



强于大市

公司名称	股票代码	股价(人民币)	评级
启明星辰	002439.SZ	26.71	买入↑
深信服	300454.SZ	91.19	增持
紫光股份	000938.SZ	38.78	买入
绿盟科技	300369.SZ	13.20	未有评级
蓝盾股份	300297.SZ	6.68	未有评级

资料来源：万得，中银国际证券
以2019年05月12日当地货币收市价为标准

“演化”系列信息安全专题 报告

等保2.0实施，市场增量几何？

等保2.0近日将推出实施，信息安全将迎重大机会。我们定量测算了短期可体现的市场增量，受云平台、大数据中心和公众服务平台新领域带动，行业或迎2倍（400-600亿）新增空间。对物联网、工控系统等远期市场因素作展望，相比传统安全市场亦有翻番机会。

支撑评级的要点

- 5月9日的2019工业安全大会上相关负责人表示《网络安全等级保护制度2.0》（“等保2.0”）将于5月13日正式出台，覆盖大型互联网企业、基础网络、重要信息系统、网站、大数据中心、云计算平台、物联网系统、移动互联网、工业控制系统、公众服务平台等。
- 云计算平台、大数据中心、公众服务平台等是近年来已普及的新对象，物联网和工业控制系统是处于发展早期的新对象。前者将对信息安全市场带来短期可见的增量空间，通过典型案例分析和梳理的项目体量可对增量空间进行估算。而且围绕网络规模的测算方法可以巧妙实现不同领域下的市场测算。
- 结合相关技术要求和等保1.0经验，我们认为等保2.0对市场的影响过程是：给出指导性框架，厂商根据自身理解推出解决方案，需要满足等保指标。因此，我们拆解了传统等保建设和云等保建设模块，细分到产品层面，并结合产品价格，计算得到云平台为安全市场带来的弹性约100%。基于网路基规模对比，测算出大数据中心产生和公众服务平台各带来弹性50%。整体可见短期市场增量约2倍于传统市场空间，约400~600亿，即网络安全市场整体增长到600~900亿。
- 结合多个第三方数据预测，物联网安全市场空间在2020年左右可达传统安全市场的一倍。工控安全虽然基数较小，但增速达50%，并且在复杂度等方面对产品价值量有提升机会，有助于安全厂商切入电力、能源等领域。

重点推荐

- 我们看好等保2.0实质带动信息安全领域迎来的历史性机会。推荐行业龙头企业启明星辰、深信服和紫光股份，关注绿盟科技、蓝盾股份等。

评级面临的主要风险

- 政策落地与监管不及预期；竞争格局恶化；现金流压力。

相关研究报告

《计算机行业2018年报及2019年一季报综述：减值后弹性势能增加，Q1看到拐点》20190507
《计算机行业周报(4.22-4.27)：板块深度调整后，关注IaaS和SaaS投资机会》20190427

中银国际证券股份有限公司
具备证券投资咨询业务资格

计算机

杨思睿

(8610) 66229321

sirui.yang@bocichina.com

证券投资咨询业务证书编号：S1300518090001



目录

等保 2.0 实施在即，量化测算短期市场增量	4
新对象：云计算平台增量	4
新对象：大数据中心和公众服务平台	8
从早期领域对远期市场增长展望	10
物联网安全：多角度看翻倍空间	10
工控安全：基数小、增速快	11
投资建议：对安全厂商的影响简判	14
哪些厂商受益更多	14
推荐个股	16
风险提示	17



图表目录

图表 1. 等保 2.0 覆盖对象及影响.....	4
图表 2. 《安全管理中心技术要求》将于 2019 年 7 月实施.....	5
图表 3. 安全管理中心模型图.....	5
图表 4. 新华三检察院等保建设方案.....	6
图表 5. 传统等保建设方案.....	6
图表 6. 云等保建设方案.....	6
图表 7. 主要安全产品的价格档次.....	7
图表 8. 云和传统网络安全产品价值量（单位：万元）.....	8
图表 9. 阿里云市占率约 43%.....	9
图表 10. 预计 2022 年全球 IoT 安全市场规模达 188 亿美元.....	10
图表 11. 物联网安全细分领域网络与边缘增速为 14.9%.....	11
图表 12. 物联网安全细分领域网络与边缘增速为 14.9%.....	11
图表 13. 2017 年全球工控信息安全市场产业结构.....	12
图表 14. 亚太地区工控安全市场规模与增速（2015~2020 年）.....	12
图表 15. 中国工控安全市场规模及预测（2014~2019 年，亿元）.....	12
图表 16. 垂直行业工业信息安全投入 CAGR（2015~2020 年）.....	13
图表 17. 云安宝和九州云腾入选 IDC “云安全创新者” 名单.....	14
图表 18. Web 应用安全厂商竞争分析.....	15
图表 19. 绿盟科技投资的安华金和入选 IDC “数据安全创新者” 名单.....	15
附录图表 20. 报告中提及上市公司估值表.....	18

等保 2.0 实施在即，量化测算短期市场增量

5月9日的2019工业安全大会上，公安部十一局七处负责人宣布《网络安全等级保护制度 2.0》（简称“等保 2.0”）将于5月13日正式出台。等保是将我国网络主体（对象）覆盖进入安全保护范畴的制度（条例）。在新版等保制度下，市场空间将如何增长一直是市场关心的重点。

本文旨在定量地预判等保 2.0 的影响，主要方法是分析新覆盖网络对象，结合典型厂商案例，基于我们整理的安全软硬件价格等数据，去系统性的对网络安全市场增量展开估算。

首先，根据上述消息以及前期相关政策内容可知，等保 2.0 的对象囊括了大型互联网企业、基础网络、重要信息系统、网站、大数据中心、云计算平台、物联网系统、移动互联网、工业控制系统、公众服务平台等。我们看到，这里面既包含了已有的老系统，又新覆盖了近年来逐渐普及的新系统，同时还有发展初期的创新型系统，列举如下：

