

方正证券研究所证券研究报告

行业专题报告

行业研究

计算机行业

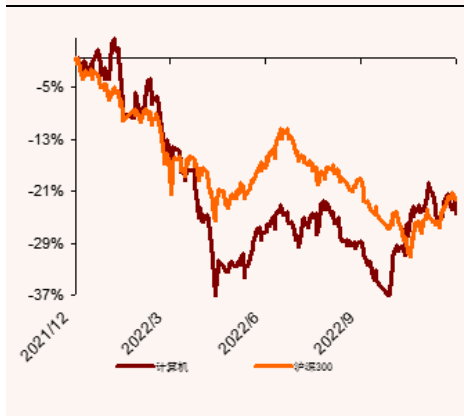
2022.12.16/推荐

分析师： 方闻千
 登记编号： S1220517040005

重要数据：

上市公司总家数	287
总股本(亿股)	1950.97
销售收入(亿元)	14883.57
利润总额(亿元)	1545.88
行业平均 PE	62.09
平均股价(元)	23.57

行业相对指数表现：



数据来源：wind 方正证券研究所

相关研究

《当前时点如何看信创的空间及节奏》
 2022.10.31

《中望软件：教育业务显著恢复，云化 CAD 产品发布值得期待》2022.10.31

信创、数据安全、关基保护三条政策主线明确，23 年网络安全行业有望迎来景气度及竞争格局的双重改善。当前，政策合规仍是国内网络安全市场的第一驱动力，以等保 2.0 为代表的安法规条例的实施带来了安全行业上一轮的景气高峰期，而随着新一轮政策主线的明确，预计未来三年网络安全未来行业增速逐渐将回复到 20% 以上的中高速增长基准线上，包括 IDC 在最新的报告中也上调了对国内网络安全行业未来 5 年增长水平的预测。同时，随着行业竞争格局的优化以及主要安全厂商人员增速的放缓，未来一年安全厂商报表质量有望持续改善。

2023 年行业的三重驱动力：信创、关基保护、数据安全。

1) 信创：行业信创及区县信创明年起将进入上量阶段，网络安全是信创的关键组成部分，新一轮信创不仅将直接带动各类安全产品采购量的增加，并且有望驱动行业集中度的提升；

2) 数据安全：《数据安全法》、《个人信息保护法》两大上位法已经出台，未来看点在于数据安全相关法规条例及各行业数据安全标准的落地，数据安全行业将继续保持高速增长；

3) 关基保护：今年 11 月我国首项关键信息基础设施保护国家标准正式发布，并将于明年 5 月 1 日实施。这预示着我国关基保护合规工作将从明年开始全面启动，我国“3 保 1 评”的网络安全保护工作有望进入新一轮高峰。

2023 年看好的三大方向：数据安全、安全攻防、信创安全。

1) 数据安全：作为近年来网络安全行业景气最高的赛道，一方面，传统数据安全市场总体规模在百亿以上，每年保持 30%+ 增长，其中综合型厂商的优势正在不断提升，同时在密评的带动下，密码行业保持较高景气度；另一方面数据信托、隐私计算作为数据安全新场景，随着互联网监管、政务大数据等应用领域的不断拓宽，未来有望撬动千亿级的市场规模；

2) 安全攻防：在上一轮网络安全景气高峰时期(2017-2020 年)，安全管理及安全攻防是国内网络安全行业景气度最高的赛道，态势感知成为爆款产品。当前外部安全威胁的不断增加驱动了政企用户实战攻防的需求，未来以 XDR 为代表的安全管理及安全攻防类产品将是下一阶段安全投入的重点；

3) 信创安全：与信创强相关的终端安全产品、网络安全产品以

及信创中催生出的增量需求产品，包括加密类、web 应用安全产品，都将显著受益于新一轮信创需求的带动。

投资逻辑：23 年网络安全行业有望迎来景气度及竞争格局的双重改善：1) 信创明年起进入上量阶段，虽然网安本身的国产化率较高，但参考上一轮信创，在信创推进过程中对防火墙、终端安全等产品采购仍有明显拉动；2) 政策面持续向好，数据安全及关基保护明年进一步落地，叠加进入十四五第三年，此前收紧的安全预算将逐渐释放；3) 行业竞争格局改善，多家头部厂商控制人员增长，报表质量同时将普遍改善。推荐标的：深信服、启明星辰、奇安信、安恒信息，相关标的：天融信、绿盟科技、卫士通、信安世纪、山石网科、迪普科技、中孚信息等。

风险提示：疫情反复导致经济下行的风险；行业竞争持续加剧的风险；政策落地不达预期的风险。

目录

1 网络行业全年回顾：三季度行业景气开始恢复.....	5
2 网络安全的三大驱动力：信创、数据安全、关基保护.....	8
2.1 信创：2013 年起将进入上量阶段.....	10
2.2 数据安全：近三年安全行业景气度最高的赛道.....	12
2.3 关基保护：明年起关保合规工作将全面启动.....	14
3 明年看好的三大方向：数据安全、安全攻防、信创安全.....	18
3.1 数据安全：看好综合型安全厂商与密码类厂商.....	19
3.2 安全攻防：XDR 引领下一轮网络安全实战化建设.....	23
3.3 信创安全：信创推进过程中将催生出新安全需求.....	26
4 投资逻辑.....	28
5 风险提示.....	29

图表目录

图表 1: 主要网络安全厂商单季度收入及同比增速 (单位: 亿元)	5
图表 2: 主要网络安全厂商单季度毛利率情况	6
图表 3: 主要网络安全厂商综合费用同比增长情况	7
图表 4: 2021-至今网络安全行业指数走势	7
图表 5: 网络安全驱动因素框架	8
图表 6: 近一年以来发生多起重大安全事件	9
图表 7: 中国网络安全市场预测 2022-2026	10
图表 8: 2023 年起信创有望进入上量阶段	10
图表 9: 信创全产业链图谱	11
图表 10: 信创产业基础软硬件及部分应用适配图谱	12
图表 11: 数据安全演进历史	13
图表 12: 数据安全相关政策及立法进程	14
图表 13: 关键信息基础设施保护相关政策及立法进程	15
图表 14: 信创产业基础软硬件及部分应用适配图谱	16
图表 15: 3 保 1 评的联系与区别	17
图表 16: 中国网络安全市场行业占比预测 (2026 年)	17
图表 17: 网络安全行业赛道规模及增速	18
图表 18: 网络安全行业 7 大赛道	19
图表 19: 什么是数据安全	20
图表 20: 数据安全厂商梳理	21
图表 21: 密评发展进程不断推进	22
图表 22: 隐私计算应用领域	23
图表 23: 企业网络安全建设发展阶段	24
图表 24: 深信服 XDR 平台	25
图表 25: 2021 年中国安全分析和威胁情报市场份额	26
图表 26: 奇安信信创安全体系	26
图表 27: 2021 年中国终端安全软件市场份额	27
图表 28: 2021 年中国 UTM 防火墙市场份额	28
图表 29: 2021 年中国统一威胁管理市场份额	28
图表 30: 主要网络安全厂商估值表	29

1 网络行业全年回顾：三季度行业景气开始恢复

回顾 22 年网络安全行业，上半年受宏观环境及疫情因素影响，行业整体需求受到冲击，三季度以来行业需求端开始复苏，四季度随着政策主线的逐渐明朗，明年行业景气度有望显著提升。今年以来在网络安全的三大下游中，行业客户特别是关基单位的预算整体保持稳健增长，但政府及企业的安全预算均受到冲击，特别是今年上半年上海、深圳、北京等地的疫情对安全采购和实施交付产生了较大的负面影响。Q3 至今行业需求端开始复苏，可以看到包括启明星辰、安恒信息、绿盟科技等多安全厂商表现增速及订单情况均有一定回升，但整体来看，由于 Q3 护网行动的拉动效果低于预期，同时此前延后的订单还未充分释放，因此 Q3 整体恢复程度略低于预期。Q4 以来，关保、数据安全、政务大数据相关政策落地节奏显著加快，明年信创、关保、数据安全三大政策主线基本明确，网络安全的景气度有望显著提升。

图表1： 主要网络安全厂商单季度收入及同比增速（单位：亿元）

		2021Q1	2021Q2	2021Q3	2021Q4	2022Q1	2022Q2	2022Q3
启明星辰	收入	5.06	7.06	8.85	22.89	5.64	6.50	9.54
	yoy	120.2%	34.5%	28.6%	3.9%	11.6%	-8.0%	7.8%
深信服	收入	10.92	14.94	17.90	24.29	11.44	16.71	19.33
	yoy	79.4%	31.6%	19.3%	9.7%	4.8%	11.9%	8.0%
安恒信息	收入	1.84	2.78	4.04	9.55	2.33	3.01	5.05
	yoy	57.8%	36.5%	18.7%	44.1%	26.9%	8.4%	25.1%
绿盟科技	收入	2.43	5.29	4.60	13.77	3.27	5.08	5.53
	yoy	47.0%	37.5%	17.1%	29.0%	34.6%	-4.1%	20.2%
天融信	收入	2.65	4.40	6.85	19.61	3.78	5.02	5.83
	yoy	-64.3%	-73.0%	-50.8%	1.4%	42.8%	13.9%	-14.8%
奇安信-U	收入	4.56	9.99	12.19	31.35	6.59	13.09	12.24
	yoy	102.1%	27.9%	41.3%	36.8%	44.5%	31.0%	0.4%
三六零	收入	25.52	30.67	29.20	23.47	25.26	22.98	21.11
	yoy	13.4%	12.7%	-2.8%	-35.5%	-1.0%	-25.1%	-27.7%
美亚柏科	收入	2.74	5.17	4.51	12.94	3.20	3.68	4.16
	yoy	19.1%	35.3%	-3.3%	-1.1%	16.8%	-28.8%	-7.7%
迪普科技	收入	1.94	2.39	3.09	2.88	2.14	1.54	2.38
	yoy	40.3%	34.1%	30.2%	-14.6%	10.3%	-35.5%	-22.9%
卫士通	收入	2.83	5.61	7.92	12.53	6.31	6.80	7.48
	yoy	379.0%	49.9%	26.7%	-10.8%	123.1%	21.2%	-5.5%
亚信安全	收入	2.59	2.27	4.93	6.88	2.85	3.08	4.36
	yoy	-	-	-42.0%	62.1%	9.8%	35.9%	-11.6%
信安世纪	收入	0.49	1.05	1.04	2.67	0.64	1.07	1.41
	yoy	30.5%	29.9%	30.3%	22.3%	31.5%	1.5%	34.8%

资料来源：Wind、方正证券研究所整理

Q3 安全厂商报表质量有所改善。相较于 Q2 及 Q1，今年 Q3 包括安恒信息、深信服、绿盟科技、奇安信、迪普科技、卫士通等多家厂商的毛利率有明显提升，其中启明星辰及天融信的毛利率有所下降，主要原因在于低毛利的集成业务及云业务占比增加，而安全业务毛利率整体依然维持稳定。在毛利率改善的同时，今年以来各安全厂商对人员的控制也见到明显成效，相较于今年 Q2、Q1 以及去年 Q3，今年 Q3 包括启明星辰、深信服、安恒信息、绿盟科技等多家安全厂商的费用增速开始明显放缓。

