拐点之时，格局之变

网络安全行业深度报告

华西计算机团队
2021年3月2日

分析师：刘泽晶
SAC NO：S1120520020002
邮箱：liuzj1@hx168.com.cn

联系人：刘忠腾
邮箱：liuzt@hx168.com

联系人：孔文彬
邮箱：kongwb@hx168.com

行业推荐主要逻辑

1、回溯过去：赛道细分、竞争分散导致龙头优势难以凸显。2015年以前国内网安市场集中度较低，CR3不足20%，仅启明星辰相对领先，产品类别过于细分、下游客户分散招标是主要原因。判断彼时并未形成真正龙头。

2、聚焦现在：产品化、服务化等因素促成集中趋势，龙头扩张迅猛。近年来行业格局快速集中化，多个细分领域CR3突破40%，头部厂商奇安信、深信服等持续扩张，一方面是受到技术演进、招标变化等外围影响，另一方面也映射了龙头的产品化/服务化实力提升。

3、展望未来：全能型龙头延续强势，专精/审查型厂商有弯道超车。大安全时代下半场，面对等保2.0撬动的千亿级市场，坚定看好全能型龙头延续强势，同时考虑到部分中小厂商（专精/审查型）受益云大物智细分赛道崛起、国家安全审查需求提升等因素，亦有望弯道超车。

4、格局变化 - 选股：龙头恒强和弯道超车两条主线下，梳理出网安五大龙头（2+1+2），推荐全能型厂商：**奇安信、深信服**；专精型厂商：**安恒信息**也有望受益；同时建议重点关注审查型厂商：**美亚柏科、中新赛克（通信组联合覆盖）**。其他受益标的包括：启明星辰、绿盟科技、天融信、山石网科、迪普科技等。

5、拐点确立 - 择时：2020Q3以来网安公司加速复工，**叠加下游政府侧预算边际放松**，业绩持续转好。从已经披露2020全年业绩（快报）的厂商来看，奇安信（营收+32%）、安恒信息（营收+40%/利润+48%）、美亚柏科（营收+15%/利润+30%）、深信服（营收+19%）等均有较优表现，龙头领先行业复苏。**结合等保2.0、关保、HW等事件催化影响，判断拐点确立，行业反转可期，建议把握当前配置窗口期。**

6、风险提示：竞争加剧风险、政策风险、下游需求波动风险、新兴技术风险。

目录

01 格局一

变迁 —— 从过去到现在，全能型厂商优势凸显

1.1 新兴高景气行业，中游软硬件厂商/集成商主导

◆ **近年来国内外网络安全事件频发，造成巨大损失：**

✓ 随着信息技术的快速演进，全球数据泄露等网络安全事件频繁发生，造成重大损失

✓ 根据CCID发布《2019年网络安全发展白皮书》，以2018年为例，全球安全漏洞数量和严重性创下历史新高；国内重大网安事件也几乎每月必现

✓ 据 Cybersecurity Ventures 预测，到 2021 年全球因网络安全事件导致的损失将高达 6 万亿美元/年

◆ **网络安全态势变得愈发复杂，行业正在迎来"大安全"景气新时代**

✓ 个人层面来看，网络安全事件会带来私人信息泄露，进而带来财产等损失

✓ 政企层面来看，针对关键性基础设施的网络攻击会导致重大安全事故，直接威胁国家安全

✓ **在此背景下，网络安全正式步入"大安全"时代，本篇报告中我们聚焦网安的过去、现在、未来格局，深度挖掘行业投资机会**

2018年全球及国内网络安全重点事件

全球网络安全重点事件盘点

• **VPNFilter木马导致超50万台路由器被控** 俄罗斯黑客攻击传播名为VPNFilter的恶意软件，可感染Netgear、TP-Link、Linksys、ASUS、D-Link等数十种主流路由器型号。	• **Github遭遇TB级Memcached DDoS攻击** GitHub遭遇史上最大规模的DDoS网络攻击，峰值为1.269亿个数据包、1.35Tbps。
• **Aadhaar中11亿公民信息遭泄露** 印度国家身份认证系统Aadhaar遭网络攻击，数据被明码标价出售。	• **Facebook8700万用户数据遭泄露** Facebook 公开承认剑桥分析公司不正当使用了8700 万未经授权的用户私人信息， 半年后Facebook再次通告称3000万用户账号信息被黑客控制利用。
• **美国运动品牌安德玛1.5亿用户信息遭泄露** 安德玛旗下健身应用MyFitnessPal因存在数据漏洞而遭到黑客攻击，造成包括用户名、电子邮件、密码等数据信息泄露。	• **万豪酒店5亿用户开房信息遭泄露** 万豪旗下喜达屋酒店客房预订数据库遭黑客入侵，包括客户姓名、地址、电话、邮箱、护照号码、喜达屋SPG俱乐部账户信息、出生日期、性别等信息遭泄露。
• **瑞士数据管理公司Veeam暴露4.45亿条数据** Veeam存储有超过200GB的数据库，处于完全无防御状态，任何人都能公开查询和访问其数据，包括姓名、电子邮件、居住地、国家等信息。	• **iOS安全漏洞"ZipperDown"** IOS爆出与开发者相关漏洞ZipperDOwn， 约有10%的iOS应用可能受此漏洞的影响。

我国网络安全重点事件盘点

2018年1月	安全漏洞	国内安卓手机APP存在应用克隆风险，可利用漏洞窃取用户隐私。
2018年2月	攻击事件	上海某公立医院HIS系统被黑客入侵，遭勒索2亿比特币。
2018年3月	基础设施攻击	黑客利用思科高危漏洞攻击网络基础设施，国内多家机构中招。
2018年6月	数据泄露	圆通10亿条快递信息遭泄露，并被发到暗网上兜售。
2018年7月	数据泄漏	上市公司数据堂相关人员涉嫌侵犯数百亿条公民个人信息被起诉。
2018年8月	数据泄漏	华住酒店5亿条用户数据疑泄露，并以8比特币的价格售卖。
2018年8月	安全漏洞	银行、移动支付APP存在短信验证码漏洞，易致资金盗刷。
2018年8月	勒索病毒	台积电感染勒索病毒WannaCry，致17.4亿元人民币损失。
2018年12月	勒索病毒	"微信支付"勒索病毒曝光，10万多台电脑被感染。

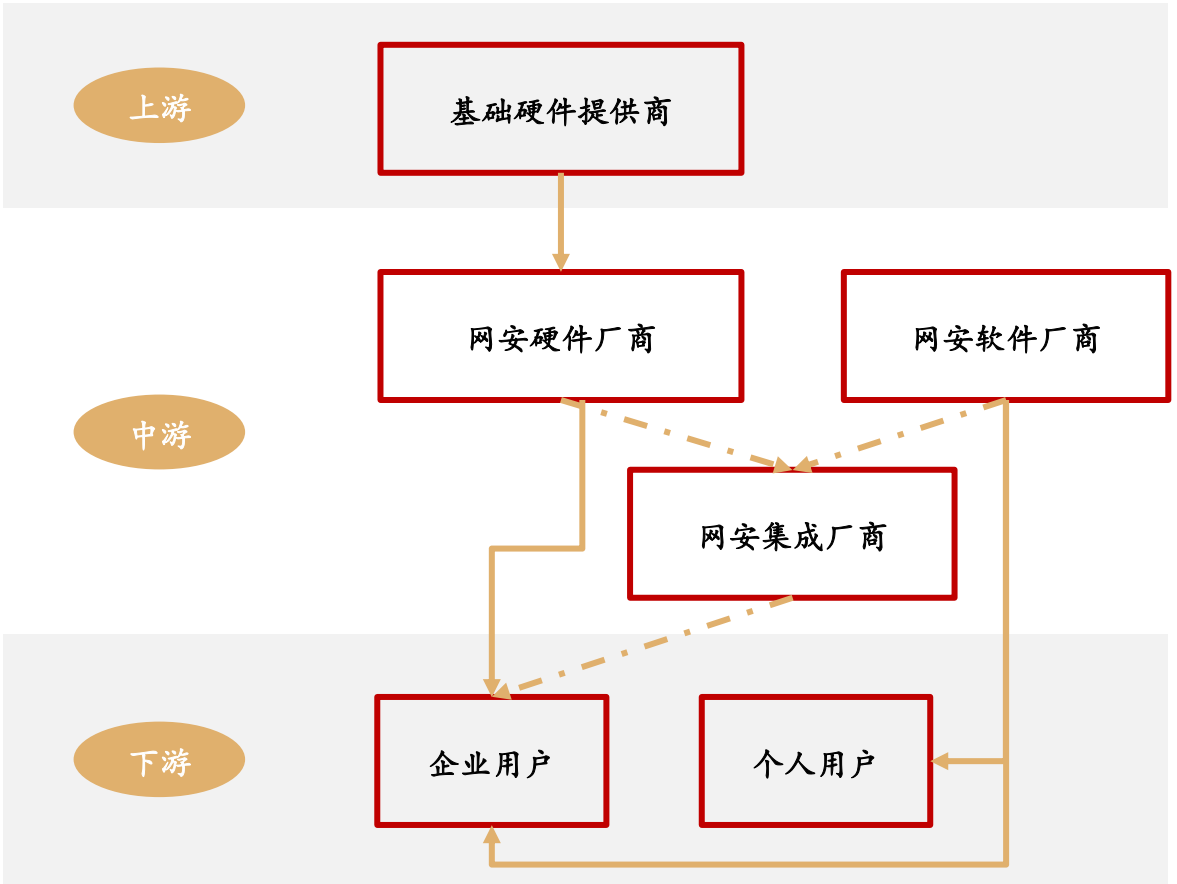
资料来源：CCID、华西证券研究所

1.1 新兴高景气行业，中游软硬件厂商/集成商主导

- ◆ **全球视角来看，网络安全行业以“硬件-软件-服务”构建产品体系，下游客户覆盖各行各业**
- ✓ **上游**：网络安全产业链上游为基础硬件提供商，为中游设备厂商提供芯片、内存等基础元器件，上游的代表性公司包括英特尔、三星等
- ✓ **中游**：产业链中游主要分为三类厂商，即安全硬件设备厂商、安全软件厂商和安全集成厂商，其中安全硬件设备厂商和安全软件厂商一部分产品直接供应给下游最终用户，另一部分产品则提供给安全集成厂商，中游代表性公司有赛门铁克、启明星辰、深信服等安全集成厂商
- ✓ **下游**：产业链下游主要为各类用户主要为政企客户，包括政府、军工、电信、教育、金融、能源等

- ◆ **目前国内的网络安全上市公司主要以中游的安全硬件设备厂商、安全软件厂商和安全集成厂商为主**

产业链构成



资料来源：CCID、华西证券研究所

1.2 格局变迁：过去到现在经历四阶段发展，当前正值加速发展期

◆ **我国网络安全发展可分四个阶段，当前正值加速发展期，聚焦网络空间安全概念**

✓ 根据安全牛披露，我国网安发展历程可分为起源期、萌芽期、成长期和加速期四个时期，分别对应通信加密时代、计算机安全时代、信息安全时代和网络空间安全时代

✓ 随着通信技术演进及移动互联网普及，企业信息化程度持续提升，自动化和远程办公的需求激增，网安关注点逐渐延伸至网络空间本身，网安行业也进入加速发展期，即“大安全”时代

✓ 关注网络空间安全的两个核心领域：1）网络边界安全，例如防火墙、VPN等；2）信息系统本身及其承载内容的安全

我国网络安全发展四阶段

资料来源：安全牛、华西证券研究所

1.3 聚焦加速期起点，2015以前市场格局分散，厂商各自为战

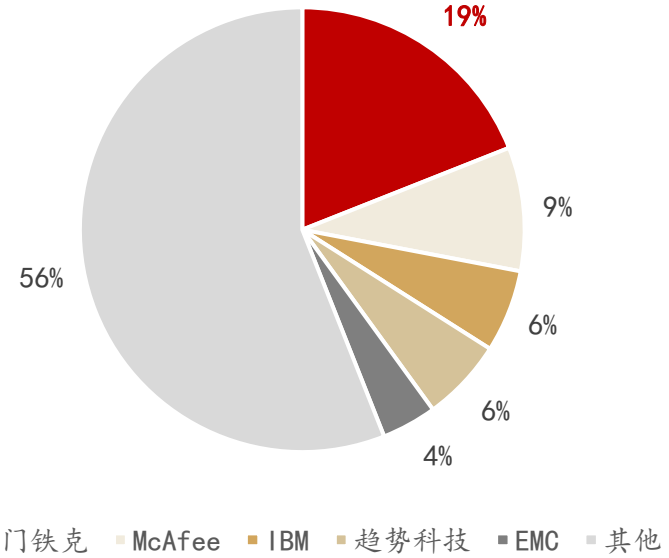
◆ 网安行业从2015/2016年步入加速期以来，行业竞争格局持续变迁

◆ 回溯过去，2015年及以前国内网络安全市场集中度相对较低，国内龙头较全球龙头差距较大

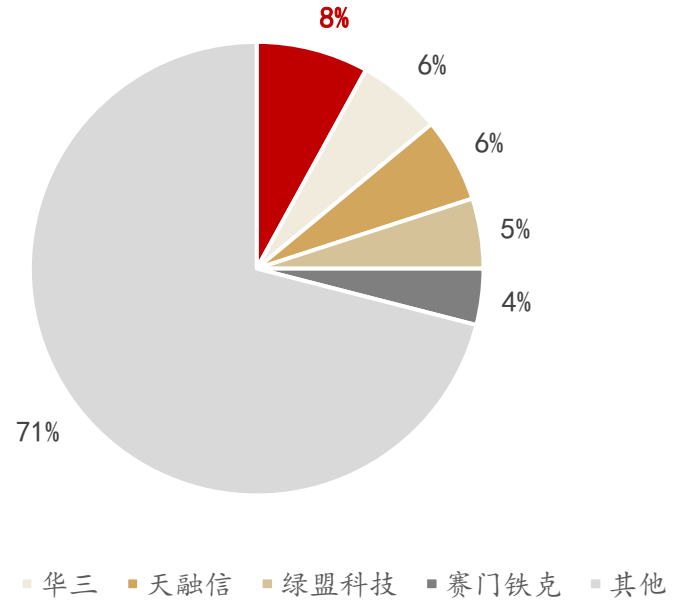
✓ 根据Gartner数据，2015年全球前三大厂商合计份额（CR3）高达34%，而国内CR3不足20%，远低于全球的市场集中度

✓ **龙头实力差距尤其巨大**：国内龙头启明星辰市占率仅8%，远低于全球龙头赛门铁克的19%（约等于国内前三大厂商市占率之和）

2015年全球网络安全市场份额



2015年我国网络安全市场份额



资料来源：Garnter、华西证券研究所

1.3 聚焦加速期起点，2015以前市场格局分散，厂商各自为战

- ◆ 将分散格局对应至安全牛网络安全企业年度榜单（业务规模/技术影响力二维评定）来看则更为清晰
- ✓ 2015年：仅启明星辰、天融信在榜单中展现相对领先的综合实力，构成头部厂商，身后卫士通、深信服、绿盟则仍在快速追赶
- ✓ 而其他各类厂商基本囤居中游、各自为战，同时以360为代表的新兴厂商持续入局，市场竞争极其激烈