- (1) **老对象**：互联网企业、基础网络、重要信息系统、网站、移动互联网等；
- (2) **较普及的新对象**：云计算平台、大数据中心、公众服务平台等；
- (3) **发展中早期的新对象**：物联网系统、工业控制系统等。

图表 1. 等保 2.0 覆盖对象及影响

类别	网络主体	等保 2.0 影响
老对象	互联网企业、基础网络、重要信息系统、网站、移动互联网等	等保 1.0 主要对象，2.0 将加强主体责任和评测，将安全防护措施补充更新到位
较普及新对象	云计算平台、大数据中心、公众服务平台等	技术较成熟但未被等保 1.0 覆盖，新纳入覆盖并将短期内对安全市场空间产生带动
发展初期新对象	物联网系统、工业控制系统等	渗透率低，安全市场空间主要随对象自身不断成熟而带动，以中远期影响为主

资料来源：Wind，中银国际证券

另外从面向的主体类别角度又可以划分为政府类（ToG）和企业类（ToB），列举如下：

- (1) **政府类**：重要信息系统、公众服务平台、大数据中心；
- (2) **大型企业类**：大型互联网企业、基础网络、云计算平台、大数据中心；
- (3) **一般企业类**：网站、移动互联网、工业控制系统。

相对等保 1.0 在政府类和大型企业类的渗透率较高而言，等保 2.0 有望将各个层级的网络主体在网络安全方面的要求提高到相同高度。

回到对市场增量分析上，可以发现，直接增长点主要来源于较普及新对象，包括云计算平台、公众服务平台和大数据中心等。我们将展开讨论。

新对象：云计算平台增量

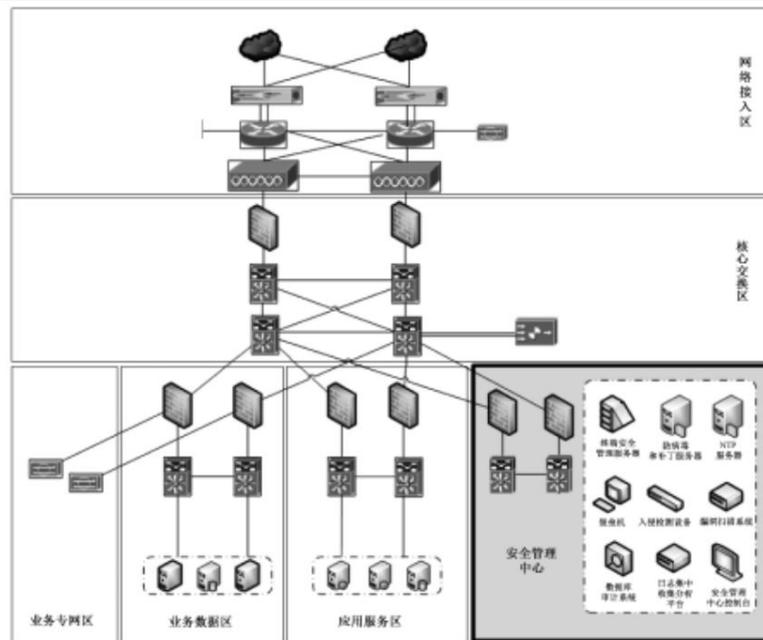
参考等保 1.0 和 2018 年发布的《信息安全技术 网络安全等级保护安全管理中心技术要求》（GB/T 36958-2018，以下简称《安全管理中心技术要求》，如图表 2）等国家标准，考虑安全“攻击”和“防护”处于频繁动态变化等特点，我们预计等保 2.0 不会落实到具体产品层面，而是从防护目标、安全系统功能、考核指标、责权管理、供应商资格等方面给出规范。这意味着，安全厂商可以根据自己的解读去设计架构，为客户提供解决方案，并最终满足等保 2.0 要求。

图表 2. 《安全管理中心技术要求》将于 2019 年 7 月实施



资料来源：市场监督管理总局、国标管理委员会，中银国际证券

图表 3. 安全管理中心模型图



资料来源：《安全管理中心技术要求》2018，中银国际证券

云计算平台是等保 2.0 新覆盖的一个重要网络主体，因为近年来云计算已经在国内得到显著的发展。阿里云、腾讯云、华为云、三大运营商等建设的云基础设施节点数快速增长，涉及的网络企业、终端设备等也数十万、数百万的增加。所以我们首先分析云平台在等保 2.0 条例实施后带动的市场增量。2019 年 4 月 19 日，由紫光集团和新华三集团主办的 2019 Navigate 领航者峰会上，我们看到新华三展示的检察院等保建设方案（传统与云平台对比，如图表 4）。

从右图可以看出，H3C 给出的方案与《安全管理中心技术要求》中核心交换区、网络接入区、业务数据区、应用服务区、业务专网区和安全管理中心的模型基本符合。因此，可以认为这是一种典型的解决方案，我们将以此为案例进行分析。