随着行业竞争格局的优化以及安全厂商人员增速的放缓，未来一年主要安全厂商报表质量有望持续改善。回顾 21 年，由于 Q4 开始政府安全预算受到影响导致需求端不达预期，叠加全年行业竞争加剧以及主要安全厂商人员增速达到历年最高水平，因此 21 年 Q4 开始行业收入端增速及盈利能力出现一定程度的恶化。当前时点来看，一方面今年安全厂商普遍对人员增长有严格控制，从 Q3 开始基本不再有大规模外部招聘，预计全年行业人员增长在 5% 以内；另一方面，以奇安信，360 为代表的头部厂商开始改变打法，其中奇安信以毛利为导向的考核体系已见成效，360 也开始针对政企安全市场的战略进行重大调整，头部厂商经营策略的变化也将对行业格局产生进一步的影响，在双重因素影响下，未来一年行业整体的报表质量有望得到明显改善。

图表2： 主要网络安全厂商单季度毛利率情况

	2021Q1	2021Q2	2021Q3	2021Q4	2022Q1	2022Q2	2022Q3
启明星辰	60.7%	60.9%	66.5%	68.5%	68.5%	66.0%	58.5%
深信服	66.5%	67.2%	63.1%	65.8%	58.9%	63.0%	63.8%
安恒信息	51.8%	58.7%	58.3%	70.3%	51.4%	54.5%	61.9%
绿盟科技	65.9%	67.7%	69.1%	55.6%	63.3%	57.8%	61.8%
天融信	60.0%	77.1%	79.5%	48.3%	67.6%	66.8%	52.3%
奇安信-U	63.8%	63.1%	61.7%	57.8%	59.2%	56.2%	67.5%
三六零	58.8%	59.0%	60.8%	72.2%	58.8%	59.9%	61.1%
美亚柏科	64.0%	58.2%	61.6%	56.1%	55.3%	49.9%	39.7%
迪普科技	71.6%	68.8%	74.7%	70.1%	67.7%	63.4%	69.6%
卫士通	42.2%	37.3%	35.8%	38.4%	34.7%	29.6%	37.5%
亚信安全	57.7%	54.1%	51.7%	52.7%	48.8%	49.7%	49.2%
信安世纪	73.1%	71.9%	68.9%	73.3%	72.7%	75.1%	71.8%

资料来源：Wind、方正证券研究所整理

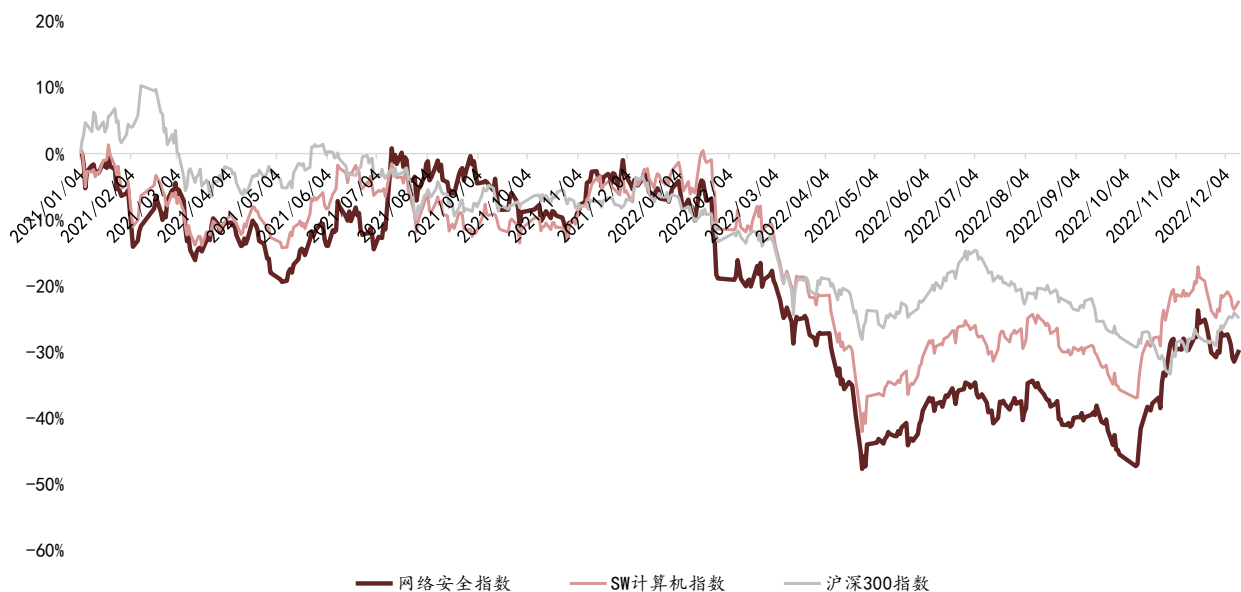
图表3： 主要网络安全厂商综合费用同比增长情况

	2021Q1	2021Q2	2021Q3	2021Q4	2022Q1	2022Q2	2022Q3
启明星辰	48%	46%	28%	23%	24%	26%	11%
深信服	46%	45%	39%	11%	28%	14%	5%
安恒信息	92%	84%	63%	33%	45%	27%	26%
绿盟科技	15%	22%	45%	21%	50%	23%	11%
天融信	19%	22%	17%	13%	24%	15%	12%
奇安信-U	21%	54%	35%	35%	21%	15%	7%
三六零	34%	66%	12%	-4%	0%	-7%	10%
美亚柏科	33%	46%	24%	-9%	13%	-6%	5%
迪普科技	44%	41%	27%	-14%	6%	-5%	0%
卫士通	25%	24%	16%	10%	12%	1%	23%
亚信安全			27%	60%	72%	42%	36%
信安世纪	20%	12%	27%	29%	9%	16%	20%

资料来源：Wind、方正证券研究所整理

回顾此前几年网络安全板块的市场表现,18-20年等保2.0及护网行动等开启了上一轮网络安全牛市,经过21年的调整之后,在多因素影响下,22年板块从年初以来持续下跌,最大跌幅达45%,跌幅超过了计算机板块及沪深300。随着年中复工复产预期的修复以及10月后信创行情的带动,网络安全板块迎来持续上涨。预计明年信创、关保、数据安全等新政策的持续落地,板块整体景气度将迎来复苏。从当前板块估值水平来看,龙头公司包括奇安信、安恒信息、深信服的PS-2023基本在4-5X,仍远低于上一轮网络安全高峰期的估值水平。

图表4： 2021-至今网络安全行业指数走势

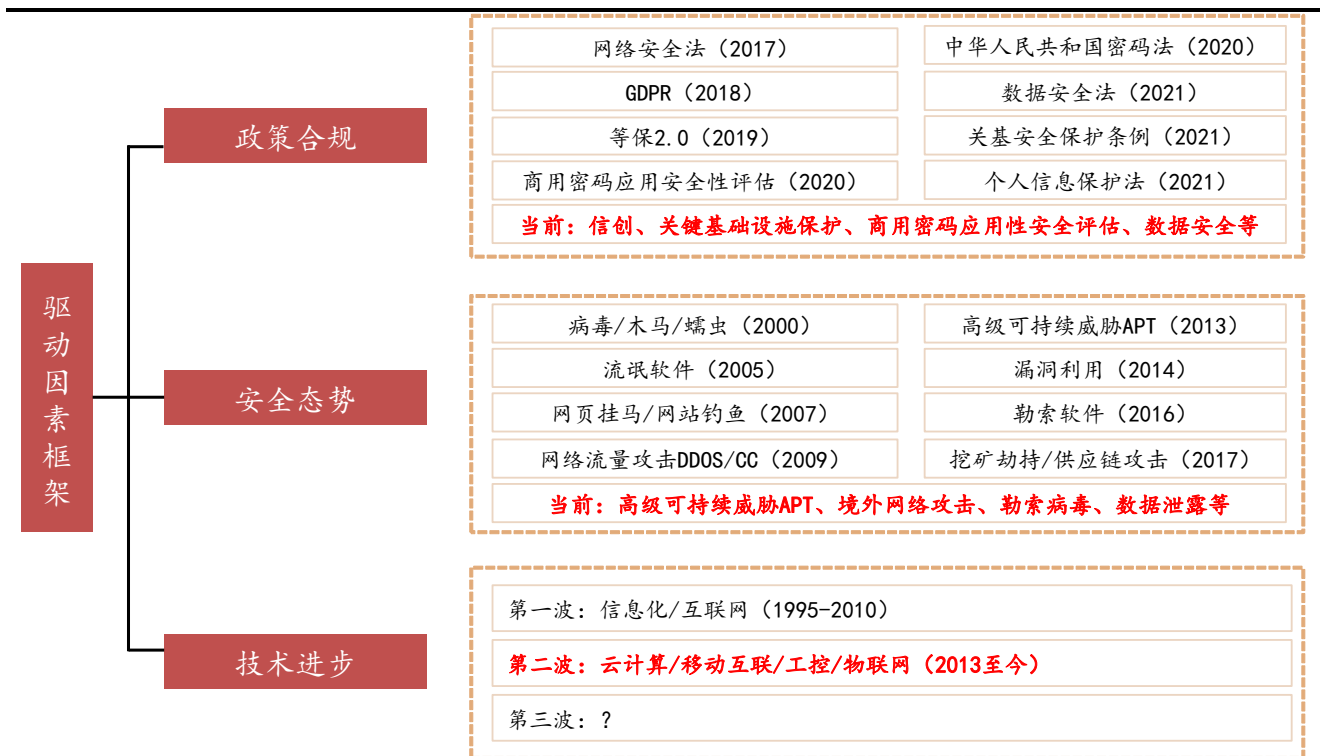


资料来源：Wind、方正证券研究所整理

2 网络安全的三大驱动力：信创、数据安全、关基保护

未来一年信创、关基保护、数据安全三大政策主线基本明确，政策合规仍是国内网络安全市场的第一驱动力。从网络安全行业的驱动力框架来看：首先，无论在全球还是在国内，政策合规都是安全行业最直接的驱动力，过去5年网络安全法、密码法、数据安全法、个人信息保护法、等保2.0以及关基条例等法律法规的出台与实施共同推进了我国网络安全监管体系的完善，并带动了行业景气度的显著提升，其中等保2.0是驱动上一轮安全景气高峰的关键。展望未来三年，信创、关保、数安三条政策主线将带动下一阶段网络安全行业的快速成长；其次，安全态势作为安全行业的底层驱动力，不同的时期的安全事件和攻击手段将会催生出不同形式的安全需求，同时又会间接影响政策的力度和走向，因而近年来数据泄露事件以及外部安全攻击的增加导致了相关政策的不断加码；最后网络安全作为IT的伴生性行业，每一轮IT产业浪潮的背后，都会伴随着网络安全行业的快速发展。