2015年传统网络安全企业 TOP 25

2015年新兴网络安全企业 TOP 10

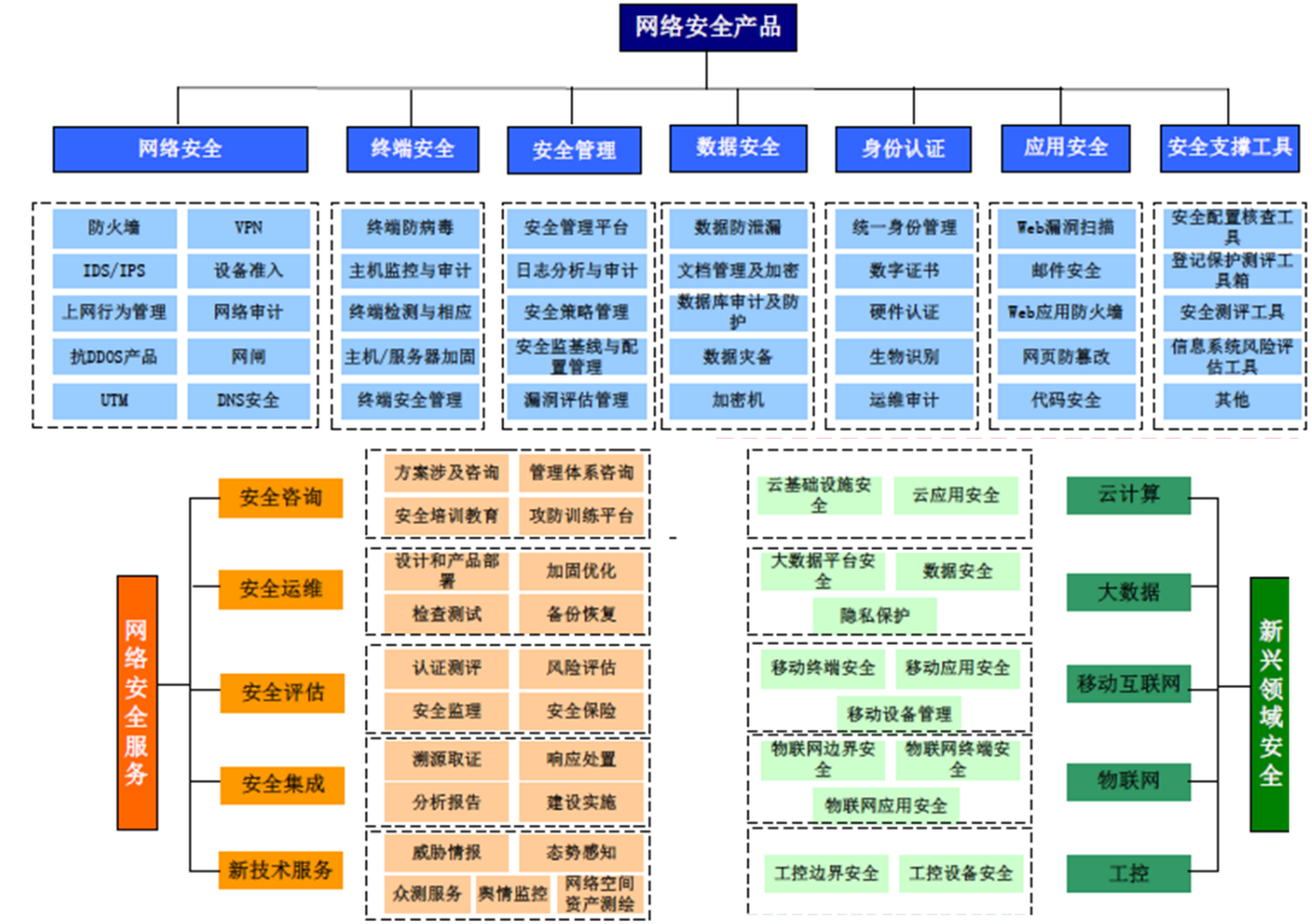
资料来源：安全牛、华西证券研究所

1.4 分散格局成因一：产品线众多，政企分散招标

- ◆ **网安产品线众多是市场分散的关键原因**
- ✓ 目前来看，软硬件网络安全产品可分为7大类、40小类，而信息安全服务也可分为5大类、21小类，细分程度非常高
- ✓ 产品线过于分散直接导致网安厂商稳守各自细分赛道，赛道壁垒阻碍"胜者全得"趋势

- ◆ **此外政企作为下游核心客户，以往多采用分散招标，导致入围的安全厂商无法提供有效的整体服务**
- ✓ 仍是由于网安产品线众多，各集团、公司、部门均可能针对特定产品进行单独招标
- ✓ 下游关键客户政企尤其如此，同时为了防止一家独大，政企往往出现刻意分散招标
- ✓ <u>最终导致彼时网安行业小公司林立、市场分散的格局</u>

网络安全产品全景图



资料来源： CCID、华西证券研究所

1.4 分散格局成因二：厂商定位狭隘，同质化竞争严重

- ◆ 市场分散的另一个原因是彼时网安厂商仍以销售硬件产品为主，产品同质化程度较高
  - ✓ 2015年正值加速发展期的起点，仍未完全摆脱此前“硬件为王”的经营思路，经营定位略显狭隘
  - ✓ 当时网安厂商的普遍自我定位为产品提供商，主要关注产品（尤其是硬件）的功能性，对于整体解决方案、一站式服务、售后服务的关注有限，导致大型厂商未在产品类型上充分延伸

- ◆ 根据IDC数据，2015年硬件领域的领军企业（Top 5）重合度较高，在同质竞争中激烈厮杀，但并未充分向软件及服务领域开拓

2015年网络安全细分市场及代表企业

硬件	
细分领域	**领军企业**
防火墙	启明星辰、华三、天融信、华为、迪普科技
入侵防御/检测	绿盟科技、启明星辰、安氏领信、东软集团、华三
统一威胁管理	启明星辰、华三、山石网科、深信服、华为
内容安全管理	华三、启明星辰、深信服、360、绿盟科技
VPN	启明星辰、天融信、华三、深信服、华为
软件	
细分领域	**领军企业**
安全性与漏洞管理	启明星辰、绿盟科技、IBM、Qualys、HP
身份管理与访问控制	吉大正元、卫士通、上海格尔、天威诚信、信安世纪
内容安全与威胁管理	Symantec、瑞星、趋势科技、冠群金辰、Intel
服务	
细分领域	**领军企业**
集成、运维与咨询	启明星辰、绿盟科技、天融信、360、安氏领信

资料来源：CCID、IDC、华西证券研究所

1.5 聚焦加速期中点，头部厂商不断扩展，优势正在凸显

- 近几年来看，头部厂商凭借综合实力的优势不断外延扩张，行业集中度提升明显

- 聚焦CR3，安全硬件和软件多个细分领域CR3已经突破40%，较2016年整体不足20%的水平提升明显
  - ✓ 举例而言，虚拟专用网络领域 CR3 高达48.4%、统一威胁管理CR3高达43.6%、安全内容管理CR3高达44.6%
  - ✓ 综合来看，启明星辰、深信服在近年来已经逐步由头部厂商蜕变为龙头厂商

- 行业竞争格局由分散向集中变迁一方面受到技术演进、企业招标模式变化等外围因素的影响，另一方面也是头部厂商加码研发推进产品化并加速产业并购的结果

2018年国内网安部分市场市占率情况

大类	细分	市占率Top 3企业
安全硬件	虚拟专用网（vpn）	深信服（30.6%）、启明星辰（10.6%）、天融信（7.2%）
	统一威胁管理	网御星云（16.2%）、深信服（14.1%）、奇安信（13.3%）
	安全内容管理	深信服（25.5%）、奇安信（13.3%）、绿盟科技（5.8%）
	入侵检测与防御	启明星辰（19.6%）、绿盟科技（19.3%）、新华三（11.3%）
	防火墙	天融信（22.4%）、华为（21.4%）、新华三（19.3%）
安全软件	终端安全软件	奇安信（22.9%）、Symantec（17.0%）、亚信安全（9.4%）
	身份和数字信任软件	吉大正元（16.3%）、亚信安全（15.0%）、格尔软件（11.3%）
	AIRO（安全分析、情报、响应和编排）	绿盟科技（21.2%）、启明星辰（16.0%）、IBM（15.6%）

资料来源：IDC、华西证券研究所

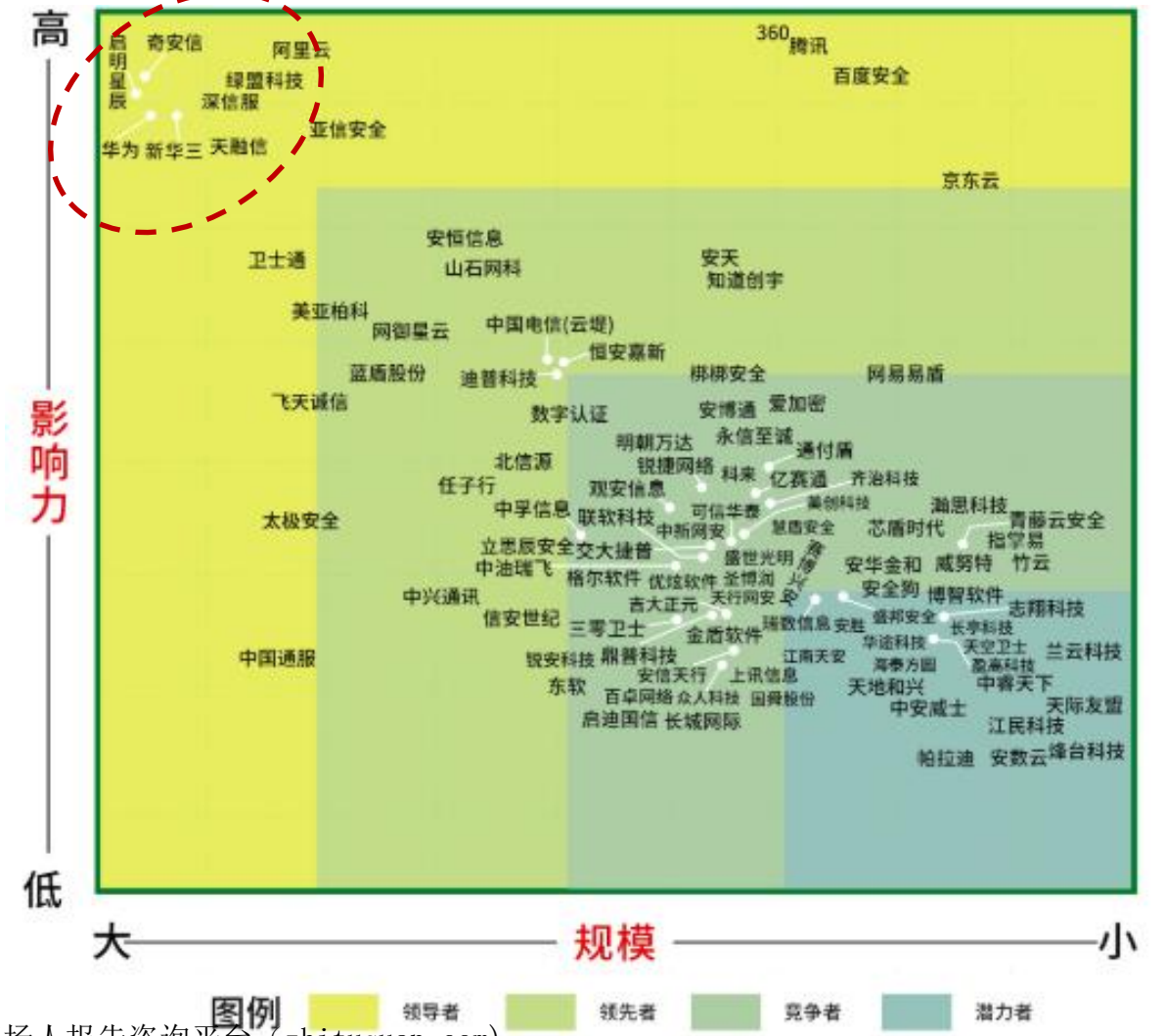
1.5 聚焦加速期中点，头部厂商不断扩展，优势正在凸显

- 将当前格局对应至最新的"安全牛网络安全企业年度榜单"（业务规模/技术影响力二维评定）：
- 2019年榜单规模较2015年扩大4倍，Top 25 → Top 100，但第一队却更为凸显
- 第一梯队愈发鲜明：启明星辰、奇安信领跑，深信服、华为、新华三（紫光股份）、天融信、绿盟科技以及阿里云紧随其后，八家公司构成第一梯队
- 其他厂商在综合实力上差距较大，退而寻求差异化竞争，依旧具有冲击第一梯队潜力的厂商包括：

✓ 亚信安全、安恒信息 、 卫士通 、安天、 山石网科 、美亚柏科 、梆梆安全、 迪普科技 、知道创宇、恒安嘉欣 、 蓝盾股份 、 北信源 、通付盾等

✓ 其中大部分都已经上市或递交了科创板上市材料

2019中国网络安全100强

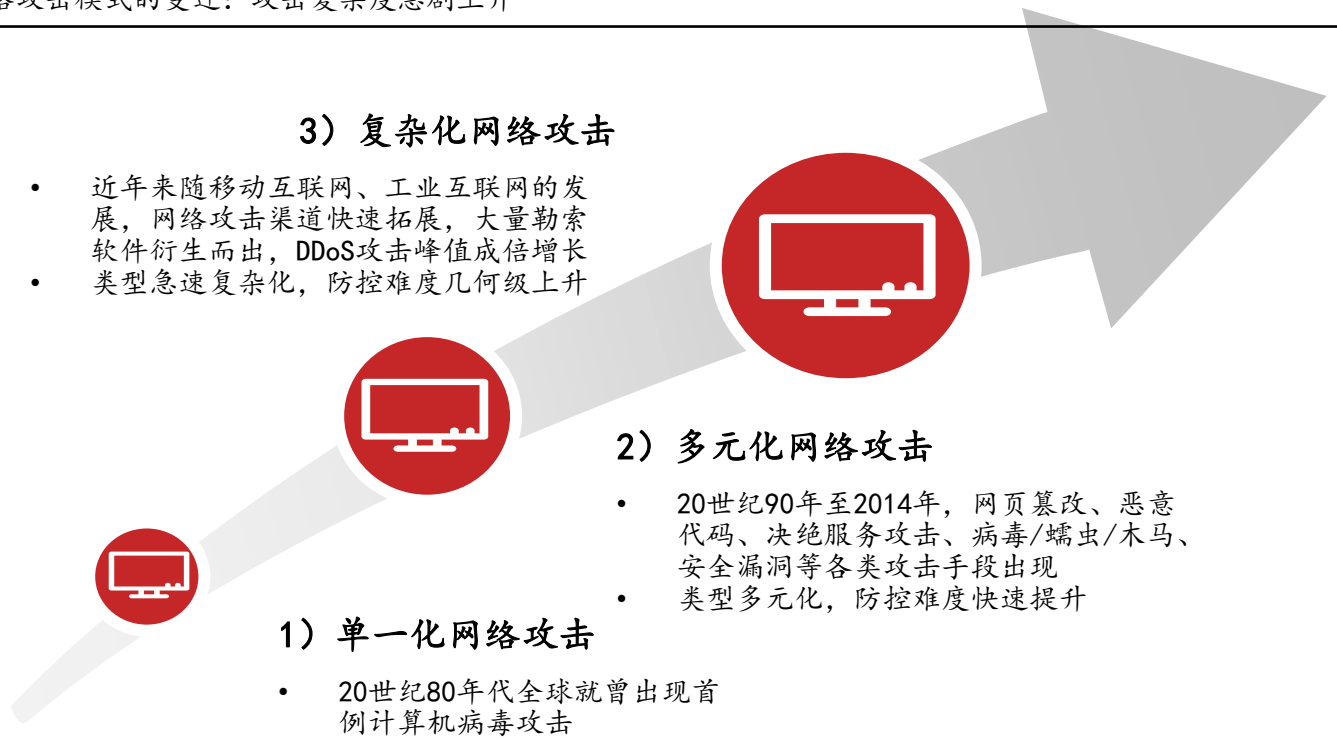


资料来源：安全牛、华西证券研究所

1.6 外部环境促成头部崛起：网络攻击急剧复杂化，全面防御需求激增

- ◆ **近几年移动互联网、工互联网的快速发展极大拓展了网络攻击的渠道，攻击模式急剧多元/复杂化，客户对网安厂商全面防御的要求提升**
- ✓ 随着互联网的高速发展及物联网、工业互联网、云计算、大数据等新兴技术的兴起，网络攻击形态日益复杂，单一领域的单一产品无法再满足网络安全防护需求，下游各类客户转而向头部厂商寻求一体化网安解决方案
- ✓ 根据IDC统计，2019年我国已经成为网络攻击中位列世界第二的国家，下游各领域客户网安需求随之激增

网络攻击模式的变迁：攻击复杂度急剧上升



资料来源：安全牛、华西证券研究所

1.6 外部环境促成头部崛起：摆脱分散招标模式，卡位厂商发力安全服务

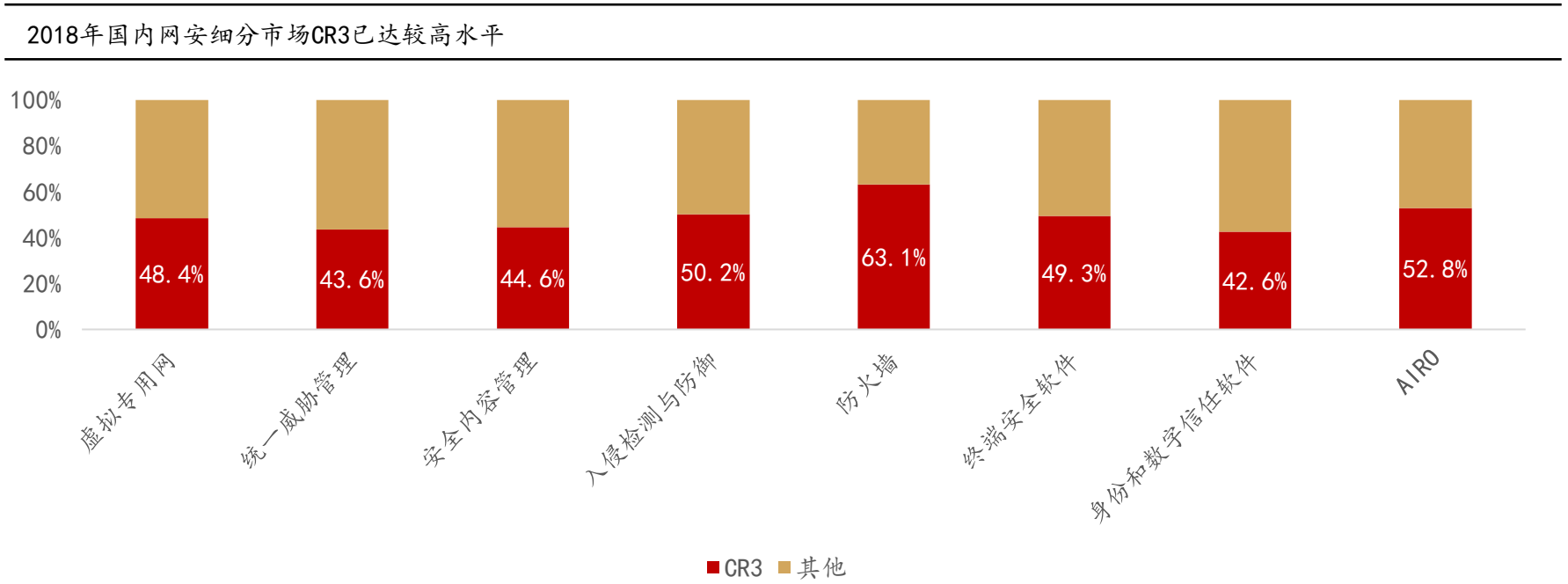
◆ **政企正在逐步摆脱分散招标，入围网安厂商的订单规模持续扩张**

✓ 对政企而言，网安需求正在从单一的产品向整体的安全防护发展，对于整体安全解决方案相关的招标数量也开始上升，拥有完整软硬件方案及系统集成能力的厂商将具备更强的竞争优势

