小额差价来维持生存。后期随着技术水平的提升，逐渐可以独立完成一些项目，从而更多的转向高毛利率的业务。

图 5 2009-2014 年公司主营业务与其毛利率情况



资料来源：WIND，东兴证券研究所

相对于第三方产品代销的约 10% 上下的毛利率，自主安全产品的销售和安全服务约 80% 的毛利率明显高得多。由于第三方产品代销的比重已低于 1%，且未来依然呈现持续下降的趋势，所以此业务不纳入本次研究的范围以内。

1.2.2 具备核心技术优势的产品是公司在行业的立足之本

公司收入主要来自于信息安全产品和安全服务，信息安全产品的销售对于安全服务有带动作用，在业务层面二者是相辅相成的。信息安全产品包括三大类：网络及终端安全产品、Web 及应用安全产品、合规及安全管理产品，分别针对硬件、应用和各种类型的安全风险。每一大类又分为若干小类，每一小类对应一种安全产品。公司提供的安全服务主要为专业安全服务，旨在降低对关键业务资产的威胁，通过企业级安全评估、安全设计、安全部署来提高安全管理的实效。此外，公司也为客户提供完备的实时安全管理外包解决方案，包括安全监控、7*24 小时全天服务安全保障、应急处理等。

表 3 公司主要安全产品及其分类情况

产品分类	二级分类	具体产品
信息安全产品	网络及终端安全产品	网络入侵检测系统（IDS）
		网络入防御测系统（IPS）
		安全网关（SG）
	Web 及应用安全产品	内网安全管理系统（EPS）
		网络流量分析系统（NTA）
		抗拒服务系统（ADS）
	合规及安全管理产品	Web 应用防护系统（WAF）
		安全配置核查系统（BVS）
		远程安全评估系统（RSAS）
安全服务	专业安全服务	内容安全管理系统（SCM）
		安全评估、安全管理、威胁管理、早期预警、网站安全监测系统（WSMS）

资料来源：招股说明书，东兴证券研究所

其中，多个明星产品得到客户的高度认可，在国内占有率第一：

- ◆ **网络入侵防护系统 NIPS** 连续 5 年 IDC 报告国内市场占有率第一（数据来源：IDC 《中国 IT 安全硬件、软件和服务全景图 2014-2018 预测与分析》报告）。
- ◆ **Web 应用防火墙** 技入选 Gartner 魔力象限，并连续四年荣登大中华区榜首。绿盟科技作为亚太区第四大 WAF 厂商，以 25.9% 的市场占有率持续领导大中华区 WAF 市场（数据来源：Frost & Sullivan 发布的《2013 年亚太区 Web 应用防火墙市场报告》）。
- ◆ **远程安全评估系统 RSAS** 在国内市场占有率排名第一，实现连续三年荣登榜首（数据来源：IDC 《中国 IT 安全硬件、软件和服务全景图 2014-2018 预测与分析》报告数据）。
- ◆ **抗拒服务攻击系统 ADS** 国内市场占有率第一。并且公司在 ADS 和 NTA 产品的基础上，进一步融合云平台技术，推出的 7x24 小时 DDoS 攻击防御解决方案。

- 还有诸如网络入侵检测系统（IDS）国内市场占有率第二，漏洞扫描评估类产品也一直占据着行业领导者的位置，在 IDC 统计的国内安全性与漏洞管理市场排名中连续三年蝉联第一。

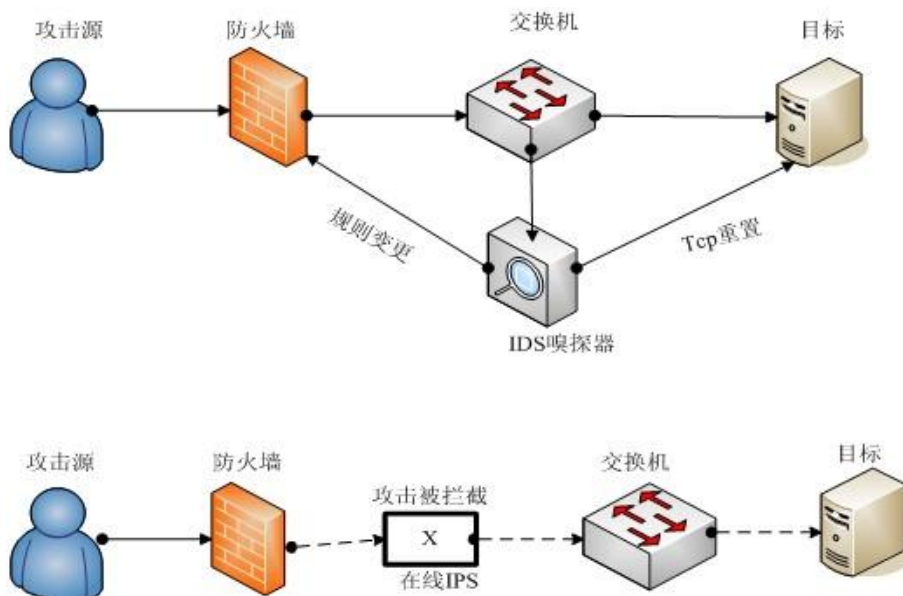
我们认为对于技术高度密集型产品或行业来说，唯有做到：人无我有，人有我精，才能在市场中真正立于不败之地。我们选取了三个具有代表性的重点产品做进一步研究。

（1）网络入侵防御系统（IPS）/网络入侵检测系统（IDS）

入侵检测系统 IDS（Intrusion Detection Systems）是依照一定的安全策略，对网络、系统的运行状况进行监视，对可能发生的各种攻击企图、攻击行为或者攻击结果做出响应告警，以保证网络系统资源的真实性、完整性和可用性。

入侵防御系统 IPS（Intrusion Prevention System）是在网络攻击技术不断提高和网络安全漏洞不断进化发展的过程中应运而生的，当传统防火墙技术加传统 IDS 的技术，已经无法应对一些特殊的具有针对性的安全威胁的时候，IPS 技术可以更加深度地感知并检测流经的数据流量，对恶意行为进行拦截以阻断攻击。

图 6 网络入侵防御系统（IPS）/网络入侵检测系统（IDS）示意图



资料来源：希赛网，东兴证券研究所

IPS 是位于防火墙和网络的设备之间的设备，如果检测到攻击，IPS 会在这种攻击扩散到网络的其它地方之前阻止它。而 IDS 只是存在于你的网络之外起到告警的作用，而不是在网络前面起到防御的作用。

公司的 IDS 为 ICEYE 系列，根据类型不同，具备对黑客攻击（缓冲区溢出、SQL 注入、暴力猜测、拒绝服务、扫描探测、非授权访问等）、蠕虫病毒、木马后门、间谍软件、僵尸网络等进行实时检测及报警，并通过与防火墙联动、TCP Killer、发送邮件、控制台显示、日志数据库记录、打印机输出、运行用户自定义命令等方式进行动态防护。

