中信建投证券
CHINA SECURITIES

证券研究报告•行业深度研究

信息安全行业变革下投资机遇

分析师：石泽蕤
shizerui@csc.com.cn
18616092669
执业证书编号：S1440517030001

发布日期：2019年1月10日

总体判断

- 政策、新需求、新技术促进下，信息安全占IT支出比例有望达到5%以上
- 网络安全法中明确关键信息基础设施范围，未来城市轨道交通网络安全、工业控制安全市场潜力巨大
- “云大物移”等新场景和新技术促进信息安全防护理念变化
- 构建完善的企业安全需要高中低三位一体能力，目前高位和中位能力较为稀缺
- 网络安全服务市场迅速增长，未来安全服务市场占比将逐步提升

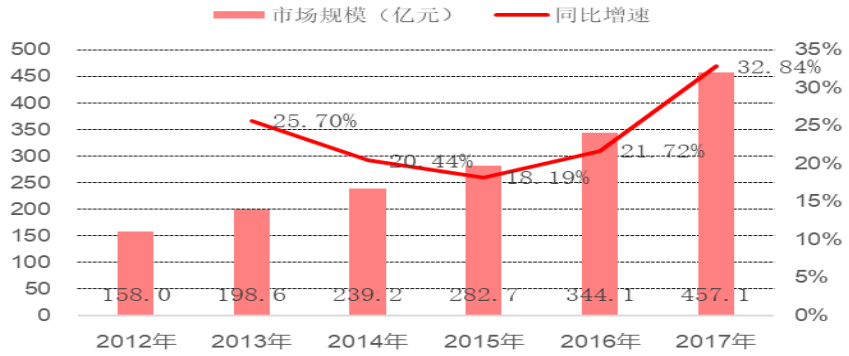
提纲

- 2015年以前中国信息安全市场受到等保标准与合规驱动，市场发展平稳，网络安全占IT开支比例不足2%
- 网络安全威胁事件频发，没有网络安全就没有国家安全，国家对网络安全重视程度进一步提高
- 网络空间战日益成为大国战略博弈的新战场，加强网络安全能力建设和投入才能匹配我国的大国地位
- 政策、新需求、新技术促进下，信息安全占IT支出比例有望达到5%以上
- 政府监管和处罚力度加大，政企合规性采购需求增加
- 网络安全法中明确关键信息基础设施范围，未来城市轨道交通网络安全、工业控制安全市场潜力巨大
- “云大物移”等新场景和新技术促进信息安全防护理念变化
- 云计算发展带动云安全需求增长，网络安全市场增长迅速
- 物联网连接数快速发展，安全成为首要考虑问题
- 新监管需求、新技术、新场景驱动安全新产品快速发展，主动防御产品增长速度更快
- 构建完善的企业安全需要高中低三位一体能力，目前高位和中位能力较为稀缺
- 中高位信息安全产品举例:态势感知平台
- 中高位信息安全产品举例：威胁情报
- 攻防博弈带来大数据、AI等新技术在安全中的应用创新
- 网络安全服务市场迅速增长，未来安全服务市场占比将逐步提升
- 企业安全市场竞争格局近年发生较大变化：互联网、云计算巨头入局
- 私有云解决方案提供商安全业务增长迅速，市占率逐步提升
- 具备“高中低”三位一体能力的信息安全龙头公司-360企业安全增长迅速
- 信息安全细分领域众多，小而美的细分领域龙头也值得关注

1. 2015年以前中国信息安全市场受到等保标准与合规驱动，市场发展平稳，网络安全占IT开支比例不足2%

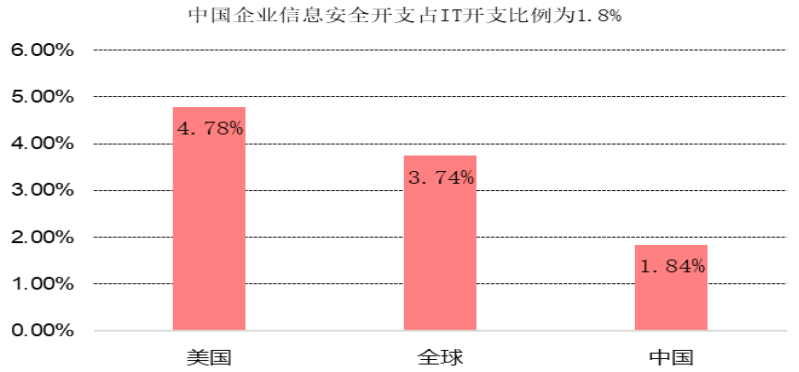
- 信息安全等级保护是我国信息安全保障的一项基本制度，是国家通过制定统一的信息安全等级保护管理规范和技术标准，对国家重要信息、法人和其他组织及公民的专有信息以及公开信息在存储、传输、处理信息时分等级实行安全保护；对信息系统中使用的信息安全产品实行按等级管理；对信息系统中发生的信息安全事件分等级响应、处置。
- 2008年等保1.0正式发布实施。过去中国的网络安全市场增长主要依赖等保监管标准提升、覆盖范围扩大，政府机关、企业按照等保要求部署相应的网络安全设备和系统，因此市场增速较为平稳，网络安全占IT开支比例不足2%。

图：2017年中国网络安全市场规模达到457亿元，同比32%增长



数据来源：中国产业信息网，中信建投研究发展部

图：2015年以前信息安全市场受到国家等保标准和合规驱动，增长平稳，中国信息安全投入占IT开支比例不足2%



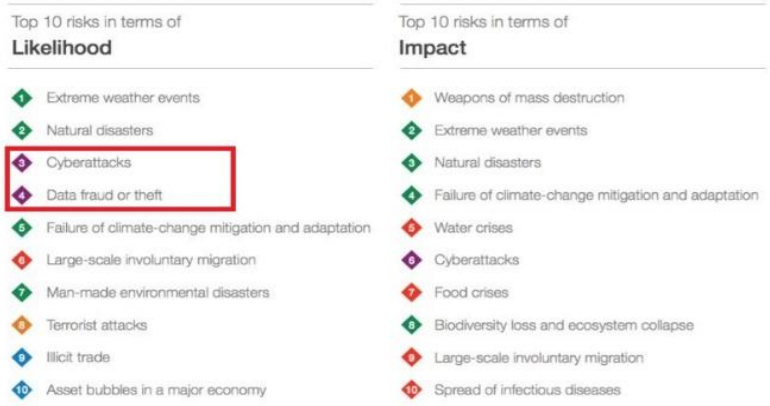
数据来源：IDC，中信建投研究发展部

中信建投证券 CHINA SECURITIES

2. 网络安全威胁事件频发，没有网络安全就没有国家安全，国家对网络安全重视程度进一步提高

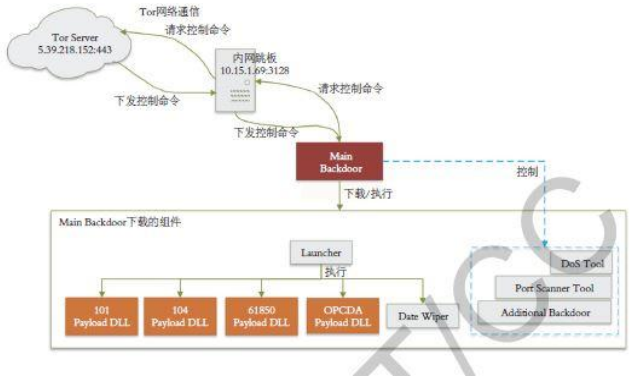
- 2018年世界经济论坛《全球风险报告》，阐述了全球企业所面临的风险，网络攻击和数据泄露排在最有可能发生的前五大风险第三位、第四位。网络攻击、病毒爆发和数据泄露事件近年在全球范围内出现越来越频繁，造成的直接、间接经济损失也越来越高。Frost & Sullivan和微软的研究表明，网络安全问题给全球造成的损失2017年高达6000亿美元，预计2021年将增至1万亿美元，遭受网络攻击数据泄露或者病毒勒索，造成的直接经济损失包括企业的收入、生产力、罚款、诉讼和补救措施；间接损失包括客户流失、声誉受损等。

