中国网络安全产业分析报告

（2019 年）

中国网络安全产业联盟

2019 年 12 月

版 权 声 明

前　言

近年来，随着信息技术和互联网的快速发展，网络安全问题对人类生活的影响已经扩展到政治、经济、社会民生等各个领域。

自 2014 年中央网络安全和信息化领导小组成立以来，尤其是在 2017 年 6 月《网络安全法》颁布实施以后，我国网络安全产业在政策、需求、资本的多重驱动下，迎来了更加快速稳定的发展，产业规模不断增长，资本的持续投入也助力了产业整合的加速发展。如今，网络安全的范畴已经升级为满足网络空间的可用性、可靠性和安全性。网络安全产业已然成为融合了技术研究开发、产品生产经营和提供相关安全服务的完整产业生态。

2019 年，中国网络安全产业联盟联合数说安全，以具备网络安全产品、服务和解决方案销售收入的我国网络安全企业作为目标研究对象，调研超过 200 家网络安全企业，经过分析研究，最终确定有效数据为 120 多家。本报告以 120 多家企业的有效数据为基础进行统计分析研究，最终得出 2018 年我国网络安全产业规模约为 393 亿元，同比增长率约为 17.8%，预计未来三年产业整体市场依然会保持 20%左右的高速增长，到 2021 年我国网络安全产业规模将达到 668 亿元。

本报告首先对我国网络安全产业概况进行了梳理，在前期开展市场调研的基础上，对我国网络安全产业的产业规模、增速、集中度等关键数据进行了分析，对企业商业模式、产业链结构及价值分配机制、市场分类方法及产业全景进行了梳理。

在企业分析部分，报告对我国网络安全主要企业上一年度的经营情况及各家企业竞争力与产业整体竞争格局进行了研究，总结了影响我国网络安全产业竞争格局的几个关键因素。

在热点细分领域部分，报告重点分析了近年来出现的热点市场和技术方向，包括数据安全、云安全、工控安全、安全管理、威胁管理、终端安全、身份与访问管理等。

在资本市场部分，报告对上市企业的资本市场表现进行了总结。同时，以我国网络安全产业发生的重大投融资事件为例，对创投市场的整体环境进行了分析，对产业内的资本动态进行了跟踪。

最后总结部分，报告对未来网络安全产业的前景和发展趋势做了展望，为今后网络安全产业规划发展提供参考。

目 录

一、我国网络安全产业概况

（一）网络安全产业的内涵及外延

从传统意义来说，网络安全产业的目标主要是针对保障网络的可用性、可靠性和安全性提供产品和服务。近年来，随着网络技术的演变与安全形势日趋复杂，在技术发展和用户需求的双重驱动下，新技术、新产品不断出现，安全产品和安全服务的融合日益紧密，网络安全产业的内涵由此得到了丰富；新应用场景不断被新的网络安全技术和产品所覆盖，网络安全产业的外延也得到了充分的扩展。

2016 年 12 月发布的《国家网络空间安全战略》指出，网络空间由互联网、通信网、计算机系统、自动化控制系统、数字设备及其承载的应用、服务和数据等组成。如今，网络安全产业已经演化为以满足网络空间的可用性、可靠性和安全性为目标，融合了技术研究开发、产品生产经营和提供相关安全服务的完整产业生态链。

本报告中，网络安全产业是指为保障网络空间安全提供技术、产品和服务的相关行业的总称。本次研究将具备网络安全产品、服务和解决方案销售收入的我国网络安全企业作为目标研究对象，分析其近三年来市场、技术、产品服务和资本的最新发展动态，并在此基础上总结归纳出网络安全产业的总体情况及未来的发展趋势。

（二）我国网络安全产业规模、增速与集中度分析

1. 我国网络安全产业规模与增速情况

根据中国网络安全产业联盟统计测算，2018 年我国网络安全产业规模约为 393 亿元，同比增长率约为 17.8%。增速相比上一年有所放缓，我国网络安全市场现已进入调整期，一方面传统安全业务增长触及天花板，另一方面新兴安全业务市场空间尚未有效释放，导致整体市场增速有所放缓。随着关键基础设施保护条例出台，等级保护 2.0 系列标准的正式颁布及实施，信息技术应用创新市场需求的逐步释放，将有望推动整体网络安全产业进入下个上升周期，预计未来三年产业整体市场依然会保持 20%左右的高速增长，到 2021 年我国网络安全产业规模将达到 668 亿元。

虽然我国网络安全产业发展态势整体良好，近几年增速也较快，但是我国网络安全产业总体规模依然较小，尚未达到千亿级，在我国在信息化项目中网络安全投入比例依然偏低，与欧美发达国家相比仍然有一定差距，我国网络安全与信息化发展还存在一定的不平衡。

图 1 2016-2021 年我国网络安全产业规模及增速

2. 我国网络安全产业集中度分析

行业集中度指数又称“行业集中率”是指该行业的相关市场内前 N 家最大的企业所占市场份额。2018 年我国网络安全市场 CR1 为 6.41%，CR4 为 21.71%，CR8 为 38.75%。根据美国经济学家贝恩对产业集中度的划分标准[1]，我国网络安全产业 CR8 小于 40%，属于竞争型市场。

