东兴证券 DONGXING SECURITIES

# 卫士通（002268）：国产自主和等保2.0驱动公司安全手机业务爆发

## ——深度系列报告之七

2019 年 09 月 09 日

强烈推荐/维持

卫士通 | 深度报告

### 报告摘要：

**1、安全手机业务驱动因素多。**首先是公司新增电信业务范围，，针对“安全通信”，“安全接入”和“安全管控”场景下行业需求，整合移动运营商优势资源，形成自有安全解决方案。深化与中国移动等战略伙伴的合作，以“移动办公业务”为核心，以行业解决方案为抓手带动终端销售。且随着等保 2.0 年底即将大规模实施，其中移动互联网安全得到空前重视，移动办公安全等成为安全手机业务强力催化因素。而预计明年开始的办公信息化国产自主大趋势下，政务安全需求也将带动安全手机业务增长。

**2、推进密码在云安全方面的应用。**安全是云计算中最重要的考虑点，而密码是解决云安全问题的最有效手段。公司大力推动产品的云化等工作，目前云服务器密码机、云密钥管理系统、云密码资源池管理平台、安全云终端等产品已实现云化；公司开展卫士云安全服务，建立云密码服务的业务模式，结合自身优势，发力云数据安全服务领域，推广以网站防护系列服务为基础的云安全服务。不断探索和谋划新业务领域，开展了云安全服务、 5G 与物联网、新型智慧城市、安全视频监控等方面的市场研究和业务策划。密码服务化是顺应云计算发展的必然趋势，结合云服务的发展路线，将密码能力以服务的方式输出可以有效适应云场景下的网络和信息安全保障需求，为公司在政务云上发力打下坚实技术基础。

**3、卫士通金融数据密码机已启动 FIPS 认证工作。**亚太地区已经成为恶意网络活动和网络犯罪的突出攻击对象，其中金融领域面临的挑战极为严峻。2015 年，亚洲企业因为网络犯罪造成的损失超过 800 亿美元，远远超过美国和欧洲企业。2016 年，金融行业遭遇的数据泄露最为严重，而且每项被盗记录的损失几乎是其他行业的两倍。而我国《网络安全法》要求关键信息基础设施运营商必须在中国内地储存个人信息和“重要数据”，若需要数据出境，则必须按照网信办的规定进行安全评估。海外相关公司敏感数据回传成为我国信息安全的重要组成部分。特别是随着人民币国际化，以及未来即将推出的数字货币，相关金融数据传输需求快速增长。卫士通推出出口型加密机，有效保障我国海外资产数据安全。

### 财务指标预测

| 指标 | 2017A | 2018A | 2019E | 2020E | 2021E |
|---|---|---|---|---|---|
| 营业收入（百万元） | 2,137.11 | 1,931.00 | 2,788.12 | 3,891.04 | 5,338.21 |
| 增长率（%） | 18.80% | -9.64% | 44.39% | 39.56% | 37.19% |
| 净利润（百万元） | 169.05 | 120.20 | 423.34 | 704.76 | 893.13 |
| 增长率（%） | 8.54% | -28.90% | 252.18% | 66.48% | 26.73% |
| 净资产收益率（%） | 3.94% | 2.73% | 9.03% | 13.66% | 15.53% |
| 每股收益(元) | 0.21 | 0.14 | 0.50 | 0.84 | 1.07 |
| PE | 111.24 | 163.60 | 46.46 | 27.91 | 22.02 |
| PB | 4.58 | 4.46 | 4.19 | 3.81 | 3.42 |

*资料来源：公司财报、东兴证券研究所*

### 公司简介：

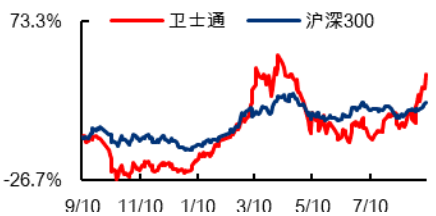
公司是国内知名密码产品、网络安全产品、互联网安全运营、行业安全解决方案综合提供商。公司从密码技术应用持续拓展，已形成密码产品、信息安全产品、安全信息系统三大信息安全产品体系，同时，基于 ISSE 体系框架，为党政、央企、能源、金融等用户提供信息系统全生命周期的安全集成与运营服务。

### 未来 3-6 个月重大事项提示：

### 交易数据

| | |
|---|---|
| 52 周股价区间（元） | 31.91-22.92 |
| 总市值（亿元） | 267.51 |
| 流通市值（亿元） | 258.44 |
| 总股本/流通 A 股（万股） | 83834/80989 |
| 流通 B 股/H 股（万股） | / |
| 52 周日均换手率 | 1.28 |

### 52 周股价走势图




*资料来源：wind、东兴证券研究所*

**分析师：陆洲**
010-66554142 luzhou@dxzq.net.cn
执业证书编号: S1480517080001

**分析师：王习**
010-66554034 Wangxi@dxzq.net.cn
执业证书编号: S1480518010001

**分析师：张卓琦**
010-66554018 zhangzq_yjs@dxzq.net.cn
执业证书编号: S1480519080003

**盈利预测：**公司是网络安全国家队，新增电信业务，进军专网运营；安全手机与中国移动合作，受益于等保 2.0 中移动互联网安全需求，且跟随办公信息化国产自主大趋势，相关密码机随之替换，移动政务安全市场也有望打开。公司基于卫士通云平台密码应用，开展卫士云安全服务，建立云密码服务的业务模式，结合自身优势，发力云数据安全服务领域，推广以网站防护系列服务为基础的云安全服务。随着人民币国际化，以及未来即将推出的数字货币，相关金融数据传输需求快速增长。卫士通推出出口型加密机，有效保障我国海外资产数据安全。我们预测公司 2019 年~2021 年净利润分别为 4.23 亿、7.05 亿和 8.93 亿，EPS 分别为 0.50 元、0.84 元和 1.07 元，维持“强烈推荐”评级。

**风险提示：**等保 2.0 推动不达预期，办公信息化国产自主业务不达预期。

# 目 录

# 表格目录

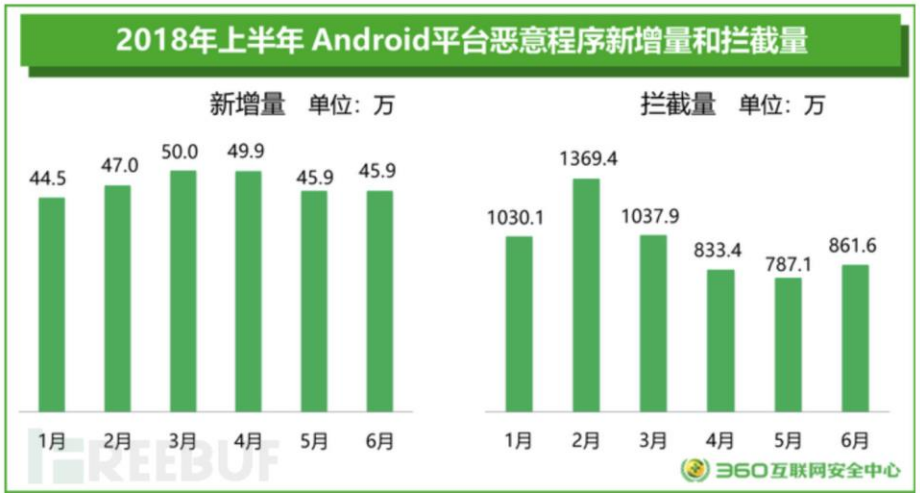


# 插图目录

# 1. 移动互联网安全制约了移动政务发展

**移动互联网恶意程序猖獗。**2018 年上半年，360 互联网安全中心累计截获安卓平台新增恶意程序样本 283.1 万个，占总新增量的 2%，比 2017 年上半年（418.4 万个）减少了 135.3 万个，平均每天截获新增手机恶意程序样本近 1.6 万个。360 手机卫士累计为全国手机用户拦截恶意程序攻击 5919.4 万次，同比 2017 年上半年（11747.5 万次）下降 49.6%，平均每天拦截手机恶意程序攻击 33 万次。下图给出了 2018 年上半年移动端恶意程序新增量与拦截量统计。2018 年上半年，360 互联网安全中心累计截获安卓平台新增恶意程序样本 283.1 万个，占总新增量的 2%，比 2017 年上半年（418.4 万个）减少了 135.3 万个，平均每天截获新增手机恶意程序样本近 1.6 万个。360 手机卫士累计为全国手机用户拦截恶意程序攻击 5919.4 万次，同比 2017 年上半年（11747.5 万次）下降 49.6%，平均每天拦截手机恶意程序攻击 33 万次。下图给出了 2018 年上半年移动端恶意程序新增量与拦截量统计。