图：2018年世界经济论坛将网络攻击、数据泄露首次列入全球企业所面临前五大风险



数据来源：财富杂志，中信建投研究发展部

图：针对工业控制系统的新型攻击武器Industroyer的攻击路径

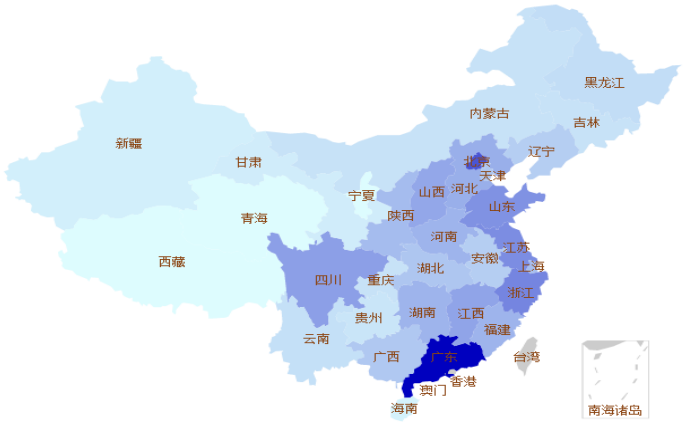


数据来源：国家互联网应急中心，中信建投研究发展部

3. 网络空间战日益成为大国战略博弈的新战场，加强网络安全能力建设和投入才能匹配我国的大国地位

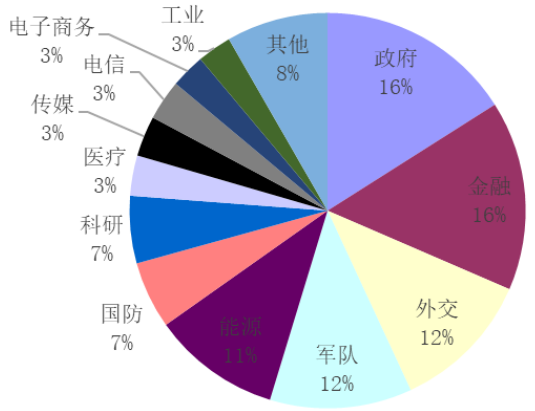
- 境外APT攻击组织对中国及“一带一路”国家发动攻击趋于频繁，国家对抗的安全需求进一步提升。截至到2018年10月，360威胁情报中心已累计监测到的针对中国境内目标发动攻击的境内外APT组织38个，攻击范围遍布国内31个省级行政区。且针对中国境内的攻击活动在2018年异常频繁，活跃的攻击组织包括海莲花、蔓灵花、白象、DarkHotol等。中国周边的国家以及中国的"一带一路"国家，也成为APT组织重点关注的对象。无论是发动APT攻击，还是披露APT攻击，均成为了现代国际关系中，大国政治与战略博弈的重要棋子，而整个网络空间就是大国战略博弈的新战场。

图：我国遭受境外APT势力攻击的区域



数据来源：360网络安全研究院，中信建投研究发展部

图：2018年中国境内遭受APT攻击的行业分布



数据来源：360网络安全研究院，中信建投研究发展部

4. 政策、新需求、新技术促进下，信息安全占IT支出比例有望达到5%以上

- **政策法律法规驱动：**从2014年以后国家从中央网络安全和信息化领导小组成立到后续各种法律法规出台，保证各单位重视网络安全系统升级，目前平均每个地市受到等保三级规则约束的企业数量达到500~800家。2017年6月《网络安全法》正式实施后，对违法网络安全法规的政府机关、企业处罚力度增加，促进企业合规性采购需求增加，2019年等保2.0将正式发布，进一步促进2019年~2020年信息安全市场快速增长。
- **数字经济发展带动信息安全新需求出现，网络安全防御思想、防护对象、防护技术变化较大，拉动信息安全高增长：**2017年中国数字经济总量达到27.2万亿元，同比增长20.3%，占GDP比重达32.9%，贡献了GDP增长的55%。2015年以前安全市场一直都很难扩大，因为企业只有在规划好整体IT系统以后最后再把安全像创可贴一样贴到信息系统上。现在企业像云端转型、数字化转型，在做整体信息化同时把信息安全和网络安全规划一起做，安全内置进入信息化系统，安全系统市场整体规模迅速扩大。
- **安全攻防博弈带来大数据、AI等新技术在安全中的应用创新，带来新的安全防护模式和新的安全产品：**传统安全产品做基础防御是采用被动防御，大数据和人工智能技术普及后，主动防御、威胁预测类、基于大数据技术的网络安全产品如态势感知平台、威胁情报、数据安全等安全智能类新产品增长迅速。尤其是基于大数据和AI攻防技术的态势感知平台目前在公安部、网信办、金融行业、电信行业、能源行业都在快速推广。

5. 政府监管和处罚力度加大，政企合规性采购需求增加

- 2017年6月1日期《中华人民共和国网络安全法》正式开始实施，其中第二十一条明确：国家实行网络安全等级保护制度。在过去一年多的法律实践中，各地都陆续出现未落实等保的企业被有关部门责令整改、行政处罚、暂停注册、暂停运营等处罚，因此地方政府网信办、公安部门对违法企业处罚力度的加大也促进了政府《网络安全等级保护条例》即等保2.0标准已在国家安标委最终审批，将在近期正式出台。

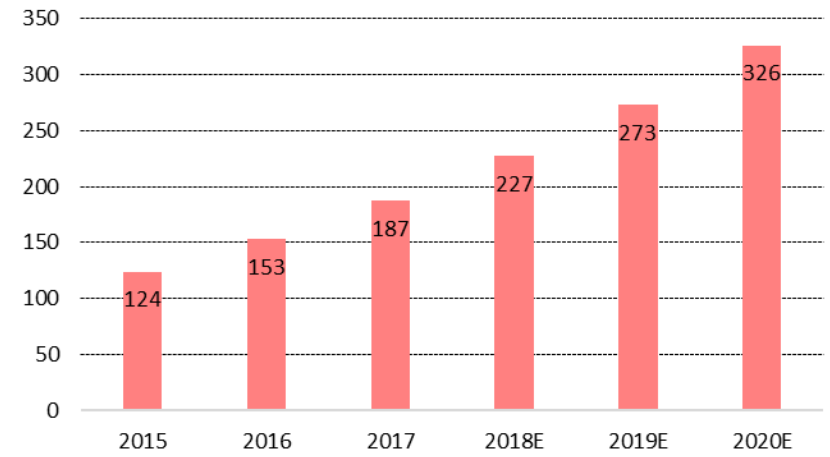
图：2017年6月份至今比较重大的网络安全违规处罚

时间	处罚行为	处罚对象	处罚措施	执法机关	处罚依据
2017.7.22	未进行定级备案、等级测评，存在高危漏洞，造成网站发生被黑客攻击入侵	四川省宜宾市翠屏区“教师发展平台”网站	对直接负责的主管人员罚款5000，机构罚款10000元	四川省宜宾市网安部门	《网络安全法》第21条、第59条第1款
2017.8.12	未进行网络安全等级保护定级备案、等级测评	安徽省蚌埠怀远县教师进修学校网站	约谈学校法定代表人、怀远县人民政府分管副县长；对学校处以巧15000罚款，对负有直接负责的主管人员处到5000罚款	安徽省公安厅网络安全保卫总队；安徽省蚌埠市局网安支队	《网络安全法》第21条、56条、第59条。
2017.8.30	未按照网络安全等级保护制度的要求落实网络安全主体责任，存在高危安全漏洞并被黑客攻击入侵，造成严重后果	哈尔滨方正县农业技术推广中心设立的“方正农业社会化服务平台”	责令整改，并处罚款20000元	黑龙江省哈尔滨市公安局网安支队	《网络安全法》第21条、第59条、第59条第1款
2017.7.21	未实名认证、未建立安全保护管理制度和安全保护技术措施	上海初生网络科技有限公司（热拉）	停机整顿6个月	上海公安网安部门	《计算机信息网络国际联安网安全护萨办法》第10条、第11条
2017.9	未落实实名制	深圳市三人网络科技有限公司	停业整顿，关闭网站	广东省通信管理局	《网络安全法》第24条、第61条
2017.8.17	未落实实名制	蘑菇互动网、虾米音乐网	暂停新用户注册7天	浙江网信办	《网络安全法》第24条、第61条
2018.1.11	未履行网络信息内容审核义务	万豪国际集团	责令万豪国际集团从当日18时起将官方中文网站、中文版APP自行关闭一周，开展全面自查整改，彻底清理违法违规信息，及时向社会公布事件调查结果和处置情况	上海市网信办	《网络安全法》第47条、第50条、第68条
2018.1.12	**未采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施，致使网站遭到攻击**	**河南省新乡市封丘县图书馆网站**	**对封丘县图书馆给予款20000元、对直接责任人处以警告，并罚款5000元**	**封丘县公安局、封丘县文化广电旅游局**	**《网络安全法》第21条、第25条、第59条第1款**