[1] 根据美国经济学家贝恩对产业集中度的划分标准，将产业市场结构粗分为寡占型（CR8 ≥ 40%）和竞争型（CR8<40%）两类。

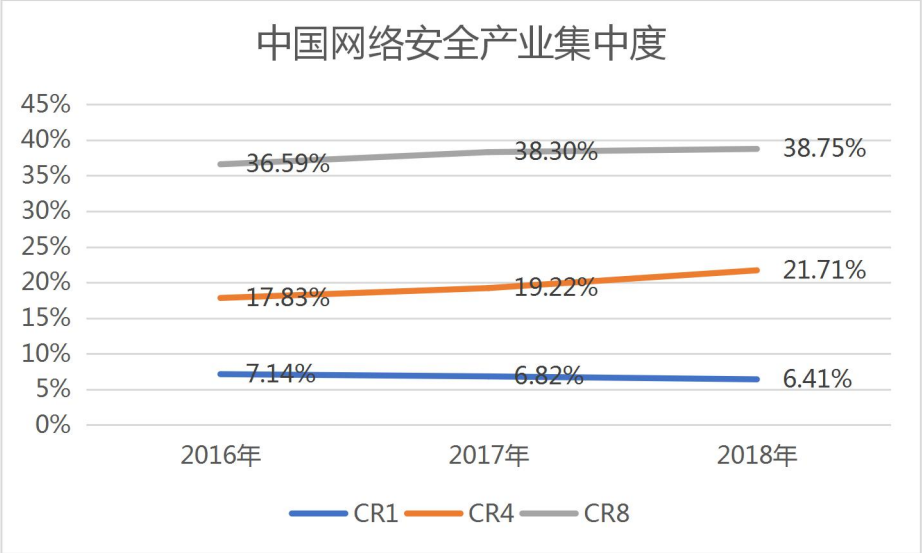


图 2 2016-2018 年我国网络安全产业集中度

通过对过去三年市场集中度情况进行了数据统计，我国网络安全产业的 CR4 和 CR8 都呈现增长态势，说明行业市场份额在向头部企业聚集，我国网络安全市场正在由竞争型市场向低集中寡占型市场转变。近三年启明星辰一直保持整体市场占有率第一的位置，但市场占有率连续三年下降；奇安信连续三年的高速增长，市场占有率从 2.43%提升至 6.09%。

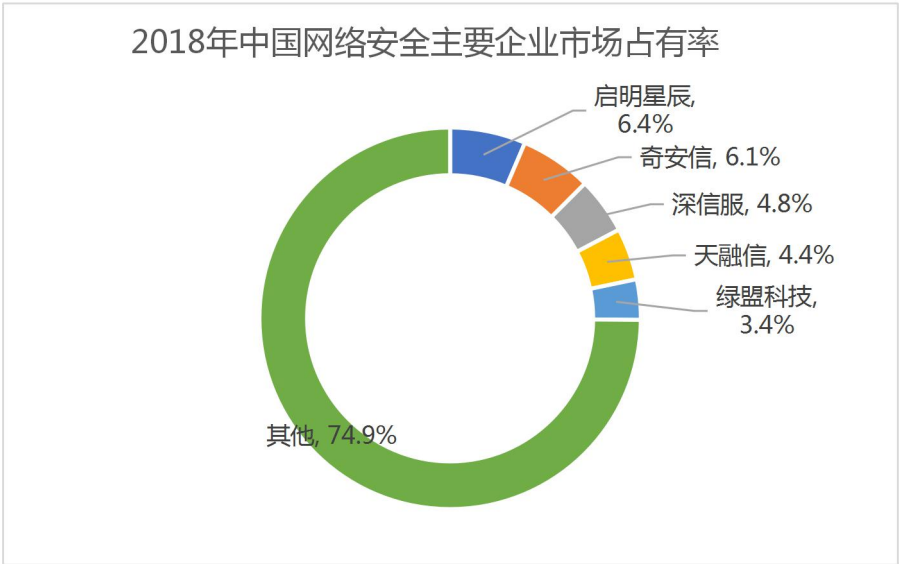


图 3 2018 年我国网络安全主要企业市场占有率

3. 网络安全市场区域分布情况

我国网络安全企业收入主要来自于华北、华东和华南三个区域，三个区域合计收入占比超过 70%，我国网络安全区域市场规模与我国区域经济发展水平呈现强相关。其中华北区域由于政府及央企的垂直效应，多年以来一直占据区域收入首位，也是网络安全企业的必争之地。虽然头部企业努力尝试海外业务拓展，但收效甚微，海外收入占行业总体市场份额仍不足 1%。我国网络安全市场仍然主要依靠内需驱动。

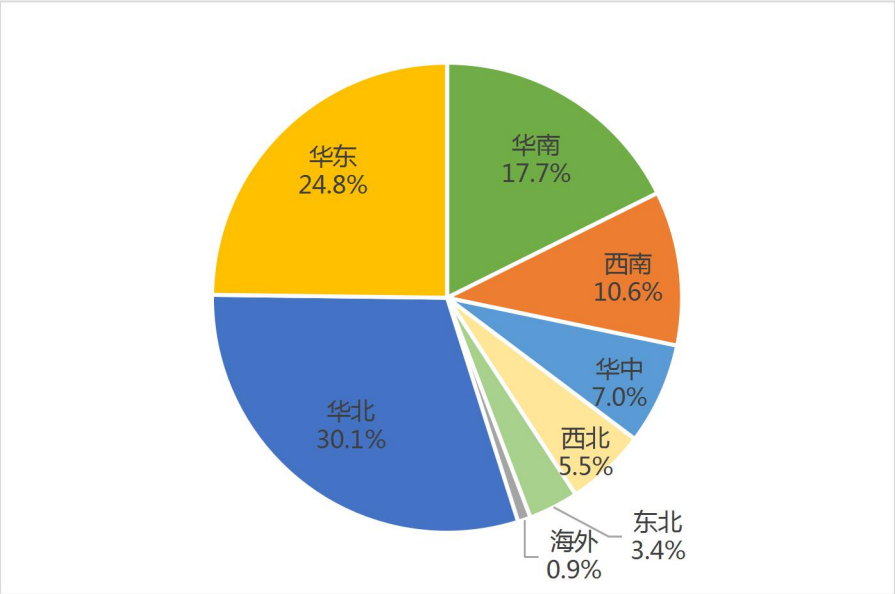


图 4 2018 年我国网络安全市场区域分布

（三）我国网络安全企业商业模式和产业链结构

网络安全企业的商业模式一直在不断进化中。传统网络安全企业最初有两种商业模式：产品型和集成服务型。之后，随着业务的拓展，这两种商业模式开始融合，诞生了以自研产品、OEM 产品和第三方产品及安全服务为主的综合型网络