◆ **我国安全服务市场还处于萌芽发展阶段，随着下游分散招标模式的放开，基于一体化解决方案的安全服务有望成为头部厂商新增长点**

✓ 目前，部分细分领域已经具备较高的行业集中度，看好同时在多个细分领域具备卡位优势的头部厂商进一步扩张

✓ 安全服务是厂商一体化服务重要组成部分，也是当前头部厂商的重点发力领域，正逐步成为新的增长引擎



资料来源：安全牛、华西证券研究所

1.6 外部环境促成头部崛起：各市加速布局安全产业园，集聚效应利好头部厂商

◆ 全国一线、强一线城市都纷纷布局安全产业园，头部厂商利用产业园的集聚效应，通过外延并购新兴安全领域的企业进行外延扩张

✓ 网络安全产业已经成为国家重点支持的产业，预计相关投入也会持续加大，当地头部企业优先受益

◆ 目前我国一线、强一线城市都在加快网络安全产业布局

✓ 以北京地区为例，2019年6月30日《国家网络安全产业发展规划》正式发布，工业和信息化部与北京市人民政府决定建设国家网络安全产业园区，提出"到2020年，依托产业园带动北京市网络安全产业规模超过1000亿元，拉动GDP增长超过3300亿元，打造不少于3家年收入超过100亿元的骨干企业"等目标

◆ 随着各城市加快网络安全产业布局，产业集聚效应有望带来行业进一步的集中

各市加快网络安全产业园布局

地点	具体政策
北京	到 2020 年，依托国家网络安全产业园区拉动 GDP 增长超过 3300 亿元，全市网络安全产业力争达到千亿元规模，将北京市建成国内领先、世界一流的网络安全高端、高新、高价值产业集聚中心。
天津	天津滨海信息安全产业园以 3 个国家级中心、3 个省部级中心、4 个行业联盟、13 家核心高新技术企业为依托，力争打造国家级信息安全产业基地
上海	将互联网信息安全产业纳入”十三五“发展重点，支持互联网安全行业加快突破，国家信息安全成果产业化（东部）基地将聚集人才、技术和资源，促进产业成果转化
杭州	先后发布并实施了《杭州市计算机信息网络安全保护管理条例》（浙江省杭州市人大常委会发布）《杭州市信息安全产业发展“十三五”规划》（杭州市经济和信息化委员会发布）等多部政策条例
武汉	武汉市人民政府发布了《关于支持国家网络安全人才与创新基地发展若干政策的通知》，提出支持体制机制创新、鼓励企业投资、保障土地供应、鼓励科技创新、加大人才引进培养力度等十项重点举措
四川	四川省人民政府发布的《四川省信息安全产业发展规划（2015-2020 年）》提出 2020 年实现安全产业规模 1100 亿元目标，国家信息安全成果产业化（西部）基地总占地面积 14 万平方米，集研发、生产、销售及服务于一体

资料来源：CCID、公开资料、华西证券研究所

1.7 内生成长加速头部崛起：研发加码聚焦产品化

◆ **研发为王，持续投入奠定产品化优势**

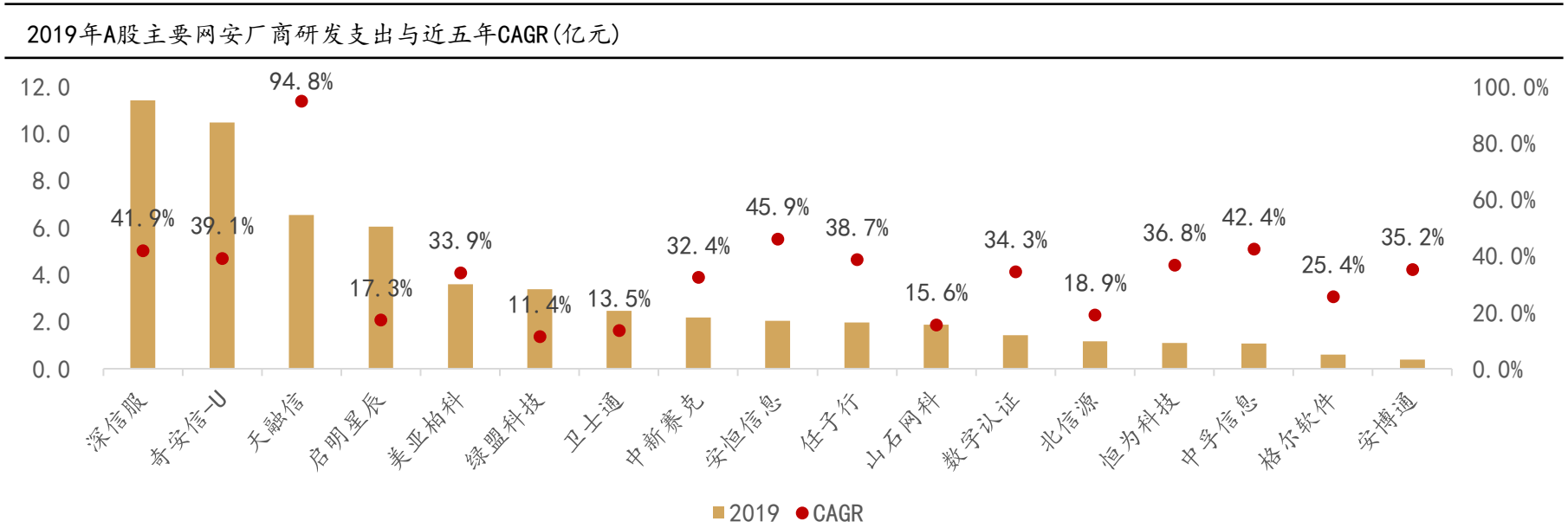
✓ 面对愈加复杂化的网络攻击，近五年来看核心技术持续升级，从传统的围墙式防护发展至主动对安全威胁进行检测/响应

✓ 网络安全已经由过去的“90%防护+10%检测与响应”变成了“60%防护+40%检测与响应”，新型传感器、不同的数据源、分析工具以及操作需求推动着整体安全技术向更全面的事件驱动软件架构变革。在此背景下，产品化能力无疑成为竞争的关键所在

◆ **2015-2019年来看，深信服、奇安信等巨头在研发投入方面遥遥领先，打造了领先业内的产品化能力**

✓ 两家公司的研发投入CAGR分别为41.9%、39.1%显示产品化战略在这一时期的展业中体现极大价值（天融信则是由于原业务的低研发特性导致）

✓ **深信服**属于这一时期的后起之秀，凭借极致的产品化投入（约为第三名两倍）一举成为头部厂商；**奇安信**则与360分家后快速崛起



资料来源：wind、华西证券研究所，备注：奇安信取2017-2019年数据

1.7 内生成长加速头部崛起：渠道建设成为跑马圈地利器

◆ **过去五年来看，在政策合规及内生需求的双重驱动下，下游行业客户群变化趋势呈现出两大特点：**

✓ 1）由中央直属部委向省、市地方政府逐级延伸的态势

✓ 2）由金融、能源行业的总部机构向其下属分支机构逐步推广的态势

◆ **面对下游细分市场，渠道体系和营销网络一定程度决定了企业的市场竞争力**

✓ 细分网络安全市场呈现区域分布广、 销售区域和用户分散的需求特征，企业借助渠道合作伙伴、采取渠道代理销售的模式可覆盖更广泛的用户群，渠道代理销售模式是业内较普遍的销售模式

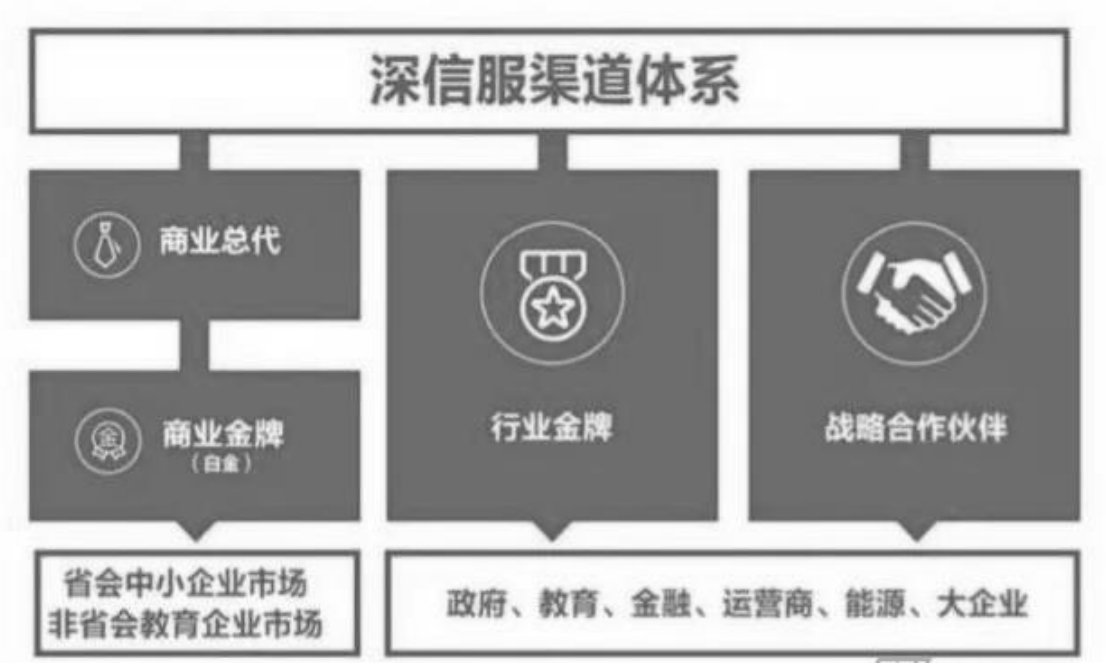
✓ 政府、金融、电信等行业对网络安全产品的需求量较大、技术和服务要 求较高，行业内企业对行业重点客户采取直销模式

◆ **渠道建设成为安全厂商在增量市场中跑马圈地的主要方式**

✓ 以华为、新华三、深信服为代表的安全厂商已经建立了相对完善的渠道体系

✓ 以深信服为例，公司推行全面渠道化战略，近三年公司代销收入均在97%以上

深信服渠道体系示意图



资料来源：深信服官网、华西证券研究所

1.7 内生成长加速头部崛起：频繁投资并购加速扩张

- ◆ 投融资和并购已经成为头部企业加快外延扩张的主要方式，新兴领域成为投融资和并购重点领域
  - ✓ 近年来全球网安领域融资并购众多，可得数据显示2018年并购整体规模达到300亿美元，热门领域包括区块链安全、云安全、IOT安全和数据安全等
  - ✓ 国内的龙头厂商也将通过并购创新厂商不断地抢占市场，与其他的安全厂商拉开距离

- ◆ 目前，启明星辰、绿盟科技、360等行业头部厂商均成立了相关产业基金，云安全、移动安全、工控安全等成为主要投资并购领域

启明星辰和绿盟科技近年来主要投资并购事件

公司	时间	交易标的	标的所属领域	交易金额（万元）
启明星辰	2017 年 1 月	智为信息 30% 的股权	抗 DDos 服务	3000
	2016 年 9 月	Cloudminds 3.5% 股权	云安全、移动安全	6300
	2016 年 7 月	书生电子 25% 股权	数据安全	6600
	2016 年 6 月	川陀大匠 85% 股权	终端安全	2700
	2016 年 6 月	赛博兴安 90% 股权	商用密码、终端安全	57915
	2015 年 6 月	书生电子 24% 股权	数据安全	5203
	2015 年 3 月	安方高科 100% 股权;合众数据 49% 股权	数据安全、大数据	37620

公司	时间	交易标的	标的所属领域	交易金额（万元）
绿盟科技	2018 年 6 月	杰思安全 14.29% 股权	安全检测与响应（EDR）	2000
	2017 年 5 月	Zenlayer 4% 股权	云计算（SDN）	1230
	2017 年 1 月	九州云腾 13.60% 股权	云安全	600
	2016 年 9 月	易霖博 10% 股权	安全培训、安全服务	500
	2016 年 4 月	逸得公司 15% 股权	大数据	600
	2016 年 4 月	NopSec 公司 9.57% 股权	威胁情报与风险管理	1491
	2016 年 3 月	阿波罗云 15.89% 股权	云计算（SDN）	850
	2015 年 6 月	杭州邦盛 11.56% 股权	反欺诈	2200
	2015 年 5 月	金山安全19.91% 股权	杀毒软件	4450
	2015 年 3 月	力控华康 11.63% 股权	工控安全	515

资料来源：wind、华西证券研究所

02 格局二：

变化 —— 由现在看未来，专精/审查型厂商并进

2.1 加速期开启下半场，龙头厂商恒强，专精/审查厂商齐飞

- 通过上一章分析不难发现：大型厂商的地位凸显并逐渐形成头部，而其余中小型厂商却仍陷于激烈竞争

- 但我们认为，在网安加速发展期的下半场，即大安全时代，强者恒强形成龙头固然是确定性趋势，但中小厂商却并非没有机会

- “大安全”时代，基于产业视角的网安厂商分类：

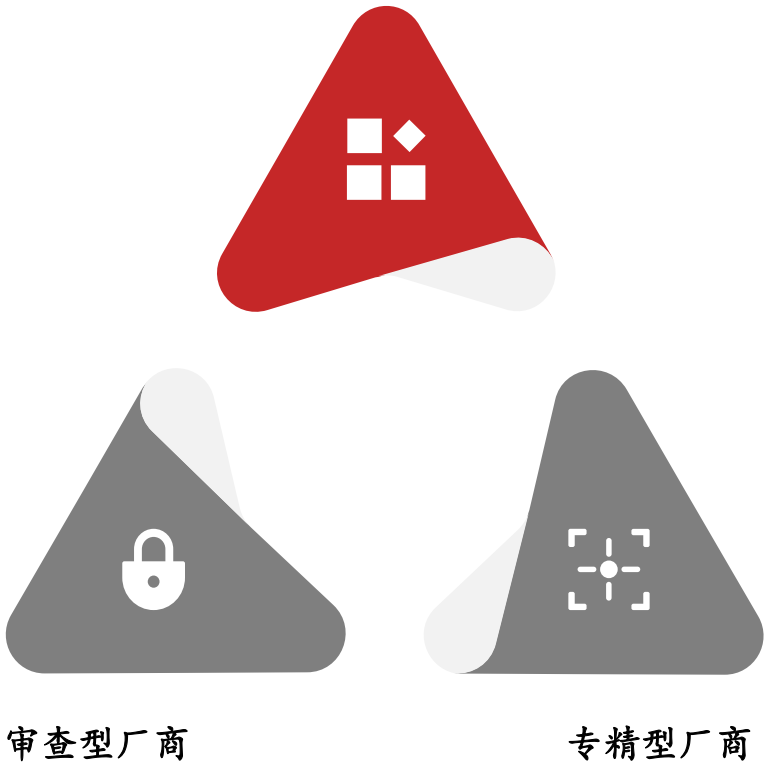
✓ 1）**全能型厂商**：具备较为齐全的安全产品线的厂商，至少在两到三个领域跻身市占率第一梯队，包括奇安信、深信服、启明星辰等