图表5：网络安全驱动因素框架

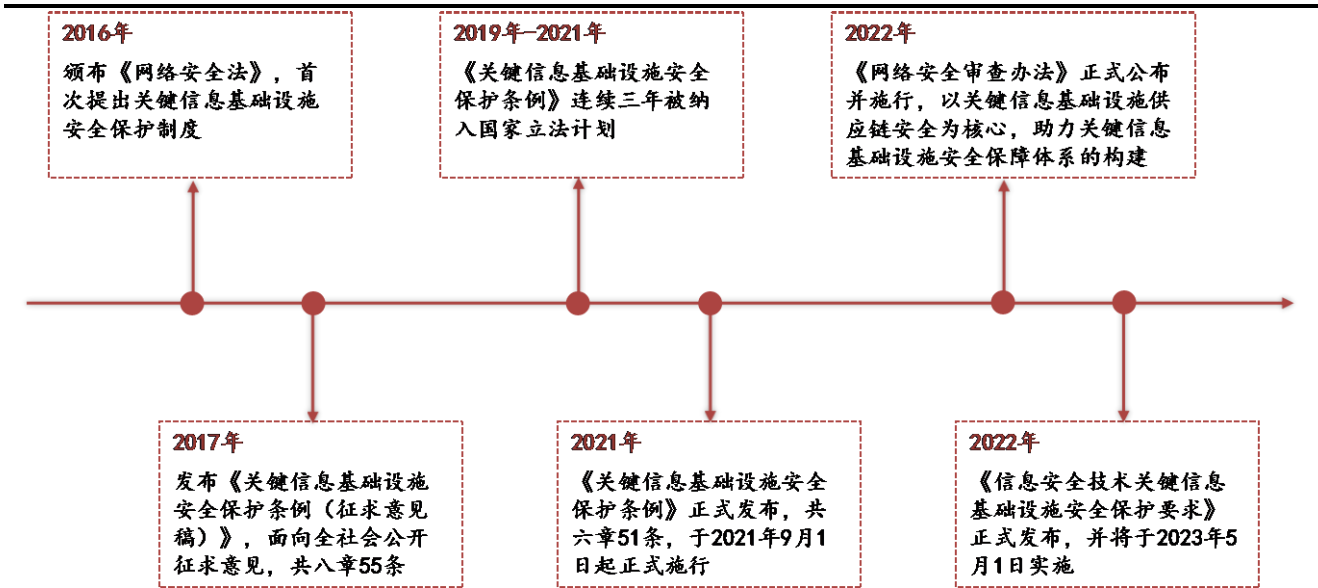


资料来源：方正证券研究所整理

从今年整体安全态势来看，最突出的特点就是外部安全攻击以及数据泄露事件的增加。1）外部网络安全态势趋向严峻：今年从俄乌战争中能看到针对关键基础设施的网络攻击层出不穷，特别是西北工业大学遭境外安全攻击等事件反映出我国面临的境外安全威胁正在持续增加，这一趋势也将对未来政企网络安全的投入产生持续影响，特别是对关基单位而言，如何应对境外安全攻击将成为今后安全投入的重中之重；2）数据泄露事件显著增加：从去年的滴滴事件开始，到今年以来多个互联网公司、关键行业发生重大数据泄露事件，数据安全已经引发国家层面的重点关注，未来加大数据安全政策力度和预算投

入是大概率事件。

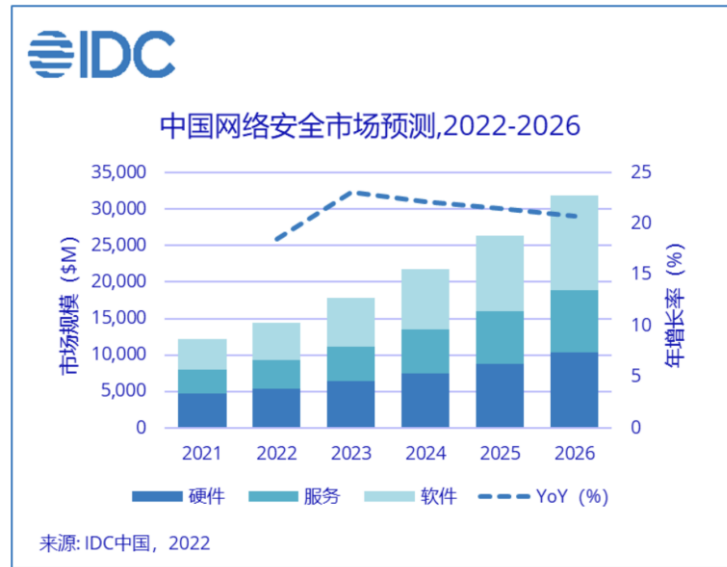
图表6： 近一年以来发生多起重大安全事件



资料来源：方正证券研究所整理

当前信创、关基保护、数据安全三条政策主线已经基本明确。1) 信创：行业信创及区县信创明年将进入上量阶段，网络安全作为信创的关键组成部分，新一轮信创不仅将直接带动安全采购的显著增加，并有望驱动行业集中度的提升；2) 数据安全：《数据安全法》、《个人信息保护法》两大上位法去年已经落地，随着《网络数据安全管理办法》、《数据出境安全评估办法》等法规条例及各行业数据安全标准的出台将共同推动数据安全行业的加速成长；3) 关基保护：外部安全威胁的增加提升了加强关键基础设施保护的重要性，今年 11 月我国首项关键信息基础设施保护国家标准正式发布，并将于 2023 年 5 月 1 日正式实施。这也预示着从明年开始我国关基保护合规工作将全面启动。在三大政策主线的共同推动下，网络安全未来行业增速将回复到 20% 以上的中高速增长基准线上，包括 IDC 在最新的报告中也上调了对国内网络安全行业未来 5 年增长水平的预测。

图表7： 中国网络安全市场预测 2022-2026



资料来源：IDC、方正证券研究所

2.1 信创：2013 年起将进入上量阶段

2023 年是 IT 产业链国产化新一轮浪潮的起点，从明年起，党政信创中的区县信创和行业信创预计将形成叠加，需求共振推动信创进入新一轮上升期。对于党政信创而言，2020-2022 年，地市以上单位的信创工作稳步推进，取得了积极的成效，而 2023 年起区县信创有望接力，拉动党政信创开启新一轮周期。对于行业信创而言，2022 年是行业信创的元年，八大行业是行业信创推进的主力，其中金融、电信等行业先行。随着信创的推进，预计行业信创无论是规模还是范围都会进一步扩大，教育、医疗领域的信创也会陆续进行。

图表8： 2023 年起信创有望进入上量阶段



资料来源：MBA 智库百科、艾媒咨询、方正证券研究所

网络安全作为信创的关键环节，将跟随信创推进节奏，相关安全产品的采购有望得到显著提升。虽然网络安全涉及细分领域众多，但结合上一轮信创推动中对网安整体的影响，我们认为与信创强相关的网络

安全产品的主要包含两大类，一是部署在 PC 或服务器上的防病毒、EDR、终端准入、资产管理、虚拟补丁等终端安全产品，其中 PC 端与服务器端的安全产品存在一定差异；二是搭载国产芯片的信创防火墙、IDPS 等网关类安全硬件产品，其中防火墙占据主要部分。此外在新一轮信创中特别是行业用户也将催生出对一些安全产品的新需求，包括了加密类产品、web 应用安全产品等。

图表9： 信创全产业链图谱



资料来源：亿欧智库、方正证券研究所整理

信创国产化适配工作有望推动行业集中度的提升。网络安全行业的国产化适配主要涉及到防火墙等安全硬件及终端防病毒等安全软件两大类产品，其中防火墙等安全硬件产品需要针对飞腾、海光、兆芯、申威等主流硬件平台进行适配，终端防病毒等安全软件产品也需要针对麒麟、统信等主流国产操作系统进行软件兼容适配认证，无论是硬件平台还是软件架构的适配，安全厂商均需要在兼容性、可靠性、安全性和功能性等方面符合一系列要求，软硬件环境更加复杂。由于头部厂商在国产化适配方面具备明显的优势，因此在信创安全的马太效应要强于通用安全市场。当前国内网络安全行业整体集中度偏低，中小厂商众多，信创的推进将推动行业集中度的提升，这也在上一轮信创采购中得到了一定程度的验证。

图表10：信创产业基础软硬件及部分应用适配图谱

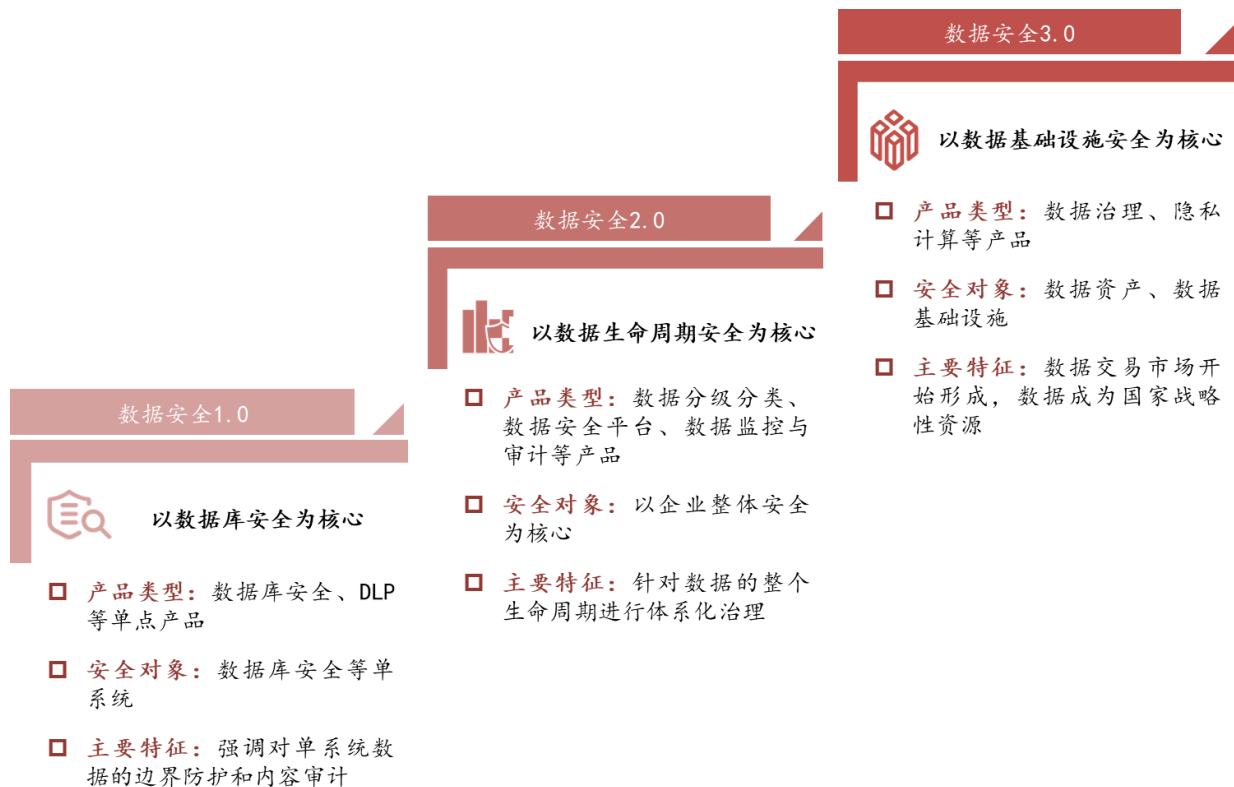


资料来源：用友网络官网、方正证券研究所

2.2 数据安全：近三年安全行业景气度最高的赛道

过去的数据安全仅停留在对单个系统乃至单个机构的安全防护，而当前数据安全的产业逻辑已经发生重大变化。目前数据资产正在脱离单独的个人或企业层面，开始逐渐演变成国家的战略资源和核心资产，特别是对于银行、电信、能源等关键基础设施机构以及阿里、滴滴、腾讯等大型互联网公司而言，数据的泄露不仅对企业造成严重损失，同时也将威胁到公共安全乃至国家安全，从去年的滴滴事件到今年的多起重大数据泄露事件均凸显出加大数据安全建设的重要性。同时，数据要素市场和数据经济产业的快速发展将带动数据安全需求的爆发。数据安全作为数据经济产业的基石，随着数字经济以及数据政府的落地，数据流通环节和数据量将会显著增加，将大幅带动数据安全的相关需求。