6. 网络安全法中明确关键信息基础设施范围，未来城市轨道交通网络安全、工业控制安全市场潜力巨大

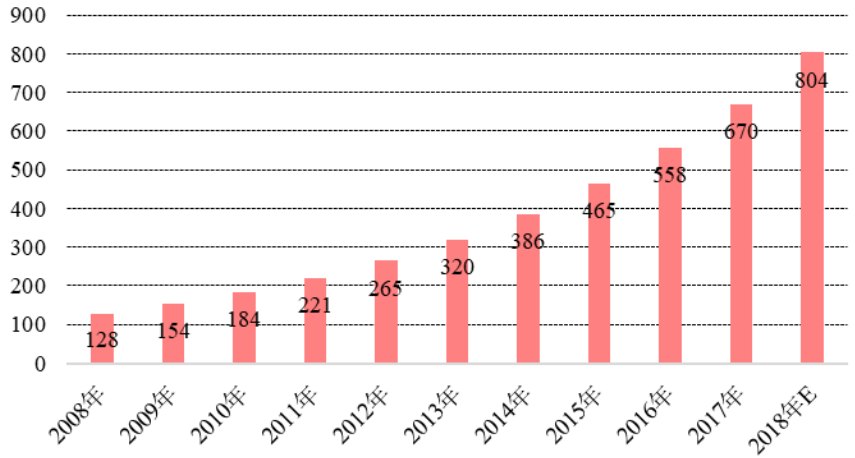
- 《网络安全法》规定“国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。”网络安全法实施后，新纳入进来且未来有较大增长潜力的行业包括城市轨道交通和工业控制的网络安全未来增长潜力巨大。

图：中国城市轨交信息化投资额（单位：亿元）



数据来源：中国产业信息网，中信建投研究发展部

图：中国电力行业信息化开支（单位：亿元）



数据来源：中国产业信息网，中信建投研究发展部

7. “云大物移”等新场景和新技术促进信息安全防护理念变化

- “云大物移”新场景驱动下防护对象改变，企业网络边界逐渐消失，政府和企业网络安全防护理念发生较大变化，网络安全不再是“补丁”模式，而是与信息系统建设同时规划，促进信息安全占IT支出占比逐步提升至5%以上。2015年以后，随着新的应用场景云计算、大数据、物联网和移动终端的普及，企业信息化程度逐步提升，网络安全领域出现了三大变化：防护对象的变化、防护思想的变化和核心技术的升级。

图：国家安全与政企数字化转型给网络安全领域提出了新的要求，网络安全领域出现的三大变化

防护对象变化

- 从传统PC、服务器、网络边缘到云计算、大数据、泛终端、新边界

防护思想的进化

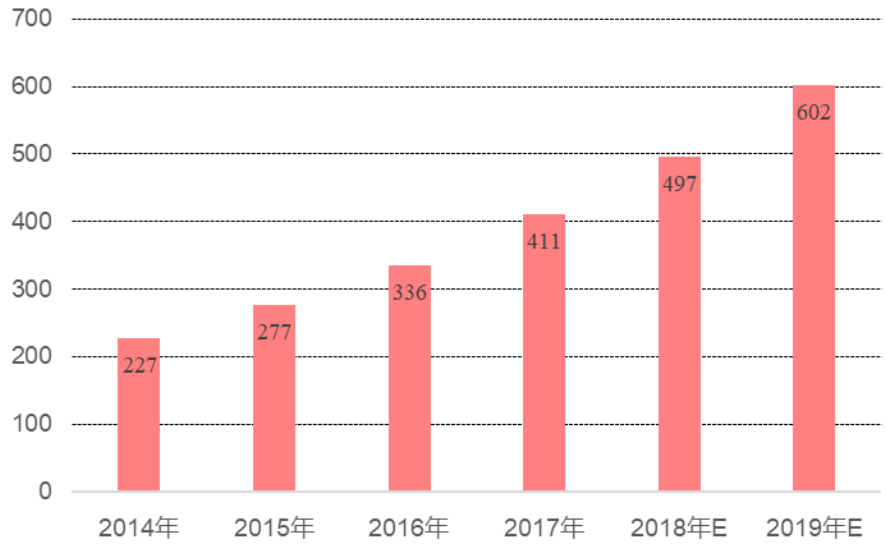
- 从“风险发现、查缺补漏”到“关口前移、系统规划”

核心技术的升级

- 从传统的围墙式防护到利用大数据等技术对安全威胁进行检测与响应

数据来源：360企业安全，中信建投研究发展部

图：中国网络安全市场规模将加速增长

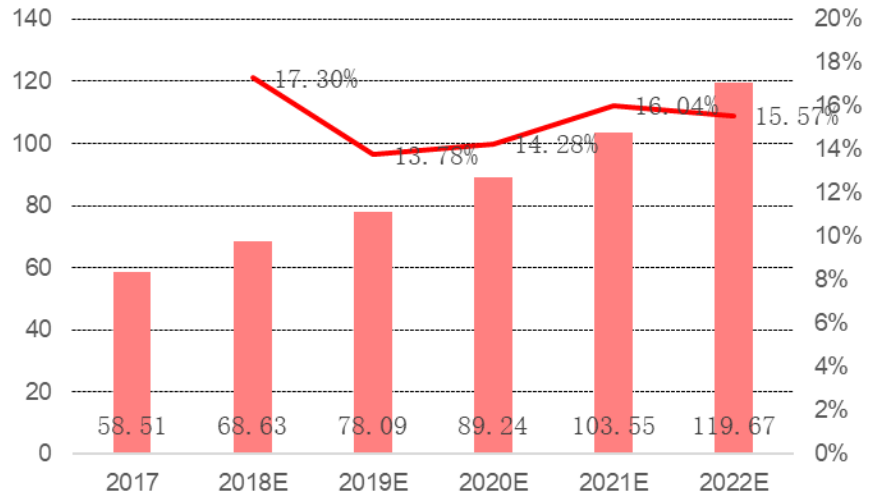


数据来源：中国产业信息网，中信建投研究发展部

8. 云计算发展带动云安全需求增长，网络安全市场增长迅速

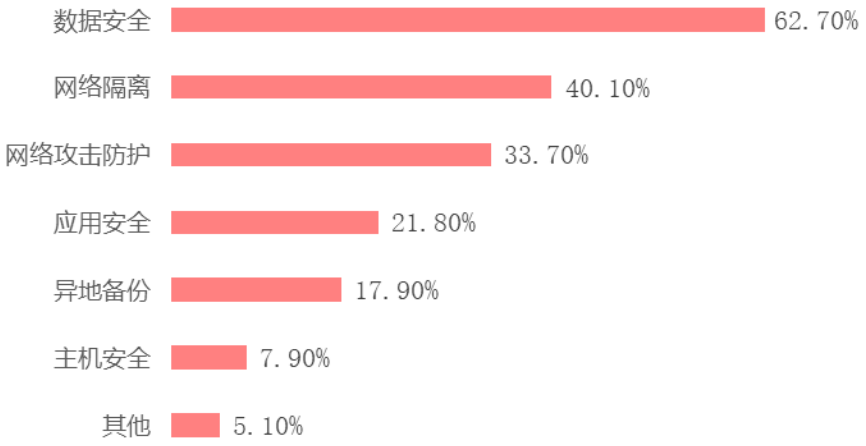
- 2017年全球云安全市场规模达到58亿美金，同比增长21%，预计2020年全球云安全市场将达到90亿美金，年复合增长速15%
- 混合云安全管理平台、公有云租户数据安全保障、网络隔离、攻击防护、主机安全、态势感知等需求是用户云安全重点需求，其中态势感知、抗DDoS、SIEM等产品在云计算推动下增速较快。