安全企业。目前，产品型、集成服务型和综合型的网络安全企业构成了网络安全产业的中坚力量。

表 1 网络安全企业的三种商业模式特点

商业模式	特点
产品型	毛利率较高，交付周期短、应收账款周转快。上游是硬件供应商，供应硬件平台。也可能会有软件供应商，供应基础软件及模块。下游主要是代理商或客户。销售模式直销和渠道混合，有的企业以直销为主，有的企业以渠道为主。
集成服务型	毛利率较低、交付周期长，应收账款周转慢。上游为安全产品企业，供应成熟网络安全产品，下游面向终端客户。集成服务型厂商整合多方产品并以整体解决方案+服务的形式交付给客户，销售模式以直销为主。
综合型	毛利率居中、企业规模大、产品线长。一般这类企业会有完善营销网络和一定的品牌影响力，在供给端还会以 OEM 形式扩充产品线，加强细分市场覆盖。销售模式也是直销与渠道混合。

以上三种商业模式的界限在实际中并不是很清晰。有的产品型网络安全企业也会做少量集成服务业务，服务型的网络安全企业往往也会有少量的自研产品。按照这种方法分析网络安全企业时，毛利率是一项重要的参考指标。此外，由于商业模式中包含了较多的关键要素，只要改变其中的任何一个环节，商业模式就会产生变化或升级。网络安全产业变革也在孕育新的商业模式，PPP 模式、网络安全保险、管理安全服务和威胁情报等在商业模式上就显著有别于产业内传统的商业模式。

由于整体产业市场空间有限，单一细分市场的规模较小，难以满足企业的增长需求，业内越来越多的企业寻求向

综合型网络安全企业转型。从战略选择层面来说，这种变化趋势就是通过产品线扩张，争取覆盖更多的细分领域，以拓展企业的生存空间。此外，也有部分企业的战略选择是向产业链的上下游延伸。

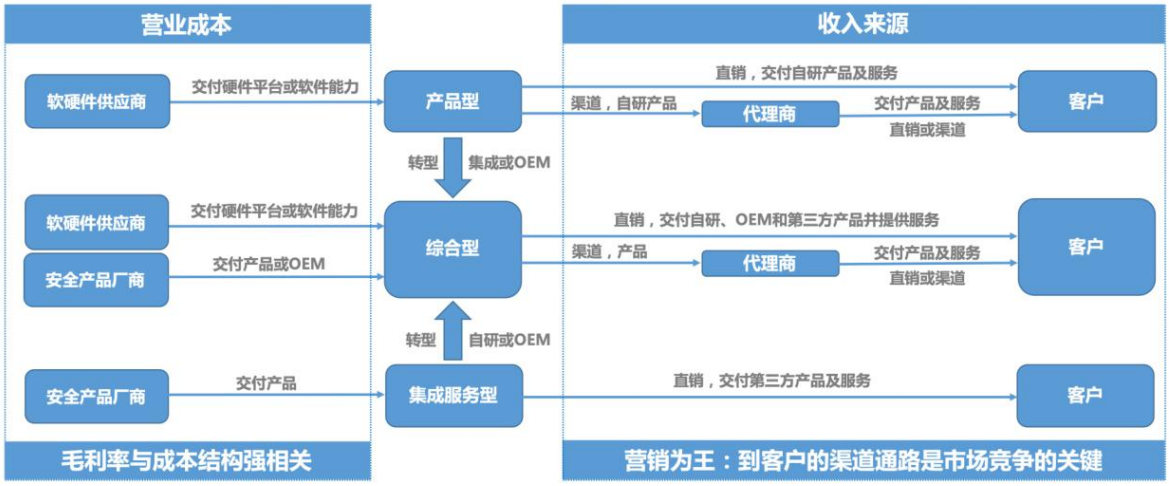


图 5 我国网络安全产业链供给关系

如图 5 所示，在整个网络安全的产业链中，处于上游的是网络安全企业的供应端，主要是由软硬件供应商和向上游扩张延伸的部分网络安全产品企业所构成。上游的软硬件供应商主要为产品型的网络安全企业提供交付硬件平台或软件的能力，安全产品企业则直接向集成服务型的网络安全企业交付产品。这部分链条构成了网络安全企业的主要营业成本，其毛利率与成本结构强相关。处于产业链下游的则是网络安全企业的收入来源端，产品型网络安全企业的收入来源主要是通过直销或者以代理商为中介的渠道两种方式，向客户交付自研产品或服务来实现的。集成服务型的网络安全企业则主要通过直销方式将第三方网络安全产品或服务交付

到客户手中。到客户的渠道通路是现阶段市场竞争的关键。我国网络安全市场发展的核心就在于网络安全产业链从产品（服务）到客户的渠道通路上所产生的价值重构。

（四）我国网络安全产业分类与全景图

网络安全产业市场的发展是一个升维的过程，网络安全从最初的基础安全产品及服务延伸到了云、移动、物联网和工业控制等不同的应用场景中，相当于拓展了一个维度。原来的问题是“如何做网络安全”，而新问题是“如何在不同场景（如，云计算）下做网络安全”。新问题的提出就意味着新的市场机会。我们尝试从基础安全、应用场景、业务、服务四个维度来描述我国网络安全产业的分类（如图 6 所示）。

其中，基础安全主要解决传统网络安全领域的核心问题，主要包括网络安全、端点安全、应用安全、数据安全、身份与访问管理、安全管理等六类。

应用场景主要包括云计算、移动互联网、工业控制、物联网等四个场景。这些应用场景的出现带来了新的安全问题，也孕育了多个新兴细分市场。

图 6 网络安全产业分类

信息技术应用创新和业务安全既不是网络安全产品也不是应用场景，而是在产品与应用场景基础上的业务维度，信息技术应用创新和业务安全与网络安全产品和应用场景相互交叉融合将会孕育出更多的细分市场。