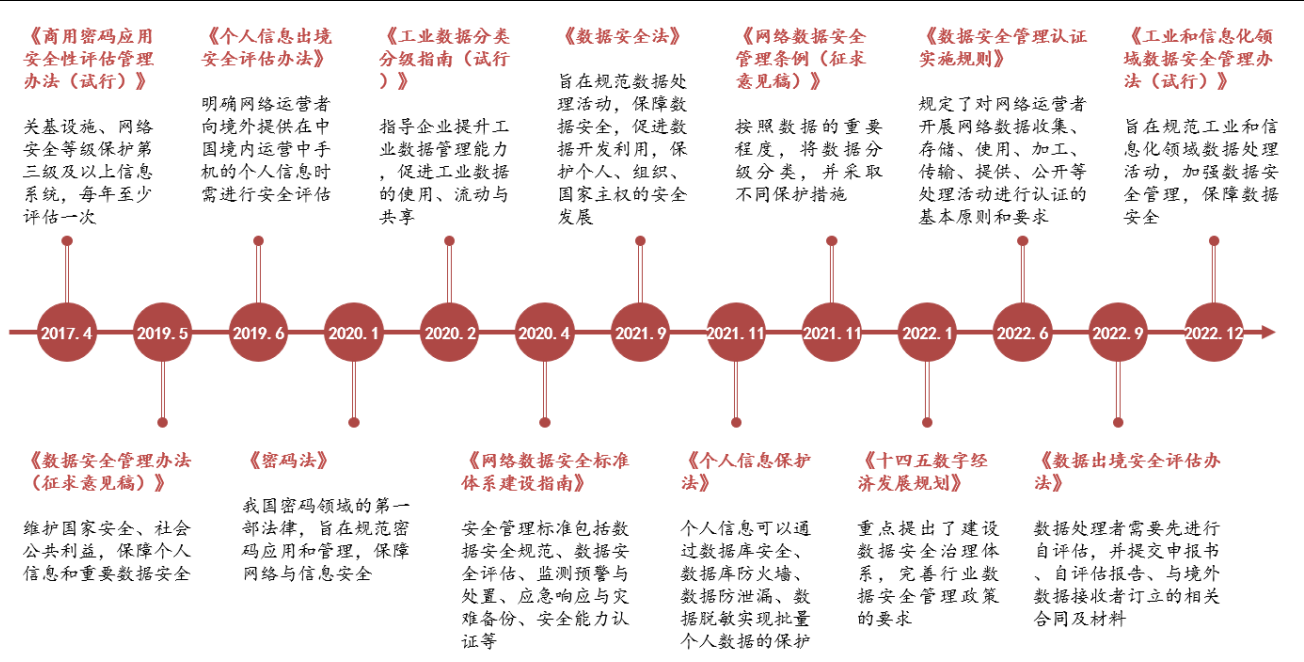
图表11：数据安全演进历史



资料来源：方正证券研究所整理

数据安全合规建设已经全面启动，数据安全是网络安全行业近年及未来增速最快的赛道。2021年9月我国第一部数据安全的上位法《数据安全法》的正式出台，为数据安全监管指明方向，随后多个数据安全细则、标准、条例，包括《网络数据安全条例》、《数据出境安全评估办法》、《数据安全法认证实施规则》、《工业和信息化领域数据安全管理办法（试行）》相继落地，特别是《商用密码应用安全性评估》的出台，要求关键信息基础设施、等保三级及以上信息系统，每年至少进行一次密评，显著推动了密码行业的景气度。未来几年，无论是国家层还是企业层面，数据安全合规建设仍将是网络安全投入的重点，从国家层面来看，未来各监管部门将加大对数据安全的监管，其中包括国家数据分类分级保护制度的建立，各地区、各部门也将按照国家数据分类分级要求，对本地区、本部门以及相关行业、领域的数据进行分类分级管理，从企业层面来看，数据安全将从过去少部分机构的风险控制需求转向全面的合规建设需求，政企用户在数据分级、数据治理，以及数据全流程管理、数据防护体系的建设成为了网络安全预算和支出的重点。

图表12：数据安全相关政策及立法进程

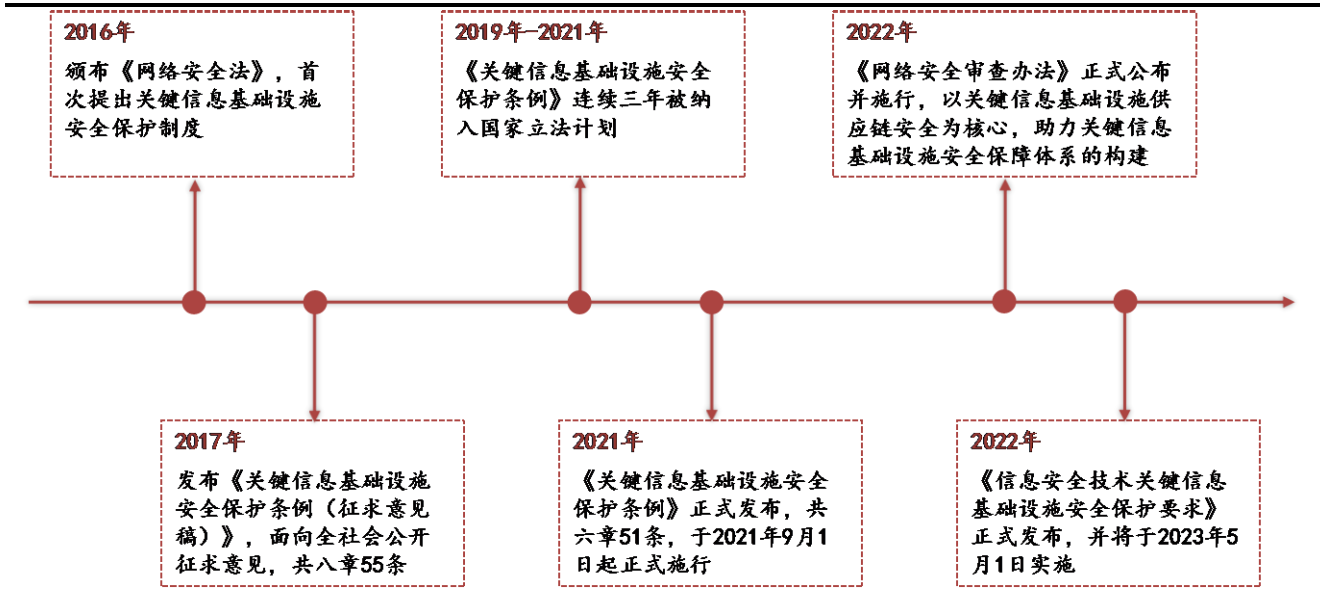


资料来源：网信办、公安部、国密局、方正证券研究所

2.3 关基保护：明年起关保合规工作将全面启动

关键基础设施保护首个重要标准《关基安全保护要求》近日出台，明年起关基保护工作将正式拉开帷幕。在2021年9月，《关键信息基础设施安全保护条例》出台，初步明确了关键信息基础设施的定义、认定程序和总体要求，对关键信息基础设施的运营者提出了一系列安全相关的责任和义务，以及违反本条例的法律责任等内容。但由于此前缺少《保护要求》等重要标准，对于的基础设施识别、边界的认定、重要数据识别等方面的认证仍不清晰，因此关基保护工作也尚未得到真正的落实。2022年10月12日，市场监管总局布公告，国家标准——GB/T 39204 2022《信息安全技术关键信息基础设施安全保护要求》正式发布，并将于2023年5月1日实施。《保护要求》作为《关键信息基础设施安全保护条例》的首个重要标准，其发布也预示着明年关基保护工作将正式拉开帷幕。

图表13：关键信息基础设施保护相关政策及立法进程



资料来源：市场监督管理总局、网信办、国务院、全国人大、方正证券研究所

《关基安全保护要求》覆盖了关键信息基础设施安全保护的全生命周期，明确了运营者需要如何针对关键信息基础设施进行全生命周期的安全保护工作。《关基安全保护要求》提出了以关键业务为核心的整体防控、以风险管理为导向的动态防护、以信息共享为基础的协同联防的关键信息基础设施安全保护3项基本原则，同时还从分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等6个方面提出了111条安全要求。《保护要求》覆盖了关键信息基础设施安全保护的全生命周期。从关基的识别认定、强化安全防护,到对运营可能存在的网络安全风险进行检测评估、并实行常态化监测预警,同时以监测发现的攻击行为为基础,进行攻防演练,提升主动防御能力和事件闭环处置能力,确保了关键信息基础设施关键业务稳定和持续运行。

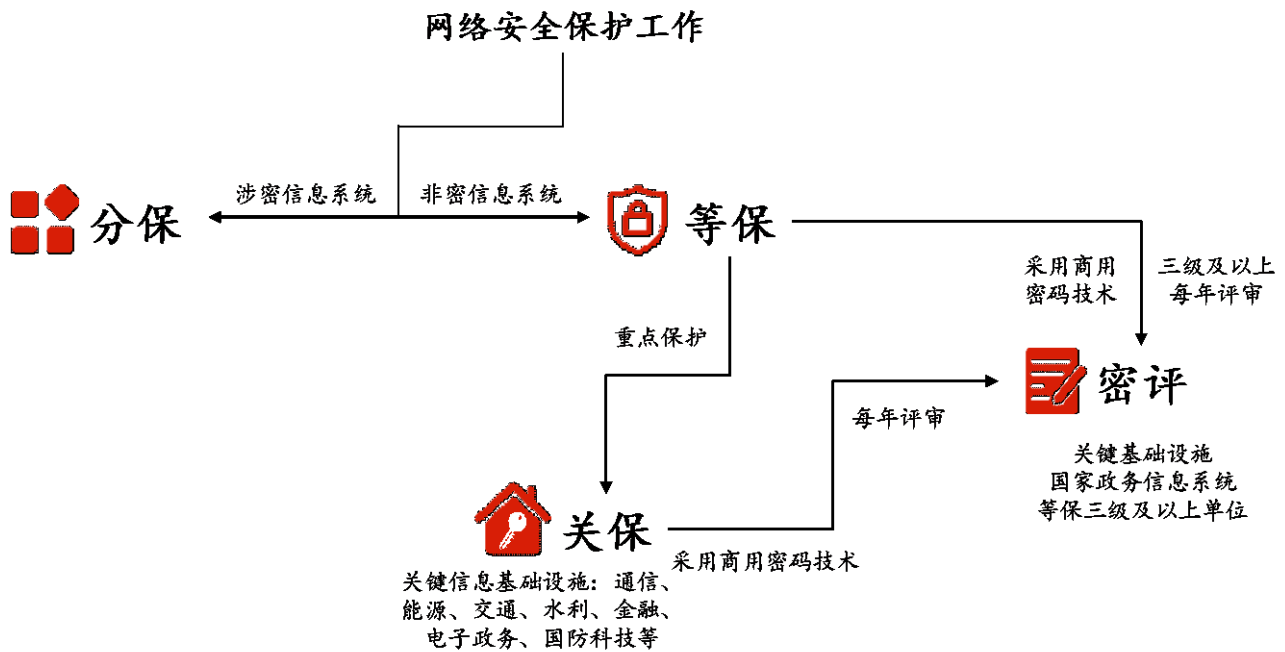
图表14：信创产业基础软硬件及部分应用适配图谱



资料来源：长扬科技、方正证券研究所

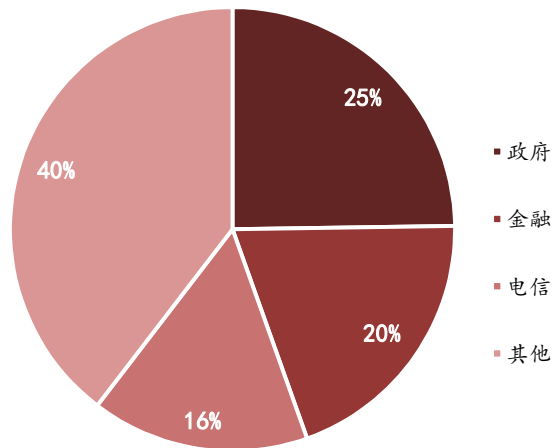
关键基础设施保护工作的开展，标志着我国三保一评（等保、分保、关保、密评）的网络安全保护工作正式迈进体系化建设新阶段。关键基础设施保护在等级保护制度的基础上，对关键基础设施施行重点保护，重点保护主要体现在两方面，第一明确了重点行业和领域，即八大行业，包括公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业，同时，由于各类大型互联网平台不但拥有海量用户，且支撑了经济社会很多基础功能的运转，不排除会有一批大型互联网平台被列为关键信息基础设施。从下游行业占比来看，关键基础设施占据了我国网络安全下游行业的半壁江山。第二明确了重点保护对象，在此前基础之上增加了关键业务、关键业务链、数据安全、供应链安全等对象，在满足等级保护的基础上需要增加额外的安全预算和投入。