✓ 2）**专精型厂商**：其他细分市场龙头，多为深耕单一领域多年的单项冠军，包括安恒信息、卫士通等

✓ 3）**审查型厂商**：特定赛道厂商，产品和服务主要用于协助维护网络空间的秩序，属于更广义的网络安全定义，包括美亚柏科、中新赛克等

✓ 值得注意的是，新华三（紫光股份）作为网关型厂商独树一帜（与深信服相似），但考虑到核心业务贡献并非来自网安，暂不予讨论

基于产业视角的网安厂商分类



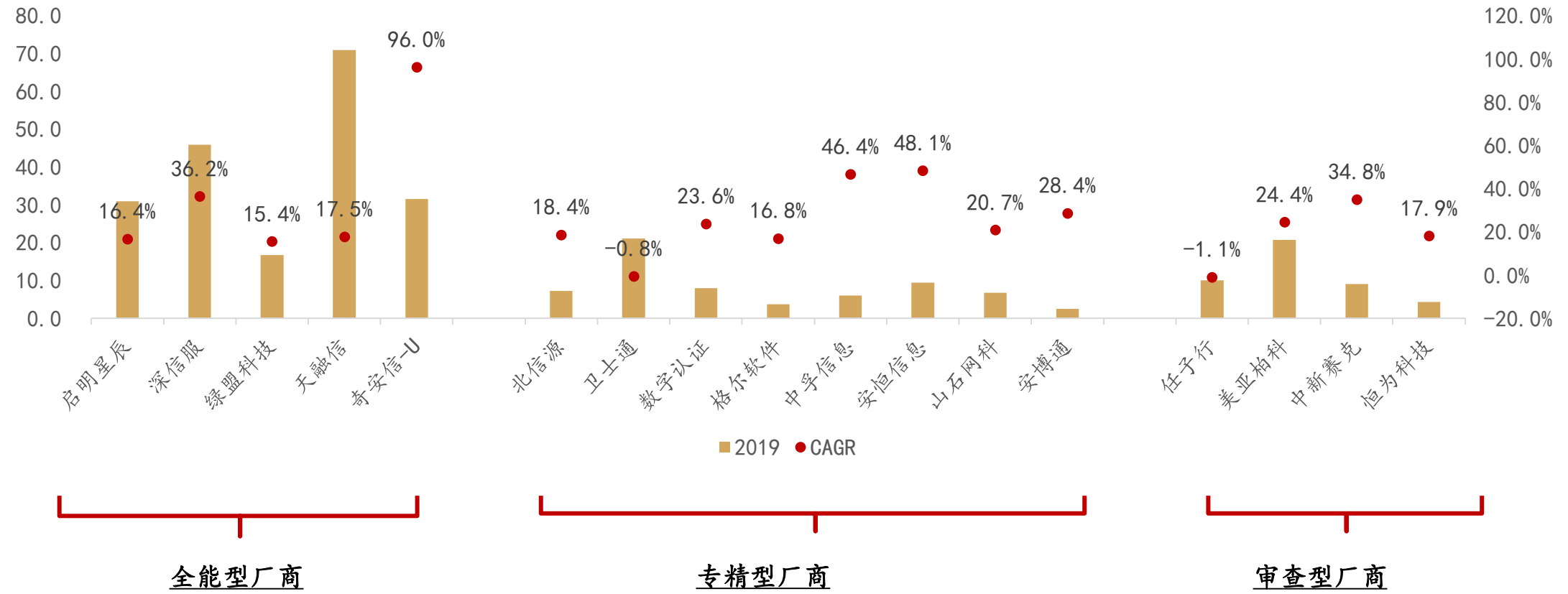
资料来源：华西证券研究所

2.2 产业视角下的网安公司划分：全能型/专精型/审查型三分天下

◆ 产业视角下的网安公司划分：全能型/专精型/审查型三分天下

✓ 过去两年间，三类厂商中的领军者大多保持高增速，部分专精型厂商和审查型厂商已经呈现异军突起之势

A股主要网安上市公司2019年营收与近两年CAGR(亿元)



资料来源：wind、华西证券研究所

2.3 全能型厂商占据头部，强势领跑

◆ **全能型厂商：高壁垒 + 产业地位强势**

✓ 从产业分析的角度来看，目前全能型厂商共五家：启明星辰、 深信服、绿盟科技、天融信、奇安信

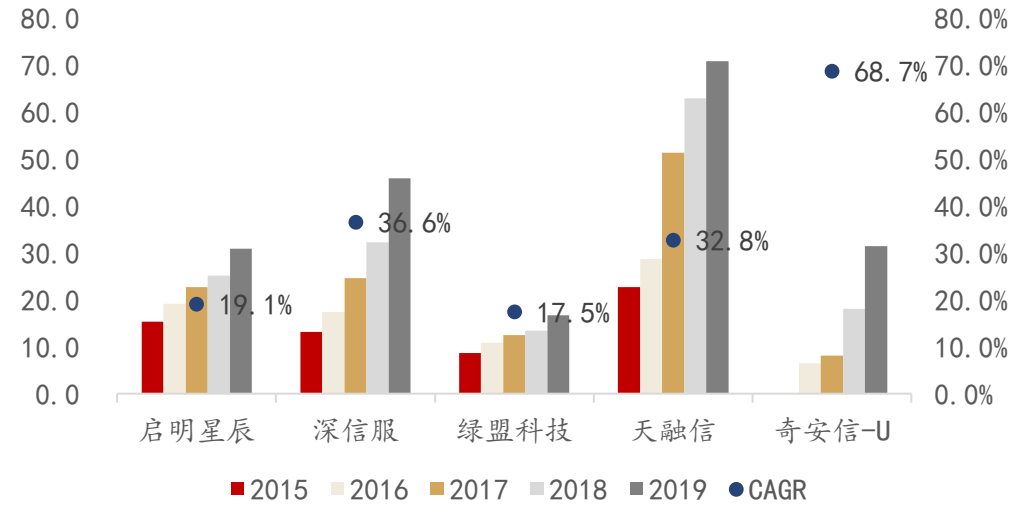
✓ 全能型厂商的特点是具备较为全面的安全防护能力，能够以自身产品对客户进行解决方案层面的构建，满足客户的整体安全需求

✓ **高技术壁垒是核心**：多元化的核心能力包括网关能力、全面攻防能力、态势感知能力，需要围绕用户具体需求进行长期高投入

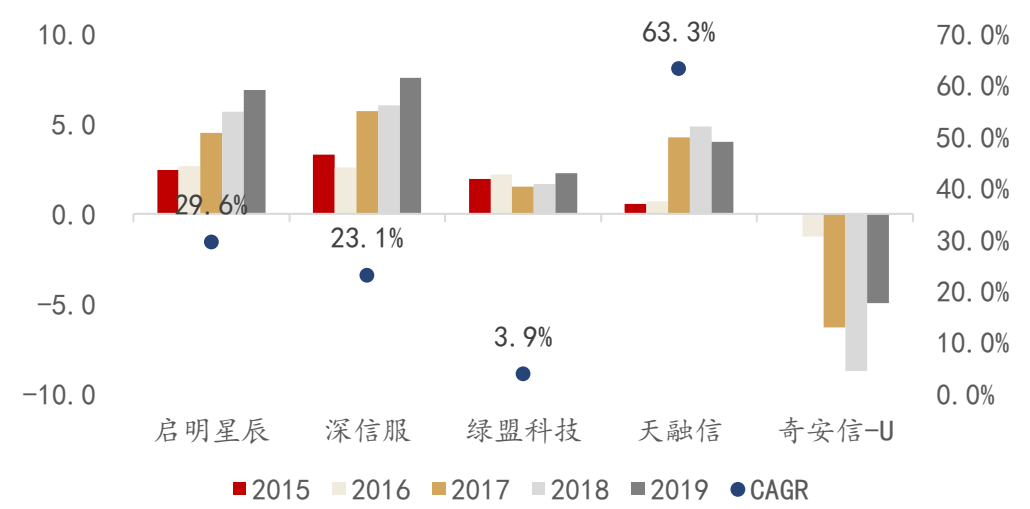
✓ 高技术能力的背后则是高研发的支撑，财务数据来看2019年五家上市的全能型厂商的研发投入基本位列行业前五，其中奇安信高举高打战略下研发亦是其重要投入，利润端尚未兑现

◆ **当前产业竞争格局来看，在未来的数年内其他的公司暂时没有成为全能型厂商的可能性**

2015-2019年网安全能型厂商营收表现及CAGR(亿元)



2015-2019年网安全能型厂商净利润表现及CAGR(亿元)



资料来源：wind、华西证券研究所，备注：奇安信取2016-2019年数据

2.4 专精型厂商偏安一隅，深耕优势凸显

◆ **专精型厂商：在细分领域呈现特色竞争优势**

✓ 目前A股专精型厂商主要包括北信源、卫士通、数字认证、格尔软件、中孚信息、以及科创板上市的安恒信息、山石网科和安博通

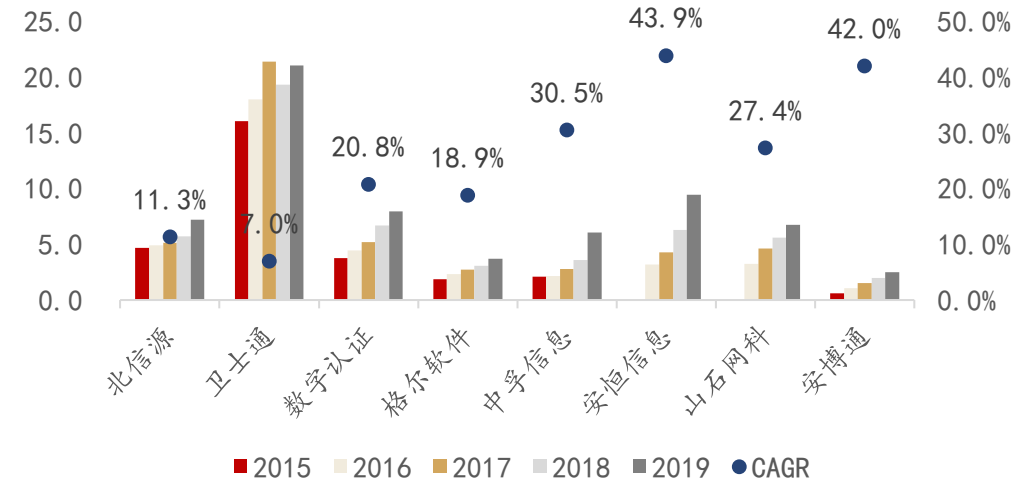
✓ 专精型厂商的特点在于，在特定细分领域往往有明确的优势，但是其在通用安全产品层面(如防火墙、入侵检测、SOC、数据安全)竞争实力较弱，且没有明确的向此方向扩张的预期

✓ 但在技术含量和技术壁垒相较于全能型厂商仍有差距

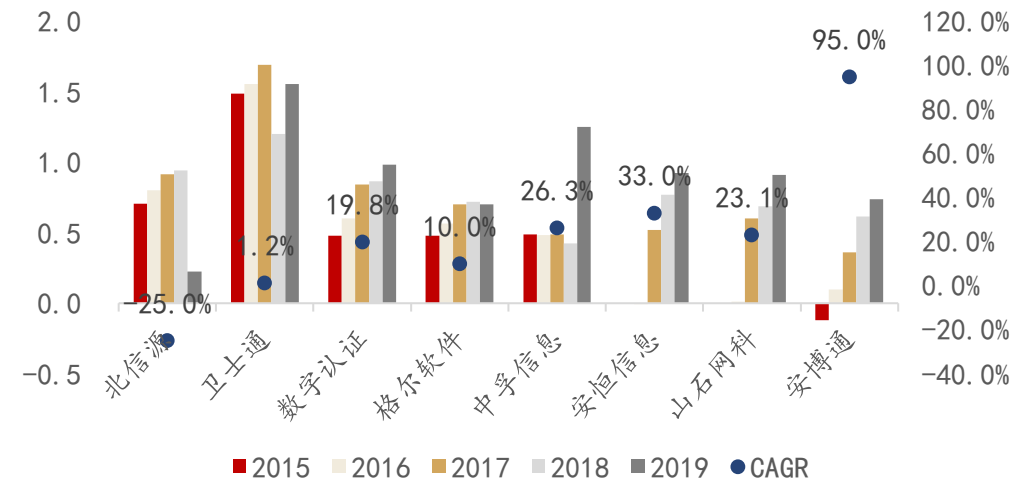
✓ 业务的拓展受到较大限制，未来发展很大程度上取决于该细分领域的景气度，目前看云大物工移等新兴安全领域机遇较大

◆ **综合来看，多数专精化厂商是小而稳的企业，其投资机会更多要关注该领域的细分产业政策以及部署实施节奏**

2015-2019年网安专精型厂商营收表现及CAGR(亿元)



2015-2019年网安专精型厂商净利润表现及CAGR(亿元)



资料来源：wind、华西证券研究所

2.5 审查型厂商弯道超车，后来居上

◆ **审查型厂商：受益网络空间治理，政策驱动特点鲜明**

✓ 网络空间治理近年受到高度关注

✓ 该产业下游往往为政法系统单位，在关键技术、产品、标准和渠道方面具有相对明确的进入门槛，产业竞争格局稳定，新进入者少

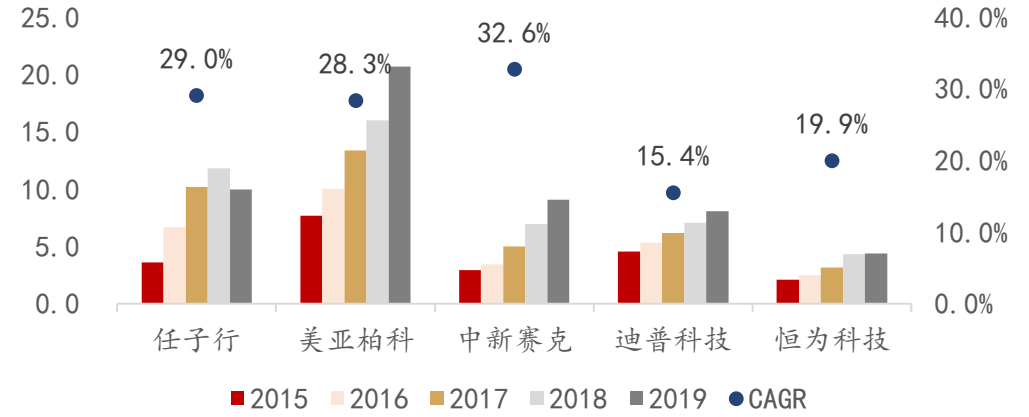
✓ 此外，网络空间治理涉及到一些大数据的能力和实施经验，这也构成了产业的壁垒

◆ **该细分领域内主要参与者有五家，分别是任子行、美亚柏科、中新赛克、迪普科技和恒为科技，近年来业绩普遍维持高增速**

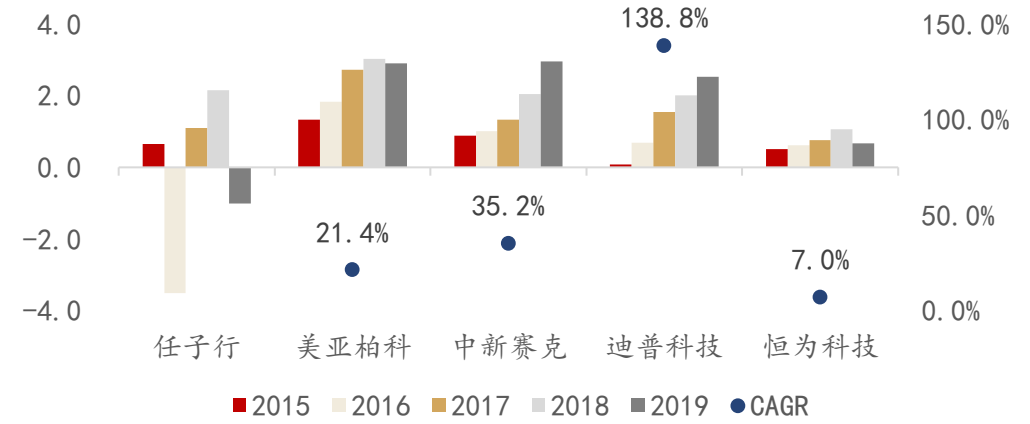
✓ 增长受政策驱动特征明显，其下游客户在需求逻辑层面和其他三类厂商有明显不同，该细分领域下游具有鲜明的网络执法属性，业绩会受到相应政策、落地节奏、更新换代的显著影响

✓ 值得注意的是，利润端来看任子行呈现较大波动，迪普科技受益低基数展现较高复合增长率

2015-2019年网安审查型厂商营收表现及CAGR(亿元)



2015-2019年网安审查型厂商净利润表现及CAGR(亿元)



资料来源：wind、华西证券研究所

2.5 审查型厂商弯道超车，后来居上

◆ 审查型厂商赛道不同于其他网安厂商，政策特点造就一定程度的“错位竞争”

◆ 美亚柏科所在审查赛道为公安大数据，当前仍是蓝海，政策红利持续释放

✓ 信息化一直是公安能力升级的重点，十九大以来公安部党委始终坚持改革强警、科技兴警，把大数据智能化建设作为科技兴警的重要抓手、上升为公安部党委的一项战略工程。近年来政策不断推行，而公安大数据的建设成为屡次被重点强调的核心，当前仍是建设高峰期