图：2017年全球云安全市场58亿美金，预计2022年达到120亿美金。（单位：亿美元）



数据来源：Gartner，中信建投研究发展部

图：私有云领域客户安全需求调查显示：数据安全、网络隔离、网络攻击防护、应用安全等需求旺盛

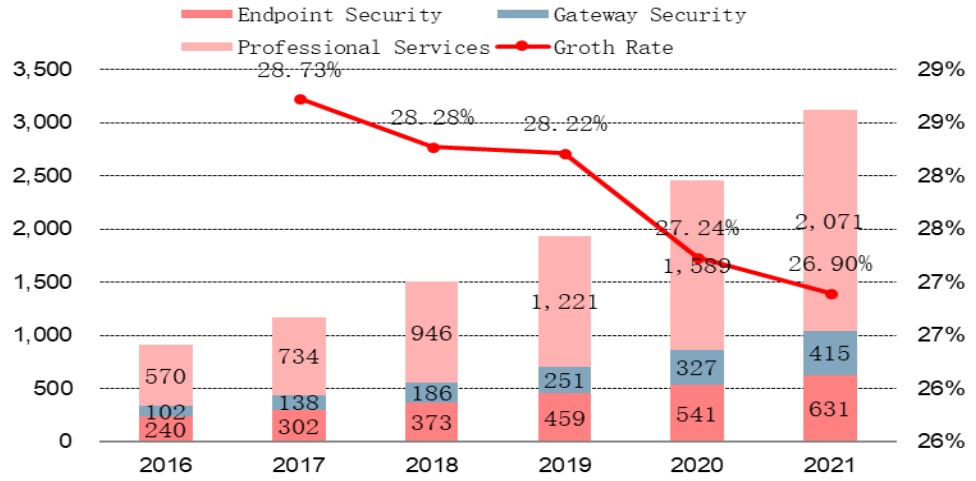


数据来源：Gartner，中信建投研究发展部

9. 物联网连接数快速发展，安全成为首要考虑问题

- 物联网连接数目前正在以每年50%的增长速度增长，预计2020年中国物联网连接数将达到50亿。根据Gartner统计，2017年全球物联网安全市场规模达到12亿美金，2018年同比增长28%，2020年全球物联网安全市场规模达到25亿。
- 物联网安全主要包含终端侧安全、网络安全、平台和、安全运营和管理四个方面，必须依靠生态各方共同维护。华为提出3T+1M物联网安全策略：适度的终端防御能力+恶意终端监测和隔离+平台及数据的保护+安全运营和管理、

图：2017年全球物联网安全市场规模12亿美金，到2020年市场规模达到25亿美金



数据来源：Gartner，中信建投研究发展部

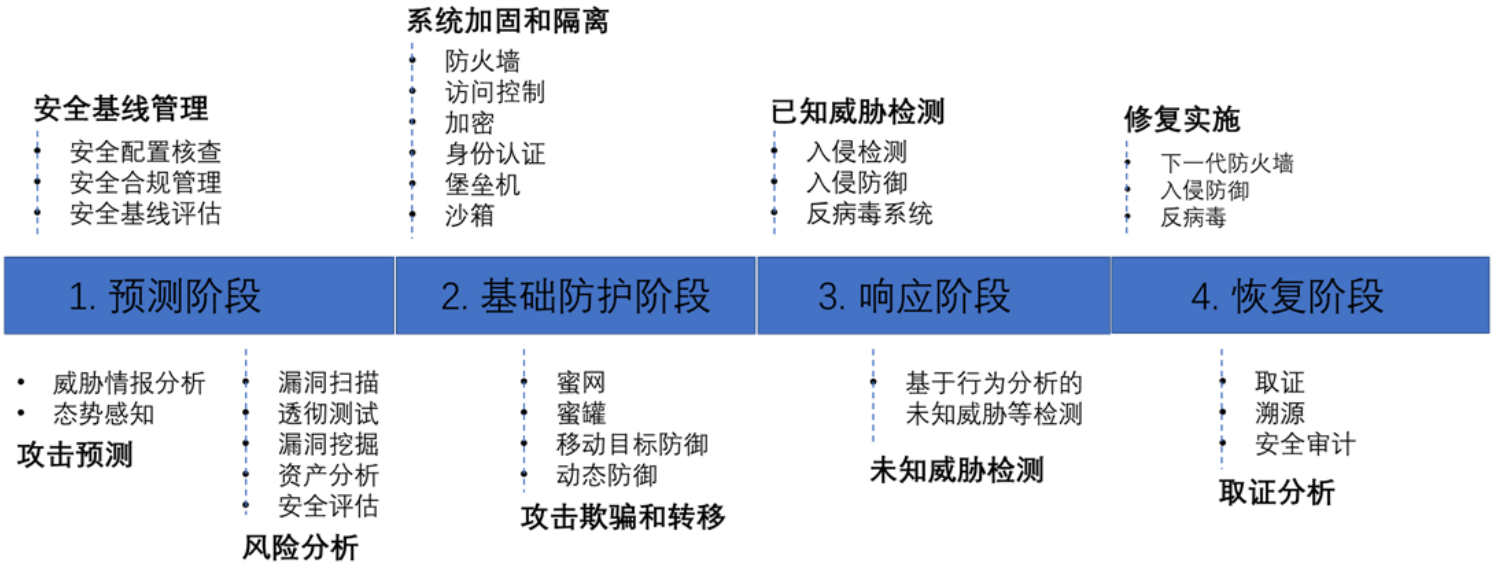
图：物联网安全包含终端安全、网络安全和平台安全，必须依靠生态各方共同维护安全

数据来源：华为官网，中信建投研究发展部

10. 新监管需求、新技术、新场景驱动安全新产品快速发展，主动防御产品增长速度更快

过去安全防护的思路一直是以防御攻击为主导，导致网络安全预测领域、主动防御，很长一段时间内是企业安全防护的薄弱区，且信息安全公司在产品技术上也相对滞后。**随着网络攻击越来越频繁、企业信息化越来越复杂、监管趋严，主动防御和预测类安全产品如态势感知、威胁情报分析、大数据安全分析、安全合规管理、安全配置核查等细分领域在近年取得快速增长。**尤其是态势感知平台，2017~2018年政府部门监管侧态势感知平台、企业端主动防御用态势感知平台项目越来越多，据安全牛统计，2017年国内态势感知市场规模约计20亿人民币，占整个安全市场的5%左右，预计2020年态势感知整体市场规模将超过50亿。