图表15：3保1评的联系与区别



资料来源：ITIL之家、方正证券研究所

图表16：中国网络安全市场行业占比预测（2026年）

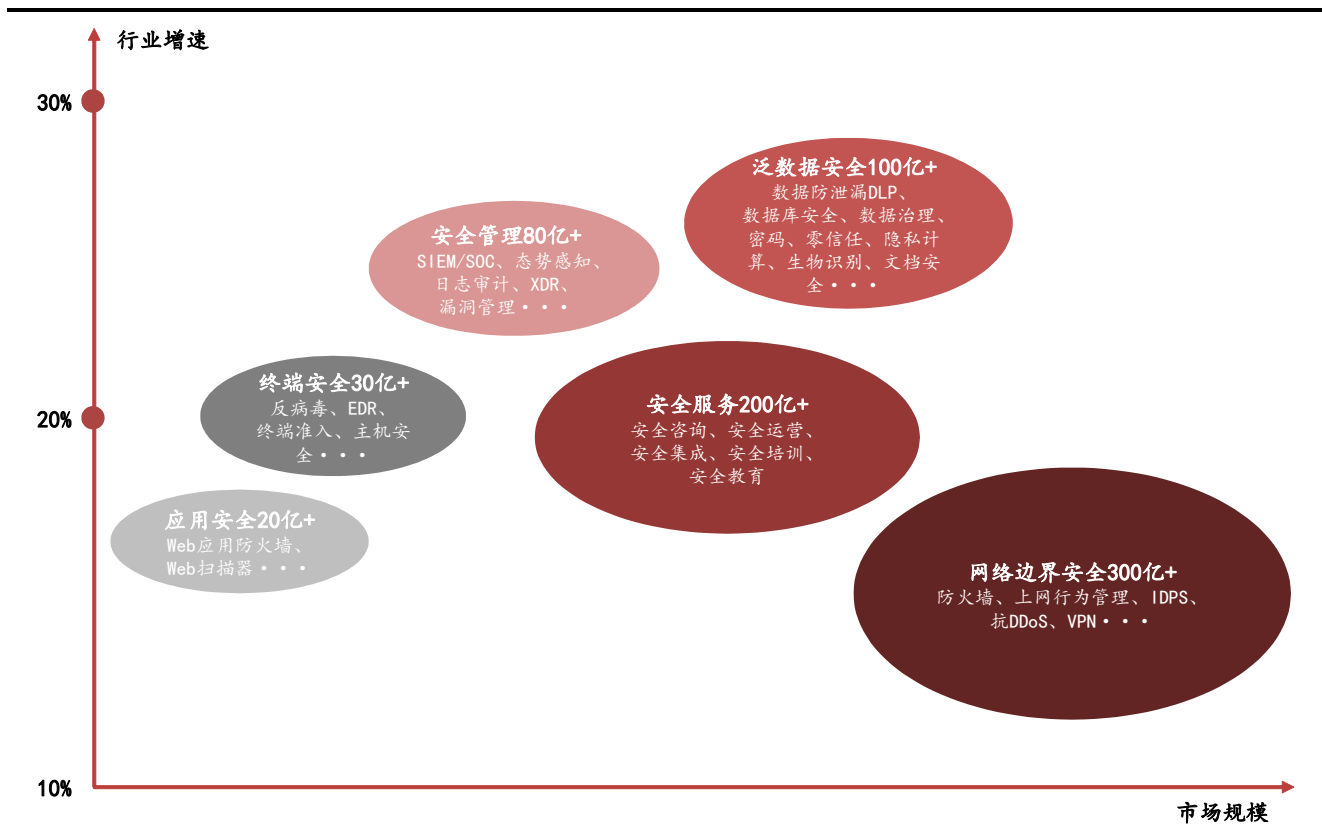


资料来源：IDC、方正证券研究所

3 明年看好的三大方向：数据安全、安全攻防、信创安全

数据安全、安全攻防、信创安全是未来三年网络安全行业景气度最高的三大方向。1) 数据安全：伴随《数据安全法》的出台以及滴滴事件的催化，政企用户在数据分级、数据治理，以及数据全流程管理、数据保护体系的建设将成为安全支出的重点；2) 安全攻防：在上一轮网络安全景气高峰期（2017-2020 年），安全管理及安全攻防是国内网络安全行业景气度最高的赛道，以态势感知、高级威胁检测等平台类产品成为爆款产品，未来安全管理及安全攻防依然是用户下一阶段安全投入的重点；3) 信创安全：与信创强相关的终端安全产品、网络安全产品以及信创中催生出的增量需求产品，包括了加密类、web 应用安全产品，都将显著受益于新一轮信创需求的带动。

图表17：网络安全行业赛道规模及增速



资料来源：方正证券研究所绘制（部分数据结合 IDC、赛迪顾问、Frost&Sullivan 等第三方机构数据估算）

图表18：网络安全行业7大赛道

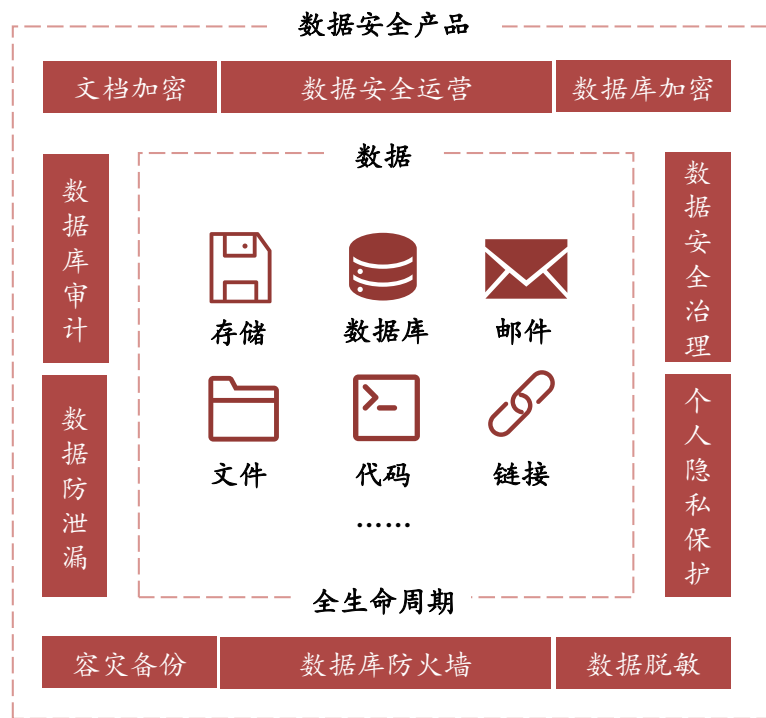
赛道	主要功能	核心技术	主要产品	头部厂商
边界安全	防入侵	网络层协议解析技术 网络流量分析技术	防火墙 入侵检测与防御IDPS 虚拟专用网VPN 上网行为管理 抗DDoS	华为、新华三、天融信、启明星辰、深信服、奇安信、绿盟科技、山石网科、迪普科技、
终端安全	反病毒	文件解析技术 漏洞检测技术 终端管控技术	杀毒软件 终端设备管控 端点保护平台EPP 终端检测与响应EDR	奇安信、亚信安全、深信服、McAfee、Broadcom、北信源
身份安全	身份与访问管理	加密技术 身份认证技术 权限管理技术 AD/LADP协议技术	统一管理平台/4A平台 访问控制/单点登录 特权账号管理/堡垒机 密码/令牌/生物识别 零信任	亚信安全、数字认证、吉大正元、上海格尔、IBM、安恒信息、启明星辰、奇安信、齐治科技、飞天诚信
安全管理	安全态势分析	可视化技术 关联分析技术 数据挖掘技术 用户行为分析技术 编排与自动化响应技术	SIEM/SOC 态势感知 威胁情报 XDR 漏洞管理	奇安信、启明星辰、安恒信息、深信服、绿盟科技、天融信
数据安全	防止数据泄露	文件透明加解密技术 文件沙箱技术 数据访问隔离技术	数据库安全 数据防泄漏DLP 文档加密 数据治理	启明星辰、安恒信息、绿盟科技、安华金和、Imperva、优炫软件、明朝万达、北信源、联软科技
应用安全	防WEB攻击	WEB漏洞扫描与防御技术 流量清洗技术 反向代理技术	Web应用防火墙 Web扫描器 网页防篡改	绿盟科技、安恒信息、阿里云、启明星辰、远江盛邦、新华三、长亭科技、知道创宇
安全服务	完善安全体系	安全框架和体系构建 安全人员梯队及培养机制 安全编排与自动化响应能力 跨区域业务布局及支撑能力	安全咨询 托管安全服务 安全实施与集成 安全培训与教育	启明星辰、奇安信、安恒信息、绿盟科技、天融信、安信天行、德勤、普华永道

资料来源：方正证券研究所整理

3.1 数据安全：看好综合型安全厂商与密码类厂商

数据安全市场包含两大赛道：1) 传统数据安全市场：产品、服务、解决方案、数据安全涉及的细分领域较多，主要赛道包括数据安全治理、数据防泄漏 DLP、数据库审计、个人隐私保护、文档加密，数据分级、数据治理和容灾备份等，其中数据防泄漏 DLP 和数据库安全是国内数据安全领域最大的两个子市场。同时，由于数据安全泛在性的特点，许多的网络安全项目均与数据安全相关，总体规模在百亿以上规模，每年保持 30%+增长；**2) 隐私计算等数据安全新场景：**隐私计算作为数据安全领域的新场景，目前应用场景主要集中在金融、医疗和政务三大领域，未来随着互联网监管、政务大数据等领域的不断拓宽，有望撬动千亿级的市场规模。