✓ 公司是传统网络空间安全专家，以电子取证聚焦在公安领域，尽享政策红利

✓ 随着产品在公安体系内多部门、多警种的应用逐步深入，公司在公安大数据领域龙头优势凸显

✓ 近期公司联合新德汇设立以大数据智能为核心的科研基地—“广东大数据研究院”，深耕公安大数据与智慧司法领域

◆ 中央网络安全和信息化领导小组的技术支撑，网络可视化景气向好

✓ 2014 年 2 月 27 日，中央网络安全和信息化领导小组正式成立，标志着网络安全与信息化已经上升至国家战略；2016 年初，网络安全被正式划入“十三五”规划的重点建设方向，2017 年 6 月 1 日，《中华人民共和国网络安全法》正式生效，从法律层面上把我国网络安全工作提高至国家安全战略的高度

✓ 中新赛克针对政府及公安部门等主要客户群体需求，不断进行产品研发与展业，并在2018、2019年中标多市公安局等公安机关项目

✓ 公司是原中兴通讯旗下公司，在网络可视化领域居于龙头地位，直接受益政策红利

✓ 近年来持续专注于大容量智能网卡及分流设备、无线增值业务、宽带增值业务的研发和市场拓展，为政府部门、运营商和行业用户提供成熟的通信安全保障解决方案和一站式的服务

资料来源：wind、华西证券研究所

2.6 他山之石：美股专精厂商Zscaler弯道超车

◆ 我们认为，在“大网安”时代，除了传统全能新龙头以外，专精型和审查型厂商也各有机会

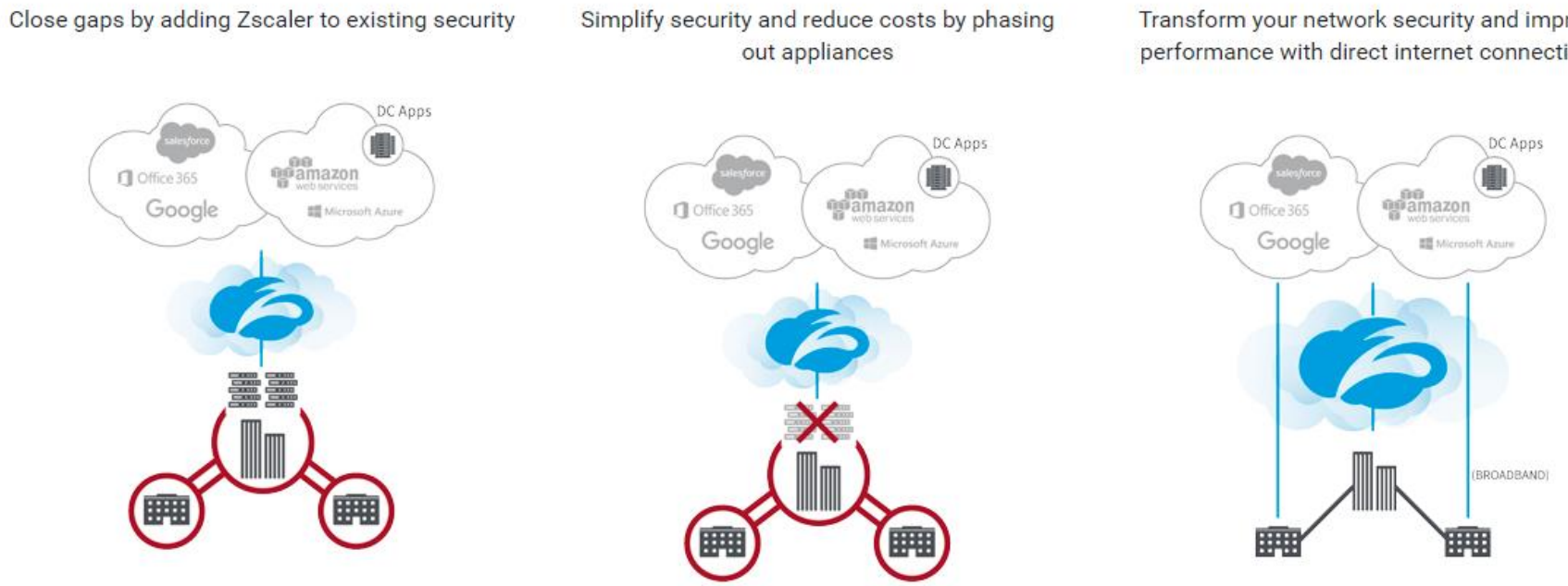
◆ 他山之石：美国发达安全市场经验可以论证我们的观点

✓ Zscaler是美国一家从事云安全服务的厂商，公司成立于2008年，彼时美国信息安全行业已被赛门铁克等传统安全厂商所占据

✓ 然而云安全服务还没有开始普及，Zscaler抓住机遇将公司业务方向全部投入到云安全领域中，后续快速发展取得突破

✓ 公司于2018年3月上市，目前市值达到100亿美元

Zscaler Internet Acces（核心产品）示意图



资料来源：Zscaler官网、安全牛、华西证券研究所

2.6 他山之石：美股专精厂商Zscaler弯道超车

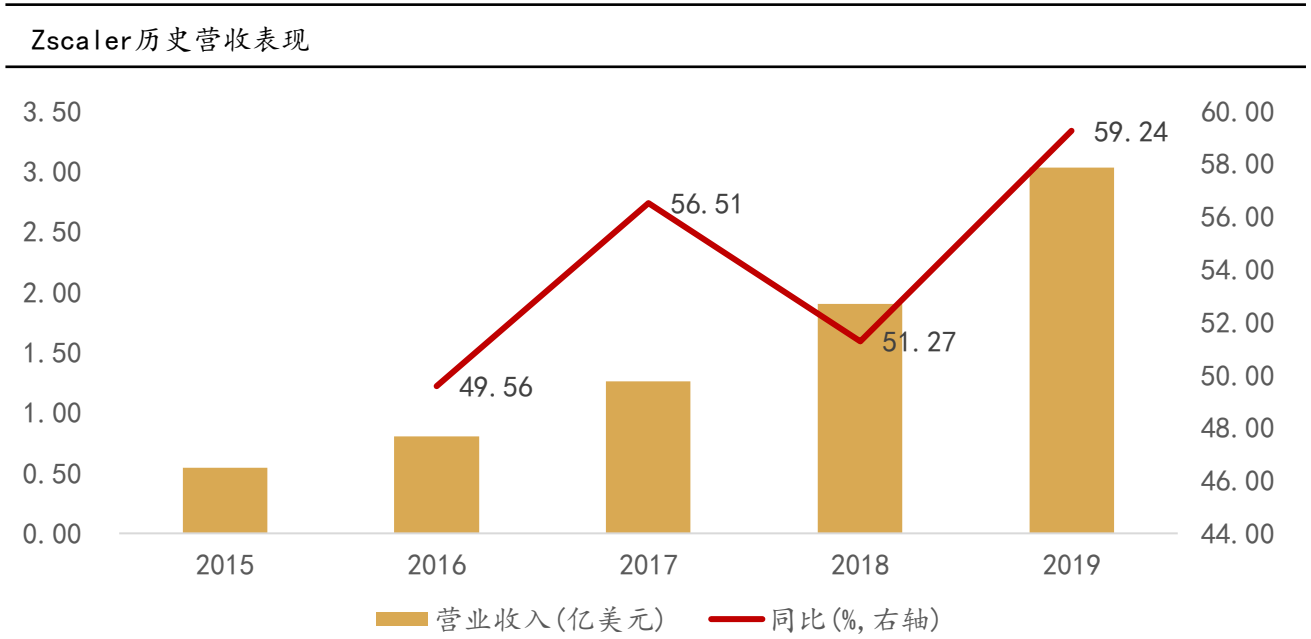
◆ 发展历程来看：

✓ 1）Zscaler成立于2008年，是最早布局云安全服务的美国网络安全公司之一

✓ 2）与传统本地部署安全设备不同，Zscaler的云平台以服务的形式提供安全服务，优化了对传统的本地安全设备的需求和维护

✓ 3）Zscaler从一个新企业通过深耕新兴赛道并不断地融资，最终突破全能型厂商（赛门铁克等）的封锁，最终于纳斯达克成功上市

◆ 通过参照Zscaler的发展路径不难发现，面对新安全技术如态势感知、云安全、威胁情报等市场的快速发展，中小型网安厂商（以专精型厂商为主）可以通过持续的研发投入不断提升在特定领域的技术壁垒，从而在新兴领域发展壮大



资料来源：wind、华西证券研究所

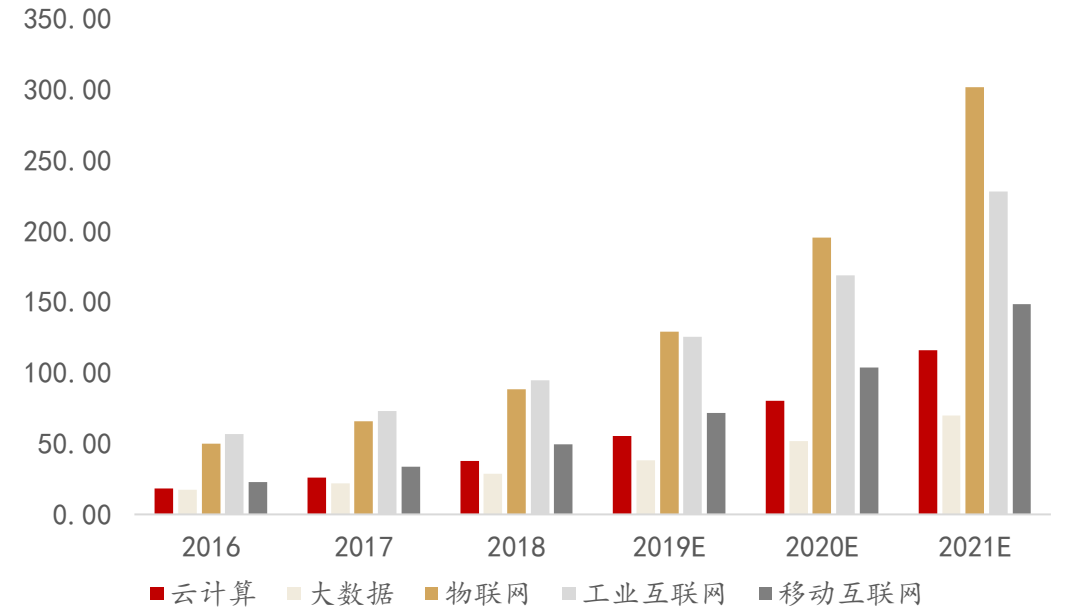
2.7 “云大物工移“ 及新兴领域是专精厂商主战场

◆ 当前来看，“云大物工移“ 相关安全领域是最有潜力的网安新兴市场

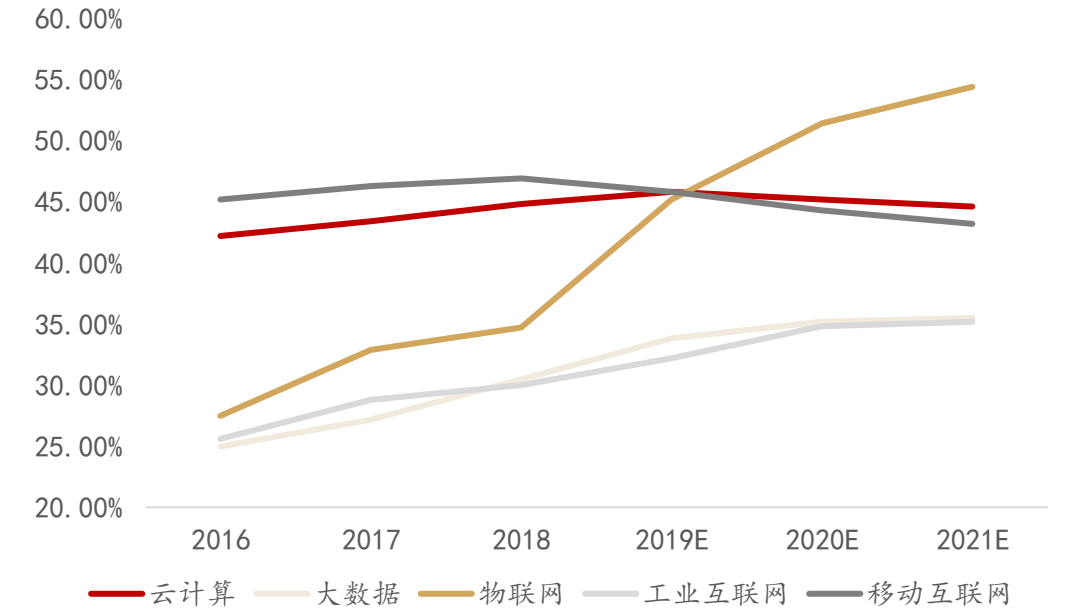
✓ 在云计算、大数据、物联网、工业互联网、移动互联网等前沿技术的驱动下，网络安全行业应用场景不断扩展 ， 市场不断增长

✓ 根据CCID预测，到 2021 年我国云计算安全、大数据安全、物联网安全、工业互联网安全、移动互联网安全市场规模分别为115.7亿元、69.7亿元、301.4亿元、 228亿元、 148.2亿元，未来两年各细分领域年均复合增速均超过30%

“云大物工移“细分市场规模及预测（亿元）



“云大物工移“细分市场规模增速及预测



资料来源：CCID、华西证券研究所

2.7 “云大物工移“及新兴领域是专精厂商主战场

- ◆ 根据《2019年网络安全白皮书》部分专精厂商已经在各新兴技术和业务领域占据先机，有望率先取得业务突破

- ◆ 但需要注意的是，随着政务云、智慧城市等IT基础设施建设集约化趋势愈发明显，传统IT巨头也在介入网络安全领域，阿里云目前也已经在云安全、物联网安全领域积极布局

- ✓ 将云服务和安全能力整合，直接提供整体解决方案给客户是未来云计算发展的大趋势，判断未来科技巨头和安全厂商的竞合关系将进一步复杂化

2018年新兴领域领导厂商

新兴技术领域	典型厂商
云安全	阿里云、知道创宇、 安恒信息 、绿盟科技、启明星辰 、奇安信
大数据安全	奇安信、 启明星辰 、 亿赛通 绿盟科技 、 绿盟科技 、 美亚柏科 、 明朝万达
物联网安全	奇安信、 青莲云 、 绿盟科技 、 阿里云 、 华为
工业互联网安全	威努特、 天地合兴 、 海天炜业 、 力控华康 、 长扬科技
移动互联网安全	梆梆安全、 爱加密 、娜迦信息、 通付盾
量子通信安全	国盾量子 、 问天量子 、 神州信息 、 中国有线 、 神州数码 、 中国通信建设 、四创电子 、 科华恒盛 、 蓝盾股份 、 新海宜 、 阿里巴巴
态势感知	奇安信 、 安恒信息 、 启明星辰 、 亚信安全 、 安博通
威胁情报	ThreatBook 、 奇安信 、 威胁猎人 、 安天 、 白帽汇
区块链网络安全	知道创宇 、 白帽汇 、 BugX 、 成都链安 、 慢雾科技 、 Halo Block