图：网络安全产品按照防御阶段分类，攻击预测和防御类产品增长速度高于行业增速

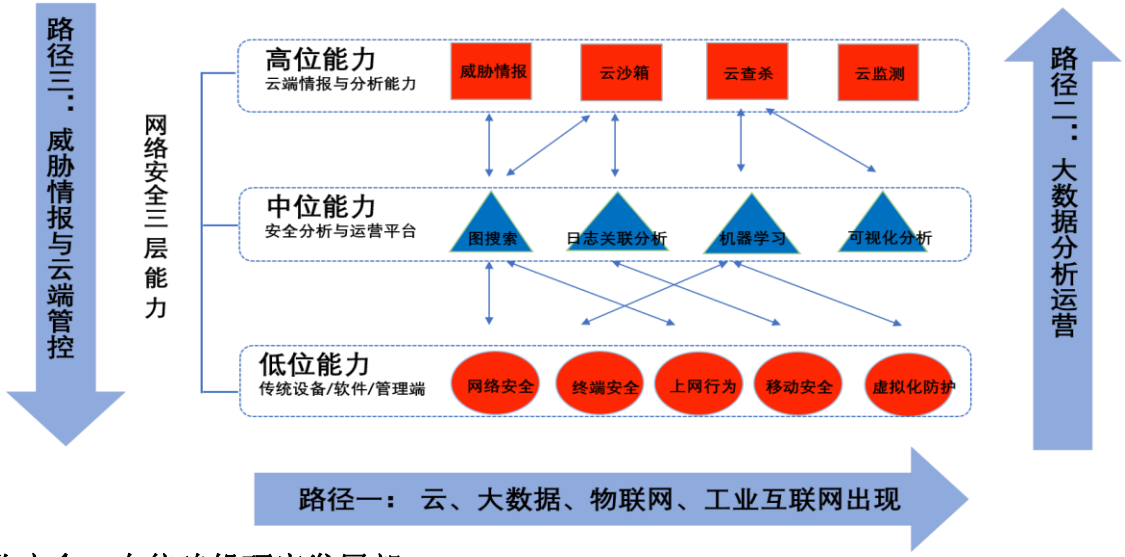


数据来源：中国信通院，中信建投研究发展部

11. 构建完善的企业安全需要高中低三位一体能力，目前高位和中位能力较为稀缺

- **面对日益复杂的网络环境和层出不穷的网络攻击威胁，政府和企业需要构建“低、中、高”三位能力的信息安全系统。**低位能力是传统的安全防御能力，包括传统的终端安全、网络安全、上网行为和移动安全等等，是数据采集层也是命令执行层，低位产品市场竞争较为激烈；中位能力是对海量数据的建模与分析能力，包括安全运营和安全分析能力；高位能力是云端威胁情报与分析能力，能对中位和低位提供支撑和决策，就像人的“大脑”，负责复杂的思考和下达行为指令。**目前中位和高位的安全能力是信息安全企业普遍欠缺**的，目前做的比较好的是互联网公司、华为和一些创业公司，传统企业安全公司相对落后。预计未来低位安全即传统边界安全、终端安全将保持平稳增长，抓住中位和高位能力的发展才能获得更高的增长速度。

图：政府和企业需要构建“低、中、高”三位能力的信息安全系统

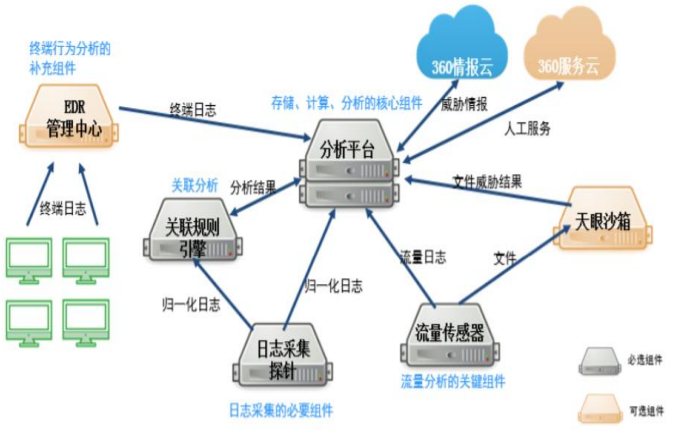


数据来源：360企业安全，中信建投研究发展部

12. 中高位信息安全产品举例：态势感知平台

- 态势感知平台分为政府部门使用的监管平台和企业使用的实施监测预警平台，目前在公安部、网信办、金融、电信、能源等行业增长迅速。态势感知平台是目前大数据安全领域规模增长最迅速的产品，据安全牛统计，2017年国内态势感知市场规模约计20亿人民币，占整个安全市场的5%左右，预计2020年态势感知整体市场规模将超过50亿。
- 态势感知通报预警平台核心功能包括：等级保护、实时监测、威胁感知、通报预警、快速处置、侦查调查、追踪溯源、情报信息、指挥调度，可以帮助用户实时掌握全局网络安全态势，实时开展预警通报、快速处置和网络安全综合管理工作。

图：企业态势感知平台架构



数据来源：360企业安全，中信建投研究发展部

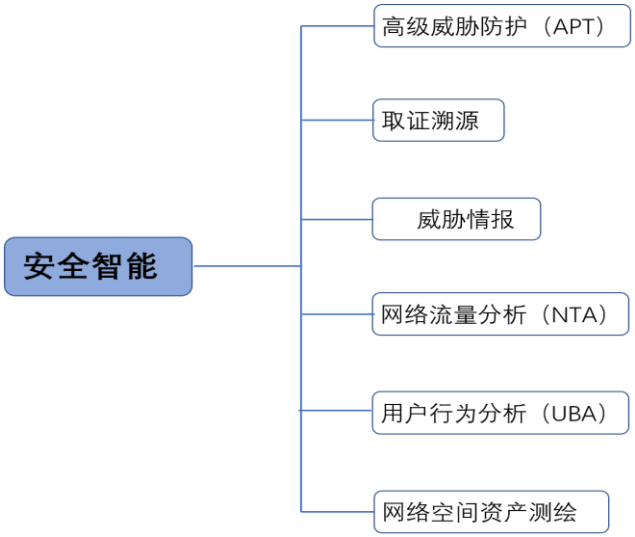
图：典型态势感知平台显示界面

数据来源：亚信安全，中信建投研究发展部

13. 中高位信息安全产品举例：威胁情报

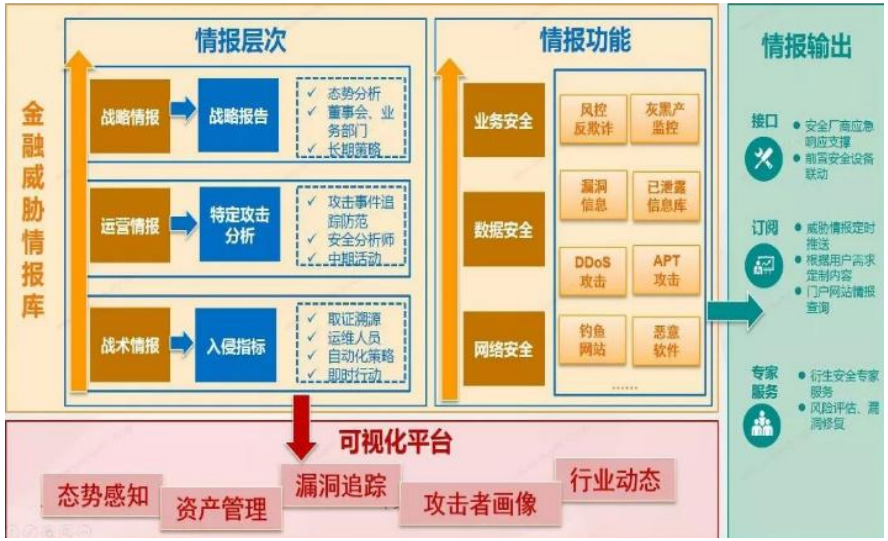
威胁情报由第三方专业机构提供的网络安全威胁数据，可进行传输交换、关联分析、挖掘应用，以反映组织存在的网络威胁和安全影响，包括但不限于设备日志、报警或描述威胁事件等情报消息。当前国内威胁情报应用主要集中在 IT 成熟度比较高和安全需求较高的行业，如金融、政府、能源等大型企业。大部分威胁情报业务主要为“大数据安全分析平台”或态势感知平台作支撑，和内部数据进行关联分析，实现对网络威胁的全面感知。根据2017年威胁情报的各种形态带来的收入为5亿到8亿元，约占整个安全市场的1.25%到2%，未来随着大数据安全分析平台和态势感知平台快速发展，2020年预计威胁情报市场规模有望超过12亿元。

