



证券研究报告 • 上市公司深度

新三板

数据安全领先者，产品线持续丰富

公司主营数据安防产品和解决方案

公司以自主数据加密、操作系统内核等技术为依托，向金融、政府、电信、能源、制造等大型行业客户提供数据综合防护产品、解决方案、数据治理、安全运维等服务。目前在银行市场占有率排名靠前，与多家股份制银行、国有银行等形成合作；在公安、海关等政府行业拥有业内单项目最高的装机量；公司完成的公安部全国移动警务移动安全项目等目前国内领先。公司营业收入在 2014-15 年复合增长率为 94.55%，16 中报则达到 188.58%；新客户拓展、老客户贡献稳定订单、产品线持续丰富是公司快速增长的核心原因。

数据安全市场增速高于信息安全整体市场

全球数据总量持续增长，预计 20 年达到 40ZB；数据安全威胁持续上升，带动数据安全产品需求；相关国内企业受益政策全面推进、自主可控进程等因素，有望获得快速发展。由于黑客攻击手段日趋多元化，以及内部安全隐患的占比高企，针对物理和运行层防护不足以化解漏洞和攻击，数据层面的保护成为必须。当前我国的数据安全市场规模在 20 亿元左右，预计数据安全市场规模将保持 30% 复合增长，在 2020 年市场规模将超过 70 亿元，数据安全市场前景广阔。

公司产品线持续丰富，竞争力不断提升

目前数据安全领域海外企业仍占据技术优势，Gartner 评选的全球领导企业包括了 Symantec、Forcepoint、IntelSecurity 等。国内参与者则有几大信息安全龙头启明星辰、绿盟科技、天融信等，以及在细分领域具有技术优势的企业如明朝万达、北信源、优炫软件等。中小企业以提供关键软件产品起家，通过被并购、产业合作、自主拓展等方式，进入综合解决方案领域。

公司拥有 16 项授权发明专利和近 60 项申报专利涉及多项核心技术；金融领域、政府领域拥有大量高端稳定客户；公安警用领域布局将持续深化公司优势地位。公司积极拓展下游业务类软件等产品，从而利用产品线优势获得更大市场份额。未来随着三家子公司在公安业务系统、大数据服务、云安全等产品的拓展，以及公司新产品的持续发力，有望实现更大范围的产品覆盖，从而提升产品竞争力。

高速成长的数据安全龙头，建议重点关注

公司传统数据安全业务领域有望保持稳步增长，数据安全产品线将保持 40% 以上快速增长。新业务布局初见成效，其中公安产品贡献营收中近一半，并在未来带来新的项目贡献；云安全、大数据安全等业务也将陆续产生贡献。预计公司 2016-2017 年营业收入 1.3、2.0、2.8 亿元，净利润 2800、4400、6000 万元，对应 EPS 0.20、0.32、0.43 元，对应 PE 38.8、24.7、18.14 倍，建议重点关注。

明朝万达（835348）

首次

增持

王慷

wangsu@csc.com.cn

010-85156319

执业证书编号：S1440512070015

发布日期：2017 年 1 月 12 日

当前股价：7.79

上证指数、沪深 300 走势图



相关研究报告

目录

一、公司概况	3
1.1 公司历史沿革和股权结构	3
1.2 公司主营业务概况	3
二、数据安全行业受到日益重视	5
2.1 数据安全在安全防护中的作用日益重要	5
2.1.1 数据安全形势日益严峻	5
2.1.2 政策加码推进行业发展	5
2.2 信息安全市场持续规模发展迅速	7
2.3 泄密事件层出不穷，数据安全日益重要	8
三、数据安全核心产品	11
3.1 数据安全在信息安全领域相对落后	11
3.2 公司主要产品线	12
3.2.1 数据加密产品线	12
3.2.2 移动数据安全产品线	12
3.2.3 数据防泄漏产品线	13
3.2.4 公安警用产品线	13
四、核心竞争力	14
4.1 行业竞争格局/代表性企业	14
4.2 国内竞争格局	14
4.3 竞争优势	15
4.3.1 技术和产品优势	15
4.3.2 细分行业客户优势	16
4.3.3 定制化服务能力优势	16
五、高速成长的细分行业龙头，中长期布局可期	17
1、数据安全产品领先，大数据领域积极布局	17
2、高速成长的数据安全龙头，建议重点关注	17
风险提示	18

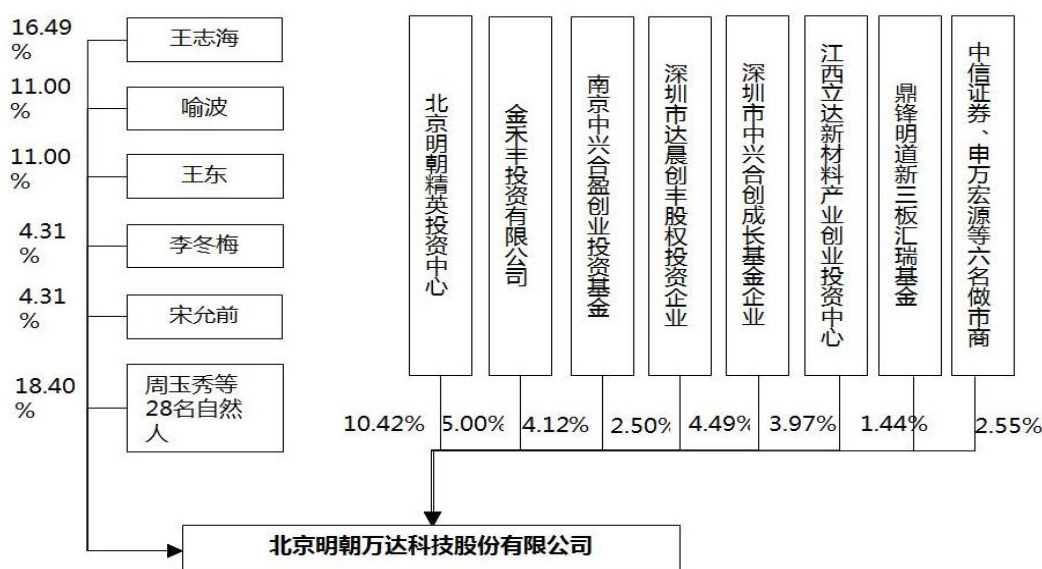
一、公司概况

1.1 公司历史沿革和股权结构

北京明朝万达公司成立于 2005 年，2012 年获中兴合创 A 轮投资，2013 年获立达资本 B 轮投资，2015 年完成 C 轮融资并完成股份制改造和员工股权激励登陆新三板。公司是国内领先的数据安全技术、产品和服务提供商。主要向金融、政府、电信、能源、制造等大型行业客户提供数据加密、移动数据安全防护、数据防泄漏等数据综合防护产品、解决方案和安全服务。

目前公司总股本 13936 万股，实际控制人为喻波、王东、王志海，公司的法定代表人王志海为公司第一大股东，持股比例 16.49%，北京明朝精英投资中心为第一大机构股东，持股比例为 10.42%。