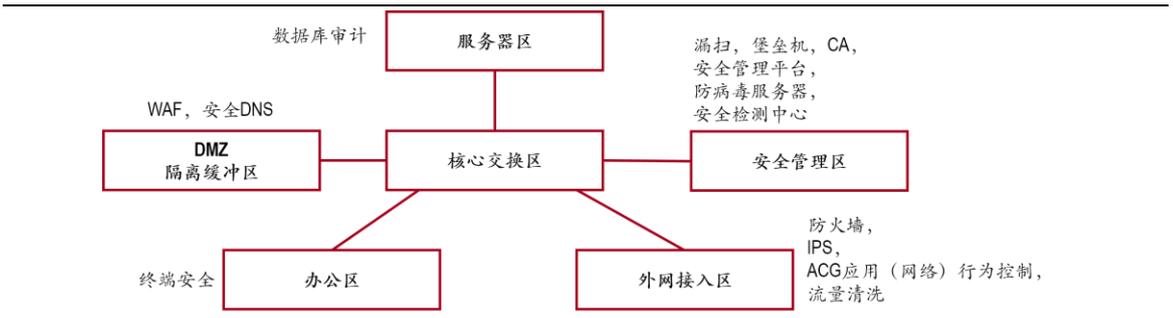
图表 4. 新华三检察院等保建设方案



资料来源: H3C, 中银国际证券

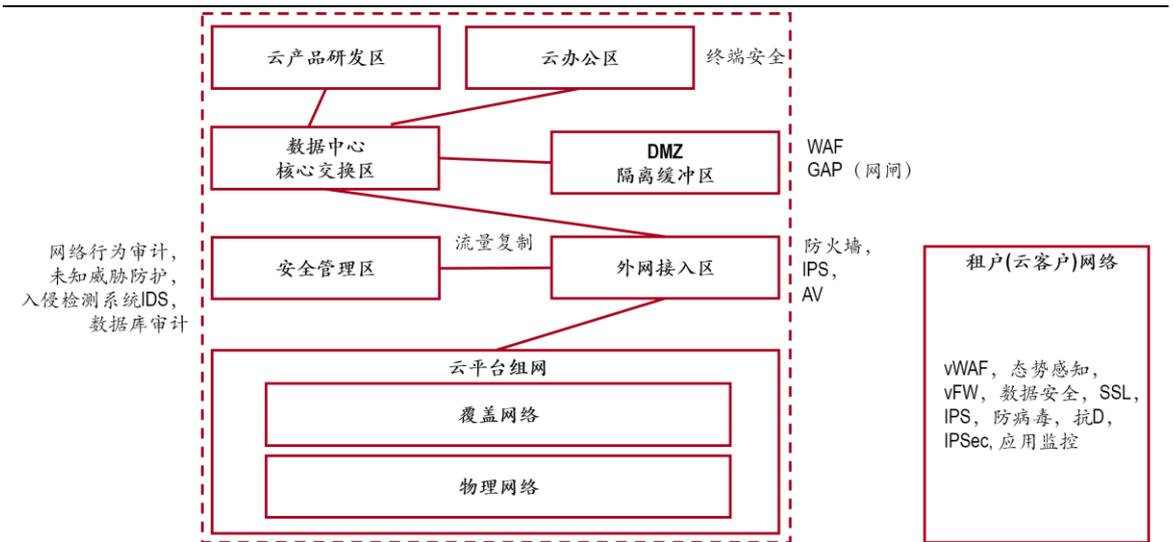
我们将 H3C 的解决方案模块化成图表 5 (传统) 和图表 6 (云), 模块旁边列出相关的安全产品需求。对比两图可以看到, 一个企业在传统网络中需要自由服务器区, 在云网络中成为一个租户, 即每个租户网络对应原传统网络 (剔除服务器部分)。这会导致两个变化: (1) 云平台产生大量新的安全产品需求, 体量远超传统网络; (2) 租户网络是基于虚拟机的, 安全由硬件形态变为软件形态 (如 vWAF、vFW 等), 以及原有软件安全模块 (如防病毒、数据安全等)。

图表 5. 传统等保建设方案



资料来源: H3C, 中银国际证券

图表 6. 云等保建设方案



资料来源: H3C, 中银国际证券

注: H3C 方案中 SLB、LLB、vSwitch、Spine 等部分产品更靠近网络基础产品, 故未列入安全类



那么如何趋势性的理解云对安全市场增长的影响呢？

1. 首先，安全产品市场是和网络规模成正比的，所以我们可以看两种情况下网络规模的大小。如果 1000 个企业从传统网络迁移到云，由于资源利用效率提高，所以云端建立的网络规模要低于原来的 1000 个传统网络之和。例如，资源利用率若提升 50%，则网络规模可缩小 1/3。

但是为了提供可靠性和高弹性，云平台在安全可靠方面的投入是**数倍甚至数十倍于**普通企业的。考虑到我国企业市场安全投入极低（仅占 1-2% 的 IT 投入），即使一些中大型企业，如果不是对网络安全很重视，也不会会在企业网络中部署图表 5 中的完备方案。因此云模式下，安全投入的提升远超出（至少是抵消）网络规模变化的影响。

2. 另外一个重要的因素是，中小企业一般是没有系统性传统网络架构的。云平台降低了传统企业采用 IT 系统的门槛，中小企业上云将显著扩大网络规模。

由于本文主要考察等保 2.0 中短期内带动的市场增量，所以我们主要考虑第一个因素。**在这种情况下，对市场增量的定量分析可以简化为新增产品价值量的分析。**

根据采招网梳理的数据，我们对两个系统中涉及的安全产品价格进行了划分。主要分为三档：高档（几十万至几百万）、中档（十万至几十万）和低档（几千至几万）。各类产品的价格划分见图表 7。

图表 7. 主要安全产品的价格档次

产品	价格档次
防火墙	中
IPS	中
AV 防病毒	低
WAF	中
GAP 网闸	中
网络行为审计	高
未知威胁防护/UTM	高
入侵检测 IDS	中
数据库审计	中
vWAF	低
态势感知	高
vOA	低
vFW	低
数据安全	高
抗 D	低
IPSec/SSL/VPN	中
应用监控	中
终端安全/安全准入	中
漏扫	中
堡垒机	低
CA	低
安全管理平台	中
安全检测中心	高
ACG 应用控制网关	中
安全 DNS	中
流量清洗	中
流量复制	中

资料来源：Wind，中银国际证券

我们在以下计算中给出三档的价格为 200 万、50 万和 2 万元。需注意的是由于安全产品规格众多，分档和价格数据不代表实际项目中的量级。由于计算的方法是统计两种模式下的市场空间比例，所以给出的价格只要有一定代表性、档次差别明显即可。



同时也不考虑设备数量的差别，实际上在不少采购项目中这些设备的数量级是一致的。即如果需要 1 台 A 设备和 5 台 B 设备，其实可采购 1 台 A 设备和 1 台高端型号的 B 设备，以减少网络复杂性和 IT 运维难度。