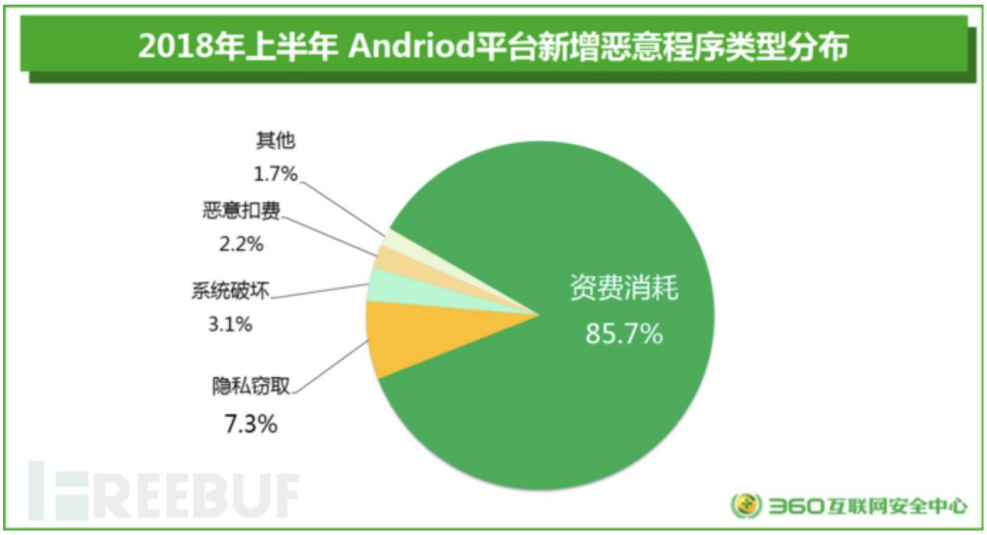
**图 1：2018 年上半年 Android 平台恶意程序新增量和拦截量**




*资料来源：2018 年上半年中国互联网安全报告，东兴证券研究所*

2018 年上半年，安卓平台新增恶意程序主要是资费消耗，占比高达 85.7%；其次为隐私窃取（7.3%）、系统破坏（3.1%）和恶意扣费（2.2%）。

**图 2：2018 年上半年 Android 平台新增恶意程序类型分布**




*资料来源：2018 年上半年中国互联网安全报告，东兴证券研究所*

**相对于 PC，用户使用手机上网、下载应用软件、电子支付更频繁，随之而来的是日益凸现的安全威胁。**目前，智能手机的信息安全逐渐受到用户和业界广泛关注。智能手机后台自动收集、回传用户个人信息，以及斯诺登事件、icloud 泄密好莱坞影星艳照事件、苹果 iOS“后门”事件，让各国手机用户开始重视手机安全。 欧盟网络与信息安全署（ENISA）报告指出，资费、隐私和数据安全，是当前智能手机用户关注重点。安全研究显示，全球手机用户中 90% 都面临密码被盗、数据被窃的风险，甚至会导致手机被黑客完全控制。这些威胁来自智能手机存在安全漏洞，其中包括苹果、谷歌和黑莓等企业采用了存有瑕疵的行业标准，智能手机四分之三采用旧版 Android 系统的设备，全球八分之一 SIM 卡存在安全漏洞等。由于智能手机具有独立操作系统，支持用户自行安装软件、游戏等第三方服务商提供的程序，并具备上网功能，其极易被病毒制作者利用，传播手机病毒等安全威胁。随着智能手机竞争越来越激烈，更多的厂商 打出“安全牌”，尤其是在手机其他功能相差不大的情况下，安全手机倍受关注，网络安全正改变着世界的经济。

## 1.1 移动互联网安全是网络安全必不可少的部分

### 1.1.1 移动智能终端漏洞居高不下，修复缓慢

移动智能终端开放的应用环境带来了日益严重的安全问题，移动智能终端操作系统漏洞近年来居高不下，严重威胁用户个人信息甚至人身财产安全。据 CVE Details 公布的数据显示 2018 全年 Android 系统漏洞和 IOS 系统漏洞数分别为 611 个和 125 个。按漏洞类型统计，代码执行、拒绝服务、内存溢出等类型漏洞占比较高，攻击者可利用这些漏洞获取系统最高权限和进行恶意操作，如窃取用户个人信息、拦截移动支付，侵害用户合法权益。

在移动智能终端漏洞居高不下的同时，移动智能终端系统漏洞修复也十分缓慢，用户长期暴露在危险、易受到攻击的状态下。研究表明，超过 9 成的设备存在已知漏洞，每台设备平均检测出的漏洞数量为 35 个，其中严重漏洞 16 个，高危 11 个，中危漏洞 8 个。不同厂商的漏洞修补水平参差不齐，终端整体表

现不好，漏洞平均存在时间较长。多数终端在 OTA 升级后漏洞数量并没有明显减少，部分终端的系统漏洞数量反而呈增加的态势。

### 1.1.2 移动互联网恶意程序持续增长，同时影响个人和企业安全

**近年来移动应用程序极大丰富，但移动互联网恶意程序也随之大量涌现，严重危害用户的个人信息安全和人身财产安全。**据相关资料显示，2018 年 Android 新增病毒包达 800.62 万个手机病毒感染用户数近 1.13 亿，支付类病毒感染用户数近 394.21 万，手机病毒类型主要是资费消耗和恶意扣费。

同时，随着移动智能终端向企业办公、移动政务等领域扩展，推动终端病毒向企业和政府等领域蔓延。个人应用和企业应用并存使得企业数据存在非授权访问风险。一方面,用户在外部网络使用移动终端可能会被恶意程序感染，在接入企业内部网络时会影响内部网络安全。另一方面，用户在安装非企业内部应用时也可能因内嵌恶意程序给企业网络带来潜伏式的攻击。

### 1.1.3 新技术带来新挑战，用户数据成安全重灾区

**随着人工智能、物联网等新技术的兴起，数据已成为制约其发展的关键点，其发展高度依赖于大数据的训练分析，需要收集、传输和存储大量的用户个人信息的数据。**在企业高度重视网络数据的资产价值并对其表现出极大热情的同时，其面临的各种问题仍不容忽视，其中最严峻的就是对用户数据的保护问题，用户数据仍是网络数据应用违法违规的重灾区。

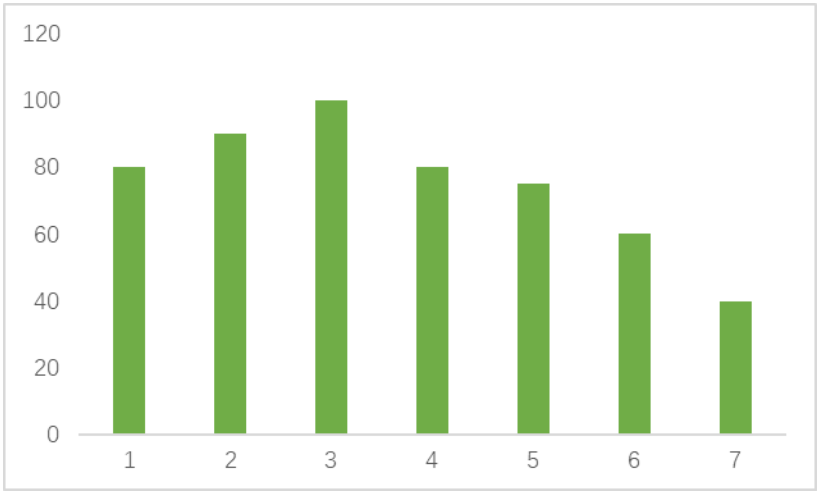
用户数据价值的提升，带来了窃取用户数据的高级持续性攻击的陆续发生。更甚者，用户数据非法买卖黑色产业链在愈演愈烈，不良网络信息等下游问题也随之加剧。据相关调查显示，2018 年个人信息泄露总体情况比较严重显示，超八成受访者曾遭遇个人信息泄露问题。

## 1.2 电子政务是信息化主要领域，已变成当前主流趋势

**当前，电子政务变成信息化构建最主要的领域之一，电子政务信息时代变成主导的趋向。**移动电子政务不但提高了政府服务效率，同时方便了群众办事，减少办事时间，为公民提供了更优质、高效和便捷的服务。根据中国互联网络发展状信息中心发布的《第 43 次中国互联网络发展状况统计报告》显示，截止到 2018 年 12 月，我国网民规模达 8.29 亿，互联网普及率为 59.6%。其中，我国“互联网+政务服务”得到了深入落实，各级政府通过网上政务服务平台，实现了“数据多跑路”“群众少跑腿”。据统计在线政务服务用户规模达到 3.94 亿，占总体网民的 47.5%。2018 年网民各类政务服务用户使用支付宝或微信提供的城市政务服务占据主流位置，占 42.1%；其次为政务微信公众号，使用率为 23.6%；政府网站、政府手机端应用及政务微博的使用率分别为 19.0%、11.6%和 9.4%。

目前，国内各级政府部门信息化水平如图 1 所示，各部委和省级城市与区县级政务信息化水平参差不齐。

**图 3：国内各级政府部门信息化水平**




*资料来源：网络数据，东兴证券研究所*

1）国务院部门主要业务；2）海关、税务、公安、审计、国土、金融监管等重点领域业务；

3）部分部委，如公安部、科技部、人民银行、审计署等；4）国家统计局和信业务电子政务；

5）省级政务部门主要业务；6）地市级主要业务；7）区县一级主要业务；

## 1.3 移动互联网安全监管重心转移，需加强网络安全态势感知能力建设

**当前，移动互联网安全监管面临着一些新的形势。**一是党的十八大以来，党中央、国务院从战略和全局高度，大力推动政府治理体系现代化，紧紧围绕处理好政府与市场关系，持续推进“放管服”改革，推动网络强国战略实施，加快政府职能转变。近年来，国务院多次召开全国深化简政放权放管结合优化服务相关会议，要改变政府管理方式，加强事中事后监管，做到“放”“管”结合，从事前审批转变为加强事中事后监管。二是《中华人民共和国网络安全法》已于 2017 年 6 月 1 日正式实施，对包括移动终端、移动应用在内的网络产品和服务的漏洞、恶意代码以及个人信息保护提出了明确要求。三是国务院发布的《“十三五”国家信息化规划》提出健全网络安全保障体系,能够“全天候全方位感知网络安全态势,加强网络安全态势感知、监测预警和应急处置能力建设,建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势，建立政府和企业网络安全信息共享机制,加强网络安全大数据挖掘分析，更好地感知网络安全态势，做好风险防范工作”。