图：安全智能产品分类



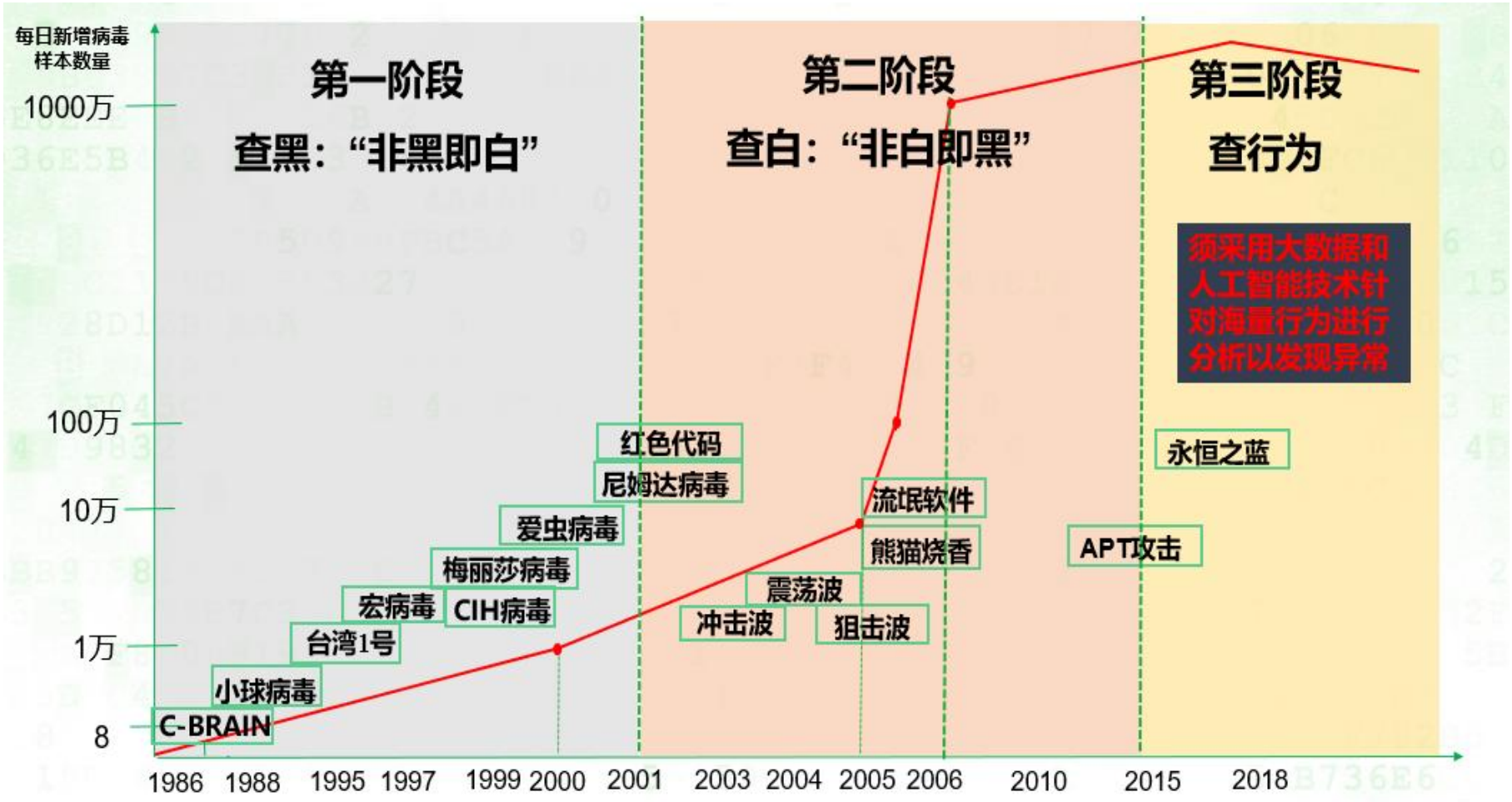
数据来源：安全牛，中信建投研究发展部

图：针对金融领域的威胁情报服务



数据来源：平安金融安全研究院，中信建投研究发展部

14. 攻防博弈带来大数据、AI等新技术在安全中的应用创新



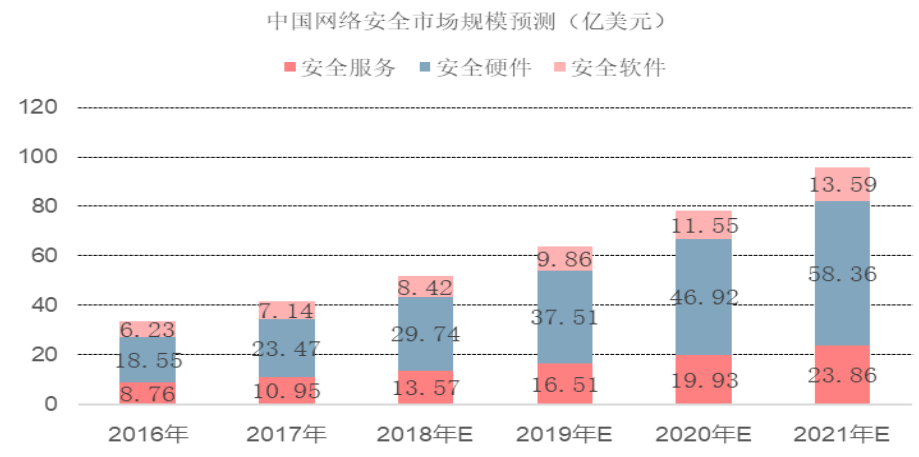
数据来源：360企业安全，中信建投研究发展部

中信建投证券 CHINA SECURITIES

15. 网络安全服务市场迅速增长，未来安全服务市场占比将逐步提升

- 在态势感知平台、大数据安全平台在各行业的快速拓展下，安全运营服务需求快速增长，信息安全行业领导公司都纷纷推出网络安全运营驻场服务或者城市安全运营中心，帮助政府机关、企业进行专业的安全运维并实现“安全大脑”功能，预计未来安全服务收入在各家企业收入占比将显著提升并保持快速增长。未来安全服务也有望为信息安全企业带来更多的销售机会，增强客户粘性。
- 网络安全人才缺口较大，尤其是高端架构师和网络安全运营人员。国际咨询机构预测， 2019年全球网络安全网络安全岗位缺口将在100-200万， 而到2021年缺口 将达到 将达到 350万个。尤其是高端安全架构师和安全运营人才大量缺乏，这也造成目前中国市场对高端安全技术人才争斗激烈，安全厂商研发费用率提升。

图：中国安全服务市场规模增长迅速



数据来源：51CTO，中信建投研究发展部

图：安全运营服务增长最快

数据来源：中国信通院，中信建投研究发展部

中信建投证券 CHINA SECURITIES

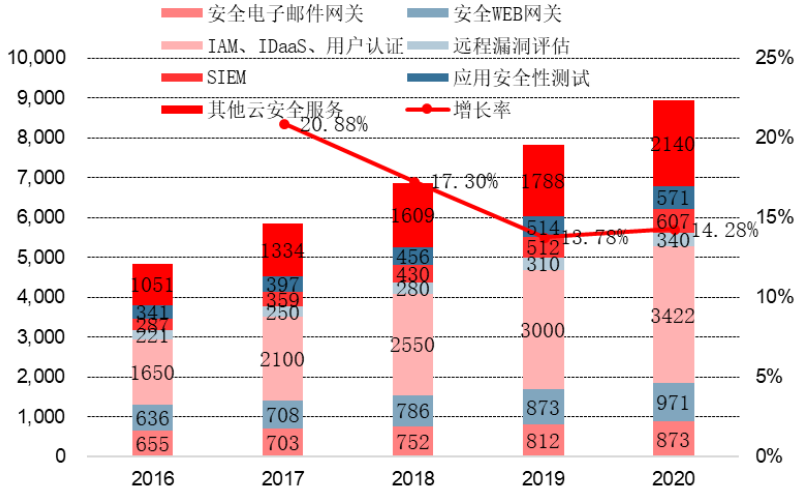
16. 企业安全市场竞争格局近年发生较大变化：互联网、云计算巨头入局（一）

- 公有云厂商利用自身资源优势提供DDoS高防IP、态势感知等服务，抗DDoS、WAF、漏洞扫描、主机安全、加密服务、态势感知成为公有云厂商标配的安全产品，并为中小客户提供免费额度，目前有20万用户在使用阿里云安全服务。
- 阿里云依靠电商平台网络安全长期积累起来的经验，目前云安全产品线最全，用户数最多。以抗DDoS产品为例，中国网站40%目前都放在阿里云上，阿里云每天承受攻击次数2000次，遭受300G以上的攻击数量占到全中国50%以上。
- 人工智能发展对网络安全是双刃剑，一方面目前可以通过机器学习来威胁进行提前预判，制定个性化防护策略，提高网络安全防御系统，另一方面人工智能也使得黑客入侵手段更多样化。