资料来源：CCID、IDC、华西证券研究所

2.8 由现在看未来，全能型厂商恒强 + 专精/审查型厂商并进

◆ 网安加速发展期的上半年（2015年至今），外围环境 + 内生成长合计六大因素促使行业集中度逐步提升，随着深信服和奇安信的异军突起，五大全能型已经稳守龙头位置

◆ 1）外部环境因素：

✓ 全面化：技术复杂化带来全面防御需求

✓ 服务化：摆脱分散招标模式，发力安全服务

✓ 集聚效应：安全产业园产生集聚效应

◆ 2）内生成长因素：

✓ 产品化：研发加码聚焦产品化

✓ 渠道化：渠道建设成为竞争关键

✓ 发力并购：频繁并购加速扩张

◆ 展望网安加速发展期的下半场，我们认为外部环境的三大趋势仍将延续，而内生成长的三方面优势甚至将进一步强化，因此龙头恒强的逻辑依旧坚挺，看好全能型厂商加速扩张

◆ 但另一方面中小厂商（专精型厂商、审查型厂商）却并非没有发展空间，新兴市场等因素带来弯道超车机遇，细分技术龙头前景可期

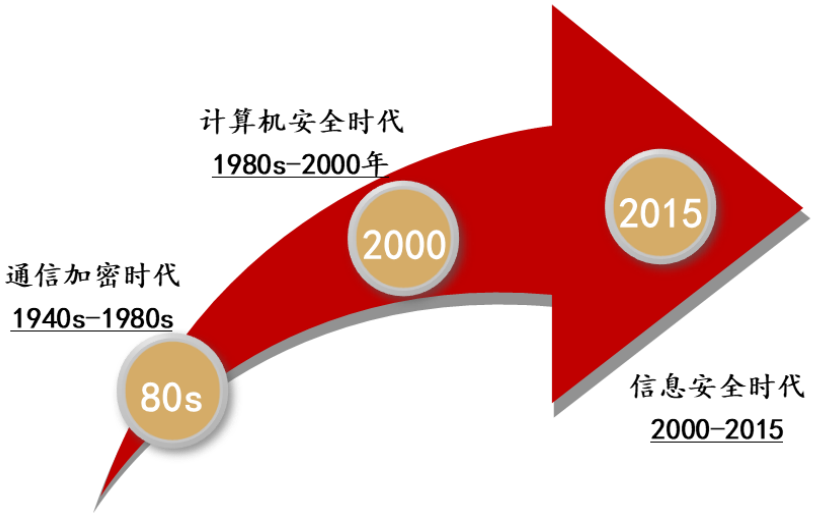
✓ 云大物智能新兴安全市场景气度高昂，为专精型厂商带来发展机遇

✓ 安恒信息的崛起正是基于这一逻辑；海外云安全厂商Zscaler的成功也是一例

✓ 此外，政策推动的审查型厂商同样迎来黄金发展期，错位竞争之下尽享政策红利

2.8 由现在看未来，全能型厂商恒强 + 专精/审查型厂商并进

我国网安行业格局演变图



外部环境因素：
- 技术复杂化带来全面防御需求
- 摆脱分散招标模式，发力安全服务
- 安全产业园产生集聚效应

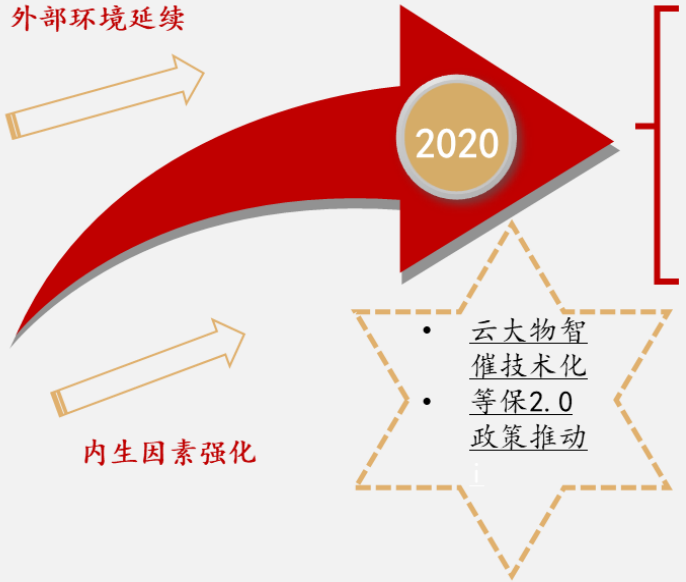
内生成长因素：
- 研发加码聚焦产品化
- 渠道建设成为竞争关键
- 频繁并购加速扩张

网络空间安全时代，即大安全时代

2015至今：加速发展期

外部环境延续

内生因素强化



- 云大物智催技术化
- 等保2.0政策推动

龙头恒强逻辑强化：
- 全能型厂商优势进一步凸显

新兴市场带来差异化竞争：
- 专精型厂商把握云大物智新趋势
- 审查型厂商尽享政策红利

相对分散：
- 启明星辰、天融信相对领先
- 其他厂商囿居中游

相对集中散：
- 启明星辰、天融信依旧领先
- 深信服、奇安信异军突起
- 头部集团优势明显

集中度继续提升

资料来源：华西证券研究所

03 空间 & 拐点

等保2.0打开千亿空间，关注后疫情拐点

3.1 政策强力推动，等保2.0驱动产业升级新需求

◆ 随着网络安全上升到国家战略高度，近年来体系列支持网络安全发展的政策，其中等保2.0更是重磅来袭，将驱动行业变革

政策面利好频密出台

时间	部门	文件	具体政策
2016年11月	全国人民代表大会常务委员会	《中华人民共和国网络安全法》	进一步界定了关键信息基础设施的范围、对攻击、破坏我国关键信息基础设施的境外组织和个人规定相应的惩治措施等。该法旨在保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展。
2017年11月	工信部	《关于开展2017年电信和互联网行业网络安全试点示范工作的通知》	在网络安全威胁监测预警、态势感知等八个方面引导企业加强技术手段建设，增强企业防范和应对网络安全威胁的能力，拉动网络安全产业发展，提升电信和互联网行业网络安全技术防护水平。
2018年3月	中央网信办、工信部	《关于推动资本市场服务网络强国建设的指导意见》	推动网信事业和资本市场协同发展，保障国家网络安全和金融安全，促进网信和证券监管工作联动。
2018年6月	公安部	《网络安全等级保护条例（征求意见稿）》	将风险评估、安全监测、通报预警、案事件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全、效果评价、综治考核等重点措施纳入等级保护制度并实施；将网络基础设施、重要信息系统、网站、大数据中心、云计算平台、物联网、工控系统、公众服务平台、互联网企业等全部纳入等级保护监管。
2018年9月	公安部	《公安机关互联网安全监督检查规定》	《规定》明确，公安机关应当根据网络安全防范需要和网络安全风险隐患的具体情况，对互联网服务提供者和联网使用单位开展监督检查，以保障互联网服务提供者和个人合法权益。
2018年10月	市场监管总局、国标委	《信息安全技术网络安全威胁信息格式规范》	对网络安全威胁信息进行结构化、标准化描述，以便实现各组织间网络安全威胁信息的共享和利用，并支持网络安全威胁管理和应用的自动化。
2018年12月	网信办	《金融信息服务管理规定》	要求金融信息服务提供者应当履行主体责任，配备与服务规模相适应的管理人员，建立信息内容审核、信息数据保存、信息安全保障、个人信息保护、知识产权保护等服务规范。
2019年3月	国务院	《中央企业负责人经营业绩考核办法》	新版较旧版增加了网络安全事件的考核要求，有助于极大增强相关企业负责人的网络安全意识并增加网络安全相关的投入，为《网络安全法》的贯彻落实提供支撑。
2019年3月	市场监管总局、中央网信办	《关于开展APP安全认证工作的公告》	APP安全认证工作开展，目的在于规范移动互联网应用程序收集、使用用户信息特别是个人信息的行为，加强个人信息安全保护。
2019年5月	**市场监管总局、国标委**	**《信息安全技术 网络安全等级保护基本要求》等**	**已发布的网络安全等级保护2.0的核心标准，明确了网络系统的等保定级标准，尤其明确了云计算、移动互联网、物联网和工业控制系统的安全扩展要求。**
2019年5月	教育部办公厅	《2019年教育信息化和网络安全工作要点》	核心目标中包含全面落实教育领域网络安全和信息化战略部署、出台落实网络安全责任制评价考核办法、建立网络安全培训机制等内容。
2019年9月	工信部	《关于促进网络安全产业发展的指导意见（征求意见稿）》	落实《中华人民共和国网络安全法》，到2025年，培育形成一批年营收超过20亿的网络安全企业，网络安全产业规模超过2000亿。

资料来源：CCID、华西证券研究所

3.1 空间：政策强力推动，等保2.0驱动产业升级新需求

◆ 等保2.0正式发布网安政策支持再升级

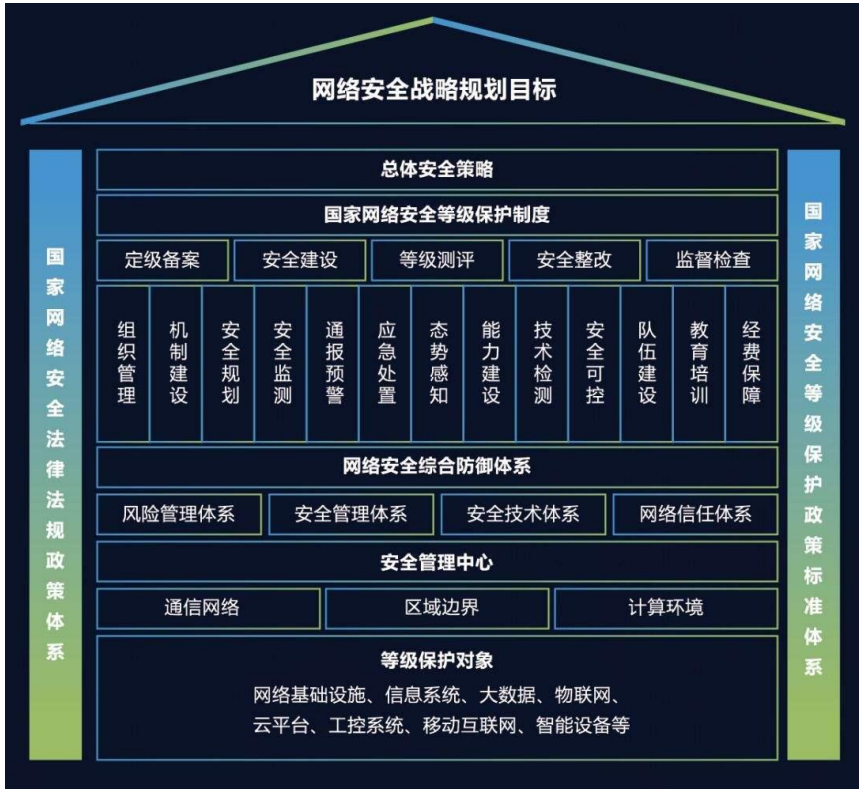
✓ 信息安全等级保护是对信息和信息载体按照重要性等级分级别进行保护的政策安排是我国网络空间安全保障体系的重要支撑

✓ 2019年5月13日《信息安全技术网络信息安全等级保护基本要求》国家标准正式发布将于2019年12月1日正式实施标志着我国网络安全等级保护工作正式进入"2.0时代

等保2.0 vs 等保1.0

	等保1.0	等保2.0
保障体系	被动防御：一个中心三重防护（防火墙、入侵检测、防病毒），以防为主	全方面主动防御：事前、事中、事后；感知预警、动态防护、安全监测、应急响应等
定级对象	信息系统	基础信息网络、工业控制系统、云计算平台、物联网、移动互联网、其他网络、大数据等多个系统
评测周期	三级的每年一次、四级的半年一次	三级以上系统每年一次
评测及格分	60分以上	75分以上
技术要求	包括技术要求（物理安全、网络安全、主机安全等）和管理要求（安全管理机构、安全管理制度、人员安全管理等）共290项	更新为技术要求（安全物理环境、安全通信网络、安全计算环境等）和管理要求（安全建设管理、安全运维管理、安全管理机构和人员等）共232项
其他新增要求	-	新增对新型网络攻击行为防护和个人信息保护等新要求；新增入侵防范（防火墙、IDS、IPS等）、恶意代码防范（邮件防护）、集中管控（VPN、堡垒机、终端安全软件、SOC/态势感知等）、安全审计（日志审计）等

等保2.0战略框架



资料来源：网络安全等级保护测评中心、梓华科技、华西证券研究所

3.1 空间：政策强力推动，等保2.0驱动产业升级新需求

◆ **等保2.0关注点一：明确新增云计算等新安全拓展要求**

✓ 从内容的结构上来看，新标准为安全通用要求+四大安全拓展要求（云计算、移动互联、物联网、工控），由此利好云计算、移动互联、物联网、工控四大信息安全新兴蓝海市场；

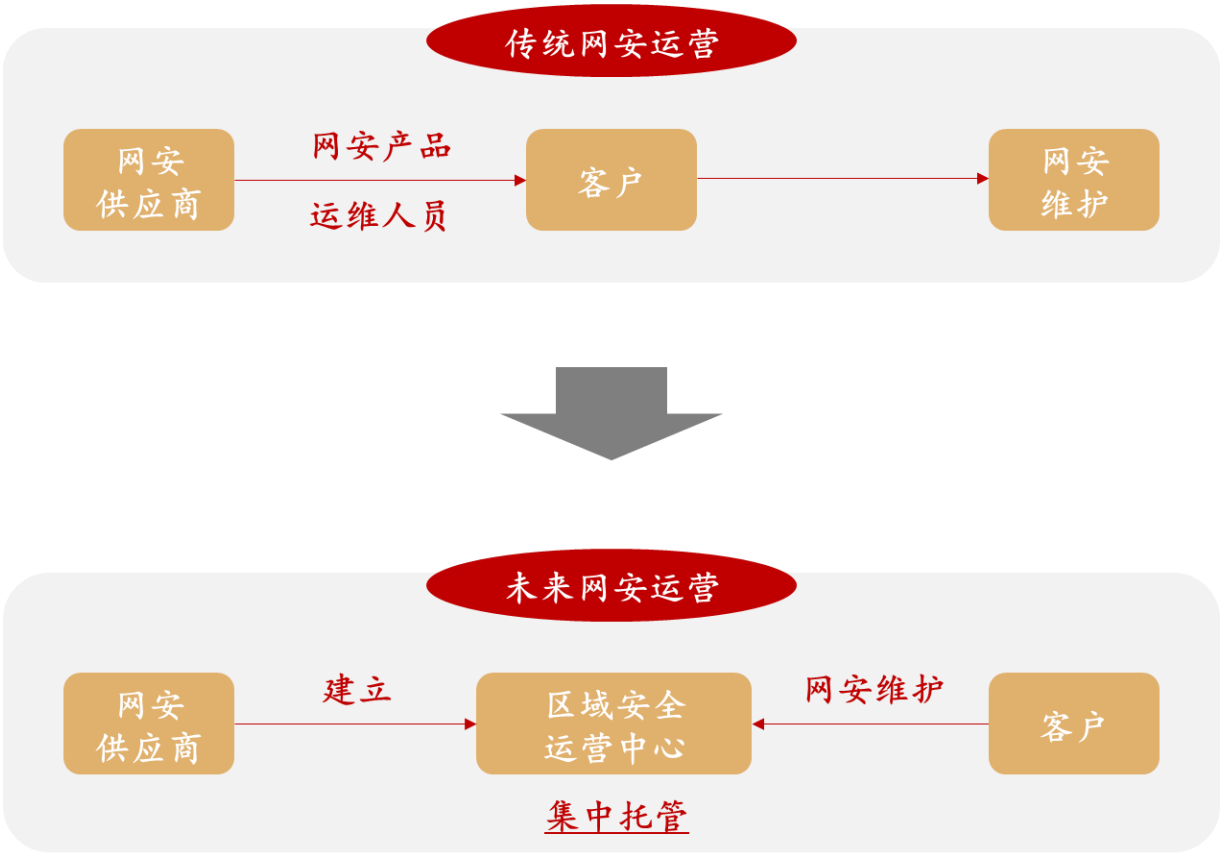
✓ 从下游需求侧产业逻辑判断，我们重点看好云安全以及工控安全新兴市场。

◆ **等保2.0关注点二：SOC迎来相应机遇**

✓ SOC（安全管理中心，或安全管理平台）内容被重点提及，二级至四级系统明确提及了SOC要求（五级安全要求公开的标准中略过，因其主要针对国家重点部门的系统）；

✓ 具体包括系统管理、审计管理、安全管理（三级&四级）、集中管控（三级&四级），后两者突出了汇总分析的功能，明确的提及了对于网络中的链路、安全设备、服务器等的运行情况进行集中监测、对于审计数据进行集中分析。

网络安全运营行业发展趋势



资料来源：网络安全等级保护测评中心、华西证券研究所

3.1 空间：政策强力推动，等保2.0驱动产业升级新需求

- 整个等保2.0以新的检查要求驱动新产品的采购，各单位为了满足等保测评分数以备案成功，往往会依照针对性新增采购。
- 新增要求项集中在入侵防范、恶意代码防范、集中管控、安全审计等方面。
- 此外SOC以及态势感知已经成为了新检查重点。

等保2.0新增新项目

属性	要求角度	新增要求项	对应产品
网络和通信安全	入侵防范	应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信；	防火墙、IPS、IDS
	入侵防范	应采取技术措施对网络行为进行分析，实现对网络公司，特别是未知的新型网络攻击的检测和分析；	APT、流量回测
	恶意代码防范	应在关键网络节点对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新；	邮件防护
	集中管控	应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；	VPN
	集中管控	应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；	堡垒机
	集中管控	应对分散在各个设备商的审计数据进行收集汇总和集中分析；	日志审计
	集中管控	应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；	终端安全
	集中管控	应能对网络中发生的各类安全事件进行识别、报警和分析；	SOC、态势感知
设备和计算安全	安全审计	访问控制的颗粒度应达到主体为用户级或进程级，客体为稳健、数据库表级；	日志审计
	集中管控	应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；	终端安全
应用和数据安全	安全审计	应强制用户首次登录时修改初始口令；应重命名默认账号或修改这些账号的默认口令；应及时删除或停用多余、过期的账号，避免共享账号的存在。	日志审计