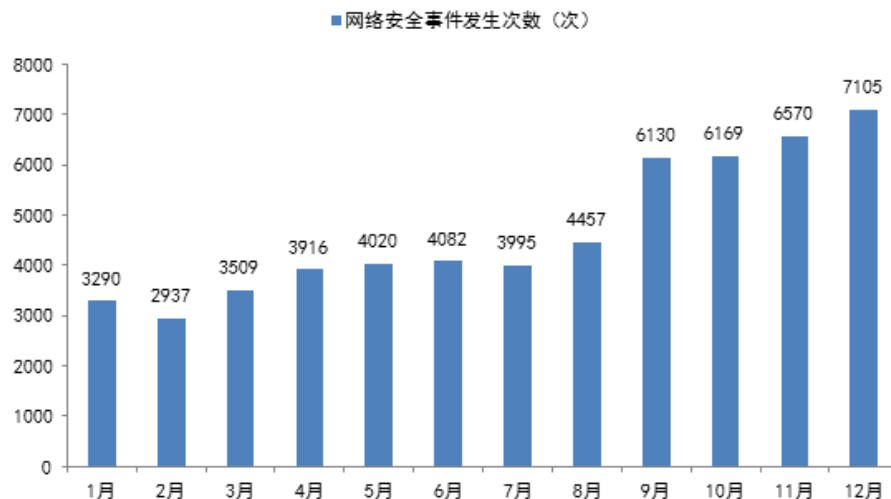
NIPS 作为一种在线部署的产品，其设计目标旨在准确监测网络异常流量，自动应对各类攻击流量，第一时间将安全威胁阻隔在企业网络外部。基于高性能硬件处理平台，为客户提供从网络层、到应用层，直至内容层的深度安全防御，以全面深入的协议分析为基础，融合权威专家系统、智能协议识别、协议异常检测、流量异常检测、会话关联分析，以及状态防火墙等多种技术，为客户提供从网络层、应用层到内容层的深度安全防护。且内置状态防火墙，支持基于网络接口、源/目的 IP 地址、协议、时间等元素，自定义访问控制策略。

（2）Web 应用防护系统（WAF）

当前网络环境中，应用已成为网络的主要载体，而网络安全的威胁也往往来源于应用层，这也使得用户对于网络访问管控提出了更高的要求。Web 应用防护系统（Web Application Firewall）是通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 Web 应用提供保护的一款产品。

由于互联网具有较强的开放性，以及互联网相关的应用或基础软件普遍存在安全漏洞或者安全隐患，是的互联网成为恶意攻击的主要目标。近年来，国内网站频繁遭遇各种形式的恶意事件，如：页面篡改，DDoS 攻击，网站挂马等，给企业带来了严重的经济和其他形式的损失。

图 7 2014 年 1-12 月网络安全事件发生次数情况



资料来源：CNCERT/CC，东兴证券研究所

2014 年 CNCERT/CC 共接收到境内外报告的网络安全事件 56180 起，较 2013 年同比增长了 77.5%。

公司的 WAF 产品有如下技术优势：

- ◆ 安全专家团队全天候远程值守以及安全平台 7x24 小时监测
- ◆ 持续调整优化防护规则，精准拦截 Web 攻击
- ◆ 专家级的定期安全报告

◆ 灵活的部署与应用方式

相比传统产品,公司的 WAF 能够针对 Web 应用攻击提供更全面、更精准的防护,尤其对一些可以跨越传统防火墙和 IPS 的攻击方式,可以做到精准地阻断,对数据盗窃、网页篡改、网站挂马、虚假信息传播、针对客户端的攻击等恶意行为,提供了完美的解决方案。

(3) 漏洞扫描评估类产品与解决方案

根据国际著名咨询机构 Gartner 在 2014 年发布的漏洞评估 (Vulnerability Assessment) 市场报告《Market Guide for Vulnerability Assessment》,公司入选代表厂商同时也是亚太厂商中唯一入选者。

公司主要 VA 产品包括面向主机系统漏洞扫描的 RSAS、面向 Web 应用漏洞扫描的 WVSS、面向主机配置检查的 BVS、面向工控漏洞扫描的 ICSScan 以及面向网站安全风险监测的 WSM。公司扫描评估类产品独特的虚拟化部署、基于多角色的访问控制、与企业工作流和安全管理工具的整合、扫描和告警自动化、整改和威胁优先级和评估分析等功能,已经得到政府、运营商、金融行业、互联网公司、企业等核心用户的广泛认可。

正是由于这些具备自主知识产权的明星产品在市场上得到的肯定,为公司在业界树立了良好的形象,使得公司逐渐获得了客户的品牌信任度。我们认为公司具备领先优势的细分行业产品在未来仍将领跑市场。

2. 国家安全战略带来行业发展确定性机遇

2.1 信息安全问题频发,影响蔓延全球

2014 年,全球大型企业检测到的安全事件数量达到 13138 起,较 2013 年增加了 44%。数据显示,全球与国内企业每年因信息安全导致的平均损失分别为 270 万美元和 240 万美元,分别较去年增长 34%和 33%,而且呈现迅速增长的态势。

其实在人们日常的生活,网络和信息安全事件一直是隐含存在的,而网络和信息安全成为全世界密切关注的焦点始于 2013 年 6 月由美国中情局前特工爱德华·斯诺登曝

光的“棱镜计划”,这一事件引发了人们对互联网高度发达时代信息泄露的担忧和网络

安全事件的惊慌。2014 年是多个网络严重漏洞集中爆发的一年,如 OpenSSL 的心脏出血(Heartbleed)漏洞、IE 的 0 Day 漏洞、Struts 漏洞、Flash 漏洞、Linux 内核漏洞、Synaptics 触摸板驱动漏洞、贵宾犬、USBbad、破壳等重大漏洞先后曝光,受影响的网站、操作系统、硬件设备范围之广、之深,前所未有的。