图 1：明朝万达股权结构图



资料来源：公司资料，中信建投证券研究发展部

1.2 公司主营业务概况

公司以自主数据加密、操作系统内核等技术为依托，以数据保护为核心业务目标，向金融、政府、电信、能源、制造等大型行业客户提供数据综合防护产品、解决方案和数据治理、安全运维等服务。

公司产品围绕数据全生命周期安全防护，覆盖数据产生、存储、交换、使用等重要环节，实现对服务器、数据库、终端（PC 终端、移动终端、云终端、物联网终端等）以及网络通信的数据进行识别、脱敏、加密和权限管理，辅以全程日志和操作行为数据审计，利用大数据技术进行关联分析和数据挖掘，及时有效发现针对数据的攻击和威胁，从而确保用户数据安全可控。

公司主要产品和服务包括软件产品、硬件产品、技术服务、技术开发四大类，其中，软件产品主要分为三大产品线：数据加密产品线、移动数据安全产品线、数据防泄漏产品线。软件产品目前主要收入来源包括数据

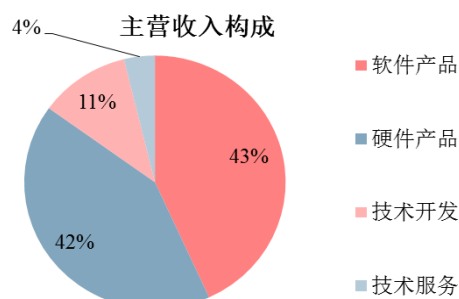
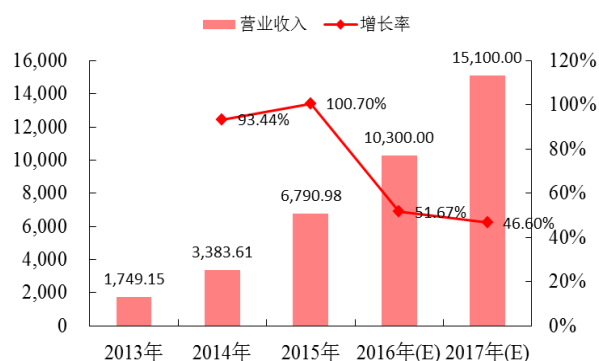
安全系列软件产品和解决方案销售收入、技术开发服务收入、系统硬件销售收入、技术服务收入等。

公司营业收入自 2013 年起快速上升，2013 年收入为 1749.15 万元，2015 年达到 6790.98 万元，复合增长率为 94.55%；16 年中报营收增长则达到 188.58%。2015 年公司因股份支付所造成的管理费用 3523.76 万元而出现亏损，而在 2016 半年报公司已实现归母净利转正。

截至 2015 年底，公司的信息安全硬件产品和软件产品为主营业务的重要组成部分，收入构成占公司总收入 85% 左右。其中硬件产品在 2015 年占比大幅上升，导致公司毛利由 14 年的 65.19% 下降到 48.87%；随着公司产品结构调整完成，这一数字将趋于稳定。

图 2：明朝万达营业收入及预测（万元）

图 3：明朝万达营业收入构成（百分比）



资料来源：wind，中信建投证券研究发展部

公司是数据安全领域的领导厂商之一。从细分市场看，公司目前在银行市场占有率排名靠前，与六家股份制银行、一家国有银行、多家城商行形成合作。公司移动数据安全产品在公安、海关等政府行业拥有业内单项目最高的装机量，超过百万级；公司完成的公安部全国移动警务移动安全项目、海关全国移动报关移动项目是目前国内电子政务领域领先的移动安全应用案例。此外，公司还是国内最早一批进入大数据安全领域的企业之一，已经申报了国家发改委信息安全专项资金支持，完成技术攻关，并在光大银行实现了规模部署。

图 4：明朝万达是数据安全领域领导厂商之一

排名TOP3的数据安全、大数据安全企业：
金融行业占有率TOP1，
研发制造行业占有率TOP2，
政府、央企行业占有率TOP3。

软件定义安全技术实力第1：
申请发明专利近60项，已授权16项，获软件著作权46项。国家发改委、科技部、工信部创新专项基金19项。



排名TOP3的企业级移动安全企业：
政府行业占有率TOP1，
金融、运营商行业占有率TOP3

安全云平台、大数据安全技术开拓者：
中国海关、中国石油、公安部等移动接入云平台。公安大数据安全平台。

资料来源：公司资料，中信建投证券研究发展部

二、数据安全行业受到日益重视

2.1 数据安全在安全防护中的作用日益重要

在大数据浪潮下，没有安全防护的大数据，将是数据灾难。所谓数据安全是指，围绕数据全生命周期安全防护，覆盖数据产生、使用、交互、存储、销毁等环节，对网络、应用、服务器、PC、移动终端的数据进行发现、采集，辅以全程日志和操作行为数据审计，利用大数据技术进行关联分析和数据挖掘，及时有效发现针对数据的攻击和威胁，从而根据不同的威胁，下达相应的管控指令，最终确保用户的数据安全可控。云计算、移动互联网、“互联网+”的深入应用，使得传统网络及系统边界模糊化，数据安全逐渐成为安全防护的核心。

2.1.1 数据安全形势日益严峻

近年来，数据泄密相关事件频发，成为信息安全领域的核心威胁。包括 2010 年维基解密事件、2013 年斯诺登事件、2016 年巴拿马信息泄露事件等，都是针对数据的窃取和泄密所导致。不断曝光的数据泄密事件和安全漏洞问题会导致巨大的国家利益和经济损失，也使各国对信息安全重视程度日益提升。

表 1：近年典型数据泄密事件

时间	政策内容
2010 年 7 月	维基网站通过英国《卫报》、德国《明镜》、美国《纽约时报》等公布 92000 份美军有关阿富汗战争的军事机密文件
2013 年 6 月	前 CIA 职员斯诺登将两份绝密资料交给英国《卫报》和美国《华盛顿邮报》，揭露美国国家安全局“棱镜”绝密项目，显示美国工业间谍活动不仅针对国家安全，也包括任何有价值的工程技术资料
2016 年 4 月	巴拿马文件泄露事件曝光，泄露涉及超 20 万家离岸企业、1150 万份共 2.6TB 内部数据，其中包括 480 万封邮件、304 万数据库、215 万 PDF 文件和 32 万 TXT 文件

资料来源：公开资料，中信建投证券研究发展部

2.1.2 政策加码推进行业发展

2.1.2.1 宏观政策环境：信息安全提升至国家战略层面

“棱镜门”事件之后，我国信息安全领域国产化趋势逐渐清晰，政府对自主安全产业的扶植政策，尤其是在政府采购上对我国具有自主知识产权安全产品的倾斜政策，将为国内安全产品厂商创造更好的产业生存和发展环境。我国将信息安全提升至国家战略高度，大力支持信息安全行业发展，信息安全产业利好政策不断，加速信息安全产业需求落地。