图：阿里云盾安全产品种类

数据来源：阿里云官网，中信建投研究发展部

图：Gartner数据显示威胁情报支持、云恶意软件沙河、云数据加密、端点保护管理、WAF等云安全服务增速较快



数据来源：中国信通院，中信建投研究发展部

中信建投证券 CHINA SECURITIES

17. 企业安全市场竞争格局近年发生较大变化：互联网、云计算巨头入局（二）

- 虽然阿里云盾目前可以45个安全功能和服务模块，覆盖了业务、运营、数据、网络等11个维度的产品，但是还是无法满足所有客户个性化的需求，很多客户也希望不止使用一家厂商的产品，几乎所有云厂商都建立了自己的安全产品生态。目前阿里云上有148家合作伙伴、350款安全产品，保证解决客户的多样化安全需求。同时阿里云也通过投资并购的方式投资、并购了一些重要领域的安全技术，比如安华金和、安恒信息、翰海源和海外的ThetaRay等。
- 依靠云安全和移动安全的快速发展，一些“小而美”的SaaS安全公司在细分市场实现突破。比如自适应云领域的青藤云、应用安全的创宇、APP加固服务的梆梆安全等。

图：阿里云近三年投资并购的安全领域公司

时间	公司名称	参与阶段	投资金额	细分领域
2016/6/22	安华金和	B轮	5000万人民币	数据库安全
2015/12/8	ThetaRay	C轮	1500万美元	数据安全
2015/11/20	安恒信息	D轮	亿元及以上人民币	信息安全提供商
2015/6/11	翰海源	并购	未透露	APT攻击防护

数据来源：互联网公开资料整理，中信建投研究发展部

图：部分一级市场较为知名的安全创业公司

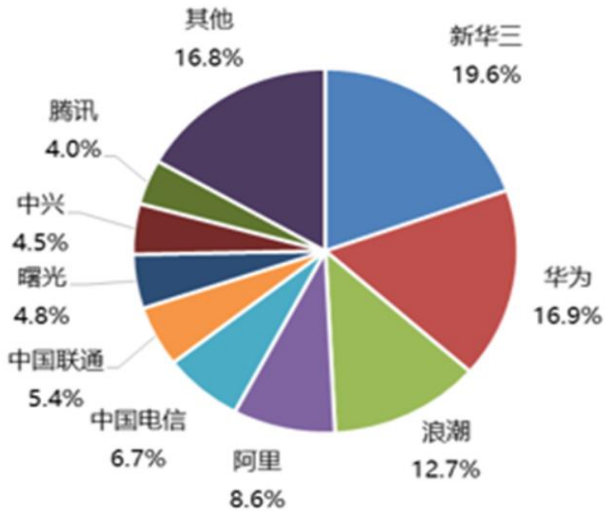
公司名称	融资额	细分领域
知道创宇	总融资额约6.3亿人民币	应用安全
山石网科	总融资额约5.94亿人民币	网络安全
明朝万达	总融资额约4.54亿人民币	数据安全
观数科技	总融资额约2000万人民币	网络安全
珊瑚灵御	总融资额约1000万人民币	数据安全、端点安全、应用安全
观安信息	总融资额约1.96亿人民币	数据安全
极验验证	总融资额约1.77亿人民币	身份与访问管理
安恒信息	总融资额约1.6亿人民币	应用安全、安全管理、网络安全
瀚思科技	总融资额约1.4亿人民币	端点安全、网络安全

数据来源：互联网公开资料整理，中信建投研究发展部

18. 私有云解决方案提供商安全业务增长迅速，市占率逐步提升

- 私有云领域占据份额前二的华为、新华三近年在企业安全市场一直保持非常高的增长速度，**新华三2016~2017年安全业务增速都在50%以上，计划2019年做到全国安全市场15%的市占率，而华为安全业务增速也高于网络设备30%的增长速度**。两家公司因为私有云产品线齐全、技术实力强，都主打“云网融合”一体化解决方案，因此将安全作为私有云集成方案中重要模块，进行销售。尤其在重视安全的政府、电信、金融等领域取得了较高的安全市场份额。
- 新华三的云安全2.0方案，包括虚拟化的防火墙、负载均衡、入侵检测、WAF、堡垒机，等软件定义安全的虚拟化产品，已经是一套较为完善的基础设施和网络防护解决方案。由于大客户越来越依靠私有云解决方案提供商提供一整套交钥匙方案（包含网络、计算、安全等），单独的安全产品越来越难销售。

图：2016年中国政务云市场份额占比



数据来源：CCW Research 2017，中信建投研究发展部

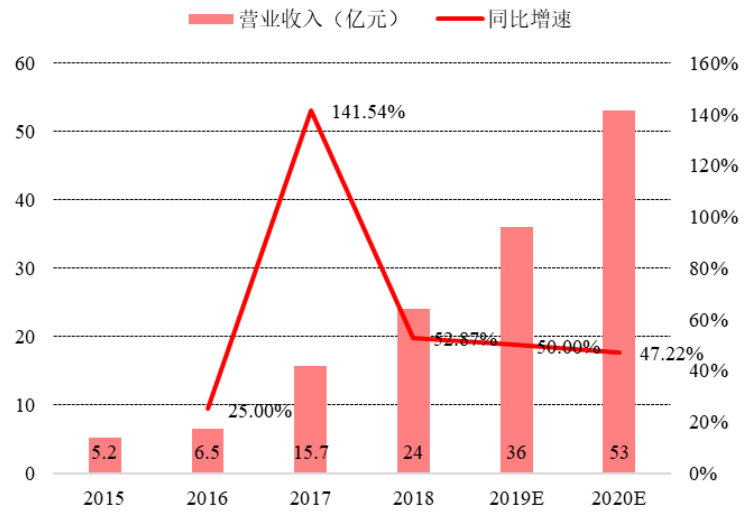
图：新华三云安全2.0产品解决方案

数据来源：H3C官网，中信建投研究发展部

19. 具备“高中低”三位一体能力的信息安全龙头公司-360企业安全增长迅速

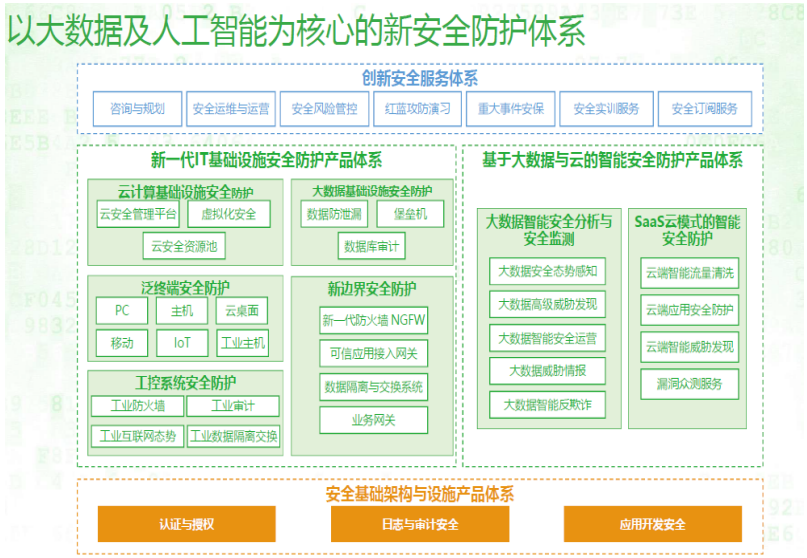
- 360企业安全2015年独立运营以后一直保持快速增长，预计2017~2019年收入分别为15亿、24亿、36亿，增长速度超过行业平均增速。
- 360企业安全收入大约40%收入来自于近年催生的新安全产品，尤其是基于攻防对抗、数据分析的：云计算边界安全、数据安全、态势感知平台、大数据智能安全分析与安全监测产品、工控系统安全防护等等，新产品收入增速远高于传统安全产品。