网络安全服务初步定义了管理安全服务、管理检测与响应和安全教育培训三个类别。无论传统领域还是新应用场景，或是业务，都需要有服务体系来支撑。目前，我国网络安全产品与服务市场分类如表 2 所示。

表 2 我国网络全产品与服务分类

类别	项目	子项目
基础安全	网络安全	防火墙、上网行为管理、入侵检测与防御、网络隔离和单向导入、防病毒网关、网络安全审计、VPN/加密机、抗拒绝服务攻击（设备）、网络准入与控制、高级持续性威胁、网络流量分析
	终端安全	恶意软件防护、终端安全管理、主机/服务器加固
	应用安全	Web 应用防火墙、Web 应用安全扫描及监控、网页防篡改、邮件安全
	数据安全	数据库安全、安全数据库、数据脱敏、数据泄露防护、电子文档管理与加密、数据备份与恢复
	身份与访问管理	运维审计堡垒机、身份认证与权限管理、硬件认证、数字证书
	安全管理	安全管理平台、日志分析与审计、脆弱性评估与管理、安全基线与配置管理、合规检查工具、网络安全资产管理、威胁管理
场景	云计算	云基础设施安全、云负载保护平台、云操作系统、云身份认证、云抗 D、云 WAF
	移动互联网	移动终端安全、移动应用安全、移动设备管理
	物联网	车联网、视频专网
	工业控制网络	工控安全
业务	信息技术应用创新	安全产品、操作系统、芯片
	业务安全	舆情分析、反欺诈与风控、区块链安全、电子取证
服务	管理安全服务	网络安全系统集成、安全运维
	管理检测与响应	风险评估、渗透测试、应急响应等
	安全教育与培训	人才培养、网络靶场等

由表 2 可以看出，我国网络安全产品的细分程度较高，不同的细分市场领域聚集着相应的数量庞大的专业厂商。网络安全产业正在呈现分散格局。造成的这种现象的主要原因是，网络安全贯穿了整个信息流链条涉及几乎所有信息设备

与软件，单个网络安全企业无法掌握全部网络安全技术，只能根据自身技术优势和渠道特点进行差异化定位，选择部分细分领域参与市场竞争。

图 7 我国网络安全产业全景图

我们按照表 2 中给出的网络安全产品和服务分类方法对我国网络安全企业进行了相应的分类整理，最终得到了图 7 中所描绘的我国网络安全产业全景图。全景图展现了我国网络安全企业的产品和服务布局。从各领域内的网络安全企业数量多少也可以感知到一些技术发展的趋势。比如，网络安全企业对 IDS、IDP 类型的产品布局热度开始逐渐减弱，转而随着高级持续威胁的热度上升，对应的网络安全企业开始增多。由于工控安全新兴市场的兴起，众多网络安全企业纷纷踏足这个领域，提前布局，抢占市场制高点。更多关于技

术热点的分析，将在后面的章节中进行详细介绍。

二、我国网络安全企业竞争力与产业竞争格局

（一）我国网络安全企业经营情况分析

据统计，2019 年上半年我国共有 3060 家公司开展网络安全业务[2]（其中生产销售网络安全产品的企业有 1346 家，提供网络安全服务的企业有 1916 家），其中北京 862 家，广东 443 家，上海 223 家，四川 187 家，浙江 148 家位列前五，川渝成为我国网络安全西部核心区域。

为分析我国网络安全企业总体经营情况，我们共选取了 16 家企业作为样本进行分析。截止 2019 年 12 月份，我国上市网络安全企业有 19 家，其中部分企业为混业经营，上市主体中包含非安全业务资产，为避免数据失真，因此未列入本次研究范围，如表 3 所示。

表 3 公开披露财务数据的主要网络安全企业

交易所	板块	代码	公司	2018 年营业总收入(万元)	2018 年净利润(万元)	是否选为研究样本
深圳	中小板	002212	南洋股份	630033.7432	48700.2266	
深圳	中小板	002268	卫士通	193099.8381	12448.2265	是
深圳	中小板	002439	启明星辰	252180.5799	56012.5469	是
深圳	创业板	300188	美亚柏科	160058.4391	30209.63	是
深圳	创业板	300229	拓尔思	84530.3095	7376.3794	
深圳	创业板	300297	蓝盾股份	228193.5557	42184.1626	

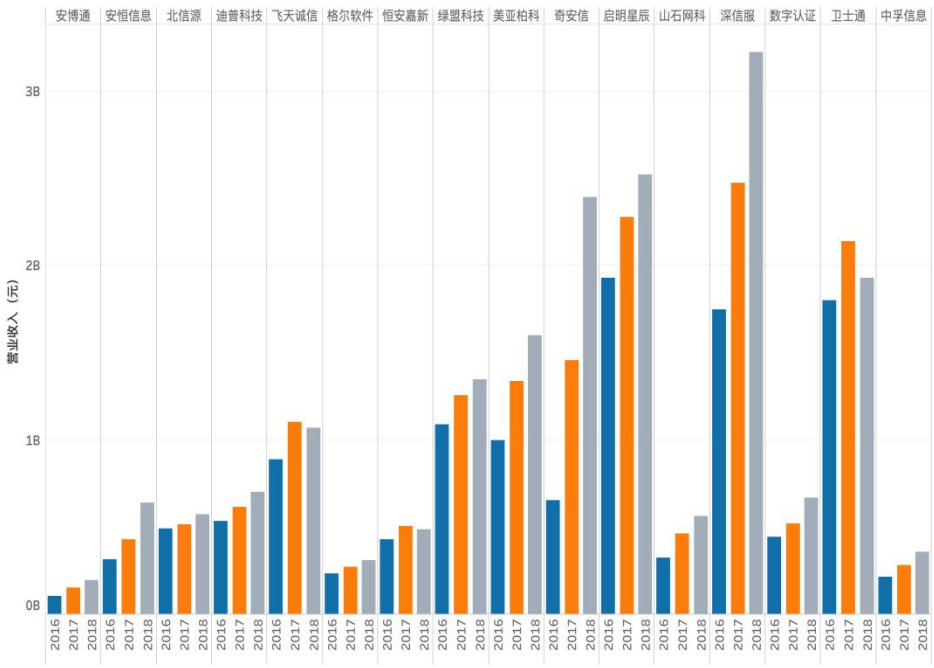
[2] 对获得网络安全相关资质认证的企业进行的数据汇总，如：计算机信息系统安全专用产品销售许可证、信息安全服务资质等。