图表 8. 云和传统网络安全产品价值量（单位：万元）

模式	产品	价格	模式	产品	价格
传统	防火墙	50	云	终端安全	50
	IPS	50		WAF	50
	ACG	2		GAP 网闸	50
	WAF	50		防火墙	50
	流量清洗	50		IPS (x2) *	100
	漏扫	50		AV 防病毒 (x2)	4
	堡垒机	2		流量复制	50
	CA	2		网络行为审计	200
	安全管理平台	50		未知威胁防护	200
	防病毒服务器	2		IDS 入侵检测系统	50
	安全检测中心	200		数据库审计	50
	数据库审计	50		vWAF	2
	WAF	50		vFW	2
	安全 DNS	50		态势感知	200
	终端安全	50		数据安全	200
	合计	708		IPSec/SSL/VPN	50
				抗 D	2
		应用监控	50		
		合计	1360		

资料来源：Wind，中银国际证券

注：* IPS 和防病毒在云平台端和租户端均有需要

图表 8 给出了计算结果。传统模式和云模式下的网络安全规模分别为 708 万和 1360 万。而租户安全约占云安全投入的 1/3。由此可见，等保 2.0 将云计算平台纳入后可将市场空间提升约 92%，存在翻倍增长的机会。

新对象：大数据中心和公众服务平台

大数据中心

我们再考虑大数据中心带来的市场增量，这里主要讨论各地大数据局和大数据中心的建设情况（企业大数据中心一般与云平台建设重叠已计入前文估计）。

根据政府工作网站、凤凰财经、新京报等报道，2018 年以来各省份陆续实施机构改革，多地因地制宜推出了各具特色的“自选动作”，其中“大数据局”最为抢眼。贵州、重庆、福建、广东、吉林、广西等 8 省份方案均明确提出组建专门机构，负责人工智能、云计算、大数据管理、信息化、智慧城市建设和等方面工作。在北京，东城、朝阳、丰台、延庆等区则在科技和信息化局加挂了大数据（管理）局的牌子。

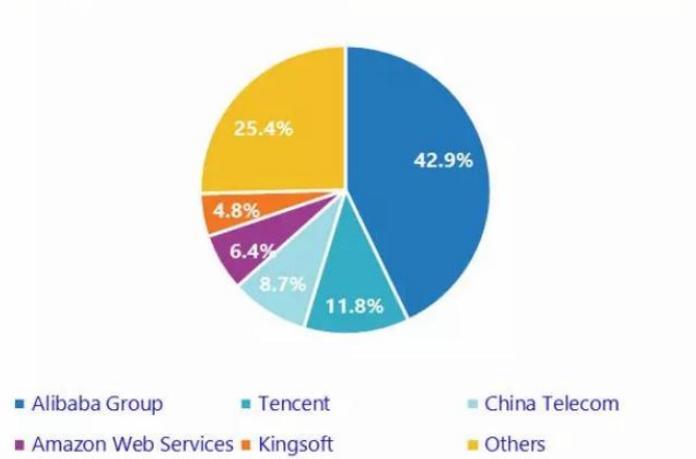
以下同样从网络规模的角度，对比大数据中心和云平台的网络规模比例，进行安全市场增量的估算。

根据阿里云云栖社区 2019 年 1 月数据，阿里云在中国大陆设有 7 个地区级节点，下设 42 个可用区，覆盖了 34 个省级区域。而国家大数据中心设有 8 个地区节点，预计未来可覆盖中国大部分省级区域。因此，可以认为随着国家大数据中心建设持续，节点规模将与阿里云平台规模接近。

而从 IDC 的数据来看，阿里云占国内公有云市场份额的 43%。考虑到阿里云同样在私有云（如城市智慧大脑）领域积极布局，我们认为其占整体云市场的份额相当。由此估计，大数据中心带来的增量有望接近 50%。

图表 9. 阿里云市占率约 43%

2018 下半年前五大中国公有云 IaaS 厂商市场份额占比



资料来源: IDC, 中银国际证券

公众服务平台（如政务云、一网通办等）系统一般建立在云和大数据基础设施上，主要是在应用层面增加了安全需求，类似于租户和云平台关系（即平台投入的 1/3）。由于前两者产生的增量是 150%，因此预计公众服务平台对安全市场的增量为 50%。

综合以上，云计算平台、大数据中心和公众服务平台等较普及系统在等保 2.0 时代将产生约 2 倍的市场空间增量。按传统安全市场 200~300 亿计算，即 400~600 亿规模。

从早期领域对远期市场增长展望

物联网和工控系统的长期发展将对远期网络安全市场进一步提升起到积极作用。首先，两者都增加了网络规模；其次，两者在数据量、实时性等方面都将增加安全产品的复杂性。本章对这两个细分领域的规模和增量进行展望。

物联网安全：多角度看翻倍空间

根据 MarketsandMarkets 预测，2020 年全球物联网的安全市场将从 2015 年的 68.9 亿美元增长至 289 亿美元，而 2015-2020 年的复合年增长率为 33.2%。IDC 对 2020 年物联网安全市场规模预测为 121 亿美元，未来几年 CAGR 为 10.2%。取两个预测的中位数约 205 亿美元（约合人民币 1,400 亿元），按中国市场占 10-20% 假设，则对应 140-280 亿元。

图表 10. 预计 2022 年全球 IoT 安全市场规模达 188 亿美元

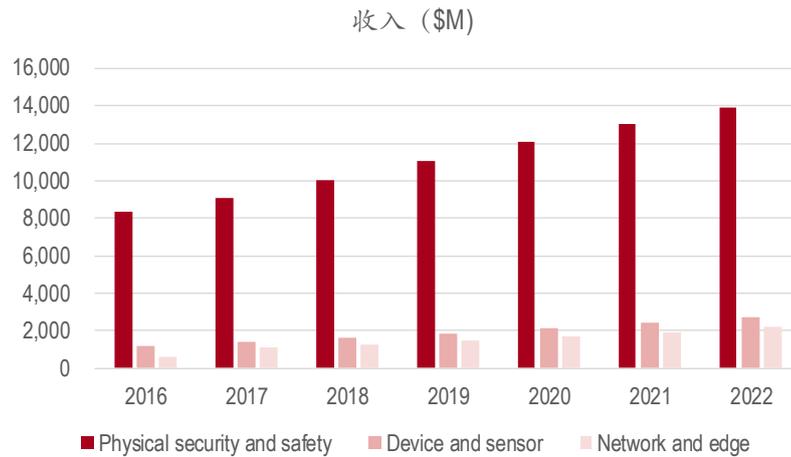


资料来源：IDC，中银国际证券

根据 2017 年 1 月工信部发布的《物联网“十三五”规划》，预计到 2020 年，我国物联网产业市场规模将超过 1.5 万亿元。按 1-2% 的安全投入占比估算，对应物联网安全市场 150-300 亿市场。与上述结论接近。是传统安全市场规模的一倍。