表 4 2014 年国际影响较大的网络安全事件

事件名称	事件简介	事件影响
------	------	------

“心脏出血”严重漏洞	心脏出血(Heartbleed)出现在开源加密库 OpenSSL, 通过此漏洞, 黑客可以读取到包括用户名、密码等敏感数据。	波及大量互联网公司, 受影响的服务器数量可能多达几十万, Imgur、OKCupid、Eventbrite、FBI 网站确认受影响
斯诺登曝光美国工业间谍活动	斯诺登曝光美国通过互联网监听从事工业间谍活动。斯诺登称, 美国的工业间谍活动所针对的不仅限于国家安全问题, 还包括任何对美国有价值的工程和技术资料。	使用云服务、搜索引擎和社交媒体均有风险, 暗示谷歌和脸谱都与政府勾结进行监听和提供“危险”服务。
2000 万韩国人信用卡信息被盗	在人口 5000 万的韩国, 至少有 2000 万人的信用卡信息被盗, 源自个人信用评估公司的内部员工监守自盗。	泄露的个人信息包括: 用户姓名、身份证号、电话、信用卡号码、信用卡有效期。这是韩国历史上最严重的信息泄露事件。
英国央行雇佣黑客进行内部攻防测试	2014 年 4 月, 英国央行(Bank of England)宣布雇佣黑客来帮助其对二十多个主要银行进行防御测试	英国走在了网络保护的前沿, 能够对消费者、企业和经济起到正面的影响作用。
微软正式停止对 XP 系统技术支持	2014 年 4 月 8 日, 微软正式宣布停止对 WindowsXP 系统提供技术支持。	此后 XP 操作系统出现任何漏洞, 微软不会再提供任何系统更新修补漏洞。
iCloud 曝安全漏洞引发“艳照门”事件	黑客利用 Find me iPhone 功能漏洞盗取用户信息, 针对某些女星的公开邮件账号反复猜测, 并获取她们相机里面的私人照片以及其它明星的邮件地址。	iCloud 服务被黑客攻破, 造成数百家户晓的名人私密照片被盗。
摩根大通银行被黑 8300 万客户信息泄露	黑客通过仅有的一台没有采取两步验证的服务器的一个账户进入了其他服务器, 盗取了 8300 万用户信息, 控制了摩根大通的 90 多台服务器。	此次事件造成了摩根大通 7600 万家庭账户和 700 万个小企业账户的户名、地址、电话和电子邮件被泄露的严重后果。
全球手机运营商现安全漏洞	问题涉及到通讯标准系统 Signaling System 7(简称 SS7), SS7 系统是一种沿用了 30 年的老系统, 该系统被手机运营商用来管理手机网络之间的连接。	黑客可以利用这种安全漏洞来监听或监视数十亿人的手机通话、短信和数据流量。
全球互联网域名管理机构 ICANN 遭黑客攻击	2014 年 11 月底开始, 互联网域名管理机构 ICANN 接连遭到不明黑客发起的严重钓鱼式攻击, 攻击采用模拟机构内部域名的方式向员工发送电子邮件。	导致 ICANN 多位员工的电邮身份信息被盗, 重要数据遭外泄。
索尼影业被黑事件	2014 年 11 月 22 日, 美国索尼影视娱乐公司受到自称“和平卫士”的黑客组织黑客攻击, 导致公司系统被迫关闭。	此次攻击造成员工信息、公司计划、产品情况、高层往来邮件、名人电子邮件在内的敏感信息泄露, 还有索尼影视未发布的几部影片都被公布到网上供网民下载。

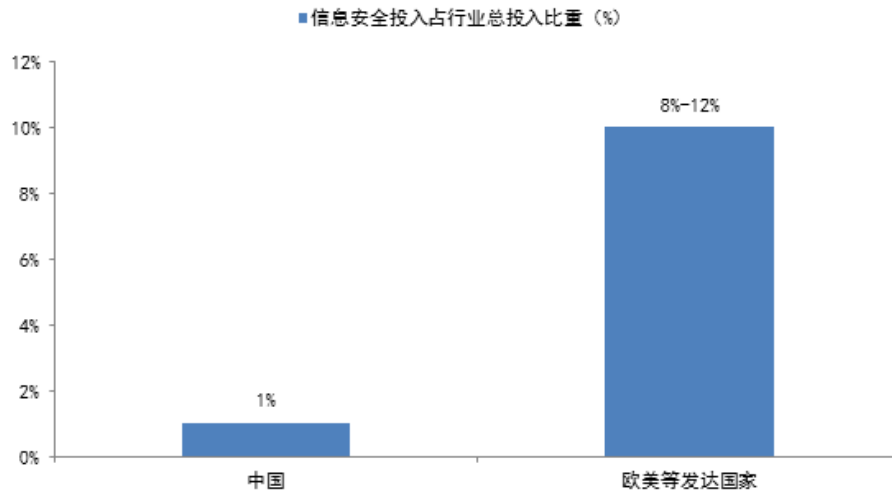
资料来源: 东兴证券研究所

即便如此, 我们所看到的、听闻的网络攻击, 实际上还只是冰山一角。未来的网络空间将出现更多错综复杂、有组织性甚至是由敌对国家发起的网络袭击。因此, 网络和信息安全防护得到各国政府机构和企业组织前所未有的重视, 网络信息安全方面的投资将会由政府主导大幅增加, 从而促进行业规模快速提升。

2.2 我国信息安全产业发展相对滞后, 具有较大发展空间

我国信息安全产业正处于发展初期, 发展相对滞后。在投入规模与市场总规模上与欧美先进国家相差比较大, 但从另一角度, 我国信息安全产业未来具有较大的发展空间。

图 8 2014 年我国与欧美等发达国家信息安全投入占比情况

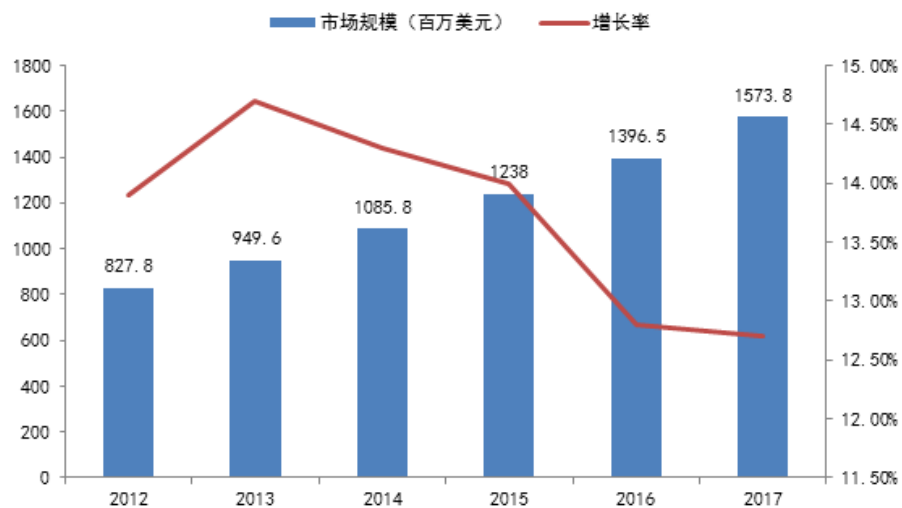


资料来源：IDC，东兴证券研究所

从全球信息安全投入规模上来看，目前我国信息安全行业投入占行业整体投入比例仅为 1% 左右。而欧美等发达国家投资占比约为 8% - 12%，在投入规模上相比我国优势明显。