**但与此同时，移动互联网安全监管也面临较大挑战。**一是缺乏持续性监管方式和应急响应能力，监管部门针对移动互联网风险持续性监管策略和能力有待完善，移动互联网安全主要依靠厂商自行维护。一方面，厂商能力参差不齐，对威胁和脆弱性感知较为被动，风险响应时效性较低；另一方面缺乏规范和监管机制推动，依靠舆情影响和厂商自律，较难保障用户权益，缺乏全面、权威的监测平台来支撑移动互联网安全风险预警响应，缺乏数据有效关联分析机制，无法支持移动互联网安全风险预警响应。二是产业链环节多，监管存在盲点,移动互联网涉及终端制造商、移动应用开发者、服务提供商、运营商、安全厂商等众多主体每个主体涉及多个产业链，监管十分复杂，同时由于主管机构职责的划分，经常会出现

**监管的盲点，让不法行为有机可乘。**卫士通当前新增电信业务，从全产业链把控移动互联网安全，形成自运营商，到终端制造商，服务提供商、安全厂商等为一体，可减少监管盲点，利于职责划分，减少安全漏洞。

## 1.4 移动互联网安全态势感知将极大提升监管能力

### 1.4.1 移动互联网安全态势感知

网络安全态势感知是指在网络环境中，采集网络通信、网络流量、计算环境、脆弱性、安全事件、运行状况、审计日志和威胁情报等数据，利用大数据和机器学习等技术，分析网络行为以及用户行为因素所构成的整个网络当前状态，获取、理解、评估能够引起网络态势发生变化的安全要素，预测网络安全态势发展趋势。在移动互联网环境中，采集移动终端及移动应用的相关的网络流量、漏洞、恶意应用、设备型号、安全事件等数据，利用大数据和机器学习等技术，分析移动终端当前状态 ，获取、理解、评估能够引起移动终端态势发生变化的安全要素，预测移动终端安全态势发展趋势。

因此，应用态势感知技术可为移动互联网安全监管提供新的思路：

1）是建立移动互联网持续性和主动性监测能力。对于用户移动智能终端受病毒感染情况、漏洞修复情况、恶意应用传播情况、垃圾短信、骚扰电话、恶意网址等进行感知监测，实现对移动互联网持续监测和管理，掌握智能终端设备运行环境安全、移动应用安全等，动态监测响应、处置、改善移动互联网安全状态。

2）是加强移动互联网事中事后监管。利用移动互联网安全态势感知，结合运营商、设备制造商、安全公司等，将海量移动互联网态势数据进行整合分析，解决移动互联网事中事后监管的关键技术难题。

3）是增强移动互联网攻击溯源与应急处置能力。能够对恶意攻击、恶意应用、安全事件讲行溯源取证，对恶意应用的发布者进行追踪。同时能够对移动终端安全进行监测预警和应急处置，准确把握网络安全风险发生的规律、动向、趋势。

### 1.4.2 采用新技术有效提升监管能力

将态势感知技术应用于移动互联网的安全监管，建立移动互联网持续性和主动性监测能力，对移动互联网恶意应用、移动智能终端漏洞、安全攻击等安全状况进行感知监测，实现对移动智能终端和移动应用的持续监测和管理，掌握移动互联网运行环境安全,动态监测、响应、处置、改善移动互联网安全状态。同时，增强移动互联网攻击溯源与应急处置，能够对恶意攻击、恶意应用、安全事件进行溯源取证，对恶意应用的发布者进行追踪。同时能够对移动终端安全进行监测预警和应急处置，准确把握网络安全风险发生的规律、动向、趋势。

## 1.5 身份认证安全问题是阻碍移动电子政务发展所面临的主要原因

### 1.5.1 移动电子政务领域发展不平衡

目前，身份认证安全问题是阻碍移动电子政务发展所面临的主要原因。传统的 PC 端的身份认证方式通过数字证书、U 盾等方式发展已相对成熟，例如银行采用 USBKEY 解决用户身份认证问题，用户私钥在 USBKEY 内产生并且终身不离开 USBKEY，有较高的安全性。而在移动电子政务领域中，远程鉴别用户身份信息的真实性至关重要，单凭用户名口令的方式，不足以鉴别用户身份，因此在移动政务领域中需要建设一套移动电子政务身份管理基础设施，通过短信验证码、移动 APP(软证书)，以及用户拥有的生物特征信息比如指纹、人脸识别等，来确认用户身份的真实性，或是通过姓名、身份证号实现对用户进行身份鉴别，对重要数据进行责任认定，确保数据在交互过程中用户身份标识的唯一性、数据的完整性、机密性及数据发送、接收的不可否认性。

### 1.5.2 移动电子政务身份鉴别方式落后

**（1）缺少移动电子政务身份管理的标准化。**随着移动互联网的发展,很多用户使用多种多样的移动设备和鉴别方式，为了满足企业和用户的需求，相继出现了国际的 FIDO 联盟、阿里巴巴的 IFAA 和腾讯的 SOTER 这样安全、通用、完整的身份鉴别框架。国内的 IAA 是阿里巴巴牵头的联盟组织，其认证形式以人脸识别为主，同时涉及虹膜、指纹和可穿戴设备，通过前端本地鉴别用户身份，并采用公钥完成前端到服务端的身份验证，在移动支付等电子商务场景得到了很好的应用和体验。电子政务领域在移动身份认证方面相对落后，迫切需要套安全性高、轻量级、统一、体验好的身份认证标准。

**（2）身份鉴别种类单一。**目前应用于移动电子政务身份鉴别的方式比较单一和落后，很多政务机构仍在使用静态口令的方式，用户通过输入用户名和口令，实现身份验证。然而这种鉴别方式存在较为严重的安全隐患，攻击者可以通过口令数据库攻击、钓鱼攻击、木马攻击等方式，获取用户名和口令。随着移动互联网的发展出现了许多强认证部手段，例如动态口令、U 盾、智能卡、短信验证码、生物识别技术，以及符合国家密码管理局认定造密钥分割技术的密码模块软证书等等，其中内置软件密码模块软证书可存放至：安全 SD 卡、安全 TF 卡、安全 SM 卡、终端内置 SE 或外置密码模块的蓝牙接口智能密码钥匙、音频接口智能密码钥匙等设备中。移动电子政务需要更多种的身份鉴别方式来保障用户的信息安全，保证互联网通信中身份的真实性、不可抵赖性。

### 1.5.3 信任域相互孤立

**移动端身份管理技术目前主要应用于电子商务领域，而在电子政务领域同样有着全生命周期管理和单点登录的需求。**随着访问控制、权限管理、身份识别等技术的发展，行业内出现了 OpenID、SAML、OAuth 等一系列身份管理技术标准，用于不同可信网络的身份认证系统的互联互通和跨域访问。

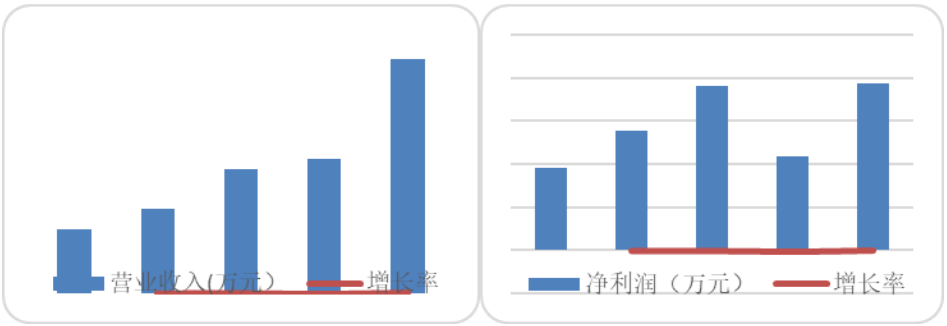
目前，我国移动电子政务已在多个领域中得到成功应用，包括交通、医疗、海关、税务等。用户需要在网上证明自己的身份，例如，当开设一个网银账号时。此时往往需要一些繁琐的流程证明身份后才能完成账号的申请。移动端身份系统应该提供一种方法，使用户可以实现统一身份认证和信任传递。该身份具有唯一性、可鉴别性和不可否认性。

# 2. 三零瑞通专注安全手机，为移动政务安全保驾护航

## 2.1 三零瑞通多年聚焦安全手机业务

三零瑞通自成立以来，一直致力于以手机为主的移动通信安全技术研究与产业发展，是国内最早开展移动通信技术及移动互联网安全应用的专业企业之一。三零瑞通是国家认定的高新技术企业、软件（双软）技术企业,获得了军民品质量管理体系认证证书，是国家密码管理局认定的商用密码产品生产定点单位及销售许可单位，是国防科研生产二级保密资格单位。

**图 4：三零瑞通历年营业收入和净利润情况**




*资料来源：2018 年上半年中国互联网安全报告，东兴证券研究所*

**在移动信息安全技术、移动信息安全服务、专业移动安全通信及智能移动终端安全防护等领域处于国内领先水平，拥有自主知识产权和核心技术。**在移动通信信息安全领域具备了较强的技术创新能力。在移动信息安全领域，拥有 22 项专利和 12 项计算机软件著作权，并与成都信息工程学院合作设立“密码芯片安全分析实验室”,通过技术合作增强公司的研发能力和自主创新能力。