边缘计算。边缘计算与云计算体量相当，边缘服务器市场规模可超万亿。根据 IDC 预测，2020 年将有超过 50% 的数据需要在网络边缘侧分析、处理与存储，意味着边缘和云端的算力需求体量相当，边缘计算成为云计算体量相当的新兴市场。由此估计，边缘计算将导致云相关的安全市场体量翻倍。而且，IDC 给出的 IoT 安全增速中，网络与边缘的复合增速 (14.9%) 要高于整体增速 (10.2%) 约 4.7pct。

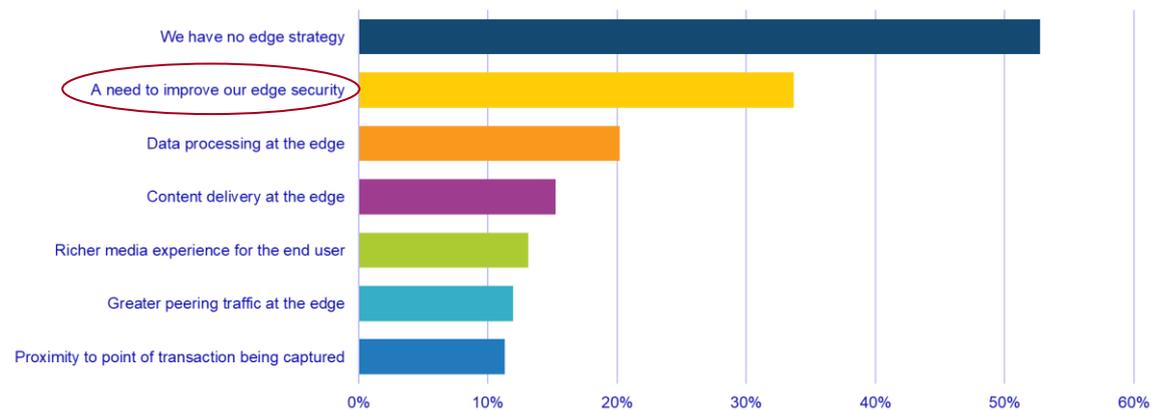
图表 11. 物联网安全细分领域网络与边缘增速为 14.9%



资料来源: IDC, 中银国际证券

通过 IDC 在 2018 年对 1,102 家企业的调查来看, 企业在考虑边缘计算技术时最大的关注也是安全, 成为已有边缘计算 IT 战略的企业中最主要的影响因素。

图表 12. 物联网安全细分领域网络与边缘增速为 14.9%



资料来源: IDC, 中银国际证券

工控安全: 基数小、增速快

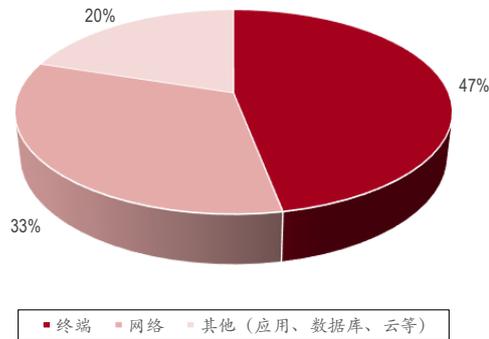
2018 年 5 月, 工业信息安全产业发展联盟发布的《中国工业信息安全产业发展白皮书》(以下简称“白皮书”) 提到 2017 年我国工业信息安全市场规模同比增长 53.6%。其中, 以工业防火墙、工业网络隔离设备、应用白名单为代表的防护类产品市场规模达 2.47 亿元, 占总额的 44%。该数据一方面显示当前工控安全市场体量较小, 另一方面也表明行业进入快车道。

另外, 和网络安全不一样的是, 网络安全以研究 TCP/IP 通信协议为主, 工控安全需要研究工业设备的传输协议, 包括 ICS、DCS、PLC 等控制系统。而且工控系统特别强调业务的连续性, 例如电厂停机造成的损失严重, 而传统网络安全可以允许短时间的网络中断。因此, 工控安全产品的价值量可能更高。

实际上, 工业控制在制造业先进国家带动的安全需求已经比较明显。根据白皮书引用 Markets and Markets 的数据, 2017 年全球工业信息安全市场规模达 138.1 亿美元, 预计在 2023 年增长至 227.9 亿美元, 年复合增速达 8.6%。其中, 工业控制系统信息安全市场规模为 102.4 亿美元, 预计年复合增速为 6.3%。

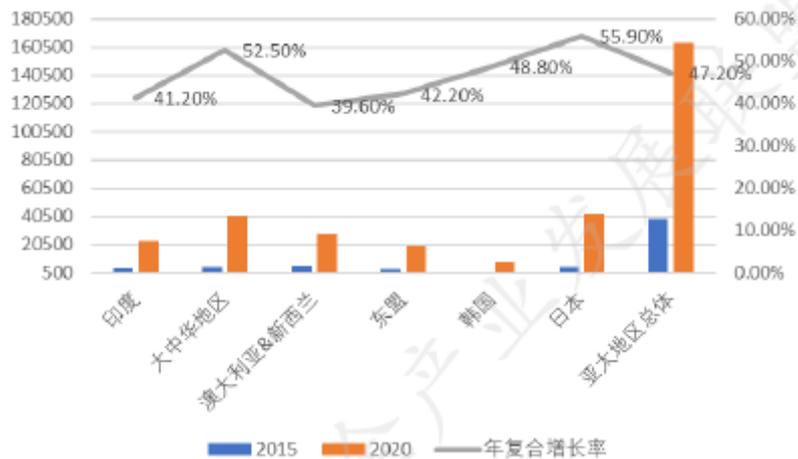
由于网络在工控信息安全市场中约占 1/3 (如图表 14)，因此虽然工业领域在对网络规模的带动之外，还有比较明显的终端和其他领域信息安全的带动。

