计算机行业

信息安全行业将持续加速，强者愈强

分析师： 刘雪峰
SAC 执证号：S0260514030002
SFC CE.no: BNX004
021-60750605
gfliuxuefeng@gf.com.cn

分析师： 庞倩倩
SAC 执证号：S0260519010004
021-60750605
pangqianqian@gf.com.cn

核心观点：

- **行业明年提速确定性强**

国内信息安全行业的典型客户包括党政军/电信/金融/能源/交通/教育等领域，受政策驱动影响较大。十三五期间，随着《网络安全法》落地及相关条例出台，客户对安全愈加重视，行业投入加大是趋势。**短期的变化体现在**

- 国资委发布的《中央企业负责人经营业绩考核办法》于 19 年 4 月实施，**将网络安全纳入央企负责人考核内容**，安全责任从信息部主任提升到央企一把手，重视程度显著提升。（来源：国资委官网）
- 2019 年广泛开展**护网行动**，实战攻防、漏洞发现让客户对安全愈发重视，虽然护网行动本身带来的服务收入增量有限，但**对客户后续追加产品采购有很大积极作用**。
- 等保 2.0 将于 19 年 12 月 1 日实施，会在明年带来较大的整改投入，**行业景气度会进一步提升，头部公司业绩提速确定性较强**。（来源：人民网）
- 头部公司收入增速已反应行业加速，**深信服安全业务、启明星辰 18H1/19H1 的收入增速分别是 24%/30%、7%/19%**（来源：公司财报）。

- **对行业未来竞争格局的判断**

过去 2 年行业的集中度从尾部向头部、科创公司集中，科创公司由于专注于新型领域实现了高于行业的增长，尾部公司整体最低，且盈利能力在持续恶化。

随着攻击的日益复杂化以及用户对安全的重视程度日益提升，以往购买点状的安全产品已经不能满足客户需求，客户会愈加看重安全厂商的技术能力、解决安全问题的能力。**在技术储备和研发投入上，头部公司更有优势，代表公司如深信服、启明星辰、天融信等。加之在整体解决方案及销售渠道上的优势，整体而言竞争力更强，较难被超越。科创板公司有望在细分领域获得持续成长，技术薄弱的小型安全公司会日益边缘化。**

- **重点标的：**在市场集中度还不太高的背景下，核心竞争力突出，技术基因和人员储备等优势明显，包括治理结构不断优化的公司，如深信服等。

- **风险提示**

行业投入加速节奏的不可把握性；来自云厂商的竞争加剧；在项目单体体量和复杂度增大的驱使下，伴随的集成业务可能对毛利率和现金流产生一定影响。

相关研究：

计算机行业:微软云增速继续回落，资本开支环比放缓	2019-10-25
计算机行业:三季报恐持续震荡回调，龙头长线机会将显现	2019-10-20
计算机行业:前三季度净利润增速大幅下降，小部分龙头依旧优异	2019-10-16

重点公司估值和财务分析表

股票简称	股票代码	货币	最新收盘价	最近报告日期	评级	合理价值（元/股）	EPS(元)		PE(x)		EV/EBITDA(x)		ROE(%)	
							2019E	2020E	2019E	2020E	2019E	2020E	2019E	2020E
恒生电子	600570	CNY	72.83	2019/08/29	买入	78.40	1.12	1.40	65.03	52.02	209.65	88.90	22.0	21.6
卫宁健康	300253	CNY	16.16	2019/10/15	买入	17.18	0.25	0.31	64.64	52.13	61.77	48.26	11.4	12.6
创业慧康	300451	CNY	17.44	2019/10/22	买入	21.00	0.42	0.49	41.52	35.59	44.27	31.77	10.7	11.2
浪潮信息	000977	CNY	24.10	2019/08/30	买入	27.58	0.69	1.00	34.93	24.10	16.55	12.21	10.0	12.7
石基信息	002153	CNY	38.11	2019/08/29	增持	36.40	0.52	0.63	73.29	60.49	86.04	63.20	6.5	7.3
深信服	300454	CNY	125.90	2019/10/25	买入	144.60	1.68	2.41	74.94	52.24	151.50	105.29	16.5	19.2

数据来源：Wind、广发证券发展研究中心

备注：表中估值指标按照最新收盘价计算

投资要点

1. 行业明年提速确定性强

国内信息安全行业的典型客户包括党政军、电信、金融、能源、交通、教育等领域，政策驱动因素的影响相对较大。

十三五期间，政府对信息安全的重视程度、战略定位大幅提升。先后于2017年6月实施《网络安全法》（首次立法）、于2017年7月发布《关键信息基础设施安全保护条例（征求意见稿）》，于2019年5月发布《信息安全技术网络安全等级保护基本要求》（等保2.0）。未来几年，由于《网络安全法》及相关条例落地、等保2.0的实施，客户对安全愈加重视，行业投入加大是趋势。**短期的变化体现在**：

- 《中央企业负责人经营业绩考核办法》于19年4月1日实施，**将网络安全纳入央企负责人考核内容**，可以理解成安全责任从信息部主任提升到央企一把手，重视程度提升会带来相关投入的增加。
- 2019年广泛开展**护网行动**，实战攻防、漏洞发现让客户对安全愈发重视，虽然护网行动本身带来的服务收入增量有限，但**对客户后续追加产品采购有很大积极作用**。护网行动始于16年，范围从16年的公安部、民航局、国家电网，到17年部分政府加入，到18年部分国企加入，再到19年工信、安全、武警、交通、铁路、民航、能源、新闻广电、电信运营商等行业广泛加入。
- 等保2.0于19年12月1日实施，会在明年带来较大的整改投入，**行业景气度会进一步提升，头部公司业绩提速确定性较强**（来源：人民网）。
- 从头部公司的收入增速来看，已有所反应行业提速，**深信服安全业务、启明星辰 18H1/19H1 的收入增速分别是 24%/30%、7%/19%**（来源：公司财报）。

2. 对行业未来竞争格局的判断

过去2年行业的集中度从尾部向头部、科创公司集中，科创公司由于专注于新型领域实现了高于行业的增长，尾部公司整体最低，且盈利能力在持续恶化（17、18年A股头部公司、科创公司、三板公司平均收入的增速分别是14%/24%、39%/34%、12%/13%）。

随着攻击的日益复杂化以及用户对安全的重视程度日益提升，以往购买点状的安全产品已经不能满足客户需求，客户会愈加看重安全厂商的技术能力、解决安全问题的能力。**在技术储备和研发投入上，头部公司更有优势，代表公司如深信服、启明星辰、天融信等。加之在整体解决方案及销售渠道上的优势，整体而言竞争力更强，较难被超越。**技术薄弱的小型安全公司会日益边缘化。

- **头部公司中深信服表现最为突出。**1）通过研发积累和渠道建设，深信服相对实现了更快增长。15-17年，同为内生增长，深信服、天融信的收入增速分别是22%、16%。14-18年，深信服（内生）、启明星辰（含并表）收入增速分别为22%、20%。2）从毛利率上看，深信服的盈利能力表现得也更

为突出。17、18年，深信服（安全业务）、启明星辰（安全产品）、天融信（安全及大数据产品）毛利率分别为88.7%/88.5%、76.9%/76.6%、78.1%/65.5%（公司财报数据）。

- **头部公司收入增速不及科创公司的原因**：头部公司收入中传统硬件产品占大头，科创公司收入中符合产业趋势的单一产品占比较高，使得头部公司整体增速表现低于一些主打新产品的公司，但头部公司本身也在加大对新领域的研发投入力度，在新型领域收入体量并不低于科创公司。

几家典型的科创安全公司各有特殊，主打的细分产品符合产业发展趋势。如在数据安全、WAF领域表现出色的**安恒信息**、在下一代防火墙领域表现不俗的**山石网科**等科创公司，以及为安全公司提供安全产品基础平台走差异化路线的**安博通**。

3. 如何看待云计算厂商带来的竞争威胁

随着传统IT架构向云化模式转变，云计算厂商也在积极布局云安全，**未来云安全厂商必须紧跟趋势才能保持行业地位。目前安全公司均积极布局云安全，短期来看无需有太多担忧**，如深信服、启明星辰等公司均推出云安全相关产品及解决方案，及深信服将安全融合在超融合架构中。

来自云厂商的竞争主要在私有云安全领域，云厂商与安全公司有竞争也有合作。私有云建设主体主要是大型政企，是安全公司的主要客户，部分私有云厂商为大型政企客户搭建私有云时，会配套销售自己的安全产品，和安全公司有一定竞争关系。私有云安全的主要竞争对手有**华为、新华三**。华为主要销售防火墙，新华三网络边界层主流安全产品均有销售。但有竞争也有合作，尤其是云上数据、应用等安全多交由安全公司，如华为、阿里均与安恒信息有合作。此外客户在搭建私有云时，安全也可能会另外招标。

公有云相关的安全对传统安全公司而言是增量市场，公有云本身安全多由云厂商自行保障。**云厂商与安全公司的竞争主要体现在面向中小企业的SaaS化安全产品上，当前市场规模尚小，未来格局有不确定性**。