表 2：我国近年出台信息安全行业相关政策

时间	政策内容
2013 年 11 月	设立国家安全委员会，完善国家安全体制和国家安全战略，确保国家安全，表明国家已将信息安全提升至国家战略层面
2014 年 2 月	成立中央网络安全和信息化领导小组，并召开第一次会议，国家主席习近平强调：网络安全和信息化是重大战略问题，要努力把我国建设成为网络强国
2014 年 8 月	工信部下发《加强电信和互联网行业网络安全工作的指导意见》，提出八大工作重点。对网络基础设施和业务系统安全防护、推进安全可控关键软硬件应用、网络数据和用户个人信息保护等做出强调



2014 年 9 月	银监会印发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，提出到 2019 年，安全可控信息技术在银行业总体达到 75%左右的使用率
2014 年 10 月	中央军委印发《关于进一步加强军队信息安全工作的意见》。《意见》指出，必须把信息安全工作作为军事斗争准备的保底工程，促进我军信息化建设科学发展、安全发展
2015 年 7 月	第十二届全国人民代表大会常务委员会第十五次会议通过《中华人民共和国国家安全法》，要求网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；网络安全法草案出台并向社会公开征求意见，立法进入最后冲刺阶段，信息安全行业迎来最大政策性红利
2016 年 4 月	召开网络安全和信息化工作座谈会，强调信息化和网络安全紧密联系，提出加快构建关键信息基础设施安全保障体系
2016 年 11 月	《中华人民共和国网络安全法》在全国人大常委会获得通过，并将于 2017 年 6 月 1 日起施行；法案明确了建设网络安全保障体系的主要举措，提出加大财政投入，深化技术研发，提升网络安全创新能力

资料来源：公开资料，中信建投证券研究发展部

信息安全行业的发展和市场应用具有很强的政策导向性，国家战略和产业政策的影响为我国的信息安全技术研究、产品开发和和应用拓展提供了自主创新与突破的机遇和空间，使得信息安全产业成为我国信息行业新的增长点和发展的突破口。

2.1.2.2 去 IOE：自主可控事关国家安全

去 IOE 是由阿里巴巴首先提出，针对 IBM（国际商用机器公司）、Oracle（甲骨文）、EMC（易安信），三家企业分别是小型机、数据库和高端存储的领导厂商。这三方基本也是过去企业已经政府信息工程建设必备的系统。

我国信息安全行业的最大痛点之一，就是我国的 IT 软硬件国产替代化程度不高而对外依存度过高，因此实现软硬件的自主可控是实现信息安全的必要手段之一。棱镜门事件之后我国政府意识到政府数据安全性的重要性，也加强了政府数据安全方面的工作。2014 年，windows 8 系统未进入中央机关政府采购名单，在之后的国产化替代上，去 IOE 的外延被扩大，不仅仅包括这三个品牌的产品，在信息化建设中大量引入国产或定制产品，保障信息安全。根据 wind 数据显示，去 IOE 指数近三年上升明显，去 IOE 浪潮意味着信息安全相关国产品牌迎来发展契机。

图 5：去 IOE 指数



资料来源: wind, 中信建投证券研究发展部

2.2 信息安全市场持续规模发展迅速

近年来,我国信息安全行业发展迅速,市场规模处于持续高速增长的态势。来自 Gartner 的最新预测,2016 年全球信息安全产品和服务的开支将达到 816 亿美元,相比 2015 年增长 7.9%。根据 IDC 研究报告,2012 年至 2013 年,国内信息安全产品市场规模分别为 8.278 亿美元和 9.496 亿美元。到 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达到 13.5%。2012 年至 2013 年,国内信息安全服务的市场规模分别为 4.41 亿美元和 4.835 亿美元。到 2017 年,国内信息安全服务的市场规模预计将达到 7.07 亿美元,2012 到 2017 年信息安全服务市场的复合增长率达到 9.9%。

图 6：国内信息安全产品市场规模（百万美元）

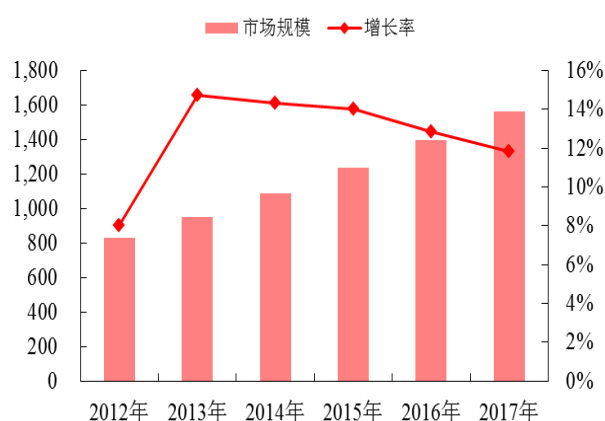
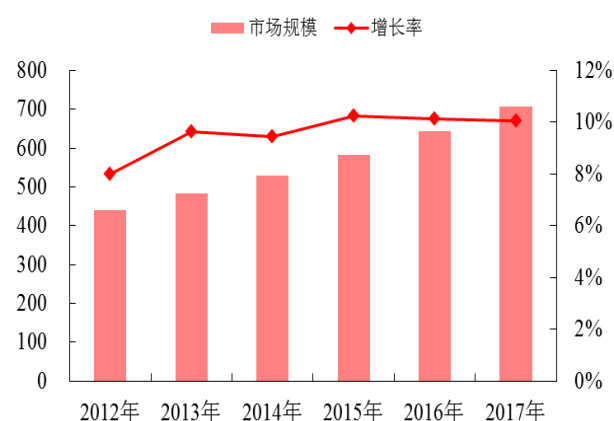


图 7：国内信息安全服务市场规模（百万美元）



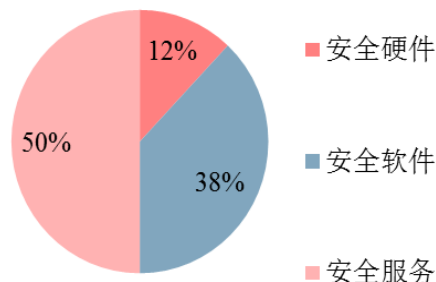
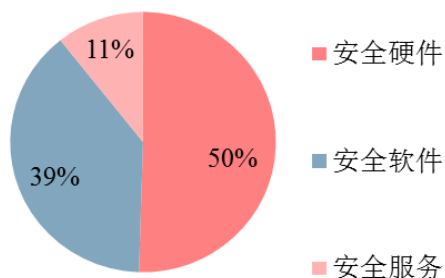
资料来源: IDC 研究报告, 中信建投证券研究发展部

我国信息安全市场硬件占据主导地位,信息安全软件和服务有巨大提升空间。根据 IDC 的研究报告,我国信息安全硬件在市场规模中占据 50%左右,信息安全软件占 39%左右,信息安全服务占据 11%;欧美信息安全市场较为成熟,信息安全硬件占据市场规模的 38%,信息安全软件占据 12%,信息安全服务占据 50%。对比欧