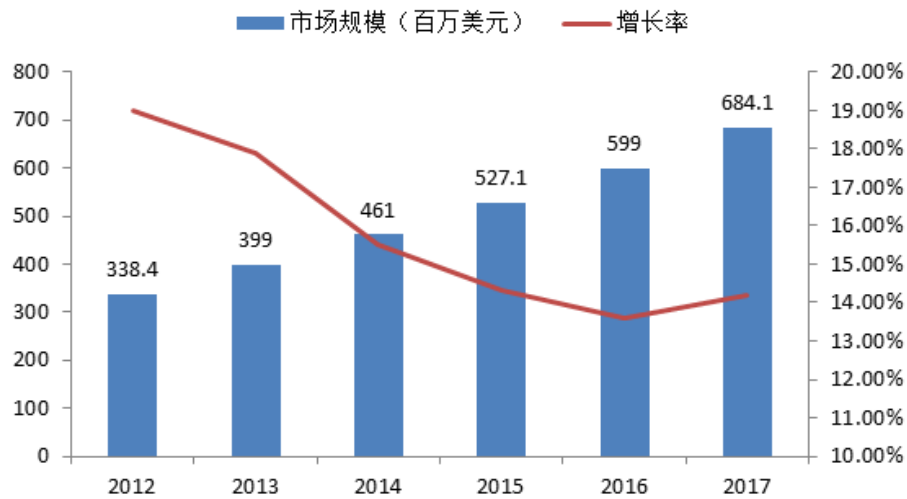
从市场规模上来看，根据 2012 年到 2015 年国内信息安全产品市场规模和增长率的统计数据，IDC 预测 2017 年国内信息安全产品的市场规模有望达到 15.62 亿美元，2012 到 2017 年信息安全产品市场的复合增长率为 13.5%。

图 9 2012-2017 年信息安全产品市场规模及增长率情况



资料来源：IDC，东兴证券研究所

IDC 预测 2017 年国内信息安全服务的市场规模将达到 7.07 亿美元，2012 到 2017 年信息安全服务市场的复合增长率为 9.9%。

图 10 2012-2017 年信息安全服务市场规模及增长率情况


资料来源: IDC, 东兴证券研究所

2.3 三大因素驱动我国信息安全行业未来发展

2.3.1 需求因素

信息安全投资的增长, 来自我国 IT 行业的投入带来的未知威胁: 近年来, 国内经济的快速增长直接带动了 IT 投入的增长, 包括三网融合、3G 网络、智能电网等基础设施的建设和发展, 同时带来了新的威胁, 这些未知的威胁直接影响着国家的安全, 从而受到中央政府和各行业上市企业的高度重视, 直接带动了安全投资的增长。

防范网络犯罪是国内信息安全行业发展的动力: 近年来, 各种获取经济利益的网络犯罪事件层出不穷, 其特点不断发展成为以应用为载体, 范围涉及各类信息终端, 且针对特定用户群, 如中国人寿广东分公司系统存在高危漏洞, 10 万客户信息存在随时大面积泄露的可能性, 防范此类网络犯罪成为国内信息安全产业发展的又一动力。

2.3.2 事件因素

近年我国网络安全事件频发, 推动着网络信息安全产业的机进一步发展。频发的网络安全事件不仅影响着我国经济发展水平的提高, 而且对全国人民社会生活造成了很大的危害。网络信息安全行业水平急需迅速提高, 为我国网络信息安全提供更加完善的保障。

表 5 近年来我国发生的网络安全事件

时间	事件简介
2014 年 1 月 21 日	我国通用顶级域的根服务器出现异常, 导致众多知名网站出现 DNS 解析故障, 用户无法正常访问。虽然很快恢复, 但由于 DNS 缓存问题, 部分地区“断网”现象仍持续了数个小时, 至少有 2/3 的国内网站受到影响, 超过 85% 的用户遭遇了 DNS 故障。
2014 年 12 月 25 日	3 万多条 12306 用户数据包括用户帐号、明文密码、身份证号码、手机号码和电子邮箱等信息泄露。黑客收集互联网某游戏网站以及其他多个网站泄露的用户名和密码信息, 通过撞库的方式利用

12306 的安全机制的缺欠来获取数据信息。

2015 年 1 月 5 日	机锋论坛泄露 2300 万用户数据，包括用户名、注册邮箱、加密后的密码等信息，由于机构数据库对用户密码仅使用了简单的 MD5 加密，黑客能够快速破解出绝大部分明文密码。
2015 年 2 月 11 日	知名连锁酒店桔子、锦江之星等，高端酒店万豪、洲际等网站存在高危漏洞——房客开房信息大量泄露，黑客可轻松获取到酒店顾客的订单信息，包括姓名、身份证、手机号、房间号、房型、开房时间、退房时间等大量敏感信息。
2015 年 2 月 27 日	江苏省公安厅发布《关于立即对全省海康威视监控设备进行全面清查和安全加固的通知》称，主营安防产品的海康威视其生产的监控设备被曝严重的安全隐患，部分设备已被境外 IP 控制，并要求各地立即进行清查，开展安全加固，消除安全隐患。
2015 年 4 月 22 日	统计数据显示，目前围绕社保系统、户籍查询系统、疾控中心、医院等大量曝出高危漏洞的省市已经超过 30 个，仅社保类信息安全漏洞统计就达到 5279.4 万条，涉及人员数量达数千万，其中包括个人身份证、社保参保信息、财务、薪酬、房屋等敏感信息，其中有一部信息在市场上处于可售卖的状态。
2015 年 8 月初	高考生信息在网上被肆意出售，10 万条信息标价 1 万元。这些高考生信息包括考生姓名、高考考分、学校、详细家庭地址和联系电话等重要内容，涉及 10 万名考生，遍及四川、湖北、贵州、河南等 13 个省区市。
2015 年 8 月 27 号	线上票务营销平台大麦网再次被发现存在安全漏洞，600 余万用户账户密码遭到泄露。在过去一年多时间里，大麦网因为“不同严重程度”的漏洞问题已经陆续被警告提醒了 41 次。
2015 年 9 月 14 号	国家互联网应急中心报告显示，“开发者使用非苹果公司官方渠道的工具 Xcode 开发苹果应用程序时，会向正常的苹果 APP 中植入恶意代码。被植入恶意程序的苹果 APP 可以在 APPStore 正常下载并安装使用。该恶意代码具有信息窃取行为，并具有进行恶意远程控制的功能。”已有微信、滴滴打车、高德地图、网易云音乐等近 350 款 APP 被感染，可致用户私密信息泄露，腾讯发布报告称受影响用户可能超过 1 亿。

资料来源：东兴证券研究所

2.3.3 政策因素

针对我国多发、易发的网络安全事件的社会环境，我国政府不断加码网络信息安全政策，直接刺激了安全投资的增加。为了网络信息安全立法，我国政府不断出台加强信息安全方面的政策。