4. 相关央企与安全公司的业务协同性分析

相关央企或可通过资本和技术绑定等多种的方式与安全公司实现业务协同。以旗下有两家上市集成公司的中电科为例，电科集团旗下上市公司华东电脑、太极股份的18年系统集成收入体量分别为**52、32**亿元（公司财报数据）。其下游客户与安全公司下游客户重叠度高，且公司本身缺乏通用安全产品。**如果相关央企在承担较多大项目时能更多通过资本和技术绑定等多种的方式在产业层面来整合通用信息安全产品公司，对双方都是极大促进和长期利好。**

5. 信息安全是什么

网络攻击是指针对计算机网络、基础设施、信息系统进行的任何类型的进攻动作，包括破坏、揭露、修改、使软件或服务失去功能、在没有得到授权的情况下偷取或访问任何一计算机的数据等。

典型的攻击方式：

- **DDOS攻击**：对资源的请求大大超过正常值，致使服务过载，使得被访问资源无法再对合理的请求进行响应。
- **木马**：木马是指未经用户同意进行非授权操作的一种恶意程序，常伪装成正常软件进行散播，主要用于盗取密码和资料，不具备传染性。
- **蠕虫**：主要利用系统漏洞或者电子邮件进行攻击，通过向软件添加代码、修改程序的工作方式，不同程度地影响电脑的正常使用。

信息安全防护的主要技术有：网络边界安全防护，安全审计技术、病毒检测与清除技术、内容检测与监控技术、加解密技术，身份认证技术等。通过将各种信息安全技术结合，应用在各种场景中，就形成了信息安全产品。

6. 信息安全产品有哪些

信息安全产品根据防护的对象划分，大致可分为网络安全、终端安全、应用安全、数据安全（数据全生命周期安全）、安全管理（全流程安全管理）。

网络安全：网络安全是指对整个局域网的安全防护，主要产品包括防火墙 /安全网关/下一代防火墙、入侵检测/入侵防御、防病毒网关、UTM 、VPN、上网行为管理、网络流量控制、抗DDOS、APT未知威胁发现、网闸、网络缓存、网络准入控制、负载均衡、加密机等。

终端安全：产品主要是指对服务器、电脑等终端的安全防护。安全产品主要包括桌面/主机审计、杀毒软件、主机加固（主要功能：修复漏洞、打补丁）、终端登陆/身份认证、计算机防火墙等。

应用安全：产品主要包括网页防篡改、Web应用防火墙（WAF）、WEB漏洞扫描、网站安全监测平台、邮件安全产品、数据库安全产品等。

数据安全：数据安全是指对处于数据生命周期不同阶段的数据进行全面安全防护，涵盖网络数据、终端数据、服务器数据安全，**和网络层、终端安全包含的内容会有些重叠，但是重点在对数据的全生命周期的防护**。主要包括访问控制、敏感数据识别、数据防泄漏（加密、脱敏）、审计等。

安全管理：强调对整体感觉状态的监测和管控，功能上可能有些重叠，侧重点有所不同。代表产品有：SIEM/日志管理/SOC、运维审计/4A/堡垒机、网管软件/ITIL、信息安全等级保护测评工具箱、网络安全态势感知等。

7. 信息安全产品评价指标

结论：安全公司核心优势体现在技术的领先度上，技术优势要通过持续的研发投入和技术创新来保持其竞争优势。如在防火墙等通用型安全产品上的持续技术创新，在杀毒等终端安全中应用人工智能技术、持续重视对漏洞挖掘和防护能力的提升，在数据安全中的算法优化、提高在安全管理中建模分析和数据挖掘能力。

具体而言，在如下五类产品上，用户重点关注了哪些指标以及企业如何通过技术创新改善产品功能：

网络安全产品：以防火墙为例，用户对产品性能指标主要包括：吞吐量、时延、

新建连接速率、并发连接数和一定的扩展性。鉴于头部厂商同价位产品性能差异不大。除了上述基本的性能评价指标，技术的领先程度会影响到防护效果，如深信服率先推出的下一代防火墙，Palo Alto率先推出基于零信任技术的防火墙。

终端安全产品：主要产品是病毒查杀软件，其重点关注的性能指标有：病毒查杀能力（如病毒信息库丰富程度、漏报率、误报率和清除能力等）；查杀病毒软件的自我保护能力，对现有资源的占用情况；对文件的恢复能力。人工智能技术的应用会提升本地数据库对新病毒的防护效果。

应用安全产品：以web应用防火墙为例、web应用弱点扫描器为例，核心能力是漏洞发掘发现能力，这也是安全厂商需要持续投入的核心竞争力之一。

数据安全产品：数据安全能力的评价重点在于对数据的防护能力，**核心在于算法**。以**数据脱敏**为例算法越丰富则越难被还原。数据脱敏的算法包括屏蔽、变形、移位、格式化保留加密、令牌化、洗牌、强加密算法等。

安全管理产品：重点关注厂商的全流量分析能力、数据分析和建模分析能力。

8. 当前国内以网络层防护为主，其他需求正在释放

目前来看，中国的信息安全市场还是以硬件为主，主要集中在网络边界层的防护上，代表产品主要有防火墙、统一威胁管理平台（UTM）、入侵检测和入侵防御（IDP）、虚拟专用网络（VPN）和安全内容管理（SCM）等。据《2018年下半年中国IT安全软件市场跟踪报告》显示，2018年各细分领域排名前3的是**深信服、启明星辰、天融信**等A股头部安全厂商，以及数通厂商**华为、新华三**。除此之外，还有一些公司，如**山石网科**（拳头产品下一代防火墙）等，在主流安全产品的技术升级上抓住了机会，因而在细分产品市场上也取得了不错的表现。

安全管理、数据安全、终端安全多以软件形式呈现，需求也在逐步释放。据《2018年下半年中国IT安全软件市场跟踪报告》显示，2018年中国IT软件市场规模为约为62.7亿元，同比增长23.98%。从细分产品规模来看，前三分别是身份和数字信任软件、终端安全软件、AIRO。身份和数字信任软件收入前三名是吉大正元、亚信安全、格尔软件。终端安全软件市场主要在杀毒领域积累较深的安全公司占主导，收入规模前三分别是奇安信、赛门铁克、亚信安全。AIRO收入前三是某老牌安全公司、启明星辰和IBM。

随着数据集中管理，客户对安全的重视程度增加，数据安全、安全管理的需求在加速。**在安全管理领域的市场机会**：安全数据分析能力、安全问题解决能力突出，能提供强效预测、溯源、恢复的公司更有优势，如深信服、启明星辰，以及专注于安全数据分析的公司，如安恒信息。**在数据安全领域的市场机会**：在数据访问控制、敏感数据识别、数据防泄漏等细分领域比较有技术实力的公司，如访问控制领域的格尔软件；数据防泄漏领域的启明星辰、明朝万达、亿赛通。

重点标的

在市场集中度还不太高的背景下，核心竞争力突出，技术基因和人员储备等优势明显，包括治理结构不断优化的公司，如深信服等。

风险提示

行业投入加速节奏的不可把握性；来自云厂商的竞争加剧；在项目单体体量和复杂度增大的驱使下，伴随的集成业务可能对毛利率和现金流产生一定影响。

目录索引

图表索引

1. 行业明年提速确定性强

国内信息安全行业的典型客户包括党政军、电信、金融、能源、交通、教育等领域，政策驱动因素的影响相对较大。

十三五期间，政府对信息安全的重视程度、战略定位大幅提升。先后于2017年6月实施《网络安全法》（首次立法）、于2017年7月发布《关键信息基础设施安全保护条例（征求意见稿）》，于2019年5月发布《信息安全技术网络安全等级保护基本要求》（等保2.0）。未来几年，由于《网络安全法》及相关条例落地、等保2.0的实施，客户对安全愈加重视，行业投入加大是趋势。**短期的变化体现在：**

- 《中央企业负责人经营业绩考核办法》于19年4月1日实施，**将网络安全纳入央企负责人考核内容**，可以理解成安全责任从信息部主任提升到央企一把手，重视程度提升会带来相关投入的增加（来源：国资委官网）。
- 2019年广泛开展**护网行动**，实战攻防、漏洞发现让客户对安全愈发重视，虽然护网行动本身带来的服务收入增量有限，但**对客户后续追加产品采购有很大积极作用**。护网行动始于16年，范围从16年的公安部、民航局、国家电网，到17年部分政府加入，到18年部分国企加入，再到19年工信、安全、武警、交通、铁路、民航、能源、新闻广电、电信运营商等行业广泛加入。
- 等保2.0于19年12月1日实施，会在明年带来较大的整改投入，**行业景气度会进一步提升，头部公司业绩提速确定性较强**（来源：人民网）。
- 从头部公司的收入增速来看，已有所反应行业提速，**深信服安全业务、启明星辰 18H1/19H1 的收入增速分别是 24%/30%、7%/19%**（来源：公司财报）。

行业重要规范等保2.0的影响：相比等保1.0（GB/T 22239-2008 《信息安全技术 信息系统安全等级保护基本要求》），**等保2.0中高标准的覆盖范围更广、增加对新场景的安全要求、本身法规性更强，会推动行业投入加大：**

■ **等保2.0三级对象覆盖范围增加，三级安全防范要求显著多于二级**

相比等保1.0，等保2.0中三级对象范围显著增加，且对三级及以上网络运营者要求的严格程度远高于二级，三级对象范围的扩展有望推动网络安全行业投入力度加大。

三级对象覆盖范围大幅扩展。等保2.0根据等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度，将信息系统的安全保护等级分为5个等级。相比等保1.0，等保2.0三级覆盖范围大幅扩展，“受到破坏会对相关公民、法人和其他组织的合法权益造成特别严重损害的重要网络”从二级上升到三级对象。