美市场，我国的信息安全软件和服务两大市场提升空间较大而且增长较快。

图 8：国内信息安全市场结构

图 9：欧美信息安全市场结构

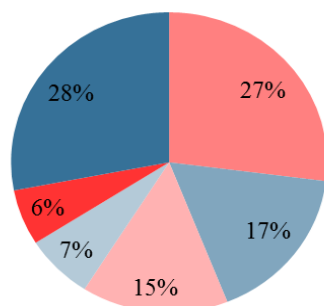


资料来源：IDC，中信建投证券研究发展部

信息安全行业的应用行业主要是政府部门、金融、能源、军队、军工等信息化程度高，且对信息安全较敏感的行业。近年来，这些行业在加大信息化建设力度的过程中逐渐加深了对信息安全管理重要性的认识，在信息安全方面的投入也不断加大，极大地推动了信息安全行业的快速发展。国内以政府、电信、金融为主要的三大行业的客户占比最高，总占比达到60%。

图 10：我国信息安全行业市场份额

■ 政府 ■ 电信 ■ 金融 ■ 教育 ■ 能源 ■ 其他



资料来源：IDC，中信建投证券研究发展部

2.3 泄密事件层出不穷，数据安全日益重要

数据安全是信息安全行业的一个细分领域，也是新一代信息安全的核心领域。据统计，平均每秒有 200 万用户在使用谷歌搜索，Facebook 用户每天共享的东西超过 40 亿，Twitter 每天处理的推特数超过 3.4 亿。同时，科学计算、医疗卫生、金融、零售业等各行业也有大量数据在不断产生。根据 IDC 数据报告显示，2012 年全球信息总量已经达到 2.84ZB，2015 年达到 8.59ZB，预计 2020 年全球数据产生量会达到 40ZB。据 Gartner 预测，2016 年全球在大数据方面的总花费将达到 2320 亿美元。

从整个信息安全的发展来看，数据泄露现象日益严重。我国互联网行业正在快速增长，移动计算、云计算、

大数据等应用产生的数据中蕴含着巨大的价值，大量企业高速发展的同时却忽略了信息安全建设，因此导致数据泄露事件频繁发生，造成极大的负面影响和经济损失。

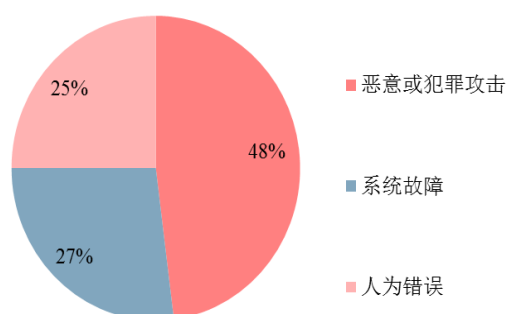
表 3：2016 年国内外数据泄露事件

主体	事件
苹果 APP Store	一款名为“JSPatch”可帮助开发者修改应用程序的软件上存在安全漏洞，导致苹果应用商店内 1000 多款使用了该框架的 IOS 应用处于黑客攻击危险之中。
土耳其国家数据库	约 5000 万土耳其公民的个人信息被黑客晒到网上，这些信息包括姓名、身份证号、出生日期、父母名字、住所等。
社交网站 MySpace	MySpace 是全球第二大社交网站，2016 年 6 月初，其 3.6 亿的用户账号以及 4.27 亿的密码被黑客取得。如若泄露事件属实，这会是互联网史上最大规模的密码泄露事件。
电信运营商 Verizon 公司	Verizon 是美国最大的电信运营商，2016 年 4 月遭受黑客盗窃的 150 万客户联系细节，其中包括一些财富 500 强企业。这些数据被黑客在暗网论坛上售卖。同时，Verizon 网站的信息安全漏洞也出现在售卖清单上。
济南免疫规划系统网络	黑客通过非法入侵免疫规划系统网络获取信息并公开售卖，导致济南 20 万名孩童信息被打包出售。信息内容包括姓名联系方式，甚至精确到门牌号信息。
信诚人寿保险公司	2016 年 1 月，信诚人寿保险公司被曝出存在严重信息安全漏洞，有关信息安全平台提交了信诚人寿保险漏洞信息，按照监测报告显示，信诚人寿保险公司面临泄漏数以万计的客户银行卡号、密码、开户行地址、身份证等敏感信息的风险。
湖南邵阳某银行	银行工作人员泄露公民征信信息，涉及公民银行个人信息 257 万条、涉案资金 230 万元

资料来源：公开信息，中信建投证券研究发展部

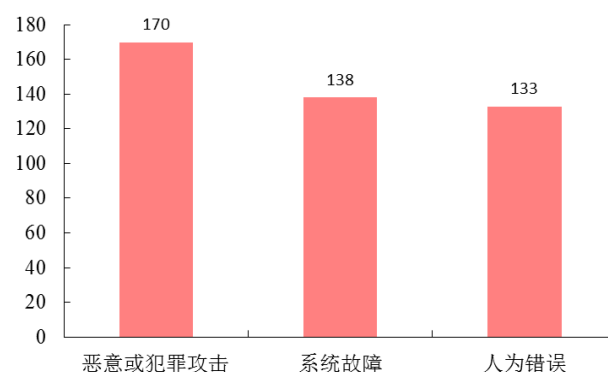
数据泄露的成本也在不断攀升。根据 IBM 与 Ponemon Institute 的数据泄露研究报告，企业的平均数据泄露总成本从 379 万美元增至 400 万美元，自 2013 年以来，数据泄露总成本增加了 29%；至于包含敏感和机密信息的记录，每条丢失或被盗记录的平均成本则从 2015 年的 154 美元增至今年研究中得出的 158 美元，自 2013 年以来，每条记录平均成本增加 15%。

图 11：数据泄露原因



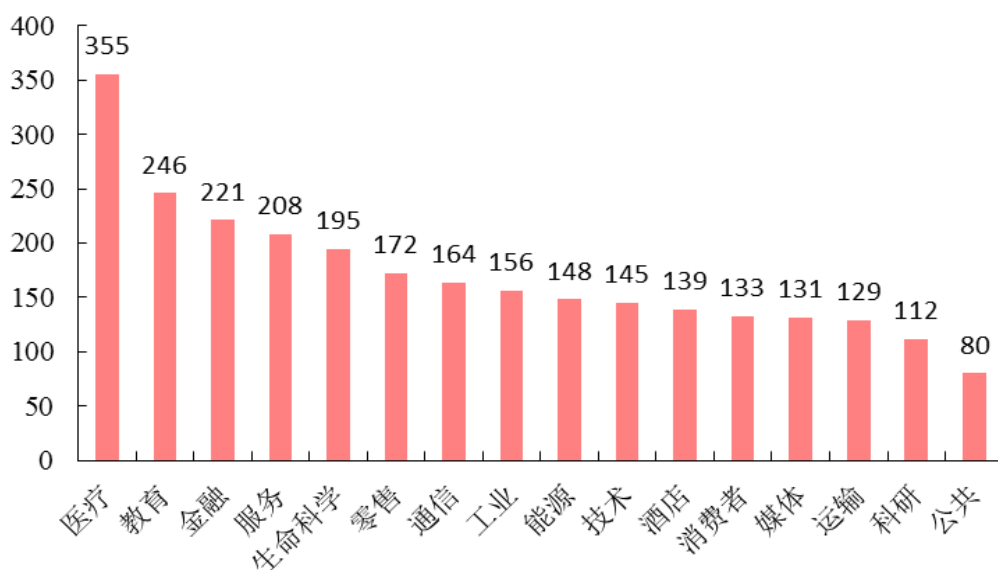
资料来源：wind，中信建投证券研究发展部

图 11：不同泄露原因的成本（美元）



某些行业的数据泄露成本较高。受到严格监管的行业，如医疗、教育和金融企业的每条记录平均数据泄露成本远高于 158 美元的整体平均值。公共部门、科研和运输机构的每条记录平均成本则低于整体平均值。