资料来源：网络安全等级保护测评中心、华西证券研究所

3.1 空间：政策强力推动，等保2.0驱动产业升级新需求

◆ 产业调研经验显示，中国等保三级的系统约为五万个，二级系统数约60万个。

✓ 假设等保三级系统中，APT的新增渗透率为35%，流量回溯的新增渗透率为40%；

✓ 假设等保二级系统中，堡垒机、集中日志审计、数据库审计的新增渗透率分别为2%，4%，4%；

✓ 假设态势感知平台的新增渗透率为1% ；

✓ 假设等保咨询服务的新增渗透率为20%。

◆ 测算可知，等保2.0带来新增市场空间225亿元，增量可观。

等保2.0带来新增产品/服务市场空间约225亿元

产品/服务	单价（万元）	二级渗透率	三级渗透率	等保二级系统（万）	等保三级系统（万）	采购增量（亿元）
APT	20	-	35%	-	5	35
流量回测	15	-	40%	-	5	30
堡垒机	10	2%	-	60	-	12
集中日志审计	20	4%	-	60	-	48
数据库审计	10	4%	-	60	-	24
态势感知平台	400	-	1%	-	5	20
二级等保咨询服务	4	20%	-	60	-	48
三级等保咨询服务	8	-	20%	-	5	8
合计						**225**

资料来源：网络安全等级保护测评中心、华西证券研究所

3.1 空间：政策强力推动，等保2.0驱动产业升级新需求

◆ **考虑到传统领域的产品仍将是等保2.0要求的重点，相关领域的龙头企业必然成为市场蛋糕变大以后最大的受益方**

✓ 参与标准制定是行业部门对公司能力的肯定与背书，同时参与标准制定也有利于企业更加深刻地理解新标准的要求，因而值得重点关注

✓ 在等保2.0标准起草机构的名单中，启明星辰参与了三大核心标准的制定新华三（紫光股份）也参与了3个标准的制定，天融信（南洋股份）和绿盟科技则参与了安全设计技术要求的制定

等保2.0标准制定参与机构

标准	参与起草企业
《信息安全技术网络安全等级保护定级指南》（GA/T 1389-2017）	新华三（紫光股份 ）、阿里云
《信息安全技术网络安全等级保护测评过程指南》（GB/T 28449-2018）	-
《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）	启明星辰、 新华三（紫光股份 ）、 阿里云 、华为、鼎普科技
《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）	新华三（紫光股份）、 启明星辰 、微步在线、梆梆安全、科来软件、鼎普科技、讯达云成、中国移动、卓识网安、风云互联、华普科工
《信息安全技术 网络安全等级保护安全设计技术要求 》（GB/T 25070-2019）	天融信 、 启明星辰 、 绿盟科技 、 中软华泰 、阿里云、江南天安、华为、和利时、海天炜业、力控华康、石化盈科、华大智宝、微分电子、中电瑞凯、广利核

资料来源：CCID、华西证券研究所

3.2 空间：场空间缺口巨大，行业千亿机遇正在开启

◆ 近年来，我国的网络安全行业市场持续较快增长

✓ 根据CCID数据，我国近三年网络安全行业市场复合增速维持在20%左右；其中2018 年市场规模达495.2 亿元，同比增长20.9%

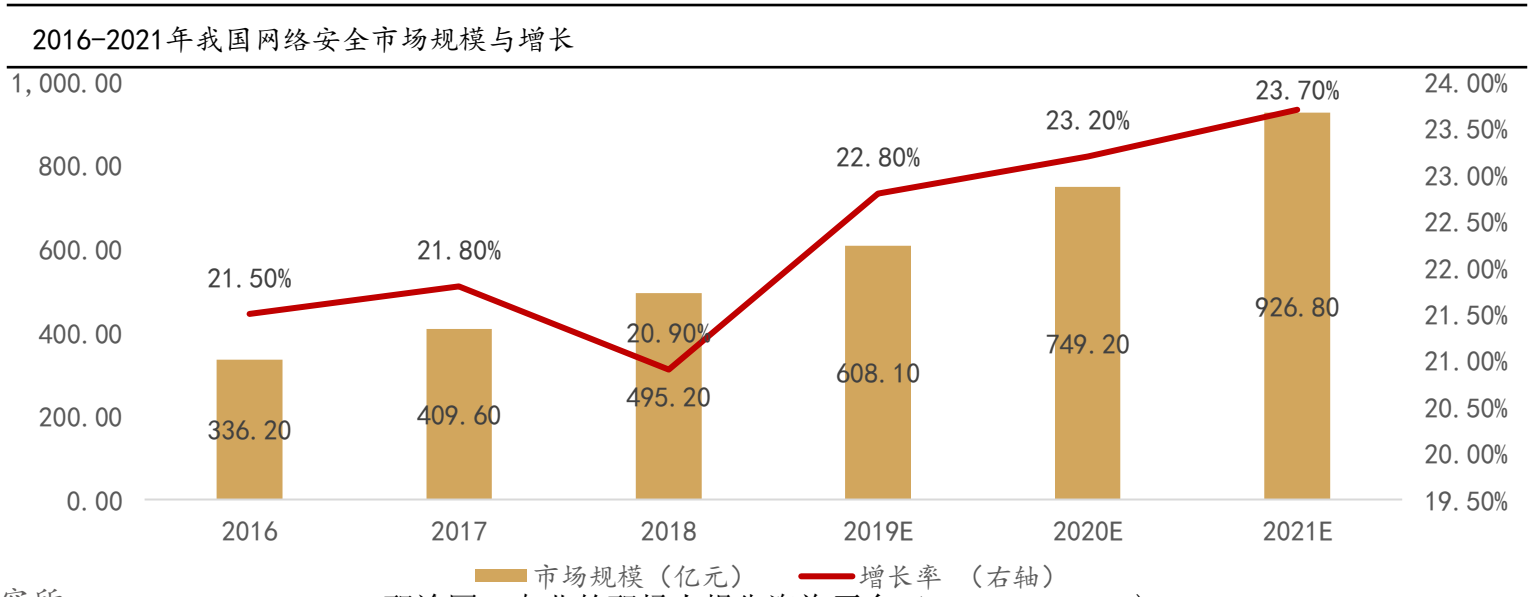
✓ CCID同时预测，2019-2021 年我国网络信息安全市场规模将由608.1 亿元增加至926.8 亿元，CAGR为23.45%

◆ 目前我国ICT市场整体规模投入完全可以支撑起千亿规模信息安全市场体量

✓ 据Gartner，2019年全球ICT支出为3.79万亿美元，全球信息安全投入为1240亿美元，占比约为3.3%

✓ CCID数据显示，我国目前ICT产业投资规模大概在2.6-2.8万亿之间，由此测算：我国整体ICT投入水平的信息安全市场规模至少应有千亿元

◆ 另一个维度来看，工信部《关于促进网络安全产业发展的指导意见（征求意见稿）》：2025 年我国网络安全产业规模将超2000 亿元



资料来源：CCID、华西证券研究所

3.2 空间：市场空间缺口巨大，行业千亿机遇正在开启

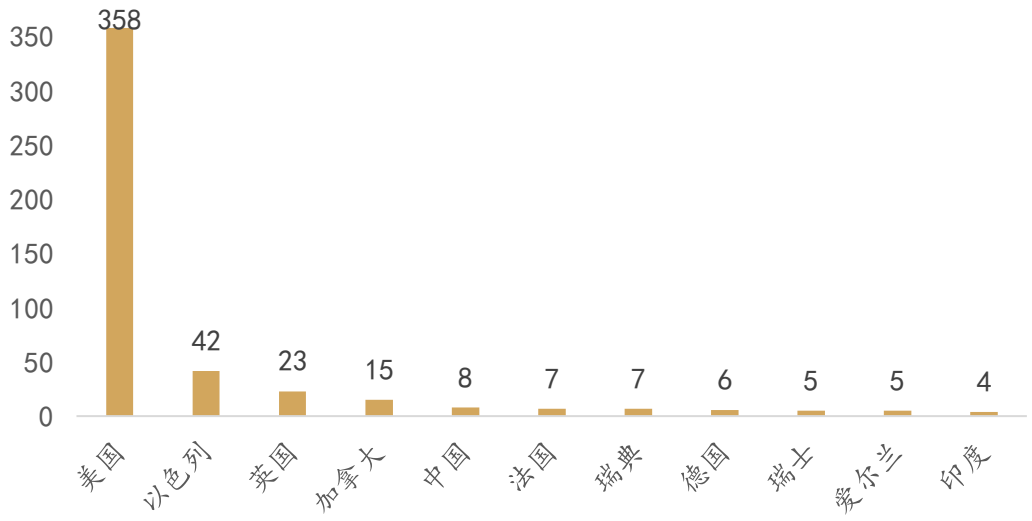
◆ 对标美国，我国网络安全市场仍具有极大成长空间

✓ Cybersecurity Ventures发布的《2018全球网络安全公司500强》显示美国在网络安全领域一枝独秀，上榜公司高358家；其次是以色列公司，共计上榜42家；中国以8家位列第五

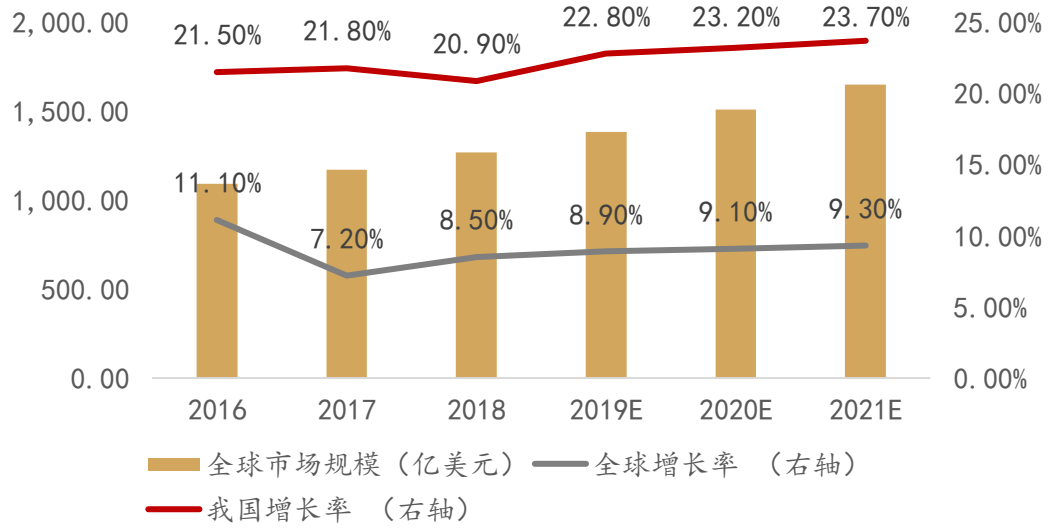
✓ 8家上榜公司分别为：安天、奇虎360、安恒信息、Nexusguard（耐誉斯凯）、瀚思、绿盟、深信服、微步在线

◆ 根据CCID的预测数据，2021年我国网络安全市场规模增速至少维持在23%水平，是全球市场规模增速的 2 倍以上， 景气度领先全球，追赶趋势迅猛

2018年全球网络安全公司500强（部分）



2016-2021年全球网络安全市场规模增速 vs 中国网络安全市场规模增速



资料来源： Cybersecurity Ventures 、华西证券研究所

3.3 空间：从与国际产业结构对比看，安全服务有大空间

◆ **国际市场规模过千亿美元，安全服务占比约一半**

✓ 2019年全球信息安全支出预测为1240亿美元

✓ 从结构上来看全球的安全的软件、硬件、服务与我国市场的区分差异很大，目前国际市场最大一部分为安全服务、642亿美元，占比约为51.7%；基础设施保护（12.4%）和网络安全设备（10.7%）也是主要的支出方向

✓ 值得注意的是，安全服务占据全球安全市场约一半的规模；但我国目前安全服务占比大概在1/4左右，还有很大的市占率提升空间，后续有望迎来网安市场整体扩张以及安全服务占比提升的双重红利

◆ **此外，全球范围内云安全市场仍然是处于早期阶段。**

✓ 2019年来看，云安全规模很小，大约4.6亿美元

✓ 1）用户习惯尚未普及，大量行业用户的系统仍然是基于传统数据中心架构或者私有云架构，可以实现基本防护

✓ 2）云计算主要虚拟化技术以及网络、存储、负载均衡、调度关键技术，相关技术更新迭代的较快，安全厂商需要一定的时间去跟进和吸收技术

2017-2019年全球信息安全市场拆分

Worldwide Security Spending by Segment, 2017-2019 (Millions of U.S. Dollars)**

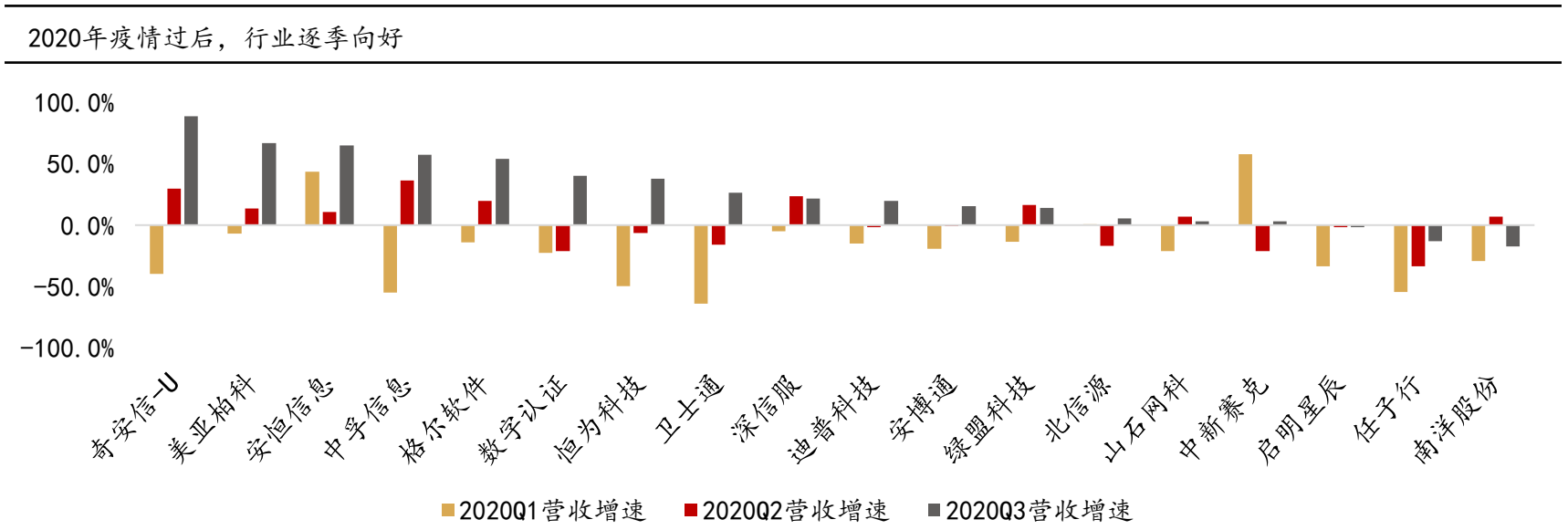
Market Segment	2017	2018	2019
Application Security	2,434	2,742	3,003
Cloud Security	185	304	459
Data Security	2,563	3,063	3,524
Identity Access Management	8,823	9,768	10,578
Infrastructure Protection	12,563	14,106	15,337
Integrated Risk Management	3,949	4,347	4,712
Network Security Equipment	10,911	12,427	13,321
Other Information Security Software	1,832	2,079	2,285
Security Services	52,315	58,920	64,237
Consumer Security Software	5,948	6,395	6,661
Total	**101,544**	**114,152**	**124,116**

资料来源：Garnter、安全牛、华西证券研究所

3.4 拐点：政府侧预算或逐步放松，关注网安行业拐点

- ◆ 2020年Q3以来网络安全公司加快复工复产，下游政府侧预算呈边际放松迹象，业绩拐点正在来临。
  - ✓ 受新冠疫情影响，2020年3月以来网络安全行业复工延迟，各公司在实施、交付、验收等方面均有延迟，Q1承压严重，Q2开始逐步好转。
  - ✓ 但考虑到疫情带来的系统性冲击，疫情趋缓的同时行业下游的政府侧客户预算投入并未全面转好，因此网安公司Q2订单及营收的增长依旧受到较大压制（也是2020年板块估值持续低迷的根本压制因素）。
  - ✓ 2020Q3、Q4来看，金融、电信等企业侧客户采购率先复苏，贡献大量订单，而政府侧客户也有边际改善迹象，行业业绩拐点正在来临。

- ◆ 从已经披露2020全年业绩（快报）的厂商来看，奇安信（营收+32%）、安恒信息（营收+40%/利润+48%）、美亚柏科（营收+15%/利润+30%）、深信服（营收+19%）等均有较优表现，龙头领先行业复苏。



资料来源：wind、华西证券研究所

3.4 拐点：年内政府侧预算或逐步放松，关注网安行业拐点

◆ **另一个角度来看，2020年12月末，我们针对网络安全上市公司进行集中的产业调研，相关总结也可从侧面佐证拐点逻辑。**

✓ **总结一：2020年来看，疫情冲击导致政府侧/企业侧对于网络安全IT的投入有所推延。**2020Q3以来，网安行业整体进入复工复产阶段，新增订单普遍呈现改善趋势，但结构仍有分化：1）政府侧需求恢复相对慢热，抗疫行动对于财政预算的挤占效应依旧明显；2）但企业侧（金融口、电信口等）的订单的同比增速则明显回升。但进入2020Q4以来，随着G端预算开始呈现边际放松，行业订单增长正在进一步加速，预计全行业订单增长和收入确认将在Q4进入高峰期，整体复苏态势或超市场预期。