表1：等保2.0与等保1.0比的等级划分区别

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	**第二级变为第三级**

社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

数据来源：GB/T 22240-2008《信息安全技术信息系统安全等级保护定级指南》、《网络安全等级保护条例》（征求意见稿）、广发证券发展研究中心

相比二级对象，等保2.0对三级监管对象有定期开展测评的要求，被监管对象的重视程度更高，会有更多安全投入。且三级对象安全防范要求显著多于二级：以等保1.0为例，对二级、三级对象的安全的要求项分别175、 290个。【不同的等级安全需防范的安全内容大致相同（控制点大致相同），但是对防范力度的要求有较大差异（控制项数量存在区别）。】

表2：等保1.0中二级、三级控制点、控制项对比

等保1.0-控制点要求

基本要求大类1.0	基本要求子类	信息系统安全等级保护级别	
		等保二级	等保三级
技术要求	物理安全	10	10
	网络安全	6	7
	主机安全	6	7
	应用安全	7	9
	数据安全	3	3
管理要求	安全管理制度	3	3
	安全管理机构	5	5
	人员安全管理	5	5
	系统建设管理	9	11
	系统运维管理	12	13
合计	/	66	73

等保1.0-控制项要求

基本要求大类	基本要求子类	信息系统安全等级保护级别	
		等保二级	等保三级
技术要求	物理安全	19	32
	网络安全	18	33
	主机安全	19	32
	应用安全	19	31
	数据安全	4	8
管理要求	安全管理制度	7	11
	安全管理机构	9	20
	人员安全管理	11	16
	系统建设管理	28	45
	系统运维管理	41	62
合计		**175**	**290**

数据来源：GB/T 22239-2008 《信息安全技术 信息系统安全等级保护基本要求》、广发证券发展研究中心

■ **等保2.0针对新技术新增扩展要求**

等保2.0在等保1.0资产防护的基础上，就云计算、物联网、移动互联网和工业控制系统提出安全防护要求。扩展要求就新技术领域提出针对性要求，部分领先公司积极布局云安全、移动互联网安全及工控安全领域，先后与阿里、腾讯等云计算厂商就云安全开展技术合作，深信服积极布局私有云安全。预计深信服、启明星辰等公司有望受益于等保2.0的推出。

■ **相比1.0，等保2.0法规性更强，执行力度、落地效果有望优于1.0**

等保2.0执行的强制力度有望优于1.0。等保1.0推行期间，缺乏相关法律作为落实保障，2017年6月起《网络安全法》正式实施，为等保2.0的落实提供了法律支撑。

整体而言，相比1.0，等保2.0的三级覆盖对象范围增加，针对新技术新增大量

扩展要求，同时有《网络安全法》为其落实提供法律保障，预计等保2.0的实施有望推动行业投入力度加大，相关公司有望受益。但等保2.0生效日期、过渡期存在不确定性，落地后对行业投入的促进作用难以量化。且需要重点关注下游公共部门的支出能力与意愿是否会继续面临挑战。

此外，国有资本参股安全公司也体现了对安全行业的重视，同时对于被参股对象获取下游关键领域的业务资质及拓展下游市场有利好作用。

虽然行业整体需求在不断改善，但市场竞争也再加剧。从企业市场加大拓展党政军市场的公司，有相对更好的边际改善预期。

2. 对行业未来竞争格局的判断

2.1 过去两年行业集中度从尾部向头部、科创公司集中

过去2年行业的集中度在提升，并且科创公司由于专注于新型领域实现了高于行业的增长，尾部公司整体最低，且盈利能力在持续恶化。

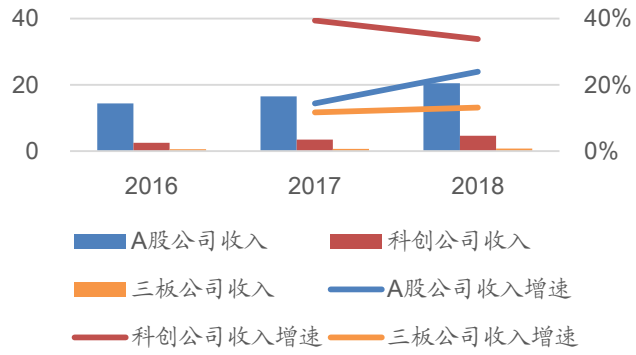
（以下数据均来自公司财报）

行业的集中度在提升：我们以A股头部公司（深信服、启明星辰、天融信）、收入规模中等的科创公司（安恒信息、山石网科、安博通）、尾部三板公司（41家安全公司）的业绩数据进行说明。以上**三类公司18年平均收入分别为：20、5、0.8亿元**。

17、18年A股头部公司、科创公司、三板公司平均收入的增速分别是14%/24%、39%/34%、12%/13%。综合实力强的A股头部公司、细分领域表现优秀的科创公司收入增速均高于三板公司，且科创公司由于专注于新型领域实现了高于行业的增长，无产品、技术优势的公司正在被边缘化。**背后的原因是客户更加重视安全，对产品的性能、品牌有更高要求**。

从盈利能力上看，A股头部公司＞科创公司＞三板公司。A股公司由于规模大更为集约化，净利率最高。科创公司正处于收入快速增长期，净利率改善明显。**三板公司则因经营情况不及净利率日益下滑，整体面临着较大的经营压力，会促进行业集中度进一步提升。**

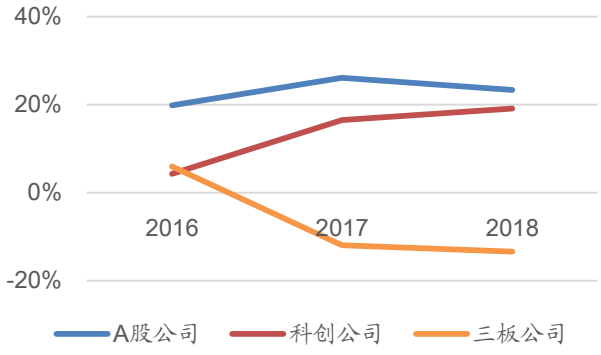
图1：安全公司收入（亿元）及增速对比



数据来源：公司财报、广发证券发展研究中心

注：深信服用的是安全业务数据；天融信 2016 年收入数据是用 16 年净利润/17、18 净利率均值推算而来

图2：安全公司净利率对比



数据来源：公司财报、广发证券发展研究中心

注：深信服用的是公司整体净利率

2.2 头部公司地位不易超越，科创公司在细分市场可获得持续成长

中国当前的信息安全市场还是以硬件为主，主要集中在网络边界层的防护上，随着攻击的日益复杂性以及用户对安全的重视程度日益提升，以往紧购买点状的安全产品已经不能满足用户需求，需要公司形成一整套智能、全面的安全防护方案。**客户会愈加看重安全厂商的技术实力、解决各种安全问题的能力。**新需求的满足不但要求安全厂商具备强大的安全技术和服务能力，而且要求安全厂商具备融合大数

据处理分析、机器学习、可视化等新型技术，持续提高产品的性能的能力。**在技术储备和研发投入上，头部公司更有优势，代表公司如深信服、启明星辰、天融信等。加之在整体解决方案及销售渠道上的优势，整体而言竞争力更强，较难被超越。**技术薄弱的小型安全公司会日益边缘化。

- **头部公司中深信服表现最为突出。1）通过研发积累和渠道建设，深信服相对实现了更快增长。**15-17年，同为内生增长，深信服、天融信的收入增速分别是22%、16%。14-18年，深信服（内生）、启明星辰（含并表）收入增速分别为22%、20%。2）**从毛利率上看，深信服的盈利能力表现得也更为突出。**17、18年，深信服（安全业务）、启明星辰（安全产品）、天融信（安全及大数据产品）毛利率分别为88.7%/88.5%、76.9%/76.6%、78.1%/65.5%（公司财报数据）。
- **头部公司收入增速不及科创公司的原因**：头部公司收入中传统硬件产品占大头，科创公司收入中符合产业趋势的单一产品占比较高，使得头部公司整体增速表现低于一些主打新产品的公司，但头部公司本身也在加大对新领域的研发投入力度，在新型领域收入体量并不低于科创公司。

几家典型的科创安全公司各有特殊，主打的细分产品符合产业发展趋势。如在数据安全、WAF领域表现出色的**安恒信息**、在下一代防火墙领域表现不俗的**山石网科**等科创公司，以及为安全公司提供安全产品基础平台走差异化路线的**安博通**。

3. 如何看待云计算厂商带来的竞争威胁

随着传统IT架构向云化模式转变，云计算厂商也在积极布局云安全，**未来云安全厂商必须紧跟趋势才能保持行业地位。目前安全公司均积极布局云安全，短期来看无需有太多担忧**，如深信服、启明星辰等公司均推出云安全相关产品及解决方案，及深信服将安全融合在超融合架构中。