**公司专注于移动通信和移动信息安全产业，在行业内具有良好的品牌知名度和较高的品牌可信度。**公司专注于移动通信和移动信息安全产业，面向公众市场努力打造“移动信息安全专家”著名品牌。公司建立了覆盖全国的营销服务网络，在北京、沈阳、西安、上海、福州、广州设立了区域营销中心，并与合作伙伴共同开展海外市场开拓，目前已在非洲、东南亚、中东、南美洲建立海外营销管道。在市场推广方面，三零瑞通与中国移动、中国联通建立了长期稳定的合作关系，与中兴、华为、长虹、海信、联芯科技等芯片及终端厂商具有丰富的项目合作与产品推广经验。三零瑞通在移动通信和信息安全领域，具备多种研发生产资质，并拥有众多的核心技术和知识产权；在客户营销经验和营销网络上具有特定的行业和区域优势。

## 2.2 手机安全标准已经立项，移动互联网安全市场空间有望快速拓展

据经济参考报 2017 年 8 月 30 日消息，从 29 日举行的中国手机网络安全高峰论坛上获悉，国家安全标准委已对安全手机标准立项，意在研究制定手机安全标准，其中将包括关键硬件、软件信息基础设施的网络安全防护能力，系统安全等级，APP 权限限定等。

移动互联网主导地位正在强化，使用手机上网比例明显增加，但因发展时间较短，快速扩张的手机网络成为蠕虫病毒等恶意程序的入侵目标。在此背景下，**手机网络安全市场空间将快速拓展，有望从目前的约 100 亿元规模扩张到千亿元以上。**

## 2.3 卫士通安全手机

三零瑞通与华为进行深度合作，对华为系列手机进行软硬件定制化改造，以实现移动终端安全。本年度推出的卫士通尊御政务安全手机有两个可选机型，分别为：HUAWEI Mate 20/Mate 20 Pro。

**图 5：卫士通尊御政务安全手机：华为 Mate 20、华为 Mate 20 pro**


*资料来源：2018 年上半年中国互联网安全报告，东兴证券研究所*

卫士通安全手机有以下特点：

**1）同时兼顾。**一台手机同时兼顾工作安全和生活通信；双 APN 同时在线，专用 APN 只能接入专网；后台系统收到消息会通知前台系统。

**2）公私分明。**用户数据分开存储，双系统间文件、应用相互不可见；工作系统支持丰富的安全办公套件，可通过卫士通 MDM 进行动态管控，防止数据泄露。

**3）快捷切换。**支持一键切换；指纹识别切换；NFC 感应切换。

**4）可信安全。**开机逐级验证系统镜像，安全启动；系统分析写入保护，动态度量系统完整性，防 root；TEE 可信环境，保障敏感数据安全存储，支持全盘加密。

**图 6：卫士通尊御政务安全手机的普通系统运行分区和安全系统运行分区**


*资料来源：卫士通微信公众号，东兴证券研究所*

## 2.4 利用自身密码优势，多维度利用密码技术实现信息安全

安全手机中主要有以下几种用到加密的地方：

1）支持国家权威认证的软件密码模块；

2）支持加密 IM，加密 VOIP；

3）支持卫士通自主研发 VPN，实现工作系统与内网的安全传输。

### 2.4.1 软件密码模块

**自主密码算法模块：**尊御 Mate20 双域安全手机完美适配卫士通自主研发的密码模块，实现了 SM2/SM3/SM4/ZUC 密码算法、随机数产生、密钥产生、密钥存储、证书存储功能、身份认证、敏感信息安全访问、传输和存储等服务。

**密码卡管家软件：**基于软件密码模块为用户提供用户登录、号码绑定、安全通道、密钥管理等功能。

**图 7：密码卡加密界面**


*资料来源：卫士通微信公众号，东兴证券研究所*

### 2.4.2 贴芯卡

贴芯卡是薄膜式可贴加密芯片，它提供了商密算法和敏感密钥、证书安全存储功能，并通过了国家商密鉴定。

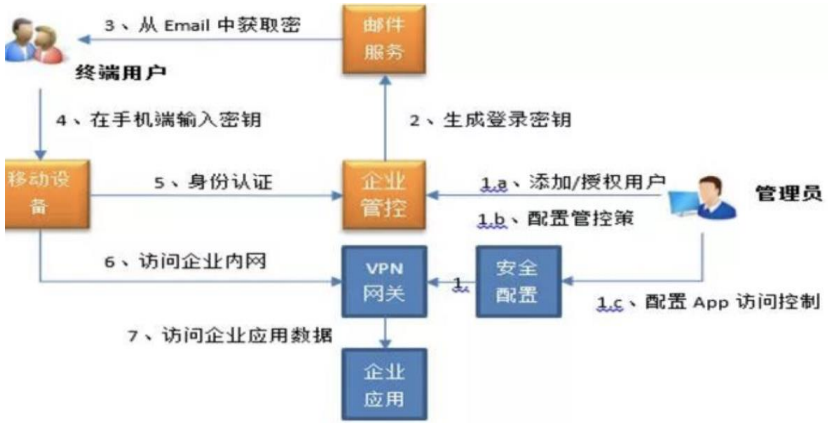
**图 8：薄膜式贴片加密芯片**

*资料来源：卫士通微信公众号，东兴证券研究所*

### 2.4.3 VPN 安全网关

用户使用安全网关通过身份认证后，可以访问企业内网资源。安全网关支持口令方式登录，保障使用安全和企业内网访问安全。

**图 9：卫士通安全网关使用流程**



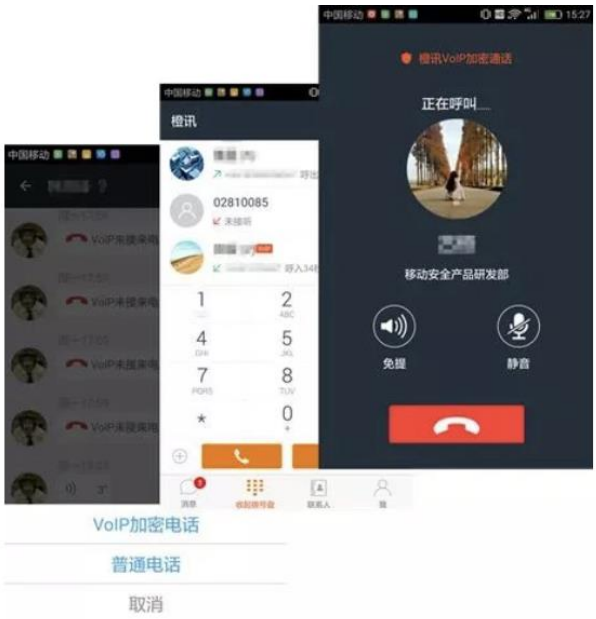

*资料来源：卫士通微信公众号，东兴证券研究所*

### 2.4.4 橙讯-安全 VoIP 加密通话

采用快速密钥协商、自适应语音编码技术，保证语音通话质量；先进的密钥协商和加密方式、身份鉴别、访问控制、权限控制多种技术保障通话安全；网络通话，实现全世界范围安全互联互通。

应用此功能需选配 TF 密码卡及密码卡管家应用。

**图 10：卫士通加密通话**




*资料来源：卫士通微信公众号，东兴证券研究所*

## 2.5 安全应用丰富，实现企业应用全生命周期管理

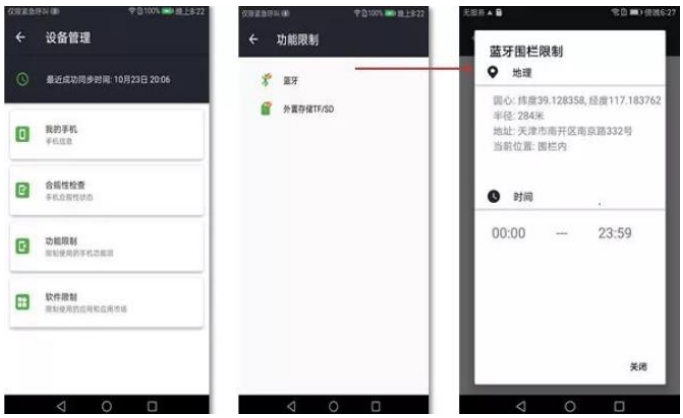
提供安全应用商店，提供企业文档中心，实现企业面向不同用户的文档可见性管理，用户可便捷搜索、查看、下载文档。