图 13： 不同行业每条记录泄露成本（美元）

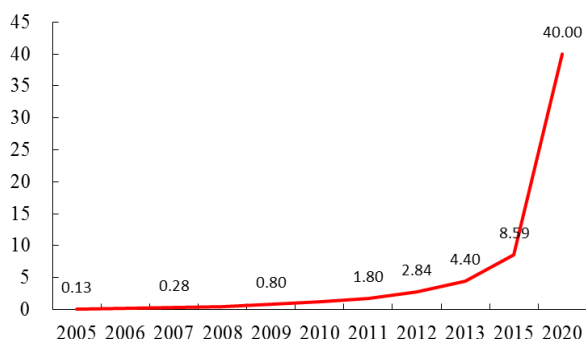


资料来源: wind, 中信建投证券研究发展部

数据泄露的原因大部分数据泄露由恶意或犯罪攻击导致。现在，大部分的网络安全事件是信息泄露，目的也大多是从整体上对研究中展示的全部 12 个行业的数据泄露主要根源进行了概括说明。48% 的事故涉及恶意或犯罪攻击，25% 因员工或承包商疏忽、人为错误导致，另有 27% 的事故涉及系统故障，其中包括 IT 和业务流程故障。2016 年，恶意或犯罪攻击引发的数据泄露成本高达 170 美元，远高于系统故障和人为因素造成的数据泄露每条记录平均成本，分别为 138 美元和 133 美元。

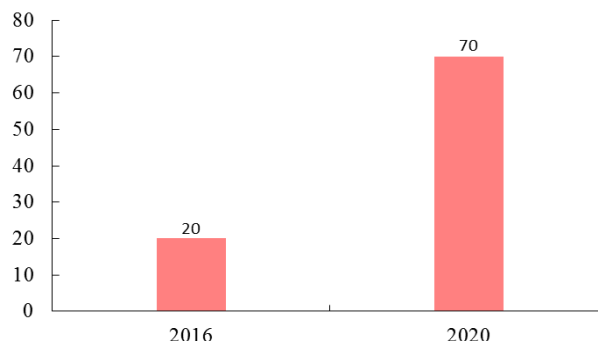
随着数据泄露安全事件的频繁发生，我国对信息安全建设的基础设施不断完善，预计以数据安全为核心的信息安全应用市场会成为行业的增长点，其成长速度将高于整体行业。当前我国的数据安全市场规模在 20 亿元左右，我们估计数据安全市场规模年增速在 30% 左右，在 2020 年市场规模将超过 70 亿元，数据安全市场前景广阔。

图 14： 全球数据产生量及预测（ZB）



资料来源: wind, 中信建投证券研究发展部

图 15： 我国数据安全市场规模及预计（亿元）



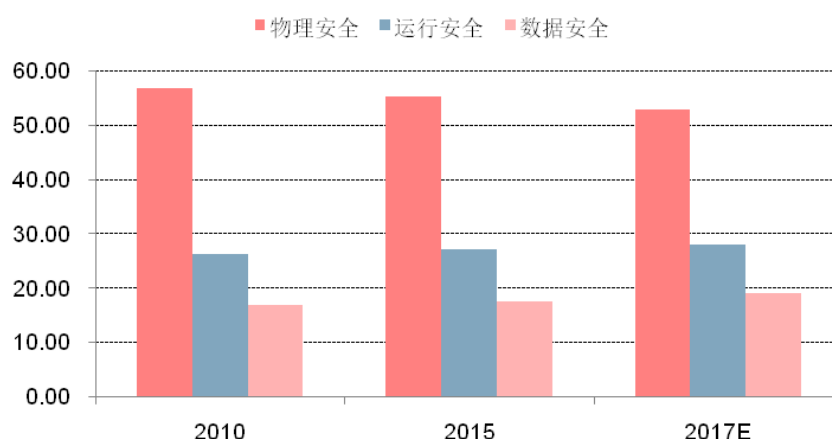
三、数据安全核心产品

3.1 数据安全在信息安全领域相对落后

在信息安全产业中进行细分，可以将其分为物理安全、运行安全和数据安全三大类。传统上的信息安全防护侧重于物理和运行层面，主要通过构建多层级防护架构实现信息安全保障；但由于黑客攻击手段日趋多元化，以及内部安全隐患的占比高企，针对物理和运行层面的防护不足以化解全部漏洞和攻击，针对数据层面的新一层保护成为必须。

从行业占比来看，目前数据安全发展处于相对落后状态，2015 年国内数据安全在整体产业中占比仅为 17.6%。但根据中国产业信息网统计，这一数字呈现持续上升趋势，并有望在 2017 年达到 19.2%。

图 16：数据安全在信息安全产业中占比呈上升趋势



资料来源：中国产业信息网，中信建投证券研究发展部

数据安全发展相对滞后的核心原因在于威胁类型的差异；数据所面临的威胁类型多样化，对防护手段、技术等需求较高，其中部分属于物理和运行安全范畴。针对物理威胁如火灾、雷击等，数据库的容灾备份是防范此类威胁的主要方法，目前普遍采用的容灾备份方式包括低带宽数据远程复制、存储虚拟化、双活数据中心等。

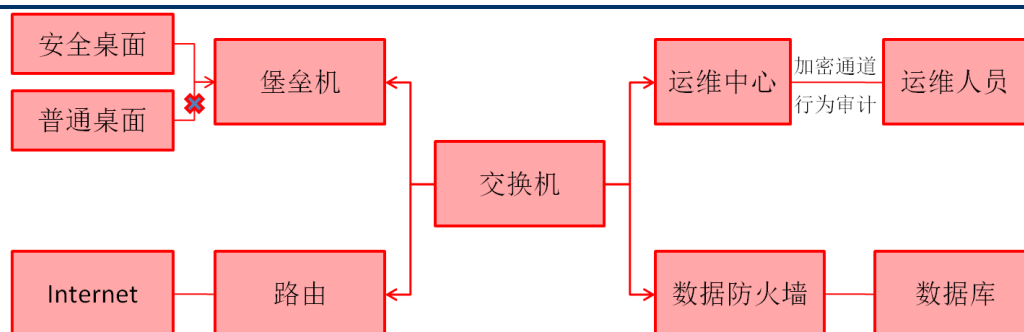
而外部数据窃取中攻击者一般会通过 SQL 注入、APT 等攻击方法对数据库进行攻击，目的包括窃取数据库信息、通过数据库发送指令获取服务器管理权限等。通常人们利用防火墙、IDS/IPS 等各种方式来防御外部攻击，在网络中设置数据库访问控制策略并检查数据库访问者是否合法，同时采用加密算法处理数据库的读写，使数据泄密的威胁降低。