图3：深信服云安全解决方案

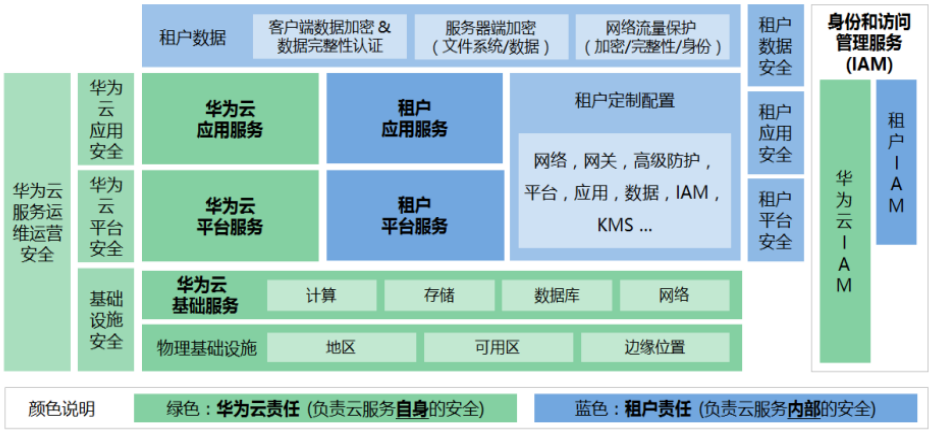
数据来源：深信服官网、广发证券发展研究中心

来自云厂商的竞争主要在私有云安全领域，云厂商与安全公司有竞争也有合作。私有云建设主体主要是大型政企，是安全公司的主要客户，部分私有云厂商为大型政企客户搭建私有云时，会配套销售自己的安全产品，和安全公司有一定竞争关系。私有云安全的主要竞争对手有**华为、新华三**。华为主要销售防火墙，新华三网络边界层主流安全产品均有销售。但有竞争也有合作，尤其是云上数据、应用等安全多交由安全公司，如华为、阿里均与安恒信息有合作。此外客户在搭建私有云时，安全也可能会另外招标。

公有云相关的安全对传统安全公司而言是增量市场，公有云本身安全多由云厂商自行保障。**云厂商与安全公司的竞争主要体现在面向中小企业的SaaS化安全产品上，当前市场规模尚小，未来格局有不确定性：**

- 对于华为、阿里、腾讯等云计算厂商，公有云本身的安全主要由云计算厂商自行维护。目前安全的主流客户是党政军、电信、金融、交通、能源等客户，公有云是增量市场，公有云厂商自行保障自身安全对传统的安全市场没有产生太多影响。

图4：华为云安全责任划分



数据来源：华为云安全白皮书、广发证券发展研究中心

- 在公有云平台上销售的SaaS化安全产品第三方厂商和公有云厂商均可提供，主要面向中小企业，市场规模尚小，非安全厂商的传统业务，未来的竞争格局尚有不确定性。

图5：阿里出售的自研安全产品

基础安全	数据安全	业务安全	安全服务	安全解决方案	身份管理
DDoS高防IP	SSL 证书	游戏盾	安全管家	企业上云安全建设解决方案	访问控制
Web应用防火墙 HOT	加密服务	内容安全	渗透测试	等保合规安全解决方案	
云安全中心（态势感知） HOT	数据库审计	实人认证	安全众测	互联网金融安全解决方案	
云安全中心（安骑士）	密钥管理服务	风险识别	等保咨询 NEW	新零售安全解决方案	
堡垒机	敏感数据保护（公测中） NEW	爬虫风险管理 NEW	应急响应	游戏安全解决方案	
云防火墙			安全培训	社交/媒体spam解决方案	
网站威胁扫描系统			安全评估	政务云安全解决方案	
操作审计（公测中）			代码审计	混合云态势感知解决方案	
			安全加固	IPv6云安全解决方案 NEW	
			安全通告服务		
			PCI DSS合规咨询 NEW		

数据来源：阿里出售的自研安全产品、广发证券发展研究中心

4. 相关央企与安全公司的业务协同性分析

相关央企或可通过资本和技术绑定等多种的方式与安全公司实现业务协同。以旗下有两家上市集成公司的中电科为例，电科集团旗下上市公司华东电脑、太极股份的18年系统集成收入体量分别为52、32亿元。其下游客户与安全公司下游客户重叠度高，且公司本身缺乏通用安全产品。**如果相关央企在承担较多大项目时能更多通过资本和技术绑定等多种的方式在产业层面来整合通用信息安全产品公司，对双方都是极大促进和长期利好。**

太极股份（据18年年报）：

- 业务结构：公司网络安全与自主可控产品（主要包含网络安全、应用安全、信息系统安全以及自主可控基础产品）收入在总收入中占比为21%（**对应6亿元销售额**），毛利率为27%，从安全业务毛利率来看，外采的比例较大。
- 下游客户：公司18年收入中来自政务、事业单位、企业（从官网上看，企业主要是指电力、制造、金融、交通等行业）的收入占比分别为45%、11%、39%。下游客户与安全公司客户重叠度高。

华东电脑（据18年年报）：

- 业务结构：公司**网络安全整体解决**方案是公司代表性的通用信息化解决方案之一（其他还包括多云平台管理解决方案、企业统一协作与通信解决方案、软件定义网络解决方案），公司本身缺乏通用性安全产品。
- 下游客户：除通用信息化解决方案外，公司为金融、运营商与互联网、企业、政府与公共服务业等行业客户提供解决方案。与安全厂商的客户重叠度高。

5. 信息安全是什么

5.1 网络攻击

网络攻击是指针对计算机网络、基础设施、信息系统进行的任何类型的进攻动作，包括破坏、揭露、修改、使软件或服务失去功能、在没有得到授权的情况下偷取或访问任何一计算机的数据等。

典型攻击方式:

- **DDOS攻击**：对资源的请求大大超过正常值，致使服务过载，使得被访问资源无法再对合理的请求进行响应。
- **木马**：木马是指未经用户同意进行非授权操作的一种恶意程序，常伪装成正常软件进行散播，主要用于盗取密码和资料，不具备传染性。
- **蠕虫**：主要利用系统漏洞或者电子邮件进行攻击，通过向软件添加代码、修改程序的工作方式，不同程度地影响电脑的正常使用。

5.2 安全防护

信息安全防护的目的：防止信息被非授权泄露、更改、破坏或使信息被非法的系统辨识、控制。

信息安全主要技术:

- **安全防护技术**：包括网络防护技术（防火墙、入侵检测防御）、应用防护技术（应用程序接口安全技术）、系统防护技术(如防篡改、系统备份与恢复技术)。
- **安全审计技术**：包括日志审计和行为审计。可在受到攻击后查看日志，评估网络配置的合理性、安全策略的有效性。可对行为进行管理、分析，确认行为的合规性。
- **病毒检测与清除技术**。
- **内容检测与监控技术**：对信息系统中的流量及应用内容进行二到七层的检测并适度监控和控制，避免网络流量的滥用、有害信息的传播。
- **加解密技术**：对传输和存储的数据进行加密和解密。
- **身份认证技术**：典型手段如用户名口令、身份认证、PKI证书和生物认证等。

通过对各种信息安全技术结合，并将其应用在各种场景中，形成了信息安全产品。

6. 信息安全产品

根据防护的对象，大致可分为网络安全产品、终端安全产品、应用安全产品、数据安全（数据全生命周期安全）及安全管理（全流程安全管理）。安全厂商的核心能力都是软件能力，但网络产品多以硬件形态呈现，其他产品多以软件形态呈现。

图6：信息安全产品及服务划分

数据来源：IDC、广发证券发展研究中心

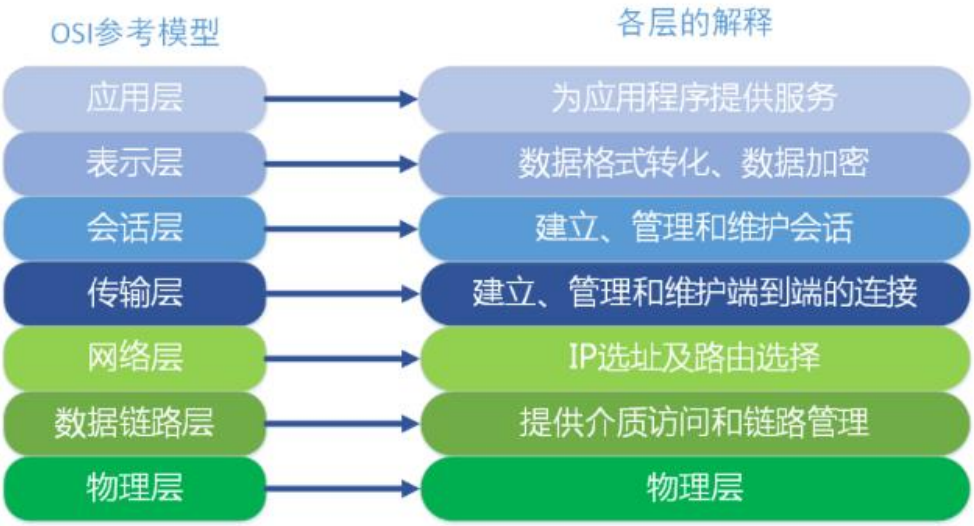
6.1 网络安全

6.1.1 网络安全产品介绍

网络安全是指对整个局域网的安全防护，主要产品包括防火墙 /安全网关/下一代防火墙、入侵检测/入侵防御、防病毒网关、UTM 、VPN、上网行为管理、网络流量控制、抗DDOS、APT未知威胁发现、网闸、网络缓存、网络准入控制、负载均衡、加密机等。