表 6 近年来我国出台的主要政策

时间	政策简介
2011 年 12 月	工信部印发《信息安全产业“十二五”发展规划》，在总结“十一五”信息安全产业发展现状、分析面临形势的基础上，规划明确了“十二五”的发展思路和目标，确定了发展重点和重大工程，提出了相关政策措施。规划的发布实施，将促进我国信息安全产业持续健康发展。
2012 年 7 月	国务院发布《关于大力推进信息化发展和切实保障信息安全的若干意见》，强调要“建立健全信息安全保障体系”，明确提出要“完善信息安全认证认可体系，加强信息安全产品认证工作”。《意见》的发布，为信息安全认证实施营造了良好的政策环境，将对推进信息安全认证事业的发展产生深远影响。

2012年12月	全国人大常委会审议并通过了《关于加强网络信息保护的决定》，规定国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息；网络服务提供者和其他企业事业单位及其工作人员对在业务活动中收集的公民个人电子信息必须严格保密，有关主管部门应在各自职权范围内依法履行职责，采取技术措施和其他必要措施，防范、制止和查处窃取或者以其他非法方式获取、出售或者非法向他人提供公民个人电子信息的行为。
2014年2月	中央网络安全和信息化领导小组成立，国家主席习近平任组长。建立新的体制，制定立法规划，完善互联网信息内容管理、关键信息基础设施保护等法律法规，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设。
2014年8月	国家网信办发布了《2014年国家网络安全检查工作方案》，对全国各地县市政府办公网络系统、各大新闻网络系统、工业控制系统及涉及重要国计民生的信息系统进行网络安全检查，确保各大网络系统的工作环境安全和稳定。
2014年8月26日	工业和信息化部发布了《关于加强电信和互联网行业网络安全工作的指导意见》，建立健全移动应用程序第三方安全检测机制。推动建立移动应用程序开发者第三方数字证书签名和应用商店、智能终端的签名验证和用户提示机制。完善移动恶意程序举报受理和黑名单共享机制。加强社会宣传，引导用户从正规应用商店下载安装移动应用程序、安装终端安全防护软件。加强新业务网络安全风险评估和网络安全防护检查。
2014年9月16日	中国银监会发布39号文件《关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见》，建立银行业信息安全审查和风险评估制度，推进银行业安全可控信息技术平台，展银行业应用安全可控信息技术示范项目，建立银行业金融机构应用安全可控信息技术工作情况的监督评价机制。

资料来源：IDC，东兴证券研究所

2013年11月12日，我国正式成立国家安全委员会，之后在2014年2月27日又成立中共中央网络安全和信息化领导小组办公室，由国家主席习近平亲自领导，将国家网络信息安全提升到国家战略层面，加大了对网络信息行业的重视力度。

2015年6月24号，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）》，从保障网络产品和服务安全，保障网络运行安全、保障网络数据安全、保障网络信息安全等方面进行了具体的制度设计。《网络信息安全》草案将成为具有真正指导意义的行业法规，有利于政府部门及其他相关单位在信息安全投入上更加常态化，是信息安全行业的最大利好。

根据IDC的数据，我国信息安全产品市场未来5年复合增长率将达到13.5%，安全服务市场未来5年的复合增长率为9.9%。但我们认为，由于以上三点因素的刺激，国内信息安全市场的实际增速应远高于IDC的预测，我们预测未来五年信息安全产品市场复合增长率约在30%左右，安全服务市场复合增长率约为25%。

3. 公司三大未来发展方向

3.1 大力发展国外业务，走国际化路线

积极开拓国际市场，走国际化经营之路是公司未来的发展战略中重要的组成部分。自2008年起，公司就开始积极拓展海外市场。现已在日本东京、美国硅谷、英国、香港设立子公司，并在欧洲、东南亚设立分支机构，深入开展全球业务。客户覆盖美国、

日本、英国、荷兰、新加坡、马来西亚、韩国、阿联酋等多个国家与地区。

表 7 公司国际化发展大事件

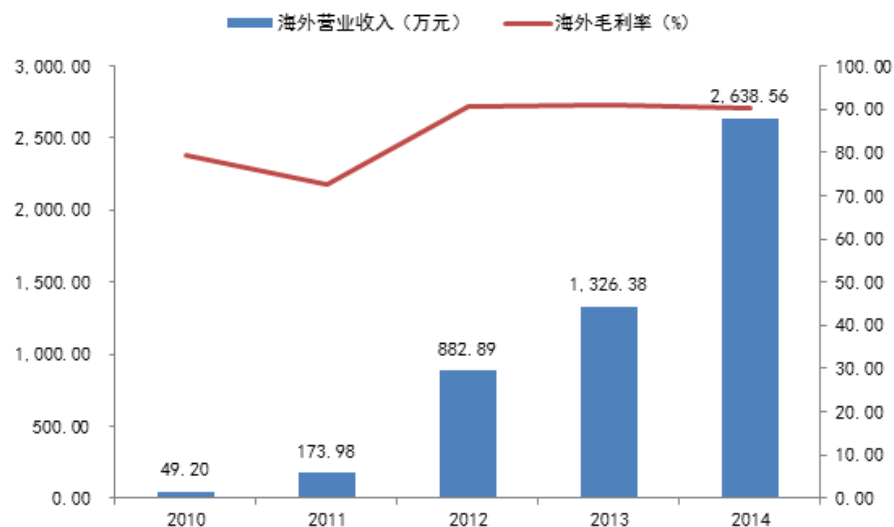
时间	公司国际化大事件
2008 年	公司开始拓展海外市场，在日本和美国设立了子公司
2008 年	成为微软主动防御计划（MAPP）在中国的第一个合作伙伴
2009 年	成为国际云安全联盟（CSA）在亚太区的首家企业成员
2010 年	发起成立国际云安全联盟国区分会（CSA Greater China Chapter）
2010 年	成为国际安全研究机构 StopBadware 的数据提供合作者
2012 年	NIPS 产品成为此产品领域第一个进入 Gartner 魔力象限的亚太区网络安全公司
2014 年	在英国、德国和香港设立了子公司
2015 年	设立了新加坡子公司，继续扩大海外业务覆盖区域

资料来源：公司年报，东兴证券研究所

国际化的好处在于一方面公司可以通过国际业务的开展直接带来收益，另一方面，国外子公司可以第一时间接收信息安全行业发展的最新动态，促使公司在技术战略上调整、缩小与国际领先企业的差距，提升公司的核心竞争力。

2014 年公司来自于海外的营业收入为 2,638.56 万元，同比增长 98.93%，国际市场业务拓展稳步推进。同时海外业务的毛利率也一直保持在比较高的水平，在近两年间甚至超过了 90%。