此外，由于企业存在外包公司进行现场开发或第三方人员运维，以及内部员工在操作上的不慎重和企业内部人员窃取行为等，导致内部存在多种方式接入到数据库，成为数据库安全的最大隐患之一。这一类安全威胁的解决方案包括文档安全管理、操作安全管理等，主要通过堡垒机、SIEM、行为审计等方式实现。

综上，目前常用的数据库安全解决手段包括：1、容灾备份解决物理安全威胁问题。2、数据库防火墙解决通过 SQL 注入、漏洞、ATP 等攻击数据库造成的拖库行为。3、堡垒机、行为审计解决运维人员对数据库操作

中的安全问题。4、文档安全管理对数据库进行不落地处理，防止数据库的泄密、丢失等人为安全隐患。5、数据库加密起到最终防范效果，在数据丢失的最坏假设下减小数据被破译造成损失的概率。

图 17：数据安全管理模式



资料来源：汉领信息，中信建投证券研究发展部

3.2 公司主要产品线

公司主要产品和服务包括软件产品、硬件产品、技术服务、技术开发四大类；其中，软件产品主要分为三大产品线：数据加密产品线、移动数据安全产品线、数据防泄漏产品线。

3.2.1 数据加密产品线

数据加密系列产品采用符合国家标准的加密算法，在各类数据产生、存储、交互、使用等过程中，透明动态地对数据进行加密、解密和权限控制，使用户在正常使用时无感知，越权使用时得到警告或控制。目前，公司该产品线已在中国光大银行、民生银行、中信银行、国家开发银行、审计署等多个金融、政府机构应用。

表 4：公司数据加密产品

产品	功能
数据加密管理平台	存储数据加密策略、系统运行和维护中心，提供用户管理、终端管理、策略管理、日志管理、密钥管理、负载和热备功能
数据安全总线	应用身份鉴别、数据加密解密、密钥申请、权限查询、权限申请、日志安全等功能，实现企业统计的数据安全服务
数据脱敏网关	将涉及敏感信息的数据脱敏后提供给数据访问方，在获得授权后恢复原始数据，用户可控制敏感数据的适用范围和频率

资料来源：公司公告，中信建投证券研究发展部

3.2.2 移动数据安全产品线

移动数据安全系列产品将数据安全防护的范围从传统终端、网络和服务端，扩展到移动终端和互联网上，通过终端安全管理技术、透明数据加解密技术等，使用户在互联网移动环境下，可以安全地使用企业数据。目前，公司该产品线已在中国银行、中信银行、海关、质检总局、最高人民法院、公安部等金融和政府机构应用，累积部署移动终端超过百万数量。



表 5：公司移动数据安全产品

产品	功能
移动控制台	提供移动安全管理基础框架，为移动产品各模块一体化应用和安全提供基础功能，包括身份认证、策略配置、用户和设备状态管理、报表管理、日志管理、设备管理
移动安全接入系统	采用符合国家标准的加密和签名技术，保护网络通道安全和数据传输机密性，支持移动终端国密标准硬件身份认证和数据加密
移动安全应用系统	提供插件式安全应用，使数据落地即为密文，应用透明展现，包括安全邮件、安全通讯录、安全浏览器等

资料来源：公司公告，中信建投证券研究发展部

3.2.3 数据防泄漏产品线

数据防泄漏系列产品采用内容识别技术，通过发现存储在终端、网络、服务器、云上的敏感数据，监控各类型数据的使用情况，阻止泄密行为，帮助用户了解企业敏感数据的分布和使用情况，并对这些数据进行保护。目前，公司该产品线已在交通银行等金融机构实施部署。

表 6：公司数据防泄漏产品

产品	功能
数据防泄漏管理平台	对 ChinaSec（安元）数据防泄漏产品线中各产品提供统一策略管理、系统运行和维护
敏感数据发现系统	通过扫描组件获得终端、服务器上各类数据，对数据内容进行分析识别和发现敏感数据，形成敏感数据报告；支持终端磁盘、电子邮件、网络访问、移动存储、数据库和云端的数据扫描

资料来源：公司公告，中信建投证券研究发展部

3.2.4 公安警用产品线

公司在 2016 年完成对金之盾的收购，进入公安警用信息化产品领域。包括应用公司核心技术推出的公安数据安全系列自主产品，以及公安核心业务系统系列产品。

表 7：公司公安警用产品

产品	功能
公安数据安全系列产品	安全集中监测与审计系统、安全数据分析系统、终端安全准入系统、主机监测、应用管控系统、数据防泄漏系统、数据交换系统、APT 防护、移动 VPN、终端安全客户端等
公安核心业务系统产品	电信反诈骗自动化平台、刑侦一体化办案系统、禁毒信息管控系统、吸毒人员社会化管控系统、情报信息综合应用平台、陆网查控系统

资料来源：公司官网，中信建投证券研究发展部

四、核心竞争力

4.1 行业竞争格局/代表性企业

目前在数据安全领域，海外企业仍然占据了主流市场。在美国，这一领域有三类企业：一是拥有核心技术优势的基础软硬件企业，如思科、微软、英特尔、苹果、高通、甲骨文等产业巨头；二是形成了综合网络安全解决方案的企业，包括赛门铁克、趋势科技、飞塔等综合性信息安全企业，火眼、视眼石、Sqr1 等专注于诸如 APT 攻击防护、大数据分析等具体领域的专业化企业；三是具有整合能力的网络安全承包商，包括洛马、雷神、波音等国防承包商，这些企业能够综合各方力量，为政府和军方提供综合性网络安全解决方案。

针对 DLP/加密这一细分领域，Gartner 评选的全球领导企业包括 Symantec、Forcepoint（Websense+雷神）、Digital Guardian 和 IntelSecurity（McAfee）。

从产品来看，Symantec、McAfee、Forcepoint 属于综合安全解决方案供应商，产品覆盖数据保护加密、数据库安全、终端保护、网络安全、服务器安全、云安全、安全管理、SIEM 等多领域，其自主产品解决方案能力、服务能力较强，可以针对客户提供全面的安全解决方案产品。而 Digital Guardian 则专注于数据保护加密领域，通过其与操作系统内核深度绑定的集中策略管理架构，执行数据为中心的访问和控制规则，具备高度的可扩展性和可用性。