### 2.5.1 移动终端管理

**卫士通 MDM 管理：**用户可以进入管理中心查看手机终端的状态参数、合规性检查项以及当前终端的设备/应用安全管控策略；

配合时间围栏和地理围栏实施移动终端设备的外设管控。

**图 11：卫士通 MDM 管理界面**




*资料来源：卫士通微信公众号，东兴证券研究所*

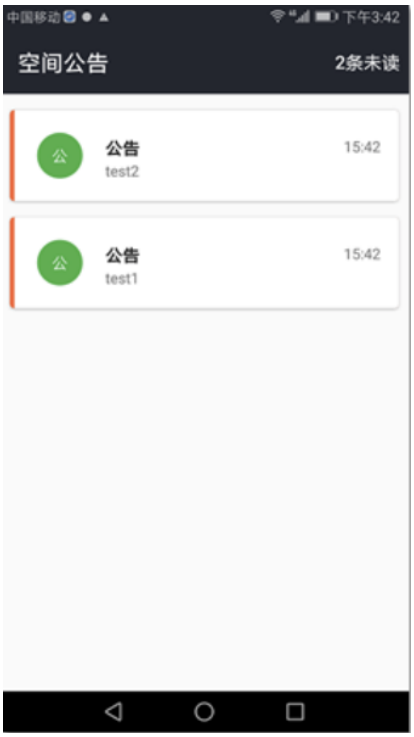
### 2.5.2 消息中心

安全工作系统中内嵌了统一消息推送引擎，用户可以在移动终端上实时查看企业发布的一些公告信息等；

管理员发布消息后，平台会通过消息推送通道实时向移动终端发送，消息中心组件收到推送信息会实时向用户发送提醒，确保了企业内部消息沟通的实时性；

统一消息推送引擎同时提供生态系统内的其它应用消息推送代理服务。

**图 12：卫士通统一消息推送引擎**




*资料来源：卫士通微信公众号，东兴证券研究所*

### 2.5.3 安全应用商店

移动安全办公套件中提供企业安全应用商店，实现了企业对指定安全应用的分发、安装、配置、卸载等全生命周期的统一管理；

企业可以快速便捷地向员工推送企业内的合规移动应用；

同时，企业应用商店作为企业安全桌面的应用发布接口，与终端原生的应用商店严格分离。

**图 13：安全应用**


*资料来源：卫士通微信公众号，东兴证券研究所*

### 2.5.4 安全文档中心

移动安全办公套件中提供企业文档中心，进入文档中心移动用户可以看到分发给该用户的所有文档，在平台端但没有分发给所属组织或者个人的文档不可见。

用户可以在文档中心查阅文档列表、在线阅读、搜索或下载需要的文档、收藏文档（或取消收藏）。

**图 14：安全文档中心**


*资料来源：卫士通微信公众号，东兴证券研究所*

### 2.5.5 移动安全管理平台

对激活工作系统的企业用户，提供移动安全管理平台，配合安全工作系统客户端，完成对设备，人员，应用，文档，配置等资源的统一集中管理平台，提供报告及审计、安全通信管理等功能，确保移动安全管理的每个环节都能顺畅、高效地实施和开展。

**图 15：移动安全管理平台**


*资料来源：卫士通微信公众号，东兴证券研究所*

### 2.5.6 橙讯安全协作

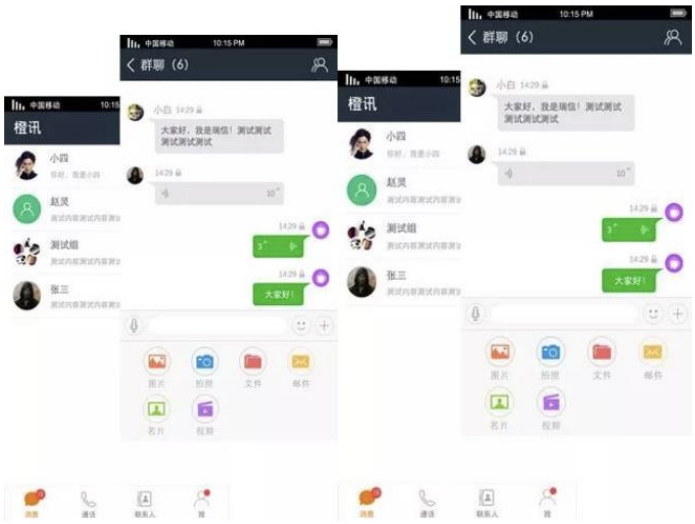
工作系统支持卫士通自主研发的高安全协作应用——橙讯，用户不需激活工作系统同样能使用橙讯。

**安全即时通信 IM：**基于国家商用密码评测认证的加密即时消息传输；使用高安全的国密算法，对文字、语音、图片、表情等即时消息进行加密传输。

**安全企业通讯录：**企业级人员信息管理软件，提供公司组织机构和员工名单管理；快速查找联系人进行安全通信。

**安全邮件：**支持国际通用算法、自主知识产权的商用密码算法，为用户提供公众级、商密级等多层次安全邮件服务；端到端安全邮件技术，邮件发出到接收全程内容加密。

**图 16：即时通信、通讯录和安全邮件**



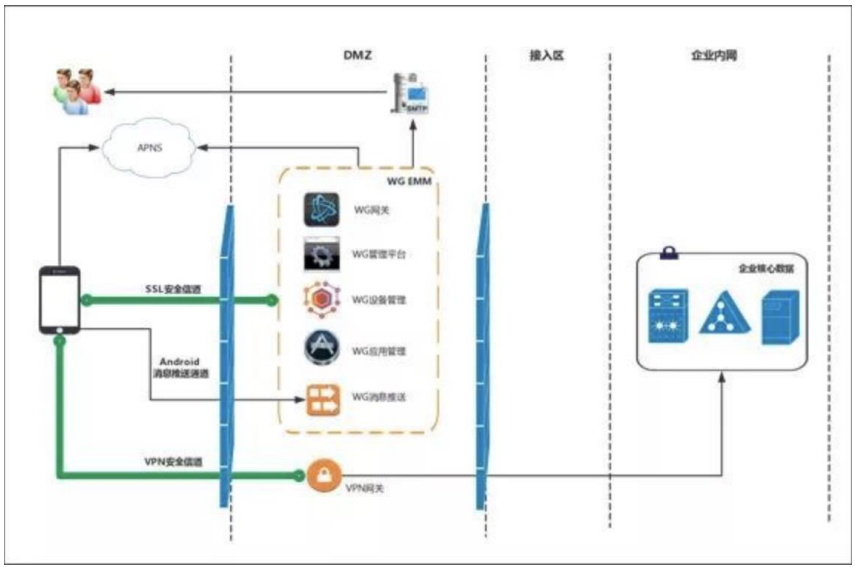

*资料来源：卫士通微信公众号，东兴证券研究所*

## 2.6 云端协作部署模式，产品资质齐全

### 2.6.1 部署模式

尊御 Mate20 双系统安全手机加载移动安全办公管理平台，采用“云端协作”方式，支持多租户云化部署、入驻式部署模式，平台为移动终端提供设备管理、应用管理和安全推送等服务，支持移动终端通过 SSL 安全通道实现对企业应用及企业敏感数据的安全访问。

**图 17：云端协作部署模式**




*资料来源：卫士通微信公众号，东兴证券研究所*

### 2.6.2 强大的产品资质

**母公司卫士通**公司具有涉密计算机信息系统集成资质（甲级）、计算机信息系统集成一级资质、CMMI—3级证书、建筑智能化系统设计专项甲级资质、电子与智能化工程专业承包壹级证书、安防一级资质和ISCCC 信息安全服务资质认证证书（信息系统安全集成一级）、国家信息安全测评信息安全服务资质证书（安全工程类一级）等。**各项资质齐全，**软件密码模块等产品已获得商密资质。

**图 18：公司商密资质**


*资料来源：卫士通微信公众号，东兴证券研究所*

## 2.7 卫士通安全手机特性总结

卫士通安全手机从多个安全角度实现移动互联网安全。

1）通信安全。集成 TF 加密卡，实现加密通话技术 4G 加密通话，彻底杜绝恶意窃听高清语音音质，通话质量清晰稳定。

2）应用安全。应用加固、数据隔离、安全存储安全通信、安全认证、单点登录符合企业安全管控策略。

3）协作安全。自主研发移动安全应用—橙讯；通过安全的加密通话、即时通信、企业通讯录、安全邮件打造快捷、高效的企业级安全协作平台；实现让人员、设备、应用、数据安全有机连接的安全协作平台。

4）平台安全。安全桌面实现企业应用环境与个人应用环境双域隔离；安全桌面系统实现应用、内存、数据、通信环境隔离；企业移动管理中心实现安全桌面内企业应用统一管理与管控。

5）数据安全。实现全程数据安全防护；结合身份认证和访问控制等多种技术手段，保证数据安全；防止恶意病毒入侵、手机丢失、用户身份被盗用、企业信息泄露风险。

**表 1 安全实现方式**

| 自主密码芯片 | 安全 4G加密 | 双层身份认证 | 移动安全生态部署 |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 国产自主高性能 TF 商用密码卡 | 中国移动 4G VoLTE 高清语音加密通信 | 芯片级硬件、指纹安全识别认证 | 支持移动办公安全生态环境部署，承载丰富安全应用，安全管控功能 |
| **高性能手机芯片** | **特色安全应用** | **全面安全防护** | **国家认证** |
| 国产自主高性能海思麒麟 970 芯片；内置 inSE 安全芯片实现金融级安全防护 | 程讯安全高效沟通协作平台 | 从硬件到软件、从系统到应用、 | 安全应用、TF 密码卡、密钥管理系统、安全终端均通过国家级商密鉴定 |