图表19：什么是数据安全



资料来源：方正证券研究所整理

目前下游用户对数据安全进行体系化建设的需求在不断提升，数据安全项目也逐渐成为一个系统工程，因此综合型安全厂商的竞争优势也正在不断提升。过去下游用户对过去的数据安全仅停留在对单个系统乃至单个机构的安全防护，针对加密、数据库安全、DLP等产品也更多的是单点采购，而当前随着数据安全合规要求的不断提升，用户对整体的解决方案的需求在不断提升，比如用户需要通过业务系统审计日志、组织架构信息、VPN日志等，检测业务系统的异常行为，如账号盗用、暴力爆破、账号共享、特权账号等；通过堡垒机日志、WAF日志、API网关流量信息，检测访问的内网资源、API数量、敏感数据数量等是否有异常；通过主机安全产品日志、VPN日志等，基于文件传输数据量和访问行为，检测主机或服务器的操作异常；通过数据库审计日志，检测对数据库访问是否异常，如越权访问、已授权数据的恶意更改、滥用或拖库等。因此安全厂商一方面需要将各类安全技术和产品有机组合起来，通过整体解决方案来实现对数据采集、传输、存储、处理、交换、销毁的全生命周期的管理；另一方面安全厂商需要具备较强的咨询能力，能够为客户建立贯穿业务、制度、流程的数据安全框架。这也导致了行业门槛的不断提高，综合型安全厂商相较于单点的产品供应商的竞争优势在不断增强。

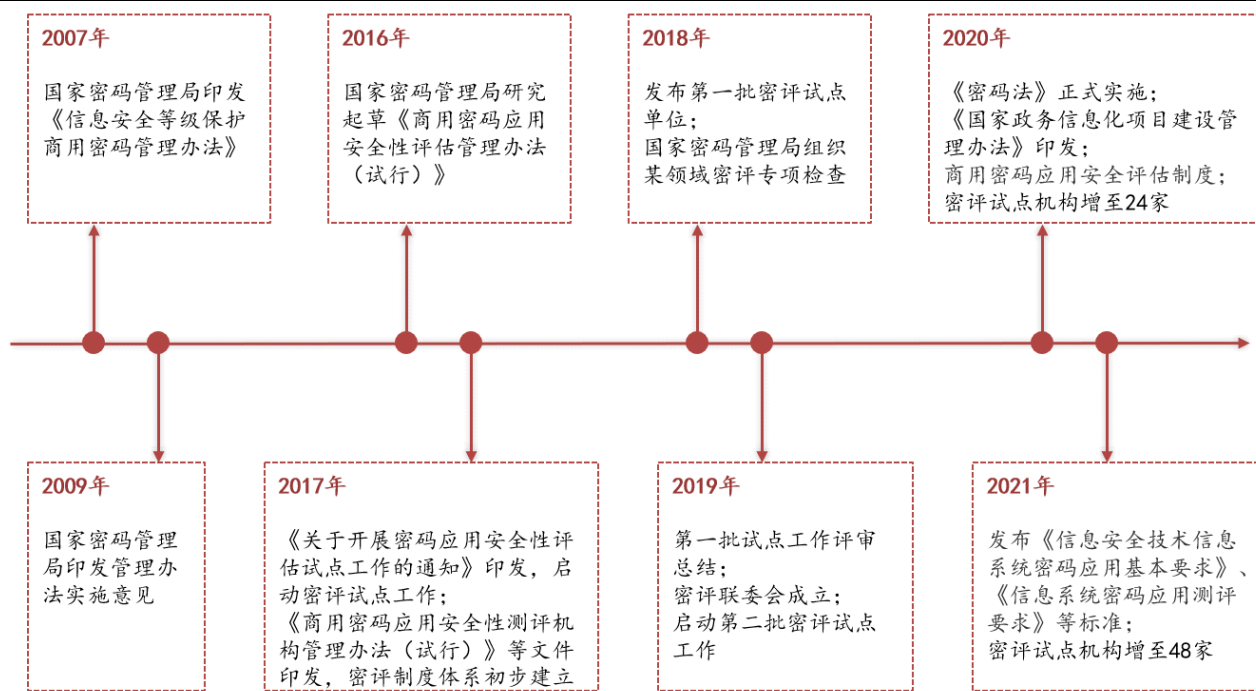
图表20：数据安全厂商梳理

数据安全治理	奇安信	卫士通	启明星辰	绿盟科技	安恒信息	安华金和
	深信服	迪普科技	数字认证	神州信息	北信源	任子行
	格尔软件	明朝万达	数安行	天空卫士	美创科技	
数据库安全	安恒信息	启明星辰	深信服	数字认证	北信源	腾讯
	格尔软件	安华金和	联软科技	威努特	美创科技	敏捷科技
	高维数据	云天安全	遥望信息	安信天行	海峡信息	世平信息
	渔翁信息	远江盛邦	华软金盾	东进技术	聚铭网络	
数据防泄漏	绿盟科技（亿赛通）	天融信	深信服	奇安信	启明星辰	
	北信源	天空卫士	明朝万达	联软科技	安华金和	
数据加密	卫士通	三未信安	吉大正元	新大陆	天融信	信安世纪
	数字认证	北信源	证通电子	格尔软件	明朝万达	江南天安
	渔翁信息	兴唐通信	新华三	安信天行	北京CA	
个人隐私保护	奇安信	天空卫士	天威诚信	智游网安	云天安全	炼石网络
	世平信息	梆梆安全	数安行	众图识人	美创科技	
容灾备份	深信服	北信源	格尔软件	安信天行	敏捷科技	

资料来源：《数据安全产品指南》、方正证券研究所整理

在数据安全所有细分行业中，密码行业近年保持着最高的景气度，包括卫士通、吉大正元、格尔软件、数字认证、飞天诚信等都是这一赛道上的老牌厂商，市场竞争格局相对稳定。密码及认证类产品主要包括设备认证、令牌和密钥、PKI、加密服务器等产品，传统的密码类产品主要应用于政府、银行等重点行业，同时一些新兴身份认证技术如生物识别、行为分析等技术，大多应用于互联网等行业。密码行业的高景气度一方面是因为密评工作的推进，在2020年《密码法》出台之后，商用密码应用安全评估工作也开始快速推进，并在今年进入高峰，根据密评要求，关基单位及等保三级以上系统，无论新建还是已建系统均需每年进行一次评估，这也极大拉动了密码行业的景气度；另一方面，密码相关产品过去主要应用于政府、银行等行业，随着明年起行业信创的推进，密码在医疗、教育、交通、能源等行业的应用场景也将不断拓宽。

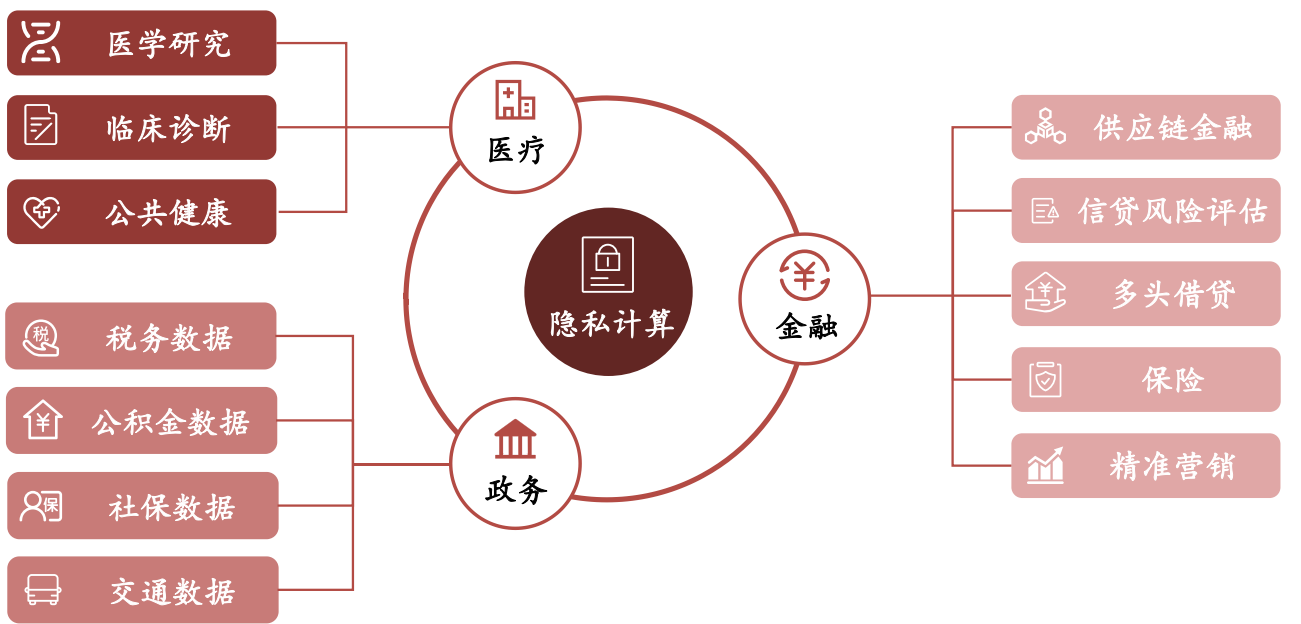
图表21：密评发展进程不断推进



资料来源：信通院、方正证券研究所

隐私计算作为数据安全领域的新场景，目前应用场景主要集中在金融、医疗和政务三大领域，未来随着互联网监管、政务大数据等领域的不但拓宽，有望撬动千亿级的市场规模。在金融领域，涉及到信贷风险评估、供应链金融、保险、精准营销、多头借贷等领域，用户行为数据和场景数据往往掌握在互联网公司及其他数据源公司手中，基于隐私计算，金融机构可以和这些数据源公司联合建模，实现跨行业的数据共享；在政务领域，涉及到社保数据、公积金数据、税务数据、交通数据等等，但数据隶属于不同部门，而隐私计算能有效保护各部门数据，利用多部门数据有效应对社会治安及突发事件，提升政府的治理水平。在医疗领域，虽然医院借助互联网平台和电子病历积累了大量的医疗数据，但是单个医疗机构在数据量方面仍有明显局限性，而跨院的数据共享依然非常困难，通过隐私计算，可以解决单个医疗机构在数据量方面的局限性，实现临床诊断、医学研究、公共健康等多个领域的应用。