图 11 2010-2014 年公司海外营收及毛利率情况



资料来源：WIND，东兴证券研究所

在未来的发展中，看好公司充分利用现有的技术和品牌优势，继续开拓国际市场，建立和完善海外分支机构，拓展海外渠道和业务伙伴体系，进一步提升公司盈利能力。我们预计未来五年海外业务在总营收的比重逐渐增大，预计 2016 年翻两番，收入破

亿; 2019 年达到五亿。

3.2 并购整合完善产业链覆盖

公司通过持续投资和并购, 不断进行外延式扩张, 以丰富产业链和着重布局信息安全和国产化。公司通过发行股份并支付现金的方式收购了以主营业务为数据安全和网络内容安全管理产品研发与销售为主营业务的亿赛 100% 股权。目前已完成全部工作, 2015 年 3 月亿赛通公司纳入本公司合并报表, 其产品也正式纳入本公司的销售体系中。参股公司安华金和专攻数据库加密技术、数据库通讯协议解析和控制技术; 控股公司敏讯科技的国内反垃圾邮件系统处于国内技术领先地位。上述公司在国内信息安全领域细分市场具有领先的技术优势。公司通过并购的方式, 使得原有的产业链不断拓展, 形成了一系列的整体解决方案, 并利用公司在核心客户以及渠道上的资源进行整体销售。

表 8 公司近年来主要并购和投资

公司	主营业务	股权比例
安华金和	国内专业数据库安全和服务提供商	25% 股权
深之度	基于 Linux 内核的 Deepin 操作系统的解决方案提供商	10% 股权
剑鱼科技	专注于移动终端相关产品的研发及推广	90% 股权
敏讯科技	国内领先的专业反垃圾邮件安全厂商	55% 股权
亿赛通	主营数据安全和网络内容安全管理产品	100% 股权
力控华康	工控安全领域先发优势明显	11.63% 股权
金山安全	产品线以终端防护为主	19.91% 股权
杭州邦盛	互联网线上、线下反欺诈、反洗钱、身份识别、极速数据流处理、企业内控、欺诈信息云平台、大数据实时征信平台及客户精准营销服务	11.56% 股权

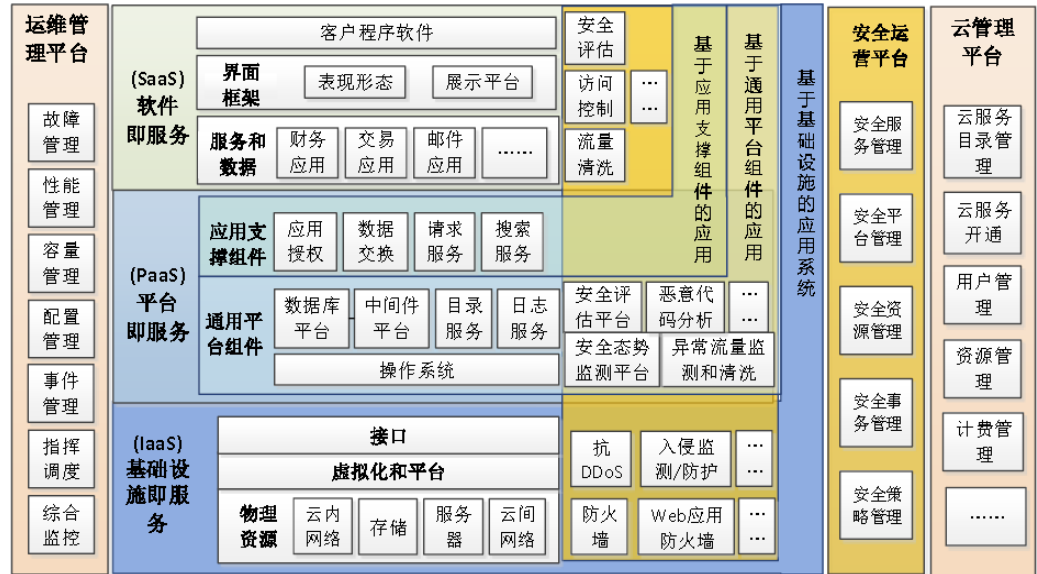
资料来源: 公司年报, 东兴证券研究所

2015 年公司将继续推进外延式扩张战略。未来还将继续寻找信息安全市场上可投资并购标的, 特别是在一些新兴信息安全领域中, 不断完善公司的战略布局。

3.3 领先布局云安全, 市场首发云安全服务平台

随着云计算与云服务应用范围的扩大化和普及程度的提高, 各种针对云的安全问题也应运而生。公司作为国内最早进入云计算和云安全领域的网络安全厂商。2014 年 5 月, 公司的云安全运营服务业务获得 ISO27001 管理体系的认证, 标志其成为国内首家通过 ISO27001 认证的可管理安全服务(简称: MSS)和安全即服务(简称: SECaaS)提供商。公司提供的云安全运营服务以网站安全为核心, 对网站面临的威胁和安全事件提供 7X24 小时全天候地监测与防护。

图 12 绿盟科技云安全体系架构简介



资料来源：绿盟科技，东兴证券研究所

2015年8月，公司在国内首发基于云的网络安全服务平台，该平台向合作伙伴、创客及行业客户提供专业的网络安全产品及服务交付能力。它集成了安全产品与服务展示、体验、交付等诸多功能，可以把它比作卖网络安全的淘宝，通过绿盟云企业用户可以在线体验各类安全服务，鉴别、交流、选择都变得简单，用户提交的建议和反馈度可以得到快速实现，解决问题的速度得以有效提升，用户将会有更多时间关注自身的业务发展。

绿盟云有三类产品及服务，包括成熟服务类、创新孵化类、市场推广类，由此合作伙伴、创客及行业客户选择绿盟云可以快速交付网络安全产品及服务能力。

图 13 绿盟云产品服务体系



资料来源：绿盟科技，东兴证券研究所

绿盟云安全服务平台的能力超强，在智慧安全 2.0 战略指引下，平台将传统网络安全攻防的经验与大数据结合，绿盟云的用户将在第一时间获得攻击溯源、态势感知、威胁情报等方面的能力。