在OSI网络层次模型中，防火墙主要在第二到第四层起作用，在第四到第七层一般很微弱。而防病毒软件主要在第五到第七层起作用。入侵检测系统对整个流量进行检测。

图7：OSI网络协议分层



数据来源：博客园-五章笔记、广发证券发展研究中心

表3：网络边界安全产品介绍

安全产品名称	介绍
防火墙（FW）	指在内网和外部网之间、专用网和公共网的边界构造的保护屏障。防火墙主要由服务访问政策、验证工具、包过滤和应用网关4个组成部分。一般基于源地址和目的地址、应用、协议以及每个IP包的端口判断是否允许信息通过。
防病毒网关	用以保护网络内（一般是局域网）进出数据的安全。主要体现在病毒杀除、关键字过滤（如色情、反动）、垃圾邮件的阻止等。
入侵检测系统（IDS）	为了弥补防火墙和除病毒软件二者在第四到第五层之间留下的空档，引入了入侵检测系统，其作用在于对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果。
入侵防御系统（IPS）	不仅能够起到检测作用，而且能够在发现入侵时，迅速作出反应，并自动采取阻止措施。在一些传统防火墙的新产品中也提供了类似功能，其特点是可以分析到数据包的内容，解决传统防火墙只能工作在 4 层以下的问题。。
统一威胁管理（UTM）	将防病毒、入侵检测和防火墙安全设备划归到一起“统一管理”的产品。
下一代防火墙（NGFW）	集成传统防火墙、IPS、WAF等功能，是一款可以全面应对应用层威胁的高性能防火墙。**下一代防火墙和UTM的区别在于**：传统UTM开启可实现功能集中，但多个模块是串行处理机制，一个数据包先过一个模块处理一遍，再重新过另一个模块处理一遍，一个数据要经过多次拆包，多次分析，性能和效率相对较低。NGFW只需要一次拆包，这些模块一起看，如URL看http头部，fw看ip，AV看数据部分，性能和效率大幅提升。
上网行为管理（AC）	控制和管理对互联网的使用，其包括对网页访问过滤、网络应用控制、带宽流量管理、信息收发审计、用户行为分析。
VPN	是指在公用网络上建立专用网络，进行加密通讯。

数据来源：广发证券发展研究中心

抗DDOS（抗拒绝服务攻击）：拒绝服务攻击（DDOS）是指恶意对资源发起大大超过正常值的请求，致使服务器过载。抗DDOS则是指对这种攻击的防御，主要措施包括:

- **异常流量的清洗过滤**：通过DDOS硬件防火墙对异常流量的清洗过滤，通过数据包的规则过滤、数据流指纹检测过滤、及数据包内容定制过滤等顶尖技术能准确判断外来访问流量是否正常，将异常流量禁止过滤。
- **分布式集群防御**：这是目前网络安全界防御大规模DDOS攻击的最有效办法。分布式集群防御的特点是在每个节点服务器配置多个IP地址，并且每个节点能承受不低于10G的DDOS攻击，如一个节点受攻击无法提供服务，系统将会根据优先级设置自动切换另一个节点，并将攻击者的数据包全部返回发送点，使攻击源处于瘫痪状态，从更为深度的安全防护角度去影响企业的安全执行决策。
- **智能DNS解析**：根据用户的上网路线将DNS解析请求解析到用户所属网络的服务器。同时智能DNS解析系统还有宕机检测功能，随时可将瘫痪的服务器IP智能更换成正常服务器IP。

APT未知威胁（高级持续性威胁）发现：APT又称高级持续性威胁，其高级性主要体现于APT在发动攻击之前需要对攻击对象的业务流程和目标系统进行精确的收集，在此收集的过程中，此攻击会主动挖掘被攻击对象受信系统和应用程序的漏洞，在这些漏洞的基础上形成攻击者所需的C&C网络。APT攻击形式多种多样，如入侵企业信息系统、恶意邮件或利用防火墙漏洞访问企业等。

网闸：实现网络隔离连接，网闸的内网处理单元连接内部网，外网处理单元连接外部网，专用隔离硬件交换单元在任一时刻点仅连接内网处理单元或外网处理单元，与两者间的连接受硬件电路控制高速切换。

图8：网闸示意图

数据来源：天行网安官网、广发证券发展研究中心

网络准入控制：只允许合法的、值得信任的终端设备（例如PC、服务器、手机）接入网络，而不允许其它设备接入。

6.1.2 网络安全产品部署

网络安全产品主要部署在网络入口处、网关侧或者部署在网关上。部署多种安全产品时一般采用串联模式。

防火墙的形态：可以是软件或者硬件的形态。软件防火墙单独使用软件系统来完成防火墙功能，将软件部署在系统主机上，占用系统资源，优点是可以同时对网络和主机进行防护。**硬件防火墙是指把防火墙程序做到芯片里面**，由硬件执行这些功能，能减少CPU的负担，使路由更稳定。

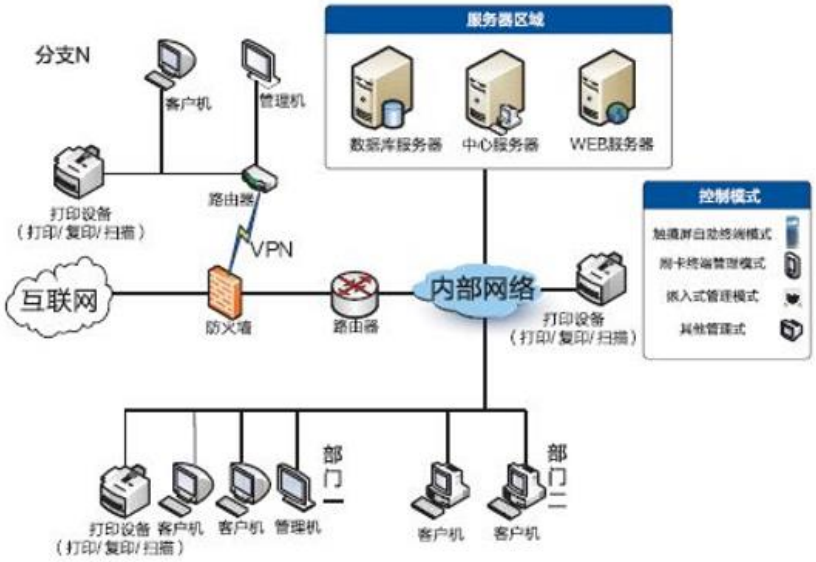
图9：硬件防火墙图示

数据来源：中关村在线、广发证券发展研究中心

硬件防火墙的部署：一般为外联出口或者区域性出口位置，对内外流量进行安全隔离。防火墙、IDS、上网行为管理产品的功能可以集成在网关上，也可以在网络上单独部署。下面以防火墙搭载上网行为管理产品单独部署为例，介绍部署模式：1）路由器/出口网关——防火墙——上网行为管理——交换机；2）路由器/出口网关——交换机—（防火墙、上网行为管理，旁挂）。（网络设备的主要构成包括交换机、路由器和网关，交换机通常被用于构建以太网，同时应用于二层网络交换；路由器则具有连通不同的网络和选择信息传送的线路的功能；而网关则是连接两个网络的设备。）

VPN的部署：在大型局域网中，可以通过在网络中心搭建VPN服务器的方法实现VPN。也可以用专用的硬件或软件实现VPN，或者在路由、防火墙等设备上集成VPN。

图10：防火墙、VPN的部署



数据来源：新浪网、广发证券发展研究中心

6.2 终端安全

终端安全产品主要是指对服务器、电脑等终端的安全防护。安全产品主要包括桌面/主机审计、杀毒软件、主机加固（主要功能：修复漏洞、打补丁）、终端登陆/身份认证、计算机防火墙。

表4：终端安全产品介绍

安全产品名称	介绍
计算机防火墙	通过在外部网络和用户计算机之间建立防火墙从而对用户计算机起到防护作用。这种防火墙主要通过对接口规则、传输协议、目的地址及被传输的信息结构进行检测，拒绝不符合规定的信息进入计算机，从而起到防护作用。
杀毒软件	用于清除电脑病毒的软件。通常具备监控识别、病毒扫描和清除、自动升级、主动防御等功能。有的还带有数据恢复功能。

数据来源：广发证券发展研究中心

6.3 应用安全

应用安全产品主要包括网页防篡改、Web应用防火墙（WAF）、WEB漏洞扫描、网站安全监测平台、邮件安全产品、数据库安全产品。

表5：应用安全产品介绍

安全产品名称	介绍
Web 应用防火墙（WAF）	与传统防火墙不同，WAF工作在应用层，WAF对来自Web应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站站点进行有效防护。WEB服务器是WAF所保护的对象，部署位置要尽量靠近WEB服务器。

网站安全监测平台	主要是指对网站的木马、网页篡改、网站可用性、关键词、web漏洞等的监测。
邮件安全产品	电子邮件安全是指为防范电子邮件可能遭到的篡改邮件、病毒邮件、垃圾邮件、邮件炸弹（通过发送巨大的垃圾邮件使对方电子邮件服务器空间溢出）威胁，对电子邮件进行加密、识别邮件病毒、采用防火墙技术进行安全防护。
数据库安全产品	通过对用户访问数据库行为的记录、分析和汇报，用来帮助用户及时阻断风险、事后生成合规报告、事故追根溯源，提高数据资产安全。数据库安全技术主要包括数据数据库漏扫、数据库加密、数据库防火墙、数据脱敏、数据库安全审计系统。