图表 13. 2017 年全球工控信息安全市场产业结构



资料来源: Markets and Markets, 中银国际证券

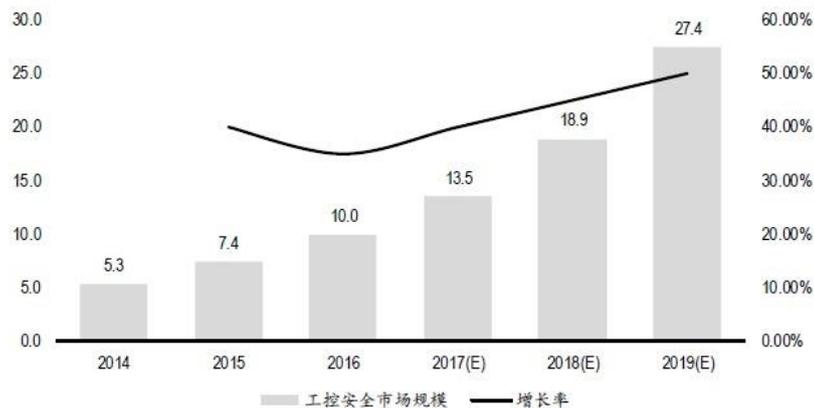
图表 14. 亚太地区工控安全市场规模与增速 (2015~2020 年)



资料来源: Frost & Sullivan, 中银国际证券

Frost & Sullivan 机构预测亚太地区整体工控安全市场规模将从 2015 年的 3.84 亿美元增长到 16.3 亿美元 (约合人民币 109 亿元)，涨幅超 4 倍。其中，大中华地区 (Greater China) 的 CAGR 可达 50%。

图表 15. 中国工控安全市场规模及预测 (2014~2019 年, 亿元)

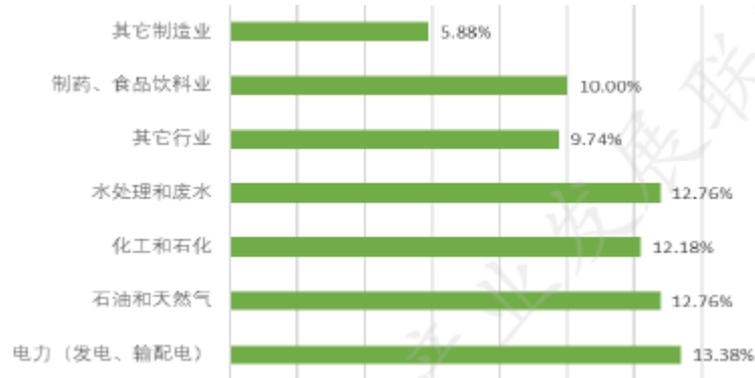


资料来源: 立鼎产业研究中心, 中银国际证券



根据立鼎产业研究中心的预测,2019年中国工控安全市场为27.4亿元,同比增长约50%。与Frost & Sullivan的预测较为一致。

图表 16. 垂直行业工业信息安全投入 CAGR (2015~2020 年)



资料来源: ARC, 中银国际证券

在下游细分行业方面,工控安全增长较快的是电力、水处理和能源领域。

综合以上,物联网对象有望在2020年之后为安全市场带来翻倍增量,工控系统则以复杂度和高增速为安全厂商带来远期机会。

投资建议：对安全厂商的影响简判

哪些厂商受益更多

等保 2.0 落地实施之后，主要的安全厂商都将受益于行业的景气度提升。实际上，在现有格局下，安全厂商的竞争面已经比较广，或许等保 2.0 可以略为部分厂商带来倾向性优势。所以，我们按照云安全、大数据中心（数据安全）和公众服务平台安全优先、传统安全与物联网、工控安全次之的思路，对安全厂商的受益程度进行简单讨论。

云安全

一方面，作为新兴业务领域，传统安全厂商在云安全的布局更多侧重于私有云。在公有云市场，往往依赖云平台厂商（阿里云、腾讯云等）及生态伙伴和创新公司来实现。因此在创新企业存在布局的传统安全厂商将更有机会把握云安全的市场机会。

绿盟科技投资的九州龙腾和任子行投资的云安宝入选了 IDC 评选的 2018 云安全创新者 (IDC Innovators) 名单。

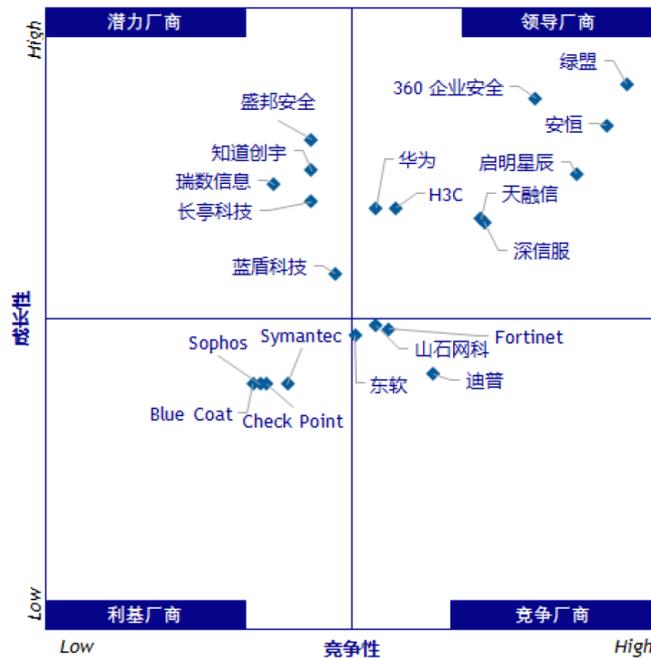
图表 17. 云安宝和九州云腾入选 IDC “云安全创新者” 名单

IDC Innovators		IDC 创新者是年营业额低于\$100M、有创新性技术或突破性商业模式的新兴厂商。	
云安全			
公司名称	创立时间	总部	
青藤云安全	2014	北京, 中国	
云安宝	2014	深圳, 中国	
九州云腾	2014	北京, 中国	
知道创宇	2007	北京, 中国	
蔷薇灵动	2017	北京, 中国	