表 3（续）

交易所	板块	代码	公司	2018 年营业总收入(万元)	2018 年净利润(万元)	是否选为研究样本
深圳	创业板	300311	任子行	120271.4301	13811.4249	
深圳	创业板	300352	北信源	57240.0446	9346.8217	是
深圳	创业板	300369	绿盟科技	134504.0751	16747.0456	是
深圳	创业板	300386	飞天诚信	107178.2405	13404.743	是
深圳	创业板	300579	数字认证	66772.0173	8645.5401	是
深圳	创业板	300659	中孚信息	35602.6444	4243.5171	是
深圳	创业板	300454	深信服	322445.0529	60327.568	是
深圳	创业板	300768	迪普科技	70405.5617	20100.6901	是
上海	主板	601360	三六零	1312926.3	350829.8	
上海	主板	603232	格尔软件	30858.545	7192.6181	是
上海	科创板	688168	安博通	19534.6549	5964.3864	是
上海	科创板	688030	山石网科	56227.6794	6891.1742	是
上海	科创板	688023	安恒信息	64042.0819	8348.8494	是
未上市	未上市	无	奇安信	239365.9261	-15771.3476	是
未上市	未上市	无	恒安嘉新	48830.2466	1837.1822	是

数据来源：数说安全根据公开资料整理

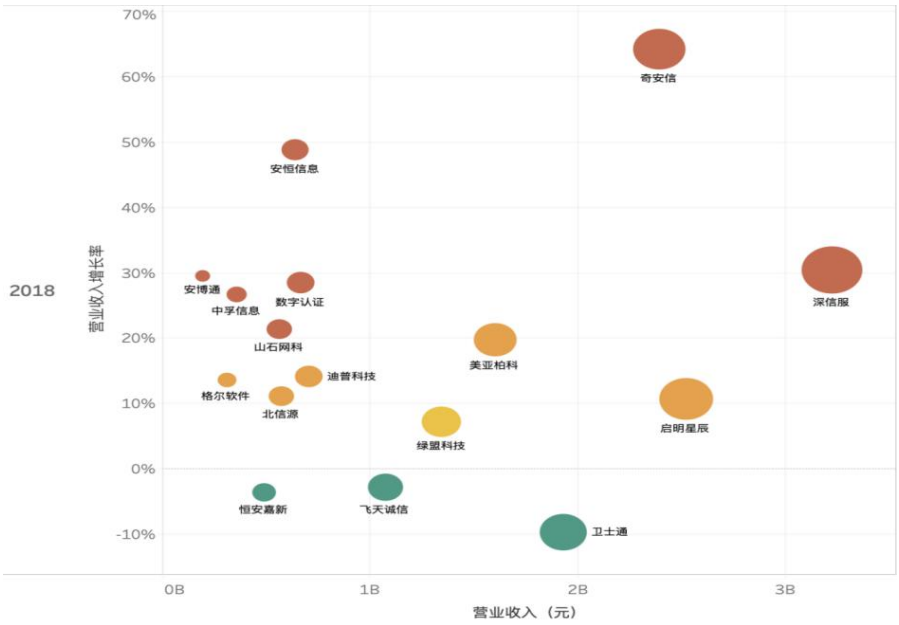
2018 年我国网络安全上市企业总体业务发展良好，16 家样本网络安全企业 2018 年营业收入合计 185.8 亿元，上一年同期营业收入合计 158.0 亿元。其中，启明星辰和奇安信安全业务收入超过 20 亿元；卫士通、深信服、美亚柏科、绿盟科技和飞天诚信安全业务收入超过 10 亿元。如图 8 所示。



数据来源：数说安全根据公开资料整理

图 8 2016-2018 年样本网络安全企业安全业务营业收入统计

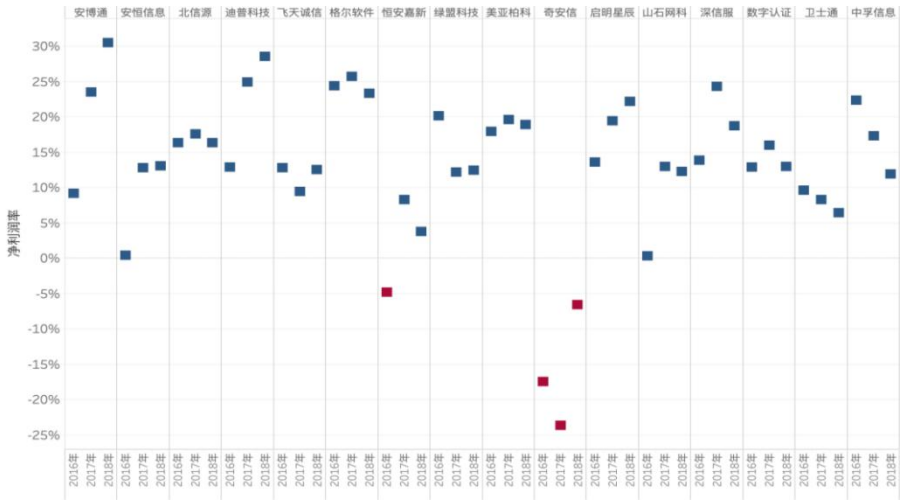
2018 年样本企业总体营业收入增长率 17.65%，相比上一年下降了 11.73%，增速大幅放缓，但依然维持较高水平。16 家样本企业中，有 7 家企业高速增长（年营业收入增长率高于 20%），6 家企业低速增长（年营业收入增长率低于 20%），3 家企业负增长（年营业收入增长率小于 0）。其中，居于首位的奇安信营业收入增长率 64.18%。如图 9 所示。