数据来源：广发证券发展研究中心

6.4 数据安全

数据安全：数据安全是指对处于数据生命周期不同阶段的数据进行全面安全防护，涵盖网络数据、终端数据、服务器数据安全，**数据安全和网络层、终端安全包含的内容会有些重叠，但是重点在对数据的全生命周期的防护；主要包括访问控制、敏感数据识别、数据防泄漏（加密、脱敏、敏感数据保护）、审计（上网行为审计、数据库审计）等。**

表6：数据安全产品介绍

安全产品名称	介绍
身份认证	用户名口令、身份认证、PKI证书和生物认证等。
数据加密	是指利用密码技术对信息进行加密，实现信息隐蔽，从而起到保护信息的安全的作用。
数据脱敏	数据脱敏是指对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。

数据来源：广发证券发展研究中心

6.5 安全管理

安全管理：强调对整体状态的监测和管控，功能上可能有些重叠，侧重点有所不同。代表产品有：SIEM/日志管理、运维审计/4A/堡垒机、信息安全等级保护测评工具箱、网络安全态势感知（SOC）。

表7：安全管理产品介绍

安全产品名称	介绍
SIEM/日志管理	内部安全日志集中管理、审计，以及分析和安全风险的监控与定位。
运维审计/4A/堡垒机	运维审计/4A/堡垒机：主要功能是用户认证管理和访问授权管理。（4A是指A：Account身份帐号管理、Authentication身份认证管理、Authorization统一授权管理、Audit统一审计管理。）
网络安全态势感知	态势感知是以安全大数据分析为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式。提供行为发现、核查处置、证据固化、攻击回溯、深度分析、事件溯源、背景研判、拓展深挖等功能。

数据来源：广发证券发展研究中心

7. 如何评价安全产品性能

结论：安全公司核心优势体现在技术的领先度上，技术优势要通过持续的研发投入和技术创新来保持竞争优势。如在防火墙等通用型安全产品上的持续技术创新、在杀毒等终端安全中应用人工智能技术、持续重视对漏洞的挖掘和防护能力、在数据安全中的算法优化、提升在安全管理中的建模分析、数据挖掘能力。

具体而言，在五类产品上，用户重点关注哪些指标以及厂商如何通过技术创新改善产品功能：

7.1 网络安全

防火墙、入侵检测/入侵防御、VPN、上网行为管理在技术实现方式、性能指标上有一定共通性。客户对产品有基础的性能要求，在同样价格水平上，头部公司主打的安全产品性能差异不大，但一些厂商会通过持续的技术创新优化产品、保持领先。

以防火墙为例子，用户对产品性能指标主要包括吞吐量、时延、新建连接速率、并发连接数、一定的扩展性。

- 吞吐量：指这台设备在一秒内所能够处理的最大流量或者说一秒内能处理的数据包个数。设备吞吐量越高，所能提供给用户使用的带宽越大。
- 时延：时延是系统处理数据包所需要的时间。防火墙时延测试指的就是计算它的存储转发(Store and Forward)时间，即从接收到数据包开始，处理完并转发出去所用的全部时间。如果防火墙的时延很低，用户就完全不会感觉到它的存在，提升了网络访问的效率。时延的单位通常是微秒，一台高效率防火墙的时延通常会在一百微秒以内。
- 新建连接速率：新建连接速率指的是在每一秒以内防火墙所能够处理的HTTP新建连连接请求的数量。一台设备的新建连接速率越高，就同时给更多的用户提供网络访问。
- 并发连接数：并发连接数就是指防火墙最大能够同时处理的连接会话个数。并发连接数指的是防火墙设备最大能够维护的连接数的数量，这个指标越大，在一段时间内所能够允许同时上网的用户数越多。
- 一定的扩展性：具有模块化设计的防火墙，后续增添其他功能的话，只需要购买模块即可，不需要更换整个硬件防火墙。

这些性能与防火墙的价格有很大关系，在同价位上，主要性能指标差异不大。以启明星辰、天融信、深信服、山石网科单价7-10万的防火墙举例，在这些参数指标上比较接近。

图11：不同厂家同价位防火墙性能指标对比

数据来源：zol 网站、广发证券发展研究中心

除了上述基本的性能评价指标，技术的领先程度会影响到防护效果。随着网络应用层出不穷，新型威胁不断涌现，传统防火墙基于端口、IP地址的访问控制日渐不能应对安全需求。为解决这些问题，**深信服**于2011年在国内**率先推出第二代防火墙**，并且在2014年国内率先发布了第二代防火墙标准。第一代防火墙遇到的主要问题有：

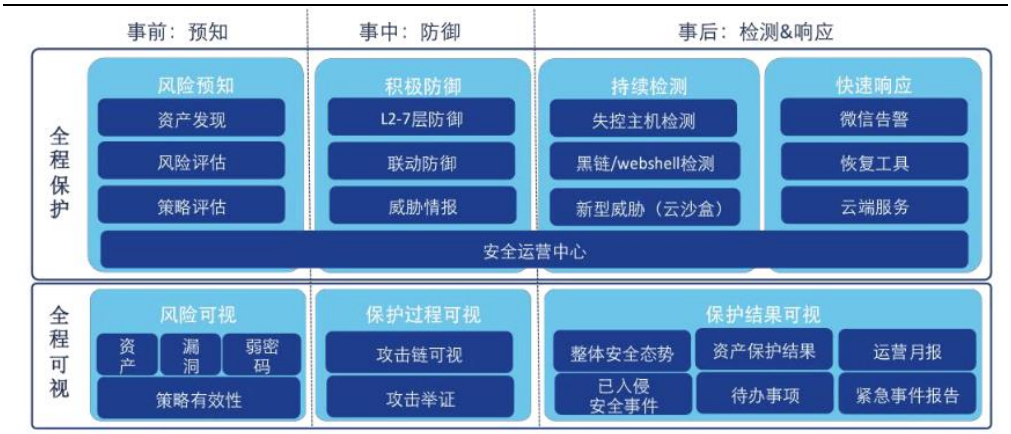
- 传统防火墙无法有效分辨和检测出当今网络中出现的各种复杂应用，其中包括低风险应用（如WebEx、ERP及Oracle等）、也包括高风险应用（如QQ），因而更无法准确的识别和拦截各类应用中的安全风险。
- UTM设备虽然比防火墙提供更全面的安全防护能力，但是将各个安全模块串联在一起，对数据包重复解码，架构效能较低。
- 传统防火墙主要功能是实现遇到威胁时实现事中防御，不能实现事前预知预判。

在此背景下出现了下一代防火墙，相较于第一代防火墙，下一代防火墙实现：

- 精确分类与辨识出包括低风险、高风险在内的多种应用，根据应用不同风险等级分别进行不同级别的安全扫描，从而及时准确的识别和拦截各种威胁攻击，保障用户网络应用的安全性。
- 通过一体化配置策略配置多种安全功能，如集入侵防护、防病毒、URL过滤、内容过滤等，可一次拆包即发现并拦截全部威胁攻击和安全风险，相比UTM，效能更高。
- 强调与云端联动，实时更新并向云端上传数据，能实现持续实时检测和风

险预知。

图12：深信服下一代防火墙



数据来源：深信服官网、广发证券发展研究中心

再如全球防火墙领头羊palo alto新一代防火墙采用零信任技术（零信任安全理念从传统IT可信发展到认为任何网络连接都不可信）。国内安全公司也纷纷追赶，积极投入研发该技术。

7.2 终端安全

最典型的终端安全产品是杀毒软件，病毒来源一般来自网上下载程序、文件、邮件或者U盘等途径传播。对于杀毒软件主要关注的性能指标有：

- 病毒查杀能力（病毒信息库丰富程度、漏报率、误报率、清除能力）；
- 杀病毒软件的自我保护能力，对现有资源的占用情况；
- 对文件的恢复能力。

厂商亦可通过对新技术的应用会提高产品的防护效果，如机器学习技术的应用。有些客户出于对数据保护不能接受来自外部的云端查杀病毒，需要软件厂商定期在客户本地为其更新病毒库。由于数据库更新的滞后性可能会导致对一些新病毒的反应能力加载滞后，将机器学习技术应用在杀毒软件中，可以通过机器学习技术学习病毒的升级路径，对变异的病毒进行及时防护，在一定程度上可以解决病毒库更新滞后的问题。

7.3 应用安全

以web应用防火墙为例、web应用弱点扫描器为例。**核心能力是漏洞发掘发现能力**，这也是安全厂商需要持续投入的核心竞争力之一。

Web应用防火墙：需要具备传统抗DDOS的性能指标，以及对SQL注入、跨站脚本攻击、数据泄露、应用层DDOS、0day漏洞的识别能力。

Web应用弱点扫描器：需关注的核心能力还是漏洞挖掘能力，需要利用漏洞产生的原理和渗透测试的方法，对Web应用进行深度弱点探测，帮助应用开发者和管理者了解应用系统存在的脆弱点。