✓ **总结二：考虑疫情的系统性影响，各上市公司普遍认为2020年仍是小年，行业平均增速远低于近年均值（约20%），但展望2021年，众多积极因素的推动下，行业增速有望上移至20-30%区间，并向区间上沿靠拢。**梳理积极因素，三方面因素受到最多提及：等保2.0（实质性）落实、攻防实战对抗（HW）扩容、建党100周年带来重大安保部署需求。除此以外，地方政府大数据基建（基于安全/数据审查）需求复苏、国产化替代进程等因素也将形成共振，进一步刺激政府侧/企业侧的采购需求释放。

✓ **总结三：云安全、大数据安全（以态势感知为代表）等新兴安全领域已经成为兵家必争之地，推测与等保2.0的新条款以及HW的打分项高度相关。**当前各类厂商多在大力研发并推广此类产品以及相关平台。除了云安全和态势感知，车联网安全和工业互联网安全、零信任安全将成为新的竞争高地，其中零信任安全或在2021年率先爆发，基于零信任的PKI平台、VPN单点登录产品、大数据延伸产品正在快速推广中。

✓ **总结四：展望行业格局，各类公司表现将趋于分化，带来整体集中度向提升。**所谓分化主要有二：1）头部集团与长尾厂商的分化。2020年来看，头部集团（以上市公司为代表）的集中度正在持续提升。当前安全市场仍活跃着约5000家安全厂商，但疫情带来的洗牌或产生深远影响，叠加新技术的全面渗透，相当数量的中小安全厂商将在竞争中淡出市场。2）头部集团中，各类厂商对于新兴安全需求（云/大/物/工安全）红利有不同程度的把握，产品高度匹配新需求的公司有望持续崛起。

资料来源：wind、华西证券研究所

3.4 拐点：政府侧预算或逐步放松，关注网安行业拐点

- ◆ 值得注意的是，2020年业绩以外，更大的看点仍在2021年，即：G端订单推延释放导致的业绩大年。
- ✓ 就行业增长驱动力来看，自上而下的三类政策驱动力至关重要：
- ✓ 1）通过等保2.0等进行合规检查；
- ✓ 2）通过攻防实战对抗（HW）检验“成绩单”；
- ✓ 3）鼓励各地G端推动大数据新基建（基于安全/数据审查）。

- ◆ 2020年以来，等保2.0合规检查和G端大数据新基建均承压严重，主要原因仍是政府财政向抗疫事项倾斜，安全类预算整体缩减，此两类需求有望在2021年触底反弹，催生大量新的订单需求。

当前我国网络安全行业增长驱动力

资料来源：wind、华西证券研究所

04 投资建议

投资建议：三型分类下，关注网安 5大金刚

4.1 标的梳理及投资建议

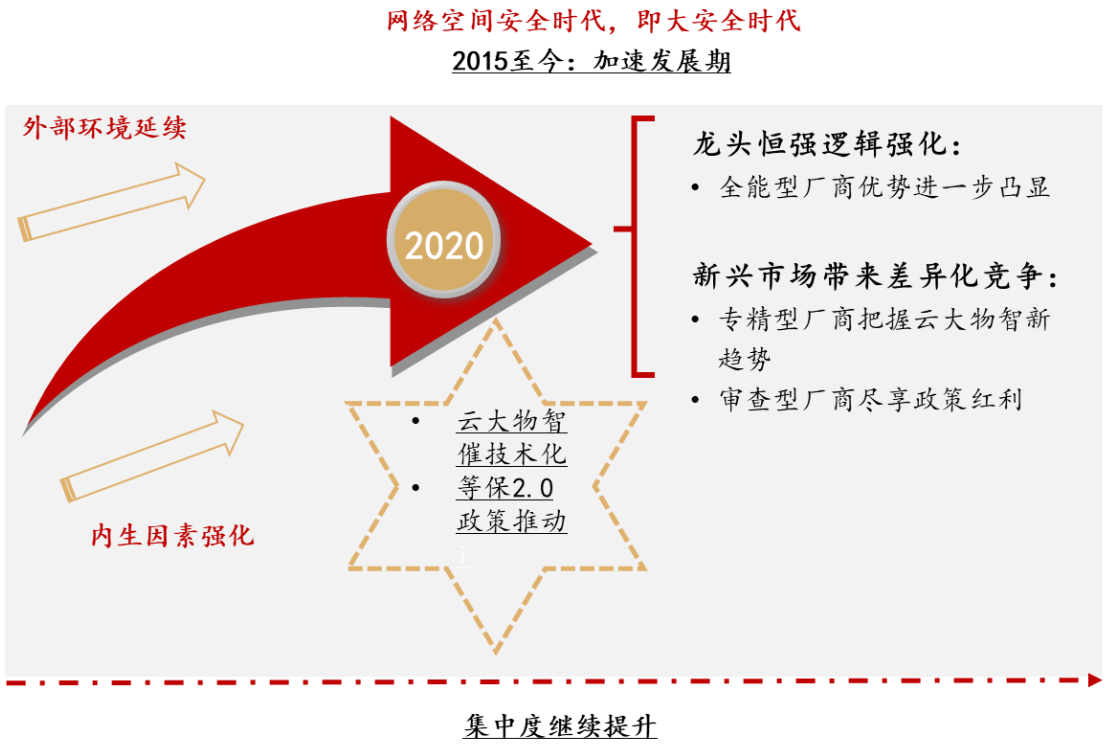
◆ 基于我们此前的产业格局变迁分析，龙头恒强和差异化竞争两条发展主线下，我们梳理出三型厂商中的5家龙头（2+1+2）

✓ 全能型：奇安信、深信服

✓ 专精型：安恒信息

✓ 审查型：美亚柏科、中新赛克

大安全时代的未来格局变化趋势



相关标的梳理：网安五大细分

全能型厂商	专精型厂商	审查型厂商
奇安信	安恒信息	美亚柏科
深信服		中新赛克

资料来源：华西证券研究所

4.1 标的梳理及投资建议

◆ 盈利预测及估值情况如下：

标的盈利预测与可比估值情况

证券代码	证券简称	类型	股价	EPS			PE		
				20A/E	21E	22E	20A/E	21E	22E
300454.SZ	**深信服**	**全能型**	**259.7**	**2.3**	**3.1**	**4.0**	**112.4**	**83.2**	**65.4**
688561.SH	**奇安信-U**	**全能型**	**112.5**	**-0.4**	**0.2**	**0.9**	-	-	-
300352.SZ	北信源	专精型	4.7	-	-	-	-	-	-
002268.SZ	卫士通	专精型	17.0	0.2	0.3	0.3	89.5	67.8	57.5
300579.SZ	数字认证	专精型	37.0	0.7	1.0	1.2	54.8	38.0	29.6
603232.SH	格尔软件	专精型	19.6	0.5	0.7	1.1	41.5	26.2	17.6
300659.SZ	中孚信息	专精型	41.9	1.0	1.5	1.9	42.5	28.3	21.6
688168.SH	安博通	专精型	49.6	-	-	-	-	-	-
300311.SZ	任子行	审查型	5.7	-	-	-	-	-	-
300188.SZ	**美亚柏科**	**审查型**	**18.5**	**0.5**	**0.7**	**0.9**	**34.9**	**26.4**	**20.1**
002912.SZ	**中新赛克**	**审查型**	**50.7**	**3.7**	**5.0**	**6.8**	**13.7**	**10.1**	**7.4**
603496.SH	恒为科技	审查型	16.7	0.2	0.6	0.9	90.3	26.0	18.5
均值							**64.5**	**40.4**	**30.7**

资料来源：华西证券研究所，备注：截至2020年3月2日，[illegible]2020年快报的公司采用快报数据

4.2 核心推荐之奇安信

◆ 核心逻辑与投资建议：

◆ **一、我们认为，奇安信之所以能成为网安新龙头，主要因为做好了以下几点：**

✓ 1）精准把握住了行业新需求变化方向：云/大/物/工等新兴安全

✓ 2）高强度研发投入，产品领先战略得以落地

✓ 3）营销层面有特色：互联网式狼性+政府端高举高打

◆ **二、安全行业发生了什么变化？我们认为，近3-4年网安行业有3点变化值得重点关注：**

✓ 1）由云大物工引起的新安全需求的变化，结果是导致新安全产品增速远高于传统安全产品增速

✓ 2）结合等保2.0的合规性需求，客户侧由业务引发的安全需求明显放大

✓ 3）网安行业格局正在发生巨大变化，“新安全”公司成长显著快于“老安全”公司

◆ **三、公司正由快速扩张期向“高质量”发展期过渡，并通过云安全，大数据安全等更贴近客户业务的新产品增强了客户粘性，构筑起了更高的业务壁垒。**

◆ **四、投资建议：**维持盈利预测不变，预计公司2020-2022年总收入分别为45.6/ 62.2/85.1亿元。参考对标公司Palo Alto（全球安全龙头）、CrowdStrike（全球云安全龙头）、 Palantir（全球大数据龙头；公司有望拓宽数据安全业务边界）的发展路径及估值，考虑公司业绩的高增长、龙头公司的估值溢价，维持“买入”评级。

资料来源：wind、华西证券研究所

4.3 核心推荐之美亚柏科

◆ 核心逻辑与投资建议：

◆ **一、产品线持续优化，“乾坤”平台引领大数据智能发力**：2020年公司营收同比增长15.4%，归母净利润同比增长29.7%，基本面持续向好。

✓ 1）在网络空间安全业务领域：公司将事后“电子数据取证”延伸为“网络空间安全”事前事中事后全赛道，由狭义网安细分赛道向广义大网安市场切入，业务边界正在拓宽。

✓ 2）在大数据智能化业务领域：公司“大数据信息化”已由“公安大数据信息化”延伸至“新型智慧城市大脑”，“乾坤”系列标准化大数据产品在2020Q4开始加速推广，能快速实现技术复用及跨行业延伸。判断“乾坤”作为典型的大数据中台产品，一方面利于提升公司项目实施效率及人均毛利；另一方面有望协助拓宽垂直赛道，打开成长空间。

◆ **二、取证短期增长放缓，新基建或将催化大数据市场**：电子取证业务短期受疫情影响较大，但长期增长逻辑不变，网络空间安全业市场仍处于增长阶段，预计2025年中国网安市场规模将达1536.1亿元。而大数据智能化业务在中短周期迎来更大发展机遇：2020年中央政府多次强调新型基础设施建设，公司大数据中台面对“新基建”、“平安中国”、“智慧城市”、“数字化业务”等多方面需求将迎来巨大的增长空间。此外，公司成立漳州市智慧城市建设与运营中心，负责信创服务器的生产和销售，积极布局信创领域，预计2021年将有更明显的积极变化。

◆ **三、国投控股入主，政府业务有望受益放量**：2019年4月1日，公告显示国投智能以总价19.44亿元收购公司部分股东的股份，获得公司的控股权，并与原大股东签下2019-2021年累计扣非净利润不低于9.03亿元的对赌协议。考虑到国投投资了大量国家核心产业，这次控股权的转让有助于公司进行政府层面的业务推广。

◆ **四、投资建议**：维持盈利预测不变，预计2020-2022年公司营收分别为26.24、34.52、45.58亿元，增速分别为26.92%、31.55%、32.06%；归母净利润分别为4.20、5.65、7.69亿元，增速分别为44.9%、34.7%、36.1%。坚定看好，维持“买入”评级。

资料来源：wind、华西证券研究所

4.4 核心受益之安恒信息

◆ 核心逻辑：

◆ **一、深耕新兴安全领域的后起龙头，产品危险、粘性渐成**

➢ 公司深耕覆盖应用安全、云安全、大数据安全、物联网安全、智慧城市安全和工业互联网安全等新兴安全领域，深度绑定政府、电信运营商、金融企业、教育机构等企事业客户，成为行业后起之秀。

➢ 公司核心产品始终占据行业领先地位，产品先于战略落地，稳扎稳打兑现新兴安全产业红利。

◆ **二、发力云安全平台，安恒云有望塑造新在增长极**：公司通过夯实云、大、物、工等新兴安全战略方向，深度布局云安全平台，为企业解决多云统一管理的难题。在Gartner发布的《2020年中国ICT技术成熟度曲线》报告中，公司凭借领先的技术实力入选，成为云安全"标杆供应商"。随着新品牌"安恒云"的发布，公司有望深度布局企业积极参与数字化转型期间。

➢ 此外，公司在大数据安全相关的态势感知细分领域已经形成差异化竞争优势。

◆ **三、行业已进入快速发展期，公司率先受益行业扩张红利**：2020年下半年，随着疫情影响消散，公司业务快速回暖，业绩领先行业反弹，叠加Q4为销售/结算的旺季因素，全年营收增速突破40%（2020年业绩快报）。

➢ 2021年来看，行业需求拐点、HW行动等是重要催化因素。

05 风险提示

风险提示

- 1、**竞争加剧风险**：网络安全行业竞争存在加剧风险
- 2、**政策风险**：等保2.0 推进不及预期
- 3、**下游需求波动风险**：宏观经济波动引发政企需求波动
- 4、**新兴技术风险**：未来新的技术变革可能导致网络安全整体需求收缩的风险

免责声明

分析师与研究助理简介

刘泽晶（首席分析师）2014-2015年新财富计算机行业团队第三、第五名，水晶球第三名，10年证券从业经验

刘忠腾（分析师）计算机+金融复合背景，3年IT产业+3年证券研究经验，深耕云计算和信创产业

孔文彬（研究助理）金融学硕士，3年证券研究经验，主要覆盖金融科技、网络安全、人工智能等研究方向

分析师承诺

作者具有中国证券业协会授予的证券投资咨询执业资格或相当的专业胜任能力，保证报告所采用的数据均来自合规渠道，分析逻辑基于作者的职业理解，通过合理判断并得出结论，力求客观、公正，结论不受任何第三方的授意、影响，特此声明。

评级说明

公司评级标准	投资评级	说明
以报告发布日后的6个月内公司股价相对上证指数的涨跌幅为基准。	买入	分析师预测在此期间股价相对强于上证指数达到或超过15%
	增持	分析师预测在此期间股价相对强于上证指数在5%—15%之间
	中性	分析师预测在此期间股价相对上证指数在-5%—5%之间
	减持	分析师预测在此期间股价相对弱于上证指数5%—15%之间
	卖出	分析师预测在此期间股价相对弱于上证指数达到或超过15%
行业评级标准		
以报告发布日后的6个月内行业指数的涨跌幅为基准。	推荐	分析师预测在此期间行业指数相对强于上证指数达到或超过10%
	中性	分析师预测在此期间行业指数相对上证指数在-10%—10%之间
	回避	分析师预测在此期间行业指数相对弱于上证指数达到或超过10%

华西证券研究所：

地址：北京市西城区太平桥大街丰汇园11号丰汇时代大厦南座5层

网址：http://www.hx168.com.cn/hxzq/hxindex.html

免责声明

华西证券股份有限公司（以下简称“本公司”）具备证券投资咨询业务资格。本报告仅供本公司签约客户使用。本公司不会因接收人收到或者经由其他渠道转发收到本报告而直接视其为本公司客户。

本报告基于本公司研究所及其研究人员认为的已经公开的资料或者研究人员的实地调研资料，但本公司对该等信息的准确性、完整性或可靠性不作任何保证。本报告所载资料、意见以及推测仅于本报告发布当日的判断，且这种判断受到研究方法、研究依据等多方面的制约。在不同时期，本公司可发出与本报告所载资料、意见及预测不一致的报告。本公司不保证本报告所含信息始终保持在最新状态。同时，本公司对本报告所含信息可在不发出通知的情形下做出修改，投资者需自行关注相应更新或修改。

在任何情况下，本报告仅提供给签约客户参考使用，任何信息或所表述的意见绝不构成对任何人的投资建议。市场有风险，投资需谨慎。投资者不应将本报告视为做出投资决策的惟一参考因素，亦不应认为本报告可以取代自己的判断。在任何情况下，本报告均未考虑到个别客户的特殊投资目标、财务状况或需求，不能作为客户进行客户买卖、认购证券或者其他金融工具的保证或邀请。在任何情况下，本公司、本公司员工或者其他关联方均不承诺投资者一定获利，不与投资者分享投资收益，也不对任何人因使用本报告而导致的任何可能损失负有任何责任。投资者因使用本公司研究报告做出的任何投资决策均是独立行为，与本公司、本公司员工及其他关联方无关。

本公司建立起信息隔离墙制度、跨墙制度来规范管理跨部门、跨关联机构之间的信息流动。务请投资者注意，在法律许可的前提下，本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或期权并进行证券或期权交易，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。在法律许可的前提下，本公司的董事、高级职员或员工可能担任本报告所提到的公司的董事。

THANKS