数据来源：数说安全根据公开资料整理

图 9 2018 年样本网络安全企业营业收入增长率

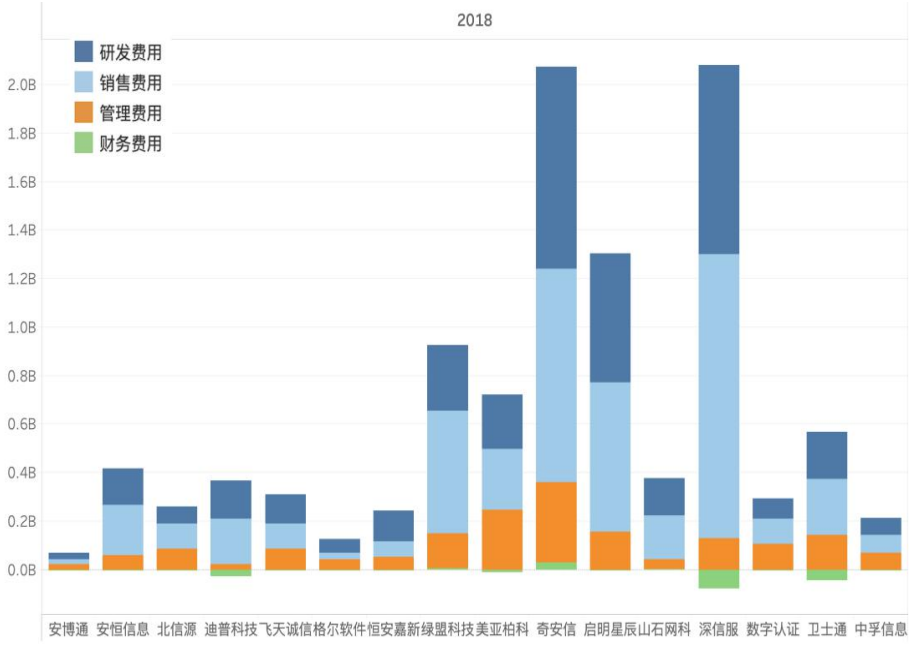
2018 年我国网络安全企业盈利能力持续改善。16 家样本网络安全企业在 2018 年净利润合计为 24.6 亿元，上一年同期净利润合计 20.3 亿元，同比增长 17.4%；总体净利润率 13.2%，相比上一年上升了 1.4%。16 家样本企业中有 15 家企业盈利，仅奇安信一家企业亏损。如图 10 所示。



数据来源：数说安全根据公开资料整理

图 10 2016-2018 年样本网络安全企业盈亏状况

16 家样本网络安全企业销售费用合计 47.2 亿元，占总体营业收入的比率为 25.4%；研发费用合计 38.5 亿元，占总体营业收入的比率为 20.7%；管理费用合计 17.4 亿元，占总体营业收入的比率为 9.3%。在网络安全企业成本结构中，销售费用、研发费用和管理费用是占比最高的三个部分。部分企业年度研发投入做了资本化处理，产业整体研发投入占当年营业收入的比例比研发费用率略高，近三年一直维持在 20%以上。如图 11 所示。

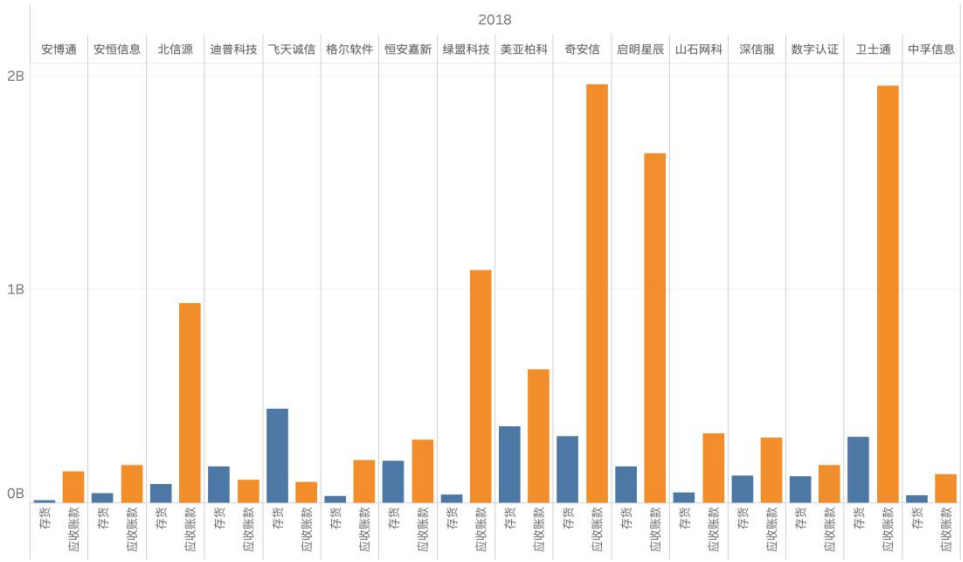


数据来源：数说安全根据公开资料整理

图 11 2018 年样本网络安全企业费用构成

16 家样本网络安全企业应收账款合计 101.8 亿元，占总体营业收入的比率为 54.8%，应收账款周转率 2.09，应收账款周转天数 172。存货合计 25.3 亿元，占总体营业收入的比率为 13.6%，存货周转次数 3.03，存货周转天数 118 天。在