7.4 数据安全

数据安全能力的评价重点在于对数据的防护能力，**核心在于算法**。以**数据脱敏**为例算法越丰富则越难被还原。具体来看，数据脱敏能力的评价重点关注以下指标：

- 对敏感数据的发现能力：需要具备多种敏感数据识别规则，根据相关法规，对数据集中的所有字段进行敏感属性识别；
- 算法的丰富性：数据脱敏的算法包括屏蔽、变形、移位、格式化保留加密、令牌化、洗牌、强加密算法等；
- 抗还原性：采用高等级的算法脱敏后的数据不易被还原；
- 对异构环境的支持：对不同数据库的支持；
- 与业务的同步性：如是否采用动态脱敏技术实现对数据的实时脱敏。

图13：数据脱敏技术的主要关注点

数据来源：腾讯云官网、广发证券发展研究中心

7.5 安全管理

以近两年兴起的**态势感知**产品为例，**重点关注厂商的数据分析及安全问题快速响应解决能力**。分析包括：

- 一是通过深度的网络会话关联分析、数据包解码分析、载荷内容还原分析、特征分析和日志分析，真实还原黑客入侵的全过程，从而对网络安全事件进行精准的定性分析；
- 二是快速提取多维度的网络元数据进行异常行为建模，为后续异常数据挖掘、分析、取证建立扎实的基础。
- 三是后续的关联回溯分析，实现从线索挖掘到整个攻击过程的完整复盘，为安全事件的准确响应提供依据。

8. 需求现状：当前以网络边界防护为主

8.1 目前国内市场以硬件形态的网络边界安全为主

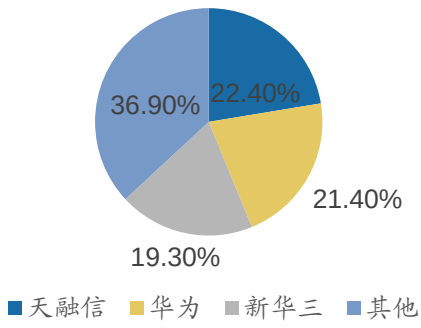
目前国内信息安全市场上的主流安全产品还是以硬件形态呈现网络边界的安全产品。主要产品包括防火墙、统一威胁管理平台（UTM）、入侵检测和入侵防御（IDP）、虚拟专用网络（VPN），安全内容管理（SCM）。

据IDC发布的《2018年第四季度中国IT安全硬件市场跟踪报告》，2018年中国IT硬件市场规模为35.3亿美元（约合人民币244.2亿元），同比增长26.51%。预计到2023年市场规模可达109.9亿美元，未来5年年复合增速为25.5%，受益于行业政策的推动，主流安全产品仍有望保持快速增长。各细分领域排名前3的主要是**深信服、启明星辰、天融信**等A股头部安全厂商，以及数通厂商**华为、新华三**。还有一些公司在主流安全产品的技术升级上有些公司抓住了机会，在细分产品市场上取得了不错表现，如**山石网科**（拳头产品下一代防火墙）。

图14：中国安全硬件市场规模及规模预测

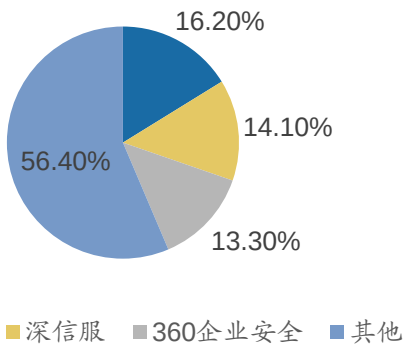
数据来源：IDC、广发证券发展研究中心

图15：2018年中国防火墙硬件市场份额



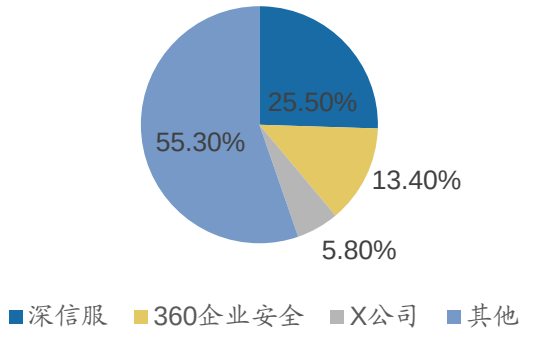
数据来源：IDC、广发证券发展研究中心

图16：2018年中国统一威胁管理硬件市场份额



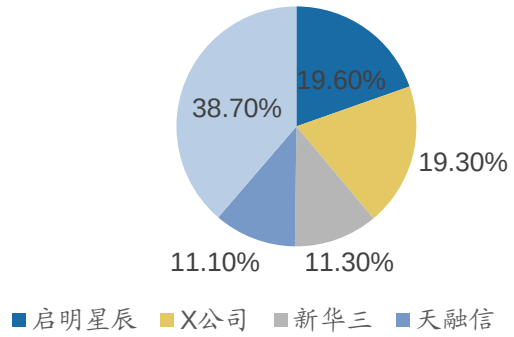
数据来源：IDC、广发证券发展研究中心

图17：2018年安全内容管理硬件市场份额



数据来源：IDC、广发证券发展研究中心

图18：2018年入侵检测与防御硬件市场份额



数据来源：IDC、广发证券发展研究中心

8.2 数据安全、终端安全、安全管理需求也在逐步释放

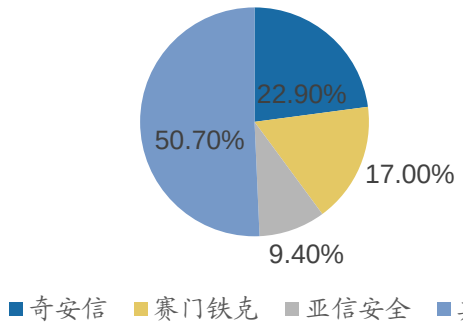
数据安全、终端安全、安全管理多以软件形式呈现，需求也在逐步释放。据《2018年下半年中国IT安全软件市场跟踪报告》显示，2018年中国IT软件市场规模为约为62.7亿元，同比增长23.98%。从细分产品规模来看，前三分别是身份和数字信任软件、终端安全软件和AIRO（ARIO是Analytics-分析、Incident-事件管理、Response-响应、Orchestration-安全编排的缩写，主要指用在安全运营中心上的软件，用于发现威胁和响应补救）。

- **身份和数字信任软件**市场与主流安全硬件需要的技术差异较大，老牌安全厂商并未涉足，收入规模前三分别是**吉大正元、亚信安全、格尔软件**。
- **终端安全软件**市场主要在杀毒领域积累较深的安全公司占主导，收入规模前三分别是奇安信、赛门铁克、亚信安全。
- **AIRO**市场老牌头部安全公司排名靠前，收入规模前三的公司分别是某A股安全公司、启明星辰、IBM。以**SOC（态势感知平台）**为代表的AIRO需求近两年才在国内兴起，头部安全公司综合安全能力强，可快速研发推出产品，而且可以广泛在政府、运营商、金融等率先有SOC需求的客户中推广该产品。