资料来源：IDC 中国(2018)，中银国际证券

云安全领域的 Web 应用安全方面，IDC 分析了相关厂商的竞争力，选举了领导厂商和潜力厂商等。绿盟科技、启明星辰、天融信（南洋股份）、深信服、H3C（紫光股份）等上市公司以及华为、360 企业安全（现为奇安信）、安恒等未上市公司进入了领导厂商象限，蓝盾股份入选了潜力厂商象限。

图表 18. Web 应用安全厂商竞争分析



资料来源: IDC, 中银国际证券

领导厂商在产品技术领先性、客户需求匹配度方面达到较高水平。例如, IDC 表示绿盟科技推出 Web 应用安全相关的硬件、虚拟化软件、SaaS 模式的解决方案。在云端训练基于机器学习的智能检测引擎, 降低误报、漏报率, 在市场竞争性及成长性方面表现良好; 奇安信在 Web 应用安全解决方案方面的大量投入, 提供网站可用性监控、挂马发现、钓鱼网站、网页篡改、暗链发现、漏洞发现、敏感信息等安全服务。

数据安全

在数据安全方面, 绿盟科技投资的安华金和也入选了 IDC 评选的 2018 年数据安全创新者名单。而启明星辰收购的书生电子也在安全文档等领域切入数据安全。

图表 19. 绿盟科技投资的安华金和入选 IDC “数据安全创新者” 名单

IDC Innovators		IDC 创新者是年营业额低于\$100M、有创新性技术或突破性商业模式的新兴厂商。	
数据安全			
公司名称:	创立时间:	总部:	
安华金和	2009	北京, 中国	
美创科技	2005	杭州, 中国	
世平信息	2010	杭州, 中国	
昂楷科技	2009	深圳, 中国	
炼石网络	2015	北京, 中国	

资料来源: IDC 中国(2018), 中银国际证券

当然, 根据图表 5、图表 6 可知, 在等保 2.0 时期传统安全产品线仍然是主要组成部分, 因此产品线较全或份额领先的厂商仍然会有更大机会拿下新增市场的蛋糕。



推荐个股

我们看好等保 2.0 实质带动信息安全领域迎来的历史性机会。推荐行业龙头企业**启明星辰**、**深信服**和**紫光股份**，关注**绿盟科技**、**蓝盾股份**等。



风险提示

- 1、政策落地与监管不及预期：**等保 2.0 政策实际推出和强制性等如果低于预期，将使得企业等下游市场渗透率低于预期。
- 2、竞争格局恶化：**明确指引后，厂商可能在细分领域同质化竞争，导致产品毛利率等指标下滑，影响收入和利润。
- 3、现金流压力：**政府等客户结算周期较长，对厂商现金流有所影响。特别是安全运营等业务，需要厂商先行投产，现金流压力可能会影响到业务的扩展性。



附录图表 20. 报告中提及上市公司估值表

公司代码	公司简称	评级	股价 (元)	市值 (亿元)	每股收益(元/股)		市盈率(x)	
					2018A	2019E	2018A	2019E
002439.SZ	启明星辰	买入	26.71	240	0.64	0.82	42	33
300454.SZ	深信服	增持	91.19	368	1.50	1.83	61	50
000938.SZ	紫光股份	买入	38.78	566	1.17	1.59	33	24
300369.SZ	绿盟科技	未有评级	13.20	106	0.21	0.30	63	43
300297.SZ	蓝盾股份	未有评级	6.68	83	0.32	0.40	21	14

资料来源: 万得, 中银国际证券

注: 股价截止日 5 月 10 日, 未有评级公司盈利预测来自万得一致预期

披露声明

本报告准确表述了证券分析师的个人观点。该证券分析师声明，本人未在公司内、外部机构兼任有损本人独立性与客观性的其他职务，没有担任本报告评论的上市公司的董事、监事或高级管理人员；也不拥有与该上市公司有关的任何财务权益；本报告评论的上市公司或其它第三方都没有或没有承诺向本人提供与本报告有关的任何补偿或其它利益。

中银国际证券股份有限公司同时声明，将通过公司网站披露本公司授权公众媒体及其他机构刊载或者转发证券研究报告有关情况。如有投资者于未经授权的公众媒体看到或从其他机构获得本研究报告的，请慎重使用所获得的研究报告，以防止被误导，中银国际证券股份有限公司不对其报告理解和使用承担任何责任。

评级体系说明

以报告发布日后公司股价/行业指数涨跌幅相对同期相关市场指数的涨跌幅的表现为基准：

公司投资评级：

- 买入：预计该公司在未来 6 个月内超越基准指数 20%以上；
- 增持：预计该公司在未来 6 个月内超越基准指数 10%-20%；
- 中性：预计该公司股价在未来 6 个月内相对基准指数变动幅度在-10%-10%之间；
- 减持：预计该公司股价在未来 6 个月内相对基准指数跌幅在 10%以上；
- 未有评级：因无法获取必要的资料或者其他原因，未能给出明确的投资评级。

行业投资评级：

- 强于大市：预计该行业指数在未来 6 个月内表现强于基准指数；
- 中性：预计该行业指数在未来 6 个月内表现基本与基准指数持平；
- 弱于大市：预计该行业指数在未来 6 个月内表现弱于基准指数。
- 未有评级：因无法获取必要的资料或者其他原因，未能给出明确的投资评级。

沪深市场基准指数为沪深 300 指数；新三板市场基准指数为三板成指或三板做市指数；香港市场基准指数为恒生指数或恒生中国企业指数；美股市场基准指数为纳斯达克综合指数或标普 500 指数。