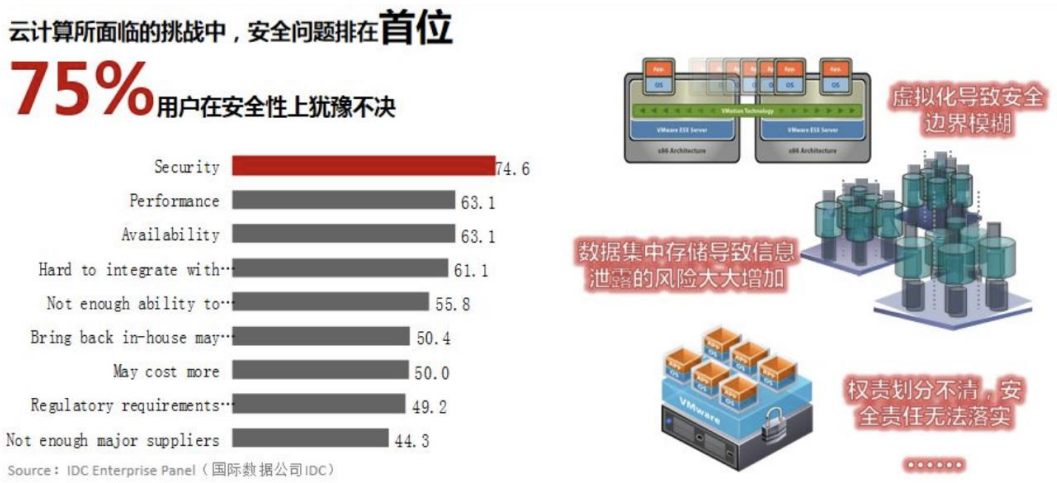
*资料来源：卫士通微信公众号，东兴证券研究所*

# 3. 卫士通云平台高性能密码推动政务云业务

## 3.1 密码是解决云安全最有效手段

**密码是解决云安全问题的最有效手段。**据 IDC 数据显示，云计算时代安全问题是用户（75%）首要关注的问题。大部分用户对于业务上云、应用上云、数据上云之后的安全问题犹豫不决，其中，最受关注的问题之一就是数据安全问题。

**图 19：云安全是用户首要关注的问题**




*资料来源：网络数据，东兴证券研究所*

安全是云计算中最重要的考虑点，而密码是解决云安全问题的最有效手段。密码因其解决网络安全问题的经济性、便捷性、有效性，以及在处理海量数据机密性保护、复杂网络实体认证等方面具有的独特优势，成为云计算产业持续发展的“内在”基因。云计算的蓬勃发展催生云上密码应用，云计算的发展带来公有云、私有云、混合云等多种业务形态，为适应云计算的多种形态必将催生新的密码应用模式，云计算发展驱动了网络、资源、终端的多维度融合，使数据逐步成为业务发展的核心和驱动力，同时使云环境下对密码和安全服务化的需求日渐迫切。**密码服务化是顺应云计算发展的必然趋势，结合云服务的发**

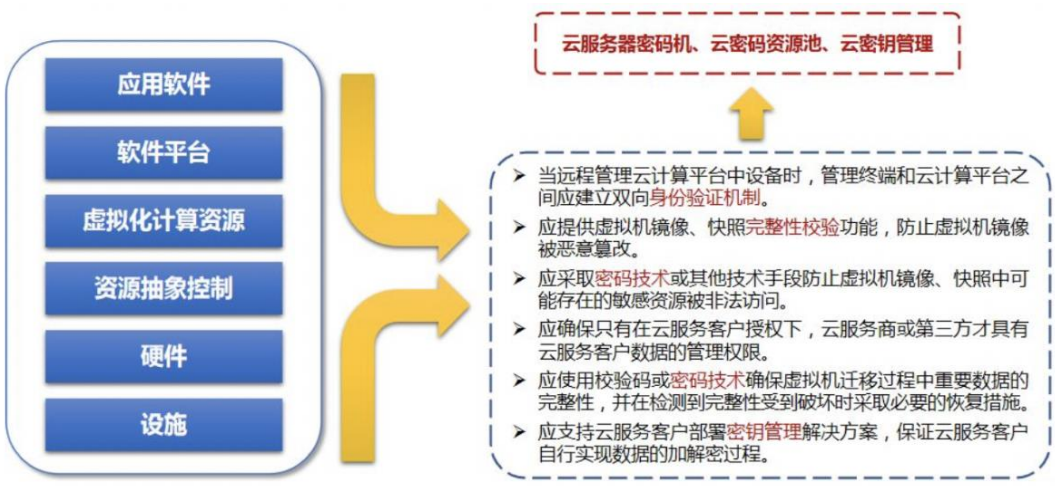
**展路线，将密码能力以服务的方式输出可以有效适应云场景下的网络和信息安全保障需求，以安全服务和业务服务为基础逐步扩展为基于商用密码的安全应用生态。**

## 3.2 国家对密码管理与应用愈加重视

近些年，国家层面愈加重视对密码管理与应用的规范化，继《商用密码管理条例》之后，密集颁布了《中华人民共和国网络安全法》《中华人民共和国密码法（草案征求意见稿）》《关键信息基础设施安全保护条例（征求意见稿）》《金融和重要领域密码应用与创新发展工作规划（2018-2022 年）》《网络安全等级保护 2.0》，对于数据安全、密码应用、测评要求还有同步体系化建设方面都提出了迫切的管理要求。

今年《信息安全技术 网络安全等级保护基本要求》国家标准的落地，也响应了密码技术应用的相关要求，新标准横向扩展了对**云计算、移动互联网、**物联网、工业控制系统、大数据的安全要求，纵向扩展了对等保测评机构的规范管理。最新的等保 2.0《基本要求》和《云计算扩展要求》中，有 20 多处提到了密码技术的应用，涉及身份鉴别、数据的完整性和保密性、抗抵赖等应用场景，同时对密码技术产品的使用也提出要求，如：应遵循密码相关的国家标准和行业标准、应使用国家密码主管部门认证核准的密码技术和产品等。在新的政策和形势下，随着《中华人民共和国密码法》的颁布，对密码应用、密码安全、密码发展促进、监督管理等方面都提出了新的要求，等级保护应在设计、建设、以及测评等各方面依照新政策新标准的相关要求，科学指导密码技术合规、正确、有效使用。

**图 20：卫士通对云计算安全扩展要求中与密码相关内容的梳理**




*资料来源：网络数据，东兴证券研究所*

## 3.3 基于密码高性能核心要求的云平台密码应用

**密码技术在云平台中的典型应用是以基础设施为支撑提供 Iaas 层和 Paas 层服务，密码云具有高性能、高安全、高可靠的技术特色。**卫士通所提出的密码技术云化应用实践是以打造密码云的形式为各类云环境提供密码服务。以政务云为例，结合政务云本身的架构模式解决云平台上“密钥如何管，密码如何用，系统如何建”等问题，实现政务云平台“用上密码、用全密码和用好密码”的三特性进行密码整体应用的设计。对于各种云上服务的调用需求，一方面通过密码计算单元弹性的对资源池化和云样虚拟机化的一些

支持，另一方面通过云密钥的应用面管理系统的一个支持，来实现对政务云以及各种云上应用的云化服务。

**图 21：云平台三特性密码整体应用设计**


*资料来源：网络数据，东兴证券研究所*

## 3.4 云平台密码应用

面向用户提供复杂的是应用密钥管理的时候，本身也要分层次，核心目标是确保这些密钥能够掌握在租户、掌握在用户自己手里，然后从而保障这个平台上的数据、用户业务的数据、租户的应用数据的安全。所以这里面在保护层次上也分了一些不同的层级，包括保护密钥，还有用户的一些主要信息以及业务密钥之间，通过分层保护关系来实施应用密钥的管理和服务。

在云盘的一个加密实践的案例，主要的要点就是通过云上的租户，租户要使用云盘，那么要向云盘系统进行一些认证和递交，同时租户自身对他的云盘上的数据密钥是起到了一个根本的加解密的密钥还原保护的过程。租户来调用相应的虚拟机、密码资源池来实施租户云盘的数据加解密，那么虽然说使用的公共的云盘存储系统，但是上面租户云盘的数据加密和密钥的使用是隔离的。

公司基于卫士通云平台密码应用，开展卫士云安全服务，建立云密码服务的业务模式，结合自身优势，发力云数据安全服务领域，推广以网站防护系列服务为基础的云安全服务。

**图 22：基于云密码的应用建议**


*资料来源：网络数据，东兴证券研究所*

# 4. 卫士通金融数据密码机已启动出口型产品研制及 FIPS 认证工作

## 4.1 海外金融安全值得重视

### 4.1.1 亚太地区金融领域面临网络犯罪挑战

近年来日益普遍的网络攻击所造成的的损失不断上升，亚太地区已经成为恶意网络活动和网络犯罪的突出攻击对象，其中金融领域面临的挑战极为严峻。2015 年，亚洲企业因为网络犯罪造成的损失超过 800 亿美元，远远超过美国和欧洲企业。2016 年，金融行业遭遇的数据泄露最为严重，而且每项被盗记录的损失几乎是其他行业的两倍。一系列针对金融机构的网络攻击凸显了金融领域面临的网络风险，这就要求金融监管机构采取更多措施，保障金融行业的网络安全和网络弹性。

### 4.1.2 我国主要监管机构

中国金融机构的网络安全监管主要由主管银行的中国银行保险监督管理委员会（银保监会）和 2016 年成立的中华人民共和国国家互联网信息办公室（网信办）。

银保监会是 2018 年 4 月机构改革由银行监督管理委员会和保险监督委员会合并新成立的目前中国商业银行最重要的金融监管机构。机构改革之前，银监会主要负责评估风险管理和信息安全控制，截至 2017 年底，银监会开展了 38 个涉及 36 家银行机构的现场检查项目。银行作为重要的信息基础设施，必须执行由《网络安全法》启动的一系列新安全措施，主要包括实施标准的安全控制和公安部、网信办不断加强关键产品和服务的安全审查系统。

此外，中国人民银行虽未明确负责制定和实施与金融机构风险管理有关的条例，但其内部审计和检查制度，要求其对总部和附属机构的信息技术系统进行内部审计和风险评估。目前中国各有关部门如网信办、国家信息安全标准化技术委员会、工业和信息化部等，都在继续积极制定新的指导方针和标准,以完善和深化《网络安全法》下的制度建设。