图 14 绿盟云产品服务体系



资料来源：绿盟科技，东兴证券研究所

在互联网+的时代，公司加速打造生态环境建设：

云安全服务合作。合作伙伴可以将他们的网络安全技术快速迁移到绿盟云安全服务平台上，用户得以通过云的方式购买或订阅这些专业的产品及服务；

渠道合作。各行业的云计算服务商及其安全商店可以获得业内优秀的云安全服务与产品，以便为用户快速形成完整的私有云、公有云解决方案；

技术孵化。网络安全领域的创客们，通过绿盟云得以快速孵化他们的创意，用户得以享受到互联网+时代的网络安全创意及速度。

图 15 公司云安全体系架构简介

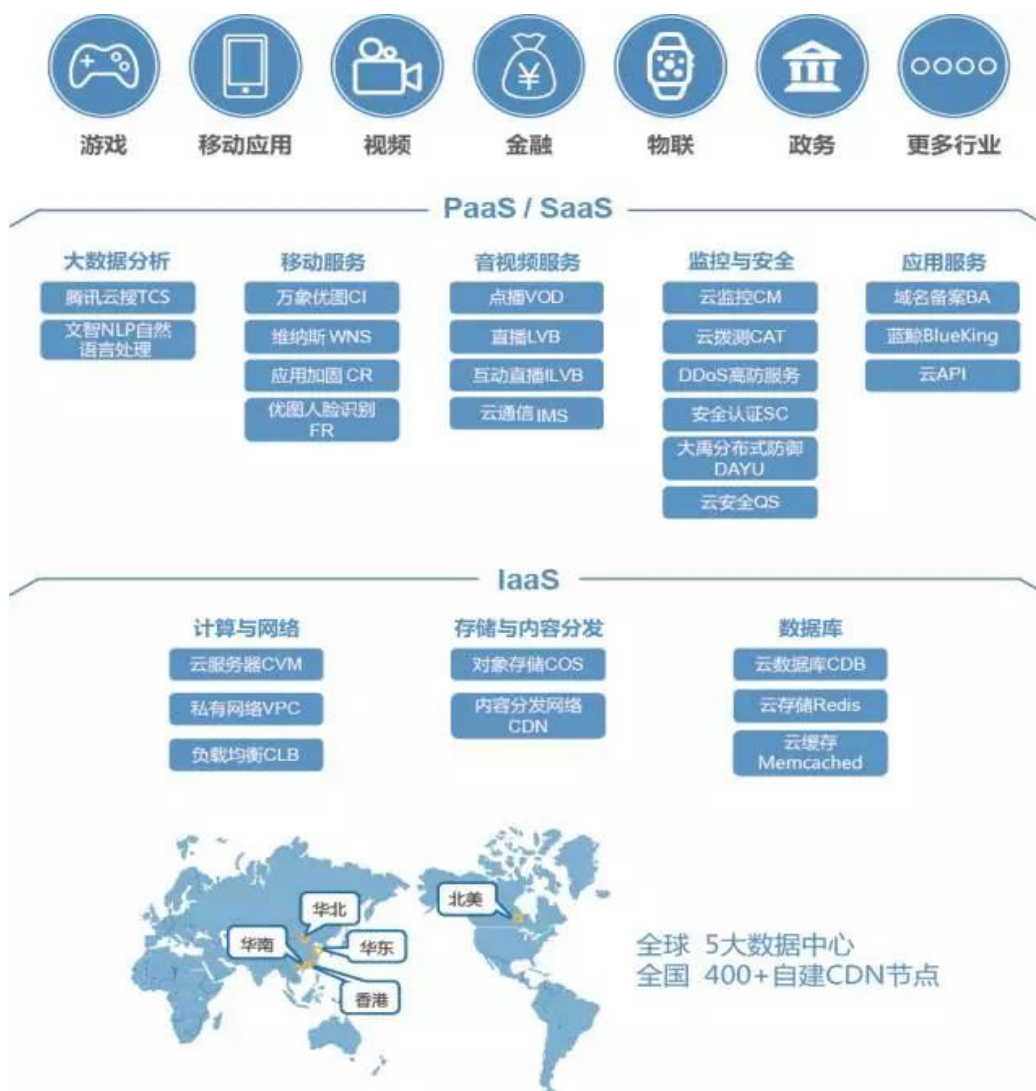


资料来源：绿盟科技，东兴证券研究所

2015年12月10日，公司与腾讯云计算签订《云计算安全防护领域合作框架协议》，本次合作主要基于两方面内容，一是云计算安全防护：包括云平台及配套设施防护、动态边界安全、按需分配的安全服务、新技术下虚拟化平台监测与防护等；二是安全云的完整交付：以腾讯云平台技术为基础，结合公司的软件定义安全技术及威胁情报和安全数据分析，提供从公有云到私有云，完整的云计算安全防护解决方案。

腾讯云是面向广大企业和个人的公有云平台，提供云服务器、云数据库、云存储和CDN等基础云计算服务，以及游戏、视频、移动、金融、物联、政企等行业解决方案。

图 16 腾讯云构架体系



资料来源：腾讯云，东兴证券研究所

绿盟科技云计算安全防护解决方案将结合腾讯云平台优势，围绕用户需求，协助云计算厂商提升云环境中的安全能力。主要从以下各个方面进行安全防护体系的设计：

保障云平台及其配套设施

云计算除了提供 IaaS、PaaS、SaaS 服务的基础平台外，还有配套的云管理平台、运维管理平台等。要保障云的安全，必须从整体出发，保障云承载的各种业务、服务的安全。

基于安全域的纵深防护体系设计

对于云计算系统，仍可以根据威胁、安全需求和策略的不同，划分为不同的安全域，并基于安全域设计相应的边界防护策略、内部防护策略，部署相应的防护措施，从而构造起纵深的防护体系。当然，在云平台中，安全域的边界可能是动态变化的，但通过相应的技术手段，可以做到动态边界的安全策略跟随，持续有效的保证系统的安全。

以安全服务为导向并符合云计算的特点

云计算的特点是按需分配、资源弹性、自动化、重复模式，并以服务为中心。因此，对于安全控制措施选择、部署、使用来讲必须满足上述特点，即提供资源弹性、按需分配、自动化的安全服务，满足云计算平台的安全保障要求。

充分利用现有安全控制措施及最新技术

在云计算环境中，还存在传统的网络、主机等，同时，虚拟化主机中也有相应的操作系统、应用和数据，传统的安全控制措施仍旧可以部署、应用和配置，充分发挥防护作用。另外，部分安全控制措施已经具有了虚拟化版本，也可以部署在虚拟化平台上，对虚拟化平台中的东西向流量进行检测、防护。

充分利用云计算等最新技术

信息安全措施/服务要保持安全资源弹性、按需分配的特点，也必须运用云计算的最新技术，如 SDN、NFV 等，从而实现按需、简洁的安全防护方案。

在安全云完整交付层面，可分为两个部分，分别为私有安全云交付及公有安全云交付。绿盟科技将为腾讯云平台提供相应的安全防护保障，将传统安全产品盒子转化为云上的安全能力，最终实现安全能力资源池化，为公有云环境租户提供便捷的安全防护；并通过与绿盟科技安全数据分析、云安全运营、云安全服务等解决方案形成整体云计算安全防护解决方案，为私有云用户提供安全的云计算环境。帮助传统企业往云端实现业务迁移的过程中，进行安全合规和真正的安全保障。

云安全作为未来行业新兴的增长点，将随着云计算应用的普及快速发展，公司的云安全目前已达国内领先水平，与腾讯云的合作标志着公司布局的逐渐完整和未来在此细分市场的主导地位。