风险提示及免责声明

本报告由中银国际证券股份有限公司证券分析师撰写并向特定客户发布。

本报告发布的特定客户包括：1) 基金、保险、QFII、QDII 等能够充分理解证券研究报告，具备专业信息处理能力的中银国际证券股份有限公司的机构客户；2) 中银国际证券股份有限公司的证券投资顾问服务团队，其可参考使用本报告。中银国际证券股份有限公司的证券投资顾问服务团队可能以本报告为基础，整合形成证券投资顾问服务建议或产品，提供给接受其证券投资顾问服务的客户。

中银国际证券股份有限公司不以任何方式或渠道向除上述特定客户外的公司个人客户提供本报告。中银国际证券股份有限公司的个人客户从任何外部渠道获得本报告的，亦不应直接依据所获得的研究报告作出投资决策；需充分咨询证券投资顾问意见，独立作出投资决策。中银国际证券股份有限公司不承担由此产生的任何责任及损失等。

本报告内含保密信息，仅供收件人使用。阁下作为收件人，不得出于任何目的直接或间接复制、派发或转发此报告全部或部分内容予任何其他人士，或将此报告全部或部分公开发表。如发现本研究报告被私自刊载或转发的，中银国际证券股份有限公司将及时采取维权措施，追究有关媒体或者机构的责任。所有本报告内使用的商标、服务标记及标记均为中银国际证券股份有限公司或其附属及关联公司（统称“中银国际集团”）的商标、服务标记、注册商标或注册服务标记。

本报告及其所载的任何信息、材料或内容只提供给阁下作参考之用，并未考虑到任何特别的投资目的、财务状况或特殊需要，不能成为或被视为出售或购买或认购证券或其它金融票据的要约或邀请，亦不构成任何合约或承诺的基础。中银国际证券股份有限公司不能确保本报告中提及的投资产品适合任何特定投资者。本报告的内容不构成对任何人的投资建议，阁下不会因为收到本报告而成为中银国际集团的客户。阁下收到或阅读本报告须在承诺购买任何报告中所指之投资产品之前，就该投资产品的适合性，包括阁下的特殊投资目的、财务状况及其特别需要寻求阁下相关投资顾问的意见。

尽管本报告所载资料的来源及观点都是中银国际证券股份有限公司及其证券分析师从相信可靠的来源取得或达到，但撰写本报告的证券分析师或中银国际集团的任何成员及其董事、高管、员工或其他任何个人（包括其关联方）都不能保证它们的准确性或完整性。除非法律或规则规定必须承担的责任外，中银国际集团任何成员不对使用本报告的材料而引致的损失负任何责任。本报告对其中所包含的或讨论的信息或意见的准确性、完整性或公平性不作任何明示或暗示的声明或保证。阁下不应单纯依靠本报告而取代个人的独立判断。本报告仅反映证券分析师在撰写本报告时的设想、见解及分析方法。中银国际集团成员可发布其它与本报告所载资料不一致及有不同结论的报告，亦有可能采取与本报告观点不同的投资策略。为免生疑问，本报告所载的观点并不代表中银国际集团成员的立场。

本报告可能附载其它网站的地址或超级链接。对于本报告可能涉及到中银国际集团本身网站以外的资料，中银国际集团未有参阅有关网站，也不对它们的内容负责。提供这些地址或超级链接（包括连接到中银国际集团网站的地址及超级链接）的目的，纯粹为了阁下的方便及参考，连结网站的内容不构成本报告的任何部份。阁下须承担浏览这些网站的风险。

本报告所载的资料、意见及推测仅基于现状，不构成任何保证，可随时更改，毋须提前通知。本报告不构成投资、法律、会计或税务建议或保证任何投资或策略适用于阁下个别情况。本报告不能作为阁下私人投资的建议。

过往的表现不能被视作将来表现的指示或保证，也不能代表或对将来表现做出任何明示或暗示的保障。本报告所载的资料、意见及预测只是反映证券分析师在本报告所载日期的判断，可随时更改。本报告中涉及证券或金融工具的价格、价值及收入可能出现上升或下跌。

部分投资可能不会轻易变现，可能在出售或变现投资时存在难度。同样，阁下获得有关投资的价值或风险的可靠信息也存在困难。本报告中包含或涉及的投资及服务可能未必适合阁下。如上所述，阁下须在做出任何投资决策之前，包括买卖本报告涉及的任何证券，寻求阁下相关投资顾问的意见。

中银国际证券股份有限公司及其附属及关联公司版权所有。保留一切权利。

中银国际证券股份有限公司

中国上海浦东
银城中路 200 号
中银大厦 39 楼
邮编 200121
电话: (8621) 6860 4866
传真: (8621) 5888 3554

相关关联机构:

中银国际研究有限公司

香港花园道一号
中银大厦二十楼
电话: (852) 3988 6333
致电香港免费电话:
中国网通 10 省市客户请拨打: 10800 8521065
中国电信 21 省市客户请拨打: 10800 1521065
新加坡客户请拨打: 800 852 3392
传真: (852) 2147 9513

中银国际证券有限公司

香港花园道一号
中银大厦二十楼
电话: (852) 3988 6333
传真: (852) 2147 9513

中银国际控股有限公司北京代表处

中国北京市西城区
西单北大街 110 号 8 层
邮编: 100032
电话: (8610) 8326 2000
传真: (8610) 8326 2291

中银国际(英国)有限公司

2/F, 1 Lothbury
London EC2R 7DB
United Kingdom
电话: (4420) 3651 8888
传真: (4420) 3651 8877

中银国际(美国)有限公司

美国纽约市美国大道 1045 号
7 Bryant Park 15 楼
NY 10018
电话: (1) 212 259 0888
传真: (1) 212 259 0889

中银国际(新加坡)有限公司

注册编号 199303046Z
新加坡百得利路四号
中国银行大厦四楼(049908)
电话: (65) 6692 6829 / 6534 5587
传真: (65) 6534 3996 / 6532 3371