图：360企业安全收入增长速度远超行业增速



数据来源：360企业安全，中信建投研究展部

图：360企业安全产品结构

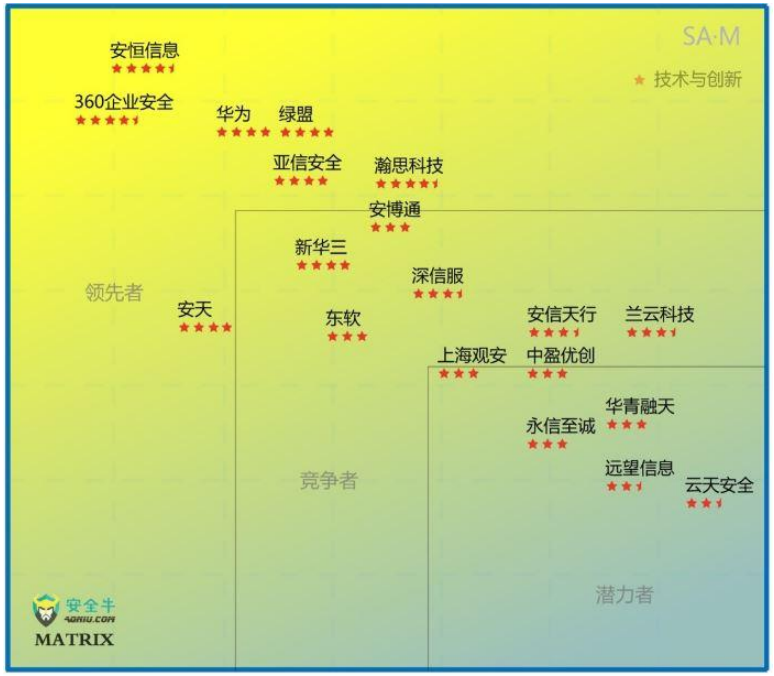


数据来源：中信建投研究发展部

20. 信息安全细分领域众多，小而美的细分领域龙头也值得关注

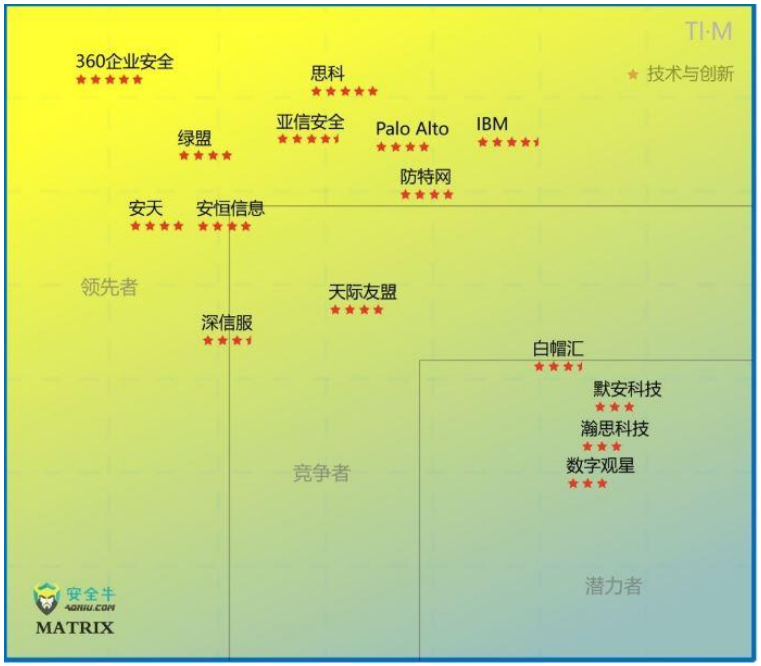
- 在应用安全、数据安全、移动安全、态势感知等领域，都有增长较快的创业公司，它们可能没有做低位的边界安全产品，只做中位、高位能力的增长较为快速的应用。
- 态势感知平台，目前360企业安全、安恒信息、韩思科技、观安都保持了非常高速的增长。
- 威胁情报领域，除了360企业安全外，安天、白帽汇、天际友盟等创业公司也都保持比较快速的增长。

图：态势感知产品矩阵



数据来源：安全牛，中信建投研究发展部

图：威胁情报产品矩阵



数据来源：安全牛，中信建投研究发展部

投资建议

建议精选行业龙头进行配置：

- 受益于主动安全防御产品增长和运营服务快速增长：360企业安全
- 传统安全厂商：深信服、启明星辰、蓝盾股份
- 受益于公安大数据平台需求增长：美亚柏科
- 受益于流量、大数据项目增长，带来前端数据采集设备增长的探针提供商：中新赛克、恒为科技
- 受益于国产化保密终端替换：中孚信息、北信源

分析师介绍

石泽蕤

TMT行业分析师，执业证书编号：S1440517030001。香港中文大学电子工程硕士，专注于产业互联网、信息安全、云计算、人工智能等领域的研究，2017年初加入中信建投证券。 2017年《新财富》、《水晶球》、wind最佳分析师通信第一名团队成员

研究服务

机构销售负责人

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

保险组

张博 010-85130905 zhangbo@csc.com.cn

杨曦 -85130968 yangxi@csc.com.cn

郭洁 -85130212 guojie@csc.com.cn

郭畅 010-65608482 guochang@csc.com.cn

张勇 010-86451312 zhangyongzgs@csc.com.cn

高思雨 gaosiyu@csc.com.cn

王罡 021-68821600-11 wanggangbj@csc.com.cn

张宇 010-86451497 zhangyuyf@csc.com.cn

北京公募组

朱燕 85156403 zhuyan@csc.com.cn

任师蕙 010-8515-9274 renshihui@csc.com.cn

黄杉 010-85156350 huangshan@csc.com.cn

杨济谦 010-86451442 yangjiqian@csc.com.cn

私募业务组

赵倩 010-85159313 zhaoqian@csc.com.cn

上海销售组

李祉瑶 010-85130464 lizhiyao@csc.com.cn

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

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

翁起帆 021-68821600 wengqifan@csc.com.cn

李星星 021-68821600-859 lixingxing@csc.com.cn

范亚楠 021-68821600-857 fanyanan@csc.com.cn

李绮绮 021-68821867 liqiqi@csc.com.cn

薛姣 xuejiao@csc.com.cn

许敏 021-68821600-828 xuminzgs@csc.com.cn

深广销售组

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

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

程一天 0755-82521369 chengyitian@csc.com.cn

曹莹 0755-82521369 caoyingzgs@csc.com.cn

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

陈培楷 020-38381989 chenpeikai@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。本报告清晰准确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。

中信建投证券研究发展部

北京

东城区朝内大街2号凯恒中心B座12层（邮编：100010）

电话：（8610）8513-0588

传真：（8610）6560-8446

上海

浦东新区浦东南路528号上海证券大厦北塔22楼2201室（邮编：200120）

电话：（8621）6882-1612

传真：（8621）6882-1622

深圳

福田区益田路6003号荣超商务中心B座22层（邮编：518035）

电话：（0755）8252-1369

传真：（0755）2395-3859