中国香港地区金融业的网络安全主要由香港金融管理局（金管局）和香港证券及期货事务监察委员会（证监会）监管。自 2014 年开始证监会开始对互联网交易平台进行网络安全审查，伺候相继发布了通告指导和监督互联网交易服务网络安全，对互联网交易从事人员制定基线要求，提高网络安全管理，减轻黑客攻击风险。

#### 4.1.3 关键信息基础设施

银行被列为国家重要的信息基础设施，因此也必须遵守关于安全测试、数据保护和风险分析的严格要求。2017 年实施的《网络安全法》对关键信息基础设施的保护有着重要约束和指导作用，如限制跨境数据传输及对侵入关键网络设备和网络安全服务的安全审查。

《网络安全法》要求所有关键基础设施运营商根据公安部多级保护系统实施安全控制，根据网络对国家安全、经济、社会的重要性，进行不同级别的安全控制。该法律还规定网络运营商必须制定网络安全事件应急预案，向中国安全部门提供技术支持和协助，并要求用户实施实名制。关键信息基础设施的运营商，包括金融机构需要服从网信办关于网络安全的认证、检测、风险评估、系统监测等。

#### 4.1.4 数据保护机制

根据《网络安全法》，经营者有义务在收集用户数据之前征得同意；明确说明所收集数据的使用目的、手段和范围；允许用户更正和修改其个人数据；并在发生数据泄露时向客户发出警告。中国政府发布的《个人信息安全规范》进一步完善了数据保护办法。该规范建立了系列数据收集、使用和传输的最佳实践，提出了对安全控制和入侵后事件响应的应对要求。目前一部单独的个人信息保护法律尚处于立法阶段，至少需要一至三年才能完成，这部法律将会对个人信息保护有更全面的要求。

#### 4.1.5 数据泄露通知

根据 2011 年发布的《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》，规定银行必须在 7 个工作日内向中国人民银行报告违反个人金融信息的行为。《网络安全法》中则要求若发生任何网络安全缺陷、漏洞或不安全事件，网络运营商立即向受影响的用户和相关政府部门报告。2018 年 6 月公安部发布《网络安全等级保护条例（征求意见稿）》要求网络运营商在 24 小时内向当地公安部门及其分支机构报告网络事件。

#### 4.1.6 数据本地化

**《网络安全法》要求关键信息基础设施运营商必须在中国内地储存个人信息和“重要数据”，若需要数据出境，则必须按照网信办的规定进行安全评估。**

2017 年，网信办发布《个人信息和重要数据出境安全评估办法（征求意见稿）》，规定经营者使用的标准，以进行自我评估和确定跨境转让资格；要求经营者对数据类型向监管机构汇报评估。目前，虽然这些规定有利于澄清《网络安全法》的数据本地化规定，但许多措辞含糊，监管机构的自性裁量权较大。

## 4.2 卫士通金融数据密码机已启动 FIPS 认证工作

### 4.2.1 FIPS 认证内容

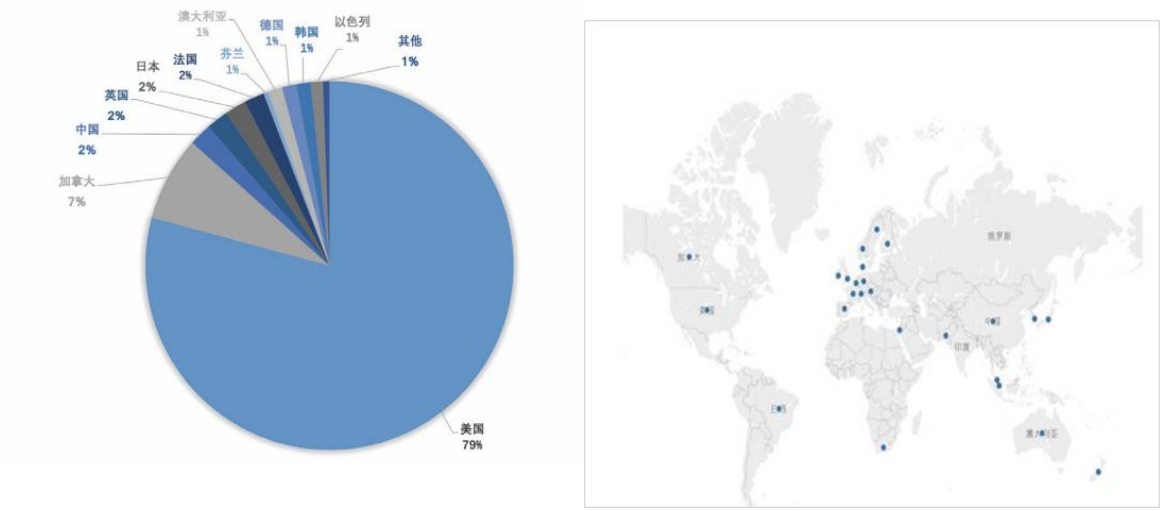
基于美国信息技术管理改革法案（公法 104-106），美国国家标准和技术委员会（NIST）制定针对联邦计算机系统的标准和方针。这些标准和方针由 NIST 发布，并作为联邦信息处理标准（FIPS）在政府机构广泛采用。NIST 针对强制性的联邦政府需求制定 FIPS 标准，比如安全和互操作性，同时针对那些尚未形成可接受的工业标准或解决方案的需求，制定 FIPS 标准。

### 4.2.2 FIPS 认证成为密码产品走向国际市场的必由之路

FIPS 认证作为接受度最为广泛的密码模块安全评估体系，目前世界上很多国家机构的采购和招标要求中也明确的提出，具有密码模块的产品需要满足 FIPS 140 合规要求。FIPS 认证证书是密码产品走向国际市场的通行证，对于有志于开拓国际市场的信息安全产品提供商，FIPS140-2 认证是必须迈过的一道门槛。

### 4.2.3 提交产品认证国家分布

**图 23：提交产品认证国家分布**




*资料来源：网络数据，东兴证券研究所*

上图统计了历史所有通过 FIPS 认证的 3200 多款产品厂商所属的国家和地区，除美国外，还有加拿大、中国、英国、韩国、德国、 法国、新西兰、澳大利亚、比利时、以色列、新加坡、瑞士、英国、芬兰等 20 多个国家和地区的厂商参与认证。其中，美国所占比例最高，达到 79%，加拿大占到 7%，中国、英国、日本、 法国分别占到 2% 左右。

在中国 FIPS 认证匮乏的环境下，卫士通首当其中，成为为数不多的争取 fips 认证的厂商之一，奠定了他数据处理的业界龙头地位。

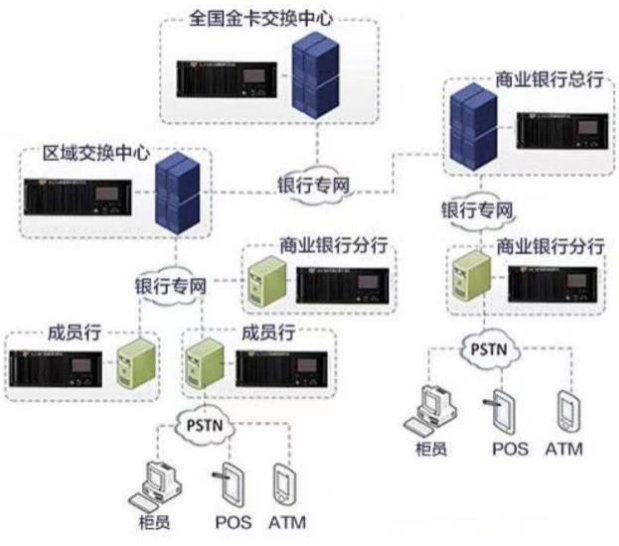
### 4.2.4 卫士通金融密码机

**图 24：卫士通金融数据密码机**


*资料来源：网络数据，东兴证券研究所*

金融数据密码机支持国密算法、符合《金融数据密码机技术规范》，采用自主研发的嵌入式架构、灵活易用的开发接口，同时提供简单、易用的管理维护工具，可广泛应用于金融、社保、电力及公交等行业，为银行卡业务系统、支付系统、社保卡业务、公交卡业务等敏感数据提供基于密码技术的安全保护。

**图 25：金融数据密码机在商业银行数据大集中典型应用部署图**




*资料来源：网络数据，东兴证券研究所*

金融数据密码机在商业银行数据大集中典型应用部署图。各成员行的 ATM、POS、CDM 等自助服务终端均连接到本行的前置主机上，本行的前置主机通过前置系统连接到区域中心的前置主机上。本行代理

他行的交易，以及异地交易，则通过区域中心连接到全国总中心。金融数据密码机作为后台服务器配置在交换中心主机、银行主机等主要网络节点的前置主机后端。金融数据密码机采用 C/S 模式，密码机作为服务器，以命令/响应的方式为前置主机提供安全服务。

目前我国在海外投资众多，相关公司敏感数据回传成为我国信息安全的一部分。特别是随着人民币国际化，以及未来即将推出的数字货币，相关金融数据传输需求快速增长。卫士通推出出口型加密机，有效保障我国海外资产数据安全。