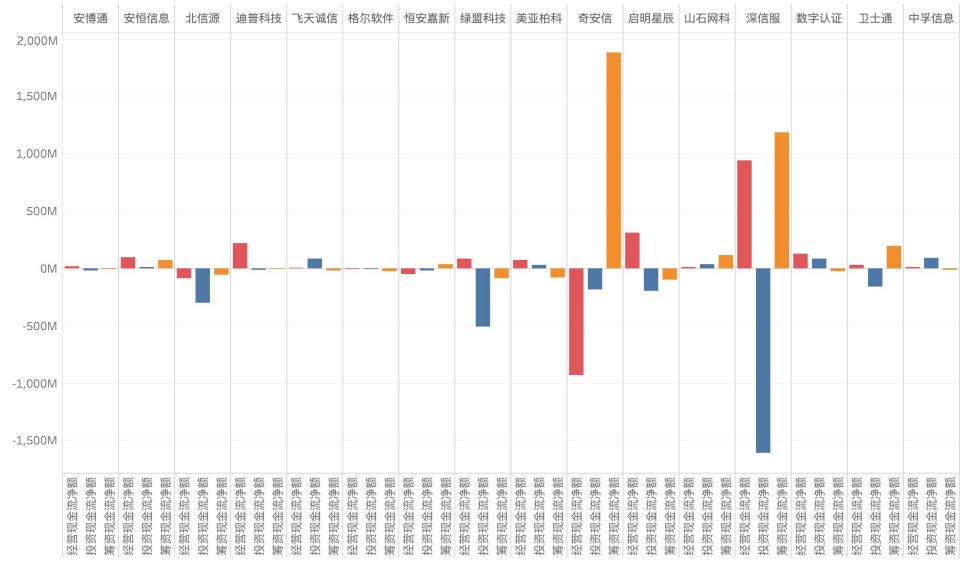
产业高速增长的过程中，应收账款和存货都有上涨趋势，网络安全企业总体资产质量略有下降。如图 12 所示。



数据来源：数说安全根据公开资料整理

图 12 2018 年样本网络安全企业应收账款和存货情况

16 家样本网络安全企业经营性现金流量净额合计 8.66 亿元。这项数据远低于净利润，这与收入确认与费用分摊有关，需要引起关注。投资活动产生的现金流量净额合计-26.9 亿元，筹资活动产生的现金流量净额为 30.8 亿元。总体现金流量画像呈现“正负正”状态，说明企业基本上把经营收入和筹集资金都投入到新项目中，产业整体处于加速扩张阶段。如图 13 所示。



数据来源：数说安全根据公开资料整理

图 13 2018 年样本网络安全企业现金流量净额

（二）我国网络安全产业竞争格局与企业竞争力

我们通过资源力和竞争力两个维度为网络安全企业进行了画像。其中，资源力是指企业所拥有的资本、技术、人力等相关资源的多寡程度，主要参考指标包括企业整体营收情况、企业市值、企业总体的人员规模等。竞争力则是指企业在当前商业模式下呈现出的总体能力。网络安全企业的竞争力分析从品牌、营销、产品、研发、服务和经营这六个维度展开。评价指标具体包括品牌知名度、品牌美誉度、网络安全业务毛利、营销及服务网络覆盖、产品线完整性、核心产品市场认可度、研发投入情况、研发投入成果物、技术服务能力、企业经营绩效、企业成长性、企业经营风险等相关指标。将上述数据通过加权计算得到了我国网络安全产业竞争格局图，如图 14 所示。

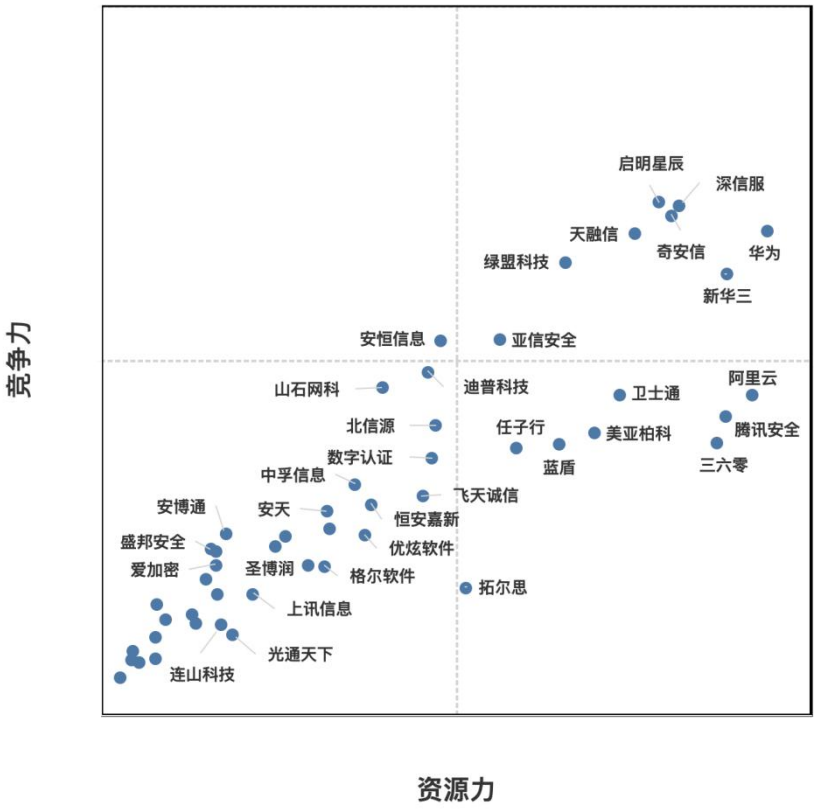


图 14 我国网络安全产业竞争格局图

通过数据可视化可以了解当前产业内各家企业竞争力的情况，新竞争者进入或新的商业模式出现会对产业格局和市场竞争的形成造成影响，竞争格局也将是动态变化的。商业竞争没有终点，在长期的中局演变过程中，如果产业规模快速增长，市场势必会涌入新玩家，导致市场竞争加剧，而当市场规模稳定后，由于产能过剩，比拼的将是精细化运营能力，多余的产能将被淘汰。我国网络安全产业近年来快速增长，但是由于网络安全市场细分领域众多，竞争较为激烈，导致产业集中度偏低，目前市场上缺少真正的龙头企业。我