4. 盈利预测及投资评级

作为国内信息安全行业具有标杆意义的龙头公司，公司直接受益于国家信息安全与自主可控政策，未来三年将进入爆发性增长期。我们预计公司 2015 年-2017 年营业收入分别为 10.01 亿元、14.31 亿元和 20.48 亿元，增速为 42.47%、42.91%和 43.16%。归属于上市公司股东净利润预计为 1.77 亿元、2.50 亿元和 3.55 亿元，增速为 22.19%，41.83%，41.61%。

表 9 类似公司 PE 情况

股票简称	2014	2015E	2016E
启明星辰	80	117	81
卫士通	112	225	85
北信源	94	226	124
平均	95	189	97

资料来源：东兴证券研究所

预计公司 2015 年-2017 年 EPS 分别为 0.49 元 0.70 元和 0.99 元，对应 PE 分别为 116.5、81.6 和 57.7。三家同类公司 2016 年平均估值为 97 倍，给予公司 2016 年行业平均估值 97 倍估值，6 个月目标价 68 元，首次覆盖给予公司“强烈推荐”评级。

5. 风险提示

季节性亏损风险：公司核心客户以政府、电信、金融、能源等领域客户为主，这些客户通常在上半年审批当年的年度预算和固定资产投资计划，在年中或下半年安排设备采购招标，设备交货、安装、调试和验收则集中在第四季度。因此，公司订单从 7、8 月份开始明显增加，全年的销售业绩集中体现在第四季度。从近几年公司第四季度营业收入占比均在 50%以上，第四季度净利润占比均在 80%以上；公司的销售以及收入确认呈现的季节性特征影响公司利润也呈季节性分布。由于费用在年度内较为均衡地发生，而收入主要在第四季度实现，因而可能会造成公司第一季度、半年度或第三季度出现季节性亏损，投资者不宜以半年度或季度的数据推测全年盈利状况。

核心人员流失的风险：公司能够保持技术领先优势，与公司拥有的核心技术和核心技术人员的研发技术密切相关。公司如出现技术外泄或者核心技术人才流失情况，会一定程度上影响公司产品的研发，公司需为此付出一定人力、物力及时间招聘及培养新的技术人员，将会对公司的业务发展造成一定影响。亿赛通由于人员的问题受到了阶段性的影响，公司已经在激励和管理上尽快将公司调整到正常轨道，预计 4 季度是公司业务的黄金期，公司已经在向业绩目标冲刺，我们认为对公司的负面影响已经过去。

利润表 (百万元)	2013A	2014A	2015E	增长率%	2016E	增长率%	2017E	增长率%
营业收入	623.05	702.67	1,001.11	42.47%	1,430.73	42.91%	2,048.29	43.16%
营业成本	130.20	154.45	219.04	41.82%	310.81	41.90%	443.59	42.72%
营业费用	161.17	190.92	272.00	42.47%	388.73	42.91%	556.52	43.16%
管理费用	253.39	252.51	300.33	18.94%	429.22	42.91%	614.49	43.16%
财务费用	(2.59)	(8.59)	(6.95)	N/A	(7.60)	N/A	(7.09)	N/A
投资收益	0.00	0.03	0.00	N/A	0.00	N/A	0.00	N/A
营业利润	54.66	89.08	163.67	83.75%	250.53	53.07%	373.10	48.92%
利润总额	118.53	158.92	207.67	30.68%	294.53	41.83%	417.10	41.61%
所得税	8.00	14.46	31.15	115.50%	44.18	41.83%	62.57	41.61%
净利润	110.53	144.46	176.52	22.19%	250.35	41.83%	354.54	41.61%
归属母公司所有者的净利润	110.53	144.50	176.52	22.16%	250.35	41.83%	354.54	41.61%
NOPLAT	48.56	73.16	133.21	82.08%	206.50	55.01%	311.11	50.66%
资产负债表 (百万元)	2013A	2014A	2015E	增长率%	2016E	增长率%	2017E	增长率%
货币资金	225.41	608.42	781.97	28.52%	737.28	-5.72%	680.03	-7.76%
交易性金融资产	0.00	0.00	0.00	N/A	0.00	N/A	0.00	N/A
应收帐款	382.01	372.64	530.92	42.47%	758.76	42.91%	1,086.27	43.16%
预付款项	15.33	7.26	7.26	0.00%	7.26	0.00%	7.26	0.00%
存货	19.15	22.57	32.01	41.81%	45.42	41.90%	64.83	42.72%
流动资产合计	668.54	1,103.96	1,485.56	34.57%	1,741.12	17.20%	2,115.62	21.51%
非流动资产	66.37	119.20	93.56	-21.51%	96.25	2.88%	88.94	-7.59%
资产总计	734.91	1,223.16	1,579.11	29.10%	1,837.37	16.35%	2,204.56	19.98%
短期借款	0.00	0.00	0.00	N/A	0.00	N/A	0.00	N/A
应付帐款	67.72	76.55	107.08	39.88%	151.94	41.90%	216.85	42.72%
预收款项	15.94	19.54	19.54	0.00%	19.54	0.00%	19.54	0.00%
流动负债合计	267.54	211.73	169.89	-19.76%	217.37	27.95%	286.08	31.61%
非流动负债	0.00	40.67	0.00	N/A	0.00	N/A	0.00	N/A
少数股东权益	0.00	0.45	0.45	0.00%	0.45	0.00%	0.45	0.00%
母公司股东权益	467.38	970.31	1,370.13	41.21%	1,580.90	15.38%	1,879.38	18.88%
净营运资本	401.01	892.23	1,315.67	47.46%	1,523.75	15.82%	1,829.54	20.07%
投入资本 IC	241.97	362.33	588.61	62.45%	844.07	43.40%	1,199.80	42.14%
现金流量表 (百万元)	2013A	2014A	2015E	增长率%	2016E	增长率%	2017E	增长率%
净利润	110.53	144.46	176.52	22.19%	250.35	41.83%	354.54	41.61%
折旧摊销	12.76	19.12	0.00	N/A	7.31	N/A	7.31	0.00%
净营运资金增加	83.25	491.22	423.44	-13.80%	208.08	-50.86%	305.79	46.96%
经营活动产生现金流	11.77	99.05	(34.24)	N/A	36.29	N/A	30.72	-15.36%
投资活动产生现金流	(19.21)	(58.21)	(20.45)	N/A	(49.00)	N/A	(39.00)	N/A
融资活动产生现金流	0.00	338.82	228.23	-32.64%	(31.98)	N/A	(48.97)	N/A
现金净增(减)	(7.44)	379.66	173.54	-54.29%	(44.69)	N/A	(57.25)	N/A

分析师简介

林阳

中国社科院经济学硕士，计算机行业首席研究员，研究所上海团队负责人。

联系人简介

杨洋

纽约大学计算机专业硕士，曾任职于华为技术有限公司云平台研发工程师。

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。

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。