图表22：隐私计算应用领域

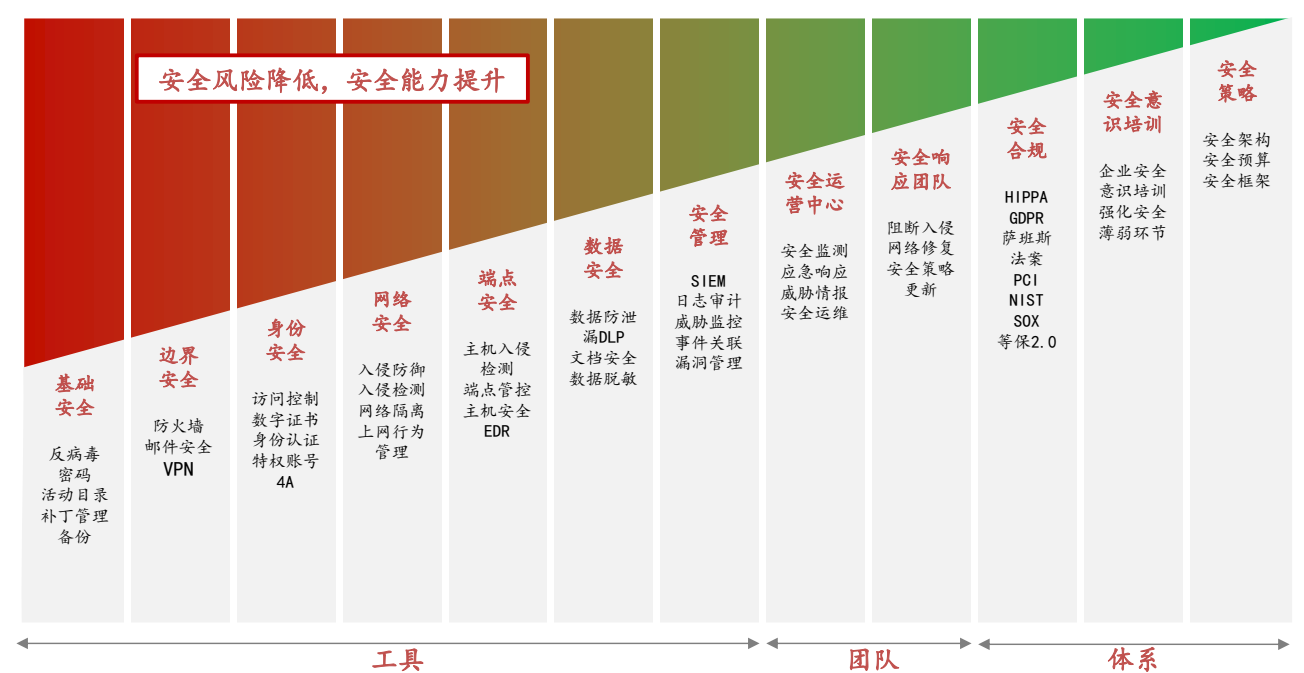


资料来源：信通院、方正证券研究所

3.2 安全攻防：XDR 引领下一轮网络安全实战化建设

在上一轮网络安全景气高峰时期（2017-2020 年），安全管理及安全攻防是国内网络安全行业景气度最高的赛道，态势感知成为爆款产品。展望未来，随着外部安全威胁的不断增加，安全管理及安全攻防依然是用户下一阶段安全投入的重点。安全管理及安全攻防类产品涵盖了 SOC、态势感知、高级威胁检测、XDR 等平台类产品，NTA、EDR、蜜罐等工具类产品，以及网络安全实训演练测试平台、红蓝对抗服务等实战化安全服务。过去用户的安全预算较多投入到了防火墙、反病毒等自动化程度较高的安全工具，近年 AI、大数据、UEBA(用户及实体行为分析)及 SOAR（安全编排及自动化响应）等相关技术的成熟，降低了安全管理平台的使用门槛，同时随着用户安全建设水平的不断提升，其安全建设的重心也开始以实战化能力为结果导向，因而安全管理及安全攻防类产品未来将保持较高的景气度。

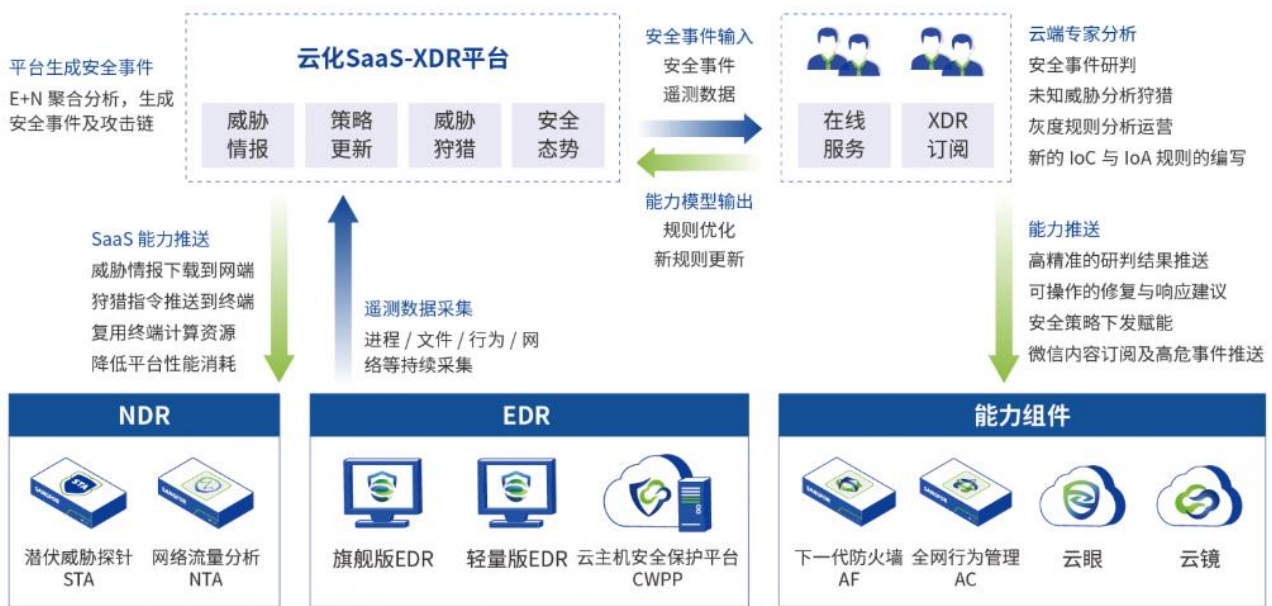
图表23：企业网络安全建设发展阶段



资料来源：信通院、方正证券研究所

XDR 平台凭借轻量化落地的优势，正在成为安全管理及安全攻防领域下一阶段的爆款产品。2015 年公安部开始率先推进态势感知和通报预警平台的建设，随后态势感知逐渐向电子政务、网信、金融等行业扩散，同时近几年攻防演练活动中，以攻防为主要场景的高级威胁检测产品已经成为众多企业用户的核心需求。过去来看 SIEM/SOC、态感类产品涉及到较多的定制化，一般的采购方主要为安全预算充足的大型企业和机构。目前以 NDR+EDR+SOAR+安全分析等多种能力形式的 XDR 解决方案开始在中型机构中快速落地，XDR 是一个统一的安全威胁检测与事件响应平台，无缝集成大量安全能力到一个安全运营系统，将来自云、网、端等多源异构数据统一整合形成数据湖，通过对接第三方组件，实现跨人员、跨设备间的交叉联动与多点处置，实现全场景的威胁治理覆盖。XDR 作为 SIEM/SOC 的替代，方案简单、轻量、易用，且标准化程度更高，是国内安全市场的重要趋势。

图表24：深信服 XDR 平台



资料来源：深信服官网、方正证券研究所

奇安信、启明星辰、安恒信息、深信服目前占据了国内安全管理安全攻防市场的头部位置，从主要厂商的竞争力来看：

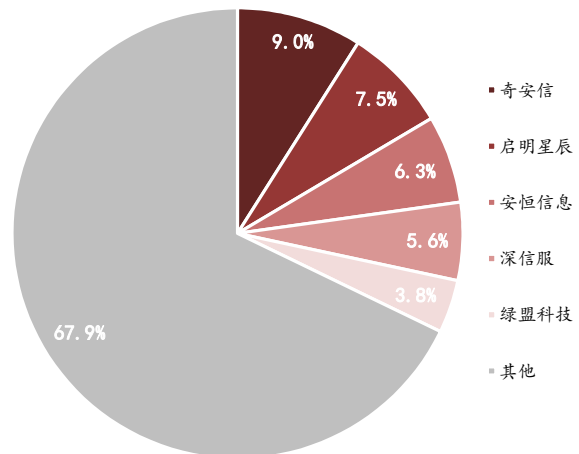
1) **奇安信**：作为国内最早布局态势感知市场的安全厂商之一，目前在态势感知市场的份额排名第一，同时凭借在安全大数据以及高级威胁检测方面的能力，公司 NGSOC 和威胁感知系统天眼也是近年来的爆款产品，综合来看公司在安全管理类产品在国内市场占据龙头地位；

2) **启明星辰**：作为国内最早开发安全管理平台产品的厂商，在 2005 年前后就推出了国内第一代安全管理平台“泰合”，同时在 2017 年启明作为首家中国厂商进入了 Gartner SIEM 魔力象限，在安管平台领域有非常深厚的技术沉淀；

3) **安恒信息**：作为新兴安全厂商，在 2014 年前后开始将态势感知及安全管理平台作为重要发展方向。安恒从公安态势感知平台切入，在打造标杆效应后，目前在重要行业成功落地态势感知案例 200 余个，在监管侧态势感知市场排名第一。同时，安恒的大数据安全平台在多源异构数据采集、海量数据存储、安全事件溯源分析等核心技术上也具备一定的领先优势。

4) **深信服**：作为安全管理赛道的新进入者，凭借成熟的渠道体系，目前市场份额也正在迅速提升，并进入到了前五的位置，公司以中型客户群体中具备较强的竞争力，且今年 5 月正式发布了新一代基于 SaaS 的安全威胁检测和事件响应平台。

图表25：2021年中国安全分析和威胁情报市场份额

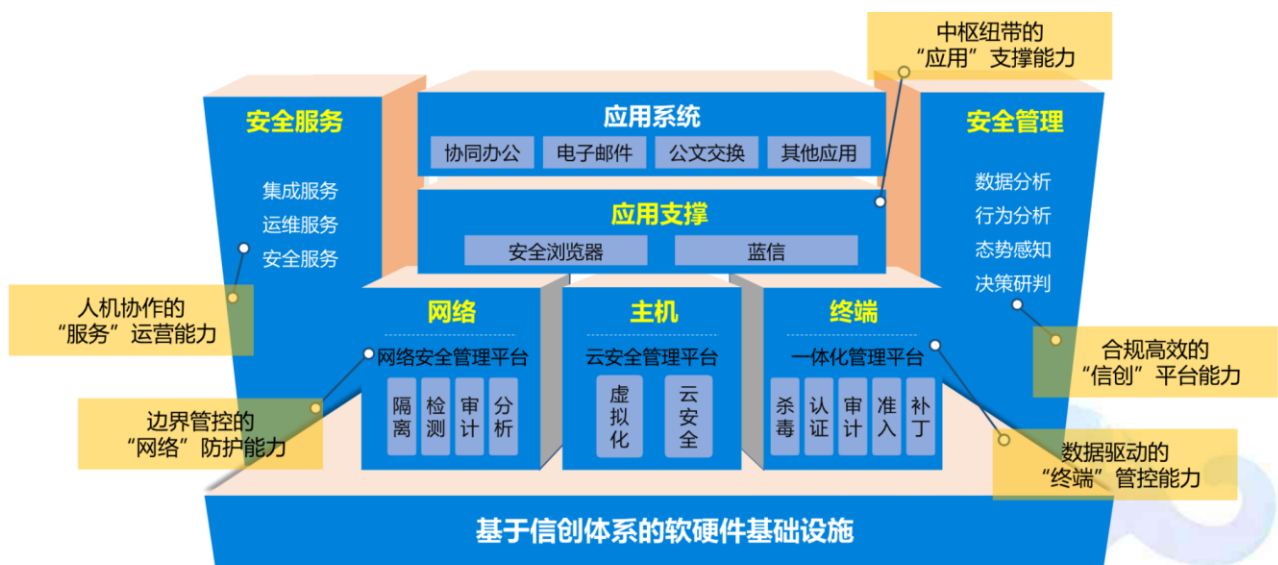


资料来源：IDC、方正证券研究所

3.3 信创安全：信创推进过程中将催生出新安全需求

目前头部安全厂商基本上已经基本搭建了比较完善的信创安全产品线，但结合上一轮信创在推进过程中对网络安全行业整体的影响，我们认为与信创强相关的网络安全产品的主要包含两大类：一是部署在PC或服务器上的防病毒、EDR、终端准入、资产管理、虚拟补丁等终端安全产品，其中PC端与服务器端的安全产品存在一定差异；二是搭载国产芯片的信创防火墙、IDPS等网关类安全硬件产品，其中防火墙占据主要部分。此外在新一轮信创中特别是行业用户也将催生出对一些安全产品的新需求，包括了加密类产品、web应用安全产品等。