图 18：DLP/数据加密领域典型企业



资料来源：Gartner，中信建投证券研究发展部

4.2 国内竞争格局

在国内市场，数据防护软件和服务市场主要包括海外大型企业 Symantec、McAfee 等，国内几大传统信息安全企业启明星辰、绿盟科技、天融信、浪潮等，以及在细分领域具有技术优势的企业如明朝万达、亿赛通、北信源、优炫软件等。从提供数据安全软件整体解决方案的角度，大型集成商主要通过集成细分领域企业产品的方式进入市场；而以提供关键软件起家的中小企业则通过被并购、产业合作、自主拓展等方式，进入综合解

决方案领域。

自主可控进程推动下，相关国产软件企业将持续受益，而中小型企业基于核心产品优势，在产品线上持续扩张，将有望成为率先受益标的。

表 8：国内外主要相关数据安全厂商

	主要数据安全产品	核心技术	核心客户
赛门铁克	数据防泄漏云、云安全代理、终端/邮件/文件加密、身份认证、权限管理、加密通信等	内容指纹、关键字匹配等多种策略、多文件类型智能机器学习、跨多种云和端保护技术	大型跨国企业客户为主，国内银行、电信、电网等有所应用
McAfee (Intel)	加密功能、数据丢失防护、策略驱动型安全保护、云存储保护、数据库安全解决方案等	动态捕捉数据库、数字权限管理、数据分类管理、用户行为分析	包括全球 82% 大型银行在内的超过 12 万用户
Forcepoint	终端+云端内容安全、数据和内部威胁防护、实时安全数据分析	结构/非结构化数据指纹采集、事件风险评分、点滴式 DLP、自动信息发掘算法	金融、医疗、政府、公安等领域 2 万客户，主要为海外和跨国机构
亿赛通 (绿盟)	数据泄露防护 (DLP) 产品，包括文档安全管理系统、涉密文档管理系统、文档加密安全网关系统；网络内容安全管理；安全服务等	动态加解密、虚拟磁盘、身份准入、操作权限控制等	具有稳定的集成商客户，成为华为、太极股份、中软等企业供应商，软件销售为主
北信源	数据泄露防护系统、文档安全管理系统、打印/光盘/移动存储/邮件监控审计系统、安全桌面等	数据加密、网络准入控制、终端大数据分析、安全即时通信、云安全管理平台	拥有政府部门、军队及军工、能源、金融等重要领域大型国有企事业单位上千个客户，终端数量过千万
优炫软件	数据库安全审计、数据库透明加密、日志审计、云数据库等	访问权限控制、多级过滤、环境监控、运维管理等	主要客户为人民银行、城商/农商行等银行客户，电力、军工、政府等领域快速发展

资料来源：相关公司官网，Gartner，中信建投证券研究发展部

4.3 竞争优势

4.3.1 技术和产品优势

在国内数据安全相关企业中，公司在加密产品线上具有独特优势。公司拥有 16 项授权发明专利和近 60 项申报专利，其中涉及身份认证、系统盘全盘加密、网络传输控制、即时通讯控制、移动存储介质管理等多项核心技术。

基于这些核心技术，公司产品在数据的产生、存储、交换、使用环节，针对服务器、数据库、终端、网络通讯等数据进行识别、加密、脱敏和权限管理，并进行全程日志和操作行为审计、分析和数据挖掘。

公司目前研发团队达到 110+ 人，研发人员占比达 45%；其中核心为来自清华大学、中科院等单位的资深研发队伍，具备稳定的创新能力。公司 2015 年研发费用达 1165 万元，占营收比重达到 17.16%，持续的研发投入是公司快速增长的核心动力。

图 19：公司产品架构示意图



资料来源：公司资料，中信建投证券研究发展部

4.3.2 细分行业客户优势

公司在创立早期以制造业客户为主，从 2010 年后向金融政府等客户延伸，新客户拓展效果良好。目前公司在金融、电信、能源、政府、军队、军工、医疗、设计院等各行业构建了行业数据安全和大数据安全解决方案。

尤其在金融、政府领域，公司产品拥有大量成功应用案例；金融领域拥有包括交通银行、光大银行、中国银行、中信银行、民生银行、国开行、中国银联、中国人寿、阳光保险、银河证券等行业龙头客户；政府领域订单则来自公安部、国家审计署、海关总署、最高法、质检总局、工信部等国家机关和下属地方单位。而公安警用移动网络、公安信息化领域的布局也将持续深化公司在该领域的优势地位。

图 20：公司下游行业龙头客户众多



资料来源：公司官网，中信建投证券研究发展部

4.3.3 定制化服务能力优势

公司在自主数据安全产品基础之上，针对下游各行业客户推出解决方案；同时基于大数据分析和数据挖掘能力，提供不断优化的解决方案服务，深入客户单位进行定制开发。

公司目前 100 人的销售团队由销售人员和资深技术服务人员构成，而研发人员中也有部分常驻客户单位，提供相关技术开发服务。公司将服务能力优势转化为强客户粘性优势，有望长期保持在核心客户群体的领先地位，并通过相同方式向新客户拓展。

五、高速成长的细分行业龙头，中长期布局可期

1、数据安全产品领先，大数据领域积极布局

公司在信息安全行业内具有最高的成长性，源于公司核心产品优势及成功的外延布局。公司 DLP/数据加密产品在国内具备一定领先性优势，并且持续投入研发，通过直接销售和部分集成厂商 OEM 进入了大量顶级客户，预计公司在该细分领域将保持中长期竞争优势。

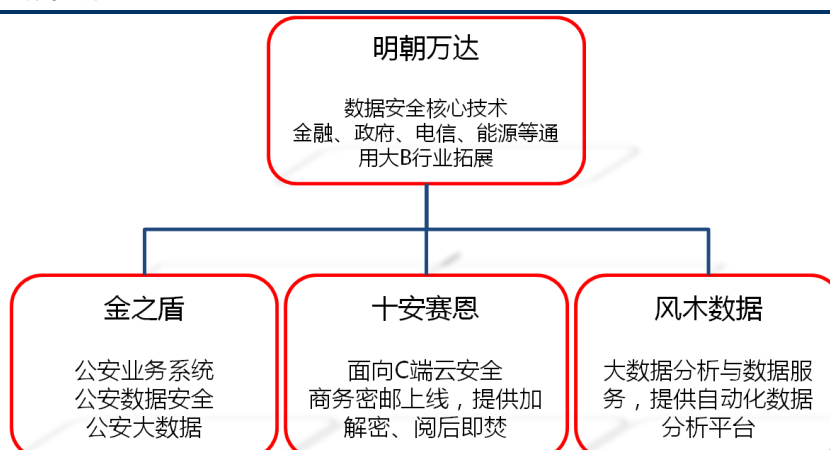
表 9：相关企业数据对比

证券简称	市值 亿元	市盈率 2015	毛利率 2015	净利率 2015	ROE 加权 2015	营业收入 2015 万元	营收 YOY 2015	营收 YOY 1H2016	归母净利 2015-扣非 万元	归母净利 YOY 2015	归母净利 YOY 1H2016
明朝万达	10.88	341.84	48.87	-37.61	-56.70	6,790.98	100.70	185.88	71.21	118.56	198.22
优炫软件	11.34	33.73	50.89	22.83	19.69	14,024.66	44.04	13.18	3,107.08	66.40	26.76
启明星辰	181.00	75.28	68.50	16.63	15.34	153,395.82	28.29	20.04	20,316.80	60.88	170.43
绿盟科技	126.50	56.86	78.31	22.04	13.44	87,766.48	24.90	42.99	16,522.54	22.43	69.16
北信源	113.20	155.22	54.37	15.05	9.54	47,001.53	78.89	34.58	6,774.07	3.90	36.72