## 投资建议

公司是网络安全国家队，新增电信业务，进军专网运营；安全手机与中国移动合作，受益于等保 2.0 中移动互联网安全需求，且跟随办公信息化国产自主大趋势，相关密码机随之替换，移动政务安全市场也有望打开。公司基于卫士通云平台密码应用，开展卫士云安全服务，建立云密码服务的业务模式，结合自身优势，发力云数据安全服务领域，推广以网站防护系列服务为基础的云安全服务。随着人民币国际化，以及未来即将推出的数字货币，相关金融数据传输需求快速增长。卫士通推出出口型加密机，有效保障我国海外资产数据安全。我们预测公司 2019 年~2021 年净利润分别为 4.23 亿、7.05 亿和 8.93 亿，EPS 分别为 0.50 元、0.84 元和 1.07 元，维持“强烈推荐”评级。

## 风险提示

等保 2.0 推动不达预期，办公信息化国产自主业务不达预期。

## 附表：公司盈利预测表

| 资产负债表 | | | | | 单位:百万元 |
|---|---|---|---|---|---|
| | 2017A | 2018A | 2019E | 2020E | 2021E |
| **流动资产合计** | 4067 | 4409 | 5890 | 8047 | 10887 |
| 货币资金 | 1881 | 1946 | 2631 | 3672 | 5038 |
| 应收账款 | 1616 | 1723 | 2487 | 3471 | 4762 |
| 其他应收款 | 67 | 67 | 97 | 136 | 186 |
| 预付款项 | 68 | 78 | 90 | 106 | 128 |
| 存货 | 211 | 310 | 329 | 444 | 605 |
| 其他流动资产 | 25 | 57 | -75 | -244 | -466 |
| **非流动资产合计** | 1686 | 1811 | 1573 | 1406 | 1240 |
| 长期股权投资 | 27 | 31 | 31 | 31 | 31 |
| 固定资产 | 265.66 | 263.20 | 1279.11 | 1121.02 | 962.93 |
| 无形资产 | 71 | 99 | 89 | 80 | 72 |
| 其他非流动资产 | 55 | 98 | 98 | 98 | 98 |
| **资产总计** | 5754 | 6220 | 7463 | 9453 | 12127 |
| **流动负债合计** | 1309 | 1689 | 2646 | 4163 | 6238 |
| 短期借款 | 0 | 250 | 842 | 2033 | 3017 |
| 应付账款 | 980 | 1042 | 1348 | 1556 | 2483 |
| 预收款项 | 60 | 88 | 128 | 185 | 263 |
| 一年内到期的非流动 | 0 | 0 | 0 | 0 | 0 |
| **非流动负债合计** | 57 | 76 | 76 | 76 | 76 |
| 长期借款 | 0 | 0 | 0 | 0 | 0 |
| 应付债券 | 0 | 0 | 0 | 0 | 0 |
| **负债合计** | 1366 | 1766 | 2722 | 4239 | 6314 |
| 少数股东权益 | 92 | 48 | 52 | 56 | 61 |
| 实收资本（或股本） | 838 | 838 | 838 | 838 | 838 |
| 资本公积 | 2558 | 2591 | 2591 | 2591 | 2591 |
| 未分配利润 | 848 | 923 | 1046 | 1251 | 1509 |
| 归属母公司股东权益 | 4296 | 4407 | 4689 | 5157 | 5752 |
| **负债和所有者权益** | 5754 | 6220 | 7463 | 9453 | 12127 |

| 现金流量表 | | | | | 单位:百万元 |
|---|---|---|---|---|---|
| | 2017A | 2018A | 2019E | 2020E | 2021E |
| **经营活动现金流** | -51 | 33 | 255 | 201 | 906 |
| 净利润 | 177 | 124 | 428 | 709 | 897 |
| 折旧摊销 | 97.30 | 120.56 | 0.00 | 158.09 | 158.09 |
| 财务费用 | -12 | -43 | 10 | 55 | 108 |
| 应付帐款的变化 | 0 | 0 | -765 | -984 | -1291 |
| 预收帐款的变化 | 0 | 0 | 41 | 57 | 78 |
| **投资活动现金流** | -181 | -162 | -9 | -60 | -118 |
| 公允价值变动收益 | 0 | 0 | 0 | 0 | 0 |
| 长期股权投资减少 | 0 | 0 | 0 | 0 | 0 |
| 投资收益 | 2 | -4 | -4 | -4 | -4 |
| **筹资活动现金流** | 1579 | 192 | 441 | 900 | 577 |
| 应付债券增加 | 0 | 0 | 0 | 0 | 0 |
| 长期借款增加 | 0 | 0 | 0 | 0 | 0 |
| 普通股增加 | 406 | 0 | 0 | 0 | 0 |
| 资本公积增加 | 2258 | 33 | 0 | 0 | 0 |
| **现金净增加额** | 1347 | 63 | 686 | 1041 | 1366 |

| 利润表 | | | | | 单位:百万元 |
|---|---|---|---|---|---|
| | 2017A | 2018A | 2019E | 2020E | 2021E |
| **营业收入** | 2137 | 1931 | 2788 | 3891 | 5338 |
| **营业成本** | 1383 | 1255 | 1645 | 2225 | 3031 |
| 营业税金及附加 | 20 | 14 | 24 | 29 | 45 |
| 营业费用 | 215 | 232 | 293 | 389 | 561 |
| 管理费用 | 330 | 143 | 319 | 425 | 573 |
| 财务费用 | -12 | -43 | 10 | 55 | 108 |
| 资产减值损失 | 74.60 | 90.90 | 75.90 | 56.00 | 114.00 |
| 公允价值变动收益 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| 投资净收益 | 1.80 | -3.99 | -3.99 | -3.99 | -3.99 |
| **营业利润** | 153 | 105 | 418 | 708 | 903 |
| 营业外收入 | 50.75 | 23.66 | 23.66 | 23.66 | 23.66 |
| 营业外支出 | 0.74 | 0.57 | 0.57 | 0.57 | 0.57 |
| **利润总额** | 203 | 128 | 441 | 731 | 926 |
| 所得税 | 26 | 4 | 14 | 22 | 28 |
| **净利润** | 177 | 124 | 428 | 709 | 897 |
| 少数股东损益 | 8 | 4 | 4 | 4 | 4 |
| 归属母公司净利润 | 169 | 120 | 423 | 705 | 893 |
| EBITDA | 238 | 183 | 596 | 930 | 1177 |
| **EPS（元）** | 0.21 | 0.14 | 0.50 | 0.84 | 1.07 |

| 主要财务比率 | | | | | |
|---|---|---|---|---|---|
| | 2017A | 2018A | 2019E | 2020E | 2021E |
| **成长能力** | | | | | |
| 营业收入增长 | 18.80% | -9.64% | 44.39% | 39.56% | 37.19% |
| 营业利润增长 | 28.11% | -31.21% | 296.88% | 69.45% | 27.43% |
| 归属于母公司净利 | 8.54% | -28.90% | 252.18% | 66.48% | 26.73% |
| **获利能力** | | | | | |
| 毛利率(%) | 40.99% | 42.83% | 43.22% | 43.22% | 43.22% |
| 净利率(%) | 8.29% | 6.45% | 15.34% | 18.22% | 16.81% |
| 总资产净利润（%） | | | | 2.94% | 1.93% |
| ROE(%) | 3.94% | 2.73% | 9.03% | 13.66% | 15.53% |
| **偿债能力** | | | | | |
| 资产负债率(%) | 24% | 28% | 36% | 45% | 52% |
| 流动比率 | 3.11 | 2.61 | | | |
| 速动比率 | 2.95 | 2.43 | | | |
| **营运能力** | | | | | |
| 总资产周转率 | 0.45 | 0.32 | 0.41 | 0.46 | 0.49 |
| 应收账款周转率 | 2 | 1 | 1 | 1 | 1 |
| 应付账款周转率 | 2.46 | 1.91 | 2.33 | 2.68 | 2.64 |
| **每股指标（元）** | | | | | |
| 每股收益(最新摊 | 0.21 | 0.14 | 0.50 | 0.84 | 1.07 |
| 每股净现金流(最新 | 1.61 | 0.08 | 0.82 | 1.24 | 1.63 |
| 每股净资产(最新摊 | 5.12 | 5.26 | 5.59 | 6.15 | 6.86 |
| **估值比率** | | | | | |
| P/E | 111.24 | 163.60 | 46.46 | 27.91 | 22.02 |
| P/B | 4.58 | 4.46 | 4.19 | 3.81 | 3.42 |
| EV/EBITDA | 74.66 | 98.28 | 30.00 | 19.38 | 15.00 |

*资料来源：公司财报、东兴证券研究所*

# 相关报告汇总

| 报告类型 | 标题 | 日期 |
| --- | --- | --- |
| 行业 | 【东兴军工】买入军工自主可控标的 | 2019-05-28 |
| 公司 | 【东兴机械军工】卫士通焦点问题再探究 | 2019-09-02 |
| 公司 | 【东兴机械军工】卫士通：大力投入布局新业务，电信业务与云安全是亮点 | 2018-08-27 |

*资料来源：东兴证券研究所*

## 分析师简介

**陆洲**

北京大学硕士，军工行业首席分析师。曾任中国证券报记者，历任光大证券、平安证券、国金证券研究所军工行业首席分析师，华商基金研究部工业品研究组组长，2017 年加盟东兴证券研究所。

**王习**

香港理工大学硕士，六年证券从业经验，曾任职于中航证券，长城证券，2017 年加入东兴证券军工组。

**张卓琦**

清华大学工业工程博士，3 年大型国有军工企业运营管理培训、咨询经验，2017 年加盟东兴证券研究所，关注新三板、军工领域。

单击此处输入文字。

## 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。