图表26：奇安信信创安全体系

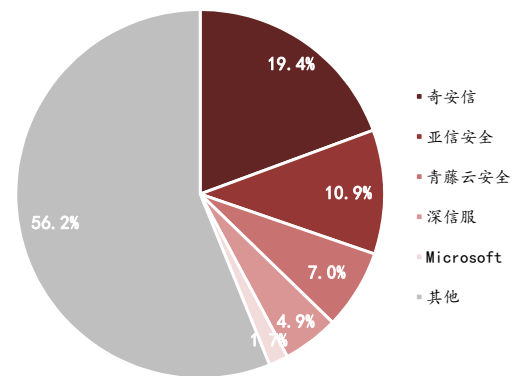


资料来源：奇安信、方正证券研究所

国内企业级终端安全市场的竞争格局已经比较明确，奇安信、亚信安

全、深信服位于前列，其中奇安信在上一轮的信创终端安全的布局上要领先于竞争对手。终端安全涉及 PC 端与服务端安全产品，PC 端产品主要包括防病毒、合规准入、认证、管控等产品，而服务器端安全主要包括 EDR、虚拟补丁、应用防护等产品，根据 IDC 的数据，2021 年，终端安全软件在所有安全软件市场中表现最为亮眼，在重点行业大量新增需求、云工作负载安全快速发展等因素带动下增速加快，实现全年 40% 以上的增长。从主要厂商来看，网络安全头部厂商奇安信在信创 PC 端终端安全的市场覆盖率已接近 70%，遥遥领先于主要竞争对手，未来随着信创的进一步下沉，奇安信市场份额有望进一步扩大。此外，亚信、青藤云以及深信服也是终端安全市场头部厂商，以服务器端安全产品为主，其中亚信在 2015 年收购了国际知名防病毒厂商趋势科技的中国业务后，目前保持终端安全市场排名第二的位置，深信服早期更侧重于服务器安全，在 2018 年以 EDR 切入终端安全市场后，份额及排名在近两年在迅速提升，目前也基本形成了完整的终端安全解决方案。

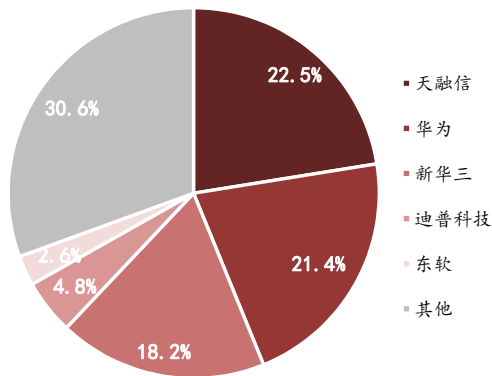
图表 27：2021 年中国终端安全软件市场份额



资料来源：IDC、方正证券研究所

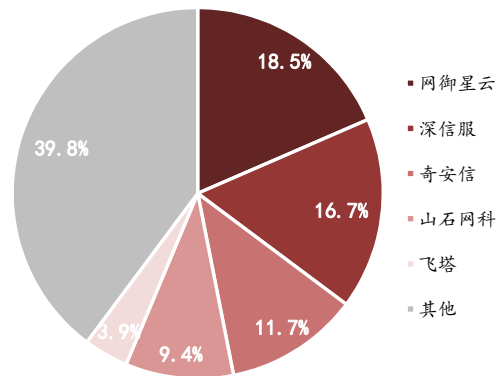
信创安全硬件产品防火墙、IDPS 等网关类产品，其中防火墙占据主要部分，防火墙是国内网络安全行业最大的赛道，也是唯一一个超过百亿体量的赛道，是国内网络安全大厂的“兵家必争之地”。目前在国内防火墙市场占据主导的是以天融信、启明星辰、深信服、奇安信为代表的安全厂商和以华为、新华三为代表的数通厂商，总体来看，防火墙市场近年来竞争格局较为稳定。以华为和新华三为代表的数通厂商的防火墙具备端口密度大、性能高、价格便宜等特性，主要应用在运营商及数据中心网络出入口等场景，突出防火墙的包过滤、NAT、访问控制等基础功能。同时，随着过去几年华为和新华三将防火墙整合到自身的云计算整体解决方案中，其在防火墙市场的份额有所提升。相较于数通厂商，安全厂商的防火墙产品更加强调防火墙的安全功能，功能更加全面，能够快速跟上安全形势的变化，在企业办公网络、中小企业及分支机构等场景则更具优势。

图表28：2021年中国UTM防火墙市场份额



资料来源：IDC、方正证券研究所

图表29：2021年中国统一威胁管理市场份额



资料来源：IDC、方正证券研究所

4 投资逻辑

信创、关基、数据安全是23年网络安全最重要的三重驱动力，看好网络安全行业明年景气度及竞争格局的双重改善。等保2.0与护网驱动了网络安全上一轮的景气高峰，明年在信创+关基+数安等多条政策主线驱动下，行业景气有望持续提升：1) 信创明年起进入上量阶段，虽然网安本身的国产化率较高，但参考上一轮信创，在信创推进过程中对防火墙、终端安全等产品采购仍有明显拉动；2) 政策面持续向好，数据安全及关基保护相关政策有望进一步落地，叠加进入十四五第三年，此前收紧预算将逐渐释放；3) 行业竞争格局改善，多家头部厂商控制人员增长，报表质量同时也将普遍改善。推荐：深信服、启明星辰、奇安信、安恒信息，相关标的：天融信、绿盟科技、卫士通、信安世纪、山石网科、迪普科技、中孚信息等。

图表30：主要网络安全厂商估值表

代码	公司简称	市值/亿元	股价/元	PE			EPS		
				22E	23E	24E	22E	23E	24E
002439.SZ	启明星辰	244.15	25.63	25.00	19.62	15.56	1.03	1.31	1.65
688023.SH	安恒信息	152.92	193.99	298.26	95.36	55.43	0.65	2.03	3.50
300369.SZ	绿盟科技	83.13	10.41	21.55	16.66	13.32	0.48	0.62	0.78
300454.SZ	深信服	458.39	110.29	149.81	76.03	46.39	0.74	1.45	2.38
002212.SZ	天融信	119.81	10.11	24.93	18.73	14.43	0.41	0.54	0.70
688030.SH	山石网科	37.20	20.64	33.81	22.86	16.32	0.61	0.90	1.26
300188.SZ	美亚柏科	108.03	13.44	33.78	25.96	20.24	0.40	0.52	0.66
603232.SH	格尔软件	36.75	15.86	37.20	26.01	17.66	0.43	0.61	0.90
002268.SZ	卫士通	281.34	33.26	70.17	47.15	34.41	0.47	0.71	0.97
688201.SH	信安世纪	74.19	53.83	38.31	29.00	21.31	1.41	1.86	2.53
300659.SZ	中孚信息	55.73	24.62	-21.86	23.72	11.68	-1.13	1.04	2.11
688168.SH	安博通	25.75	33.84	27.55	20.81	15.83	1.23	1.63	2.14
300768.SZ	迪普科技	85.44	13.27	31.25	23.13	17.86	0.42	0.57	0.74
688561.SH	奇安信-U	444.65	65.19	1563.31	132.58	66.12	0.04	0.49	0.99
601360.SH	三六零	490.17	6.86	59.81	40.45	30.19	0.11	0.17	0.23
688225.SH	亚信安全	71.24	17.81	43.59	30.78	22.09	0.41	0.58	0.81

资料来源：来自 Wind 一致预期（采用 12.14 收盘价），方正证券研究所

5 风险提示

疫情反复导致经济下行的风险。面对疫情反复，经济增长动力不足，供需出现同步疲软态势，导致相关网络安全公司项目及回款周期延长，业务恢复速度放缓。

行业竞争持续加剧的风险。目前网络行业竞争逐渐加剧，一方面包括深信服、奇安信、新华三、华为等公司在安全领域持续发力，另一方面在云安全、工控安全等新场景领域，新兴安全公司也正在迅速成长，市场竞争不断加剧。

政策落地不达预期的风险。未来两年包括等保 2.0、数据安全法，以及关键基础设施保护等政策的落地是行业增长的主要驱动力，若政策落地时间延后，或落地效果不达预期，将对相关网络安全公司业务开展产生一定的负面影响。

分析师声明

作者具有中国证券业协会授予的证券投资咨询执业资格，保证报告所采用的数据和信息均来自公开合规渠道，分析逻辑基于作者的职业理解，本报告清晰准确地反映了作者的研究观点，力求独立、客观和公正，结论不受任何第三方的授意或影响。研究报告对所涉及的证券或发行人的评价是分析师本人通过财务分析预测、数量化方法、或行业比较分析所得出的结论，但使用以上信息和分析方法存在局限性。特此声明。

免责声明

本研究报告由方正证券制作及在中国（香港和澳门特别行政区、台湾省除外）发布。根据《证券期货投资者适当性管理办法》，本报告内容仅供我公司适当性评级为C3及以上等级的投资者使用，本公司不会因接收人收到本报告而视其为本公司的当然客户。若您并非前述等级的投资者，为保证服务质量、控制风险，请勿订阅本报告中的信息，本资料难以设置访问权限，若给您造成不便，敬请谅解。

在任何情况下，本报告的内容不构成对任何人的投资建议，也没有考虑到个别客户特殊的投资目标、财务状况或需求，方正证券不对任何人因使用本报告所载任何内容所引致的任何损失负任何责任，投资者需自行承担风险。

本报告版权仅为方正证券所有，本公司对本报告保留一切法律权利。未经本公司事先书面授权，任何机构或个人不得以任何形式复制、转发或公开传播本报告的全部或部分内容，不得将报告内容作为诉讼、仲裁、传媒所引用之证明或依据，不得用于营利或用于未经允许的其它用途。如需引用、刊发或转载本报告，需注明出处且不得进行任何有悖原意的引用、删节和修改。

公司投资评级的说明：

强烈推荐：分析师预测未来半年公司股价有20%以上的涨幅；
推荐：分析师预测未来半年公司股价有10%以上的涨幅；
中性：分析师预测未来半年公司股价在-10%和10%之间波动；
减持：分析师预测未来半年公司股价有10%以上的跌幅。

行业投资评级的说明：

推荐：分析师预测未来半年行业表现强于沪深300指数；
中性：分析师预测未来半年行业表现与沪深300指数持平；
减持：分析师预测未来半年行业表现弱于沪深300指数。

地址	网址： https://www.foundersc.com	E-mail: yjzx@foundersc.com
北京	西城区展览馆路48号新联写字楼6层	
上海	静安区延平路71号延平大厦2楼	
上海	浦东新区世纪大道1168号东方金融广场A栋1001室	
深圳	福田区竹子林紫竹七道光大银行大厦31层	
广州	天河区兴盛路12号楼 隽峰苑2期3层方正证券	
长沙	天心区湘江中路二段36号华远国际中心37层	