资料来源：WIND，中信建投证券研究发展部

目前相关企业中，公司在规模方面不占优势，源于公司传统业务产品线较少。信息安全企业在销售中难以先验的展示产品优势，因此用户往往倾向于使用拥有完整解决方案的企业所提供的产品；公司积极拓展下游业务类软件等产品，从而利用产品线优势获得更大市场份额。未来随着三家子公司在公安警用业务系统、大数据安全和分析服务、云安全等产品的推广，以及公司在新产品方面的持续发力，有望实现更大范围的产品覆盖，从而获得更强的产品竞争力。

图 21：公司各产品线布局初显



资料来源：公司官网，中信建投证券研究发展部

2、高速成长的数据安全龙头，建议重点关注

基于公司产品+客户优势，传统数据安全业务领域有望保持稳步增长，新客户持续拓展、老客户采购 License



和模块数量上升，并有望在稳定使用后开始贡献服务费收入，信息安全产品线将保持 40%以上快速增长。新业务布局初见成效，其中公安产品贡献营收中近一半，并在未来带来新的项目贡献；云安全、大数据安全等业务也将陆续产生贡献。

预计公司 2016-2017 年营业收入 1.3、2.0、2.8 亿元，净利润 2800、4400、6000 万元，对应 EPS 0.20、0.32、0.43 元，对应 PE 38.8、24.7、18.14 倍，建议重点关注。

风险提示

- 1、信息安全领域政策推进不达预期
- 2、公安产品等新业务带来的毛利率下降风险



分析师介绍

王慷: 中国科学院金属研究所工学博士, 非金属建材行业分析师。2013、2014 年度作为团队核心成员获得新财富非金属建材行业最佳分析师第四名。

报告贡献人

张怀 15901025279 zhanghuai@csc.com.cn

研究服务

社保基金销售经理

彭砚苹 010-85130892 pengyanping@csc.com.cn

姜东亚 010-85156405 jiangdongya@csc.com.cn

机构销售负责人

赵海兰 010-85130909 zhaohailan@csc.com.cn

北京地区销售经理

张博 010-85130905 zhangbo@csc.com.cn

黄玮 010-85130318 huangwei@csc.com.cn

李祉瑶 010-85130464 lizhiyao@csc.com.cn

朱燕 010-85156403 zhuyan@csc.com.cn

李静 010-85130595 lijing@csc.com.cn

赵倩 010-85159313 zhaoqian@csc.com.cn

黄杉 010-85156350 huangshan@csc.com.cn

任师蕙 010-85159274 renshihui@csc.com.cn

王健 010-65608249 wangjianyf@csc.com.cn

周瑞 18611606170 zhourui@csc.com.cn

刘凯 010-86451013 liukaizgs@csc.com.cn

上海地区销售经理

陈诗泓 021-68821600 chenshihong@csc.com.cn

邓欣 021-68821600 dengxin@csc.com.cn

黄方禅 021-68821615 huangfangchan@csc.com.cn

戴悦放 021-68821617 daiyuefang@csc.com.cn

李岚 021-68821618 lilan@csc.com.cn

潘振亚 021-68821619 panzhenya@csc.com.cn

肖垚 021-68821631 xiaoyao@csc.com.cn

吉佳 021-68821600 jijia@csc.com.cn

朱丽 021-68821600 zhuli@csc.com.cn

杨晶 021-68821600 yangjingzgs@csc.com.cn

深广地区销售经理

胡倩 0755-23953859 huqian@csc.com.cn

芦冠宇 0755-23953859 luguanYu@csc.com.cn

张苗苗 020-38381071 zhangmiaomiao@csc.com.cn

许舒枫 0755-23953843 xushufeng@csc.com.cn

王留阳 0755-22663051 wangliuyang@csc.com.cn

廖成涛 0755-22663051 liaochengtao@csc.com.cn

券商私募销售经理

任威 010-85130923 renwei@csc.com.cn



评级说明

以上证指数或者深证综指的涨跌幅为基准。

买入：未来 6 个月内相对超出市场表现 15% 以上；

增持：未来 6 个月内相对超出市场表现 5—15%；

中性：未来 6 个月内相对市场表现在-5—5%之间；

减持：未来 6 个月内相对弱于市场表现 5—15%；

卖出：未来 6 个月内相对弱于市场表现 15% 以上。

重要声明

本报告仅供本公司的客户使用，本公司不会仅因接收人收到本报告而视其为客户。

本报告的信息均来源于本公司认为可信的公开资料，但本公司及研究人员对这些信息的准确性和完整性不作任何保证，也不保证本报告所包含的信息或建议在本报告发出后不会发生任何变更，且本报告中的资料、意见和预测均仅反映本报告发布时的资料、意见和预测，可能在随后会作出调整。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，不构成投资者在投资、法律、会计或税务等方面的最终操作建议。本公司不就报告中的内容对投资者作出的最终操作建议做任何担保，没有任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺。投资者应自主作出投资决策并自行承担投资风险，据本报告做出的任何决策与本公司和本报告作者无关。

在法律允许的情况下，本公司及其关联机构可能会持有本报告中提到的公司所发行的证券并进行交易，也可能为这些公司提供或者争取提供投资银行、财务顾问或类似的金融服务。

本报告版权仅为本公司所有。未经本公司书面许可，任何机构和/或个人不得以任何形式翻版、复制和发布本报告。任何机构和/或个人如引用、刊发本报告，须同时注明出处为中信建投证券研究发展部，且不得对本报告进行任何有悖原意的引用、删节和/或修改。

本公司具备证券投资咨询业务资格，且本文作者为在中国证券业协会登记注册的证券分析师，以勤勉尽责的职业态度，独立、客观地出具本报告。本报告清晰地反映了作者的研究观点。本文作者不曾也将不会因本报告中的具体推荐意见或观点而直接或间接收到任何形式的补偿。

股市有风险，入市需谨慎。

地址

北京 中信建投证券研究发展部

中国 北京 100010

东城区朝内大街 2 号凯恒中心 B 座 12 层

电话：(8610) 8513-0588

传真：(8610) 6518-0322

上海 中信建投证券研究发展部

中国 上海 200120

浦东新区浦东南路 528 号上海证券大厦北塔 22 楼 2201 室

电话：(8621) 6882-1612

传真：(8621) 6882-1622