图19：2019-2023年中国安全软件市场规模及规模预测

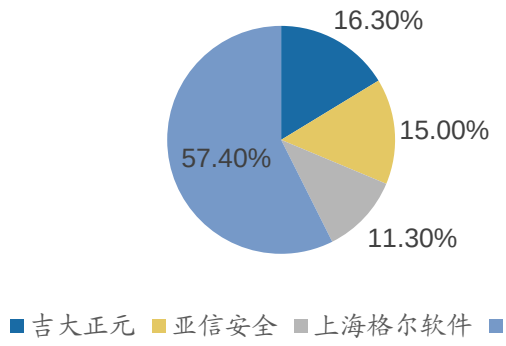
数据来源：IDC、广发证券发展研究中心

图20：2018年中国终端安全市场份额



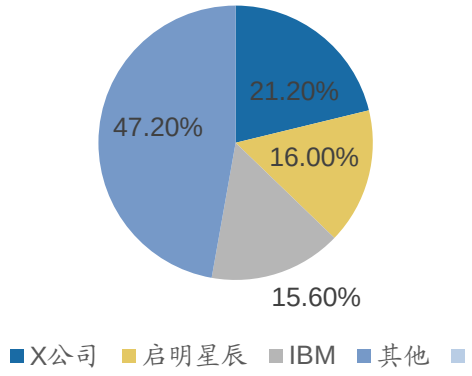
数据来源：IDC、广发证券发展研究中心

图21：2018年中国身份和数字信任软件市场份额



数据来源：IDC、广发证券发展研究中心

图22：2018年中国AIRO市场份额



数据来源：IDC、广发证券发展研究中心

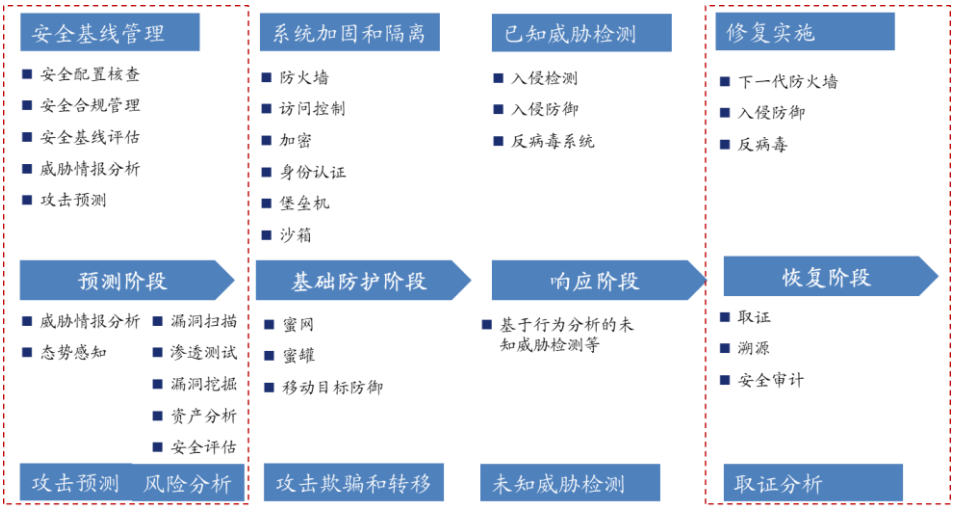
9. 需求变化：安全管理、数据安全需求加速

9.1 客户重视安全管理，头部厂商优势更明显

从产品需求变化上来看，由于更重视预测、溯源，相应需要安全管理平台做全流量分析，需要产品满足联动、智能防护的需求。

客户愈加重视预测、溯源，安全管理需求兴起。信息安全的防护可以分为预测阶段、基础防护阶段、响应阶段和恢复阶段。我国安全产品目前大部分集中在基础防护和已知威胁检测阶段，该阶段典型安全产品以防火墙、入侵检测、入侵防御、身份认证为代表。由于客户更加重视安全，相应需要安全管理平台做全流量分析，以实现预测、溯源。从产品变化上来看，全面管控型的态势感知平台需求兴起，安全产品向联动、智能方向发展。

图23：信息安全安全防护阶段划分



数据来源：广发证券发展研究中心

态势感知领域代表公司有启明星辰、安恒信息等，在数据分析领域积累较深，安全数据分析能力、安全问题解决能力突出，能提供强效预测、溯源、恢复。**产品研发能及时响应客户智能联动需求的代表公司如深信服**，深信服安全产品均在朝着联动、智能的方向发展，提出安全产品之间的全线联动，可实现下一代防火墙可与安全态势感知平台之间，安全防护可与云端之间闭环联动。通过闭环联动，可实现防御、检测、响应和预测。

图24：安全态势感知平台和下一代防火墙联动示意图

数据来源：深信服安全产品宣讲材料、广发证券发展研究中心

图25：云端闭环联动示意图

数据来源：深信服安全产品宣讲材料、广发证券发展研究中心

9.2 数据安全需求增加，深耕数据安全的公司更有机会

安全防护以往强调对网络边界层的防护，专门针对数据的安全防护较少。随着数据集中管理、用户对安全的重视程度增加，数据安全的需求在加速。

近些年，传统安全公司的数据安全业务呈现快速增长。如启明星辰的数据安全业务、数据安全公司明朝万达近几年的收入增速都得到了快速增长。启明星辰17、18年数据安全业务收入增速分别是30%、27%，远高于公司整体收入增速18%、11%。以数据安全业务为主的明朝万达16、17年整体收入增速分别是57%、56%（以上数据均来自公司财报）。

数据安全主要涉及数据访问控制、敏感数据识别、数据防泄漏等细分领域，访问控制领域代表公司有**格尔软件**；数据防泄漏领域代表公司有**启明星辰、明朝万达、亿赛通**。

重点标的

在市场集中度还不太高的背景下，核心竞争力突出，技术基因和人员储备等优势明显，包括治理结构不断优化的公司，如深信服等。

风险提示

行业投入加速节奏的不可把握性；来自云厂商的竞争加剧；在项目单体体量和复杂度增大的驱使下，伴随的集成业务可能对毛利率和现金流产生一定影响。

广发计算机行业研究小组

刘 雪 峰：首席分析师，东南大学工学士，中国人民大学经济学硕士，1997 年起先后在数家 IT 行业跨国公司从事技术、运营与全球项目管理工作。2010 年 7 月始就职于招商证券研究发展中心负责计算机组行业研究工作，2014 年 1 月加入广发证券发展研究中心。

王 奇 珏：资深分析师，上海财经大学信息管理学士，上海财经大学资产评估硕士，2015 年进入广发证券发展研究中心。

郑 楠：资深分析师，北京邮电大学计算机专业学士，法国巴黎国立高等电信大学移动通信硕士，2010 年起就职于外资企业软件公司从事研发、咨询顾问等工作，2015 年加入广发证券发展研究中心。

庞 倩 倩：资深分析师，华南理工大学管理学硕士，曾就职于华创证券，2018 年加入广发证券发展研究中心。

钱 砾：研究助理，东南大学信息工程学士、生物医学工程医学电子影像方向硕士，先后在电子信息行业和医疗影像设备行业工作超过 6 年，2017 年加入广发证券发展研究中心。

广发证券—行业投资评级说明

买入：预期未来 12 个月内，股价表现强于大盘 10%以上。

持有：预期未来 12 个月内，股价相对大盘的变动幅度介于-10%～+10%。

卖出：预期未来 12 个月内，股价表现弱于大盘 10%以上。

广发证券—公司投资评级说明

买入：预期未来 12 个月内，股价表现强于大盘 15%以上。

增持：预期未来 12 个月内，股价表现强于大盘 5%-15%。

持有：预期未来 12 个月内，股价相对大盘的变动幅度介于-5%～+5%。

卖出：预期未来 12 个月内，股价表现弱于大盘 5%以上。

联系我们

	广州市	深圳市	北京市	上海市	香港
地址	广州市天河区马场路 26 号广发证券大厦 35 楼	深圳市福田区益田路 6001 号太平金融大厦 31 层	北京市西城区月坛北街 2 号月坛大厦 18 层	上海市浦东新区世纪大道 8 号国金中心一期 16 楼	香港中环干诺道中 111 号永安中心 14 楼 1401-1410 室
邮政编码	510627	518026	100045	200120	
客服邮箱	gfyf@gf.com.cn				

法律主体声明

重要声明

广发证券股份有限公司及其关联机构可能与本报告中提及的公司寻求或正在建立业务关系，因此，投资者应当考虑广发证券股份有限公司及其关联机构因可能存在的潜在利益冲突而对本报告的独立性产生影响。投资者不应仅依据本报告内容作出任何投资决策。

本报告署名研究人员、联系人（以下均简称“研究人员”）针对本报告中相关公司或证券的研究分析内容，在此声明：（1）本报告的全部分析结论、研究观点均精确反映研究人员于本报告发出当日的关于相关公司或证券的所有个人观点，并不代表广发证券的立场；（2）研究人员的部分或全部的报酬无论在过去、现在还是将来均不会与本报告所述特定分析结论、研究观点具有直接或间接的联系。

研究人员制作本报告的报酬标准依据研究质量、客户评价、工作量等多种因素确定，其影响因素亦包括广发证券的整体经营收入，该等经营收入部分来源于广发证券的投资银行类业务。

本报告仅面向经广发证券授权使用的客户/特定合作机构发送，不对外公开发布，只有接收人才可以使用，且对于接收人而言具有保密义务。广发证券并不因相关人员通过其他途径收到或阅读本报告而视其为广发证券的客户。在特定国家或地区传播或者发布本报告可能违反当地法律，广发证券并未采取任何行动以允许于该等国家或地区传播或者分销本报告。

本报告所提及证券可能不被允许在某些国家或地区内出售。请注意，投资涉及风险，证券价格可能会波动，因此投资回报可能会有所变化，过去的业绩并不保证未来的表现。本报告的内容、观点或建议并未考虑任何个别客户的具体投资目标、财务状况和特殊需求，不应被视为对特定客户关于特定证券或金融工具的投资建议。本报告发送给某客户是基于该客户被认为有能力独立评估投资风险、独立行使投资决策并独立承担相应风险。

本报告所载资料的来源及观点的出处皆被广发证券认为可靠，但广发证券不对其准确性、完整性做出任何保证。报告内容仅供参考，报告中的信息或所表达观点不构成所涉证券买卖的出价或询价。广发证券不对因使用本报告的内容而引致的损失承担任何责任，除非法律法规有明确规定。客户不应以本报告取代其独立判断或仅根据本报告做出决策，如有需要，应先咨询专业意见。

广发证券可发出其它与本报告所载信息不一致及有不同结论的报告。本报告反映研究人员的不同观点、见解及分析方法，并不代表广发证券的立场。广发证券的销售人员、交易员或其他专业人士可能以书面或口头形式，向其客户或自营交易部门提供与本报告观点相反的市场评论或交易策略，广发证券的自营交易部门亦可能会有与本报告观点不一致，甚至相反的投资策略。报告所载资料、意见及推测仅反映研究人员于发出本报告当日的判断，可随时更改且无需另行通告。广发证券或其证券研究报告业务的相关董事、高级职员、分析师和员工可能拥有本报告所提及证券的权益。在阅读本报告时，收件人应了解相关的权益披露（若有）。

本研究报告可能包括和/或描述/呈列期货合约价格的事实历史信息（“信息”）。请注意此信息仅供用作组成我们的研究方法/分析中的部分论点/依据/证据，以支持我们对所述相关行业/公司的观点的结论。在任何情况下，它并不（明示或暗示）与香港证监会第 5 类受规管活动（就期货合约提供意见）有关联或构成此活动。

权益披露

(1)广发证券（香港）跟本研究报告所述公司在过去 12 个月内并没有任何投资银行业务的关系。

版权声明