国网络安全企业按照规模主要分为三种类型：大规模头部企业、中等规模企业和小规模初创型企业。

- 大规模头部企业以启明星辰、深信服、奇安信、天融信和绿盟科技等为代表的综合型网络安全企业为主。它们在网络安全产业深耕多年，在品牌、营销及服务网络、资质认证等方面构建了较高的竞争壁垒。未来，头部企业之间的竞争将会更加激烈，竞争将从业务和资本两个维度展开，预计三至五年内将会出现 1-3 家具备一定领先优势的龙头企业。
- 中等规模网络安全企业随着科创板快速落地开板，预计未来两三年内进入上市潮。上市后由于资本加持，这些企业将会进入一段高速发展期，向头部企业发起冲击。在这个过程中，一些企业有望突围成功，也会有企业将进入较为平稳的成熟期。
- 小规模初创型网络安全企业一般业务方向较为单一。由于市场细分领域众多导致单一细分市场天花板较低，加之行业竞争壁垒较高，当业务规模逐渐触及天花板时，初创企业一般有两个选择，一是适时退出。被大中型网络安全企业并购，利用买方的品牌、营销网络和资源等方面优势快速占据该细分市场份额；二是独立发展。独立发展过程中必然会伴随着扩展企业人员规模，构建完整营销服务网络、扩充产品线等动作，这个过程中也将会面临一定的经营风险，最终只有少

数优秀团队能够成功突围，成为中等规模企业。

（三）我国网络安全产业竞争格局关键影响因素分析

1. 时间窗口

受限于产业特性及现有商业模式，网络安全企业原生性成长速度相对较慢。根据历史数据的统计，网络安全企业从创立到上市一般需要 10 年以上的成长时间。近年来由于利好产业发展政策不断，加之科创板降低了上市条件，这个周期平均值有望缩短到 8 年。当前政策红利时间窗口未来三到五年内将会关闭，网络安全整体市场将进入较为平稳的成熟期，产业竞争格局将会逐渐固化。

2. 产业内的并购重组

目前市场上，在头部企业中，启明星辰是通过并购网御星云、赛博兴安、杭州合众等企业而重组的大型网络安全集团。奇安信则是在 360 部分业务基础上整合网神和网康等企业后发展起来的。在现有网络安全产业竞争格局下，无论是龙头企业之争还是中等规模企业寻求领导者地位，除了业务层面的竞争外一定伴随着资本市场操作，甚至资本市场操作将会成为竞争的主要手段。未来产业内投资、并购及重组行为仍会对产业整体竞争格局产生重大影响。

3. 大型互联网企业的竞合关系

以阿里、腾讯和 360 为代表的互联网企业面对传统网络安全企业具有较强的资源优势，这是完全的非对称性竞争。若其强势进入传统网络安全市场将会对传统安全企业形成降维打击。网络安全产业现有市场空间较小，商业模式产出效率偏低，尚不足以吸引互联网厂商强势介入，因此这些企业普遍选择以“生态”为关键词的合作战略。阿里与腾讯介入安全的主要战略意图在于云计算市场竞争，360 由于没有云计算业务作为抓手，政企安全业务是其参与产业互联网时代竞争的重要筹码。

4. 技术革新导致产业链结构及价值分配机制变化

网络安全是伴生性技术，与信息技术的革新密切相关。信息技术的革新将会催生出一些新兴的应用场景，同时一些应用场景也会逐渐消亡。正是由于安全的伴生性技术的属性，网络安全难以独立发展革新，更多是进行适应性创新。与这个过程同步，也会导致产业链结构发生变化，同时原有市场的价值分配机制也会随之调整。云计算就是比较典型的例子，当原有数据中心云化以后，原来以物理形态呈现在数据中心的网络安全产品应用场景消亡，随之而来的需求是在如何在云场景下进行安全防护。过去营销路径上系统集成商的角色的部分职能转移到了云计算服务提供商，价值分配机制也会随之发生变化。

5. 国有资本加码网络安全企业

国家除了通过发布宏观政策，对网络安全产业施加影响以外，也在以向网络安全民营企业注入国家资本的方式，改变着网络安全竞争格局。今年以来，一批优质的网络安全民营企业相继融入国家资本，如，中电子投资奇安信、中电科投资绿盟、国投收购美亚柏科 100%股权。网络安全“国家队”的形成将能够更好地服务国家战略，有助于增强国家的网络安全防御能力，以应对未来可能出现的网络安全威胁。随着 2019 年 6 月，工业和信息化部正式发布《国家网络安全产业发展规划》，网络安全的国家战略将进一步得到落实，对未来网络安全产业的发展将起到巨大的指引意义。未来，相信会有更多优质的网络安全民营企业受到国资的青睐，网络安全的“国家队”阵容将得到进一步的完善，形成网络安全竞争格局中一支举足轻重的力量。

三、我国网络安全产业热点细分领域分析

（一）数据安全

近年来，全球各地数据泄露和数据滥用事件频发，各国数据和隐私保护法规日趋严格并不断颁布实施。2018 年 5 月，欧盟《通用数据保护法案》正式生效。随着我国相关法律规范的相继颁布实施，数据安全开始逐步被纳入到合规性需求

市场，针对数据层面的安全体系建设也愈发受到各大企业重视，数据安全市场热度不断上升。表 4 列出了数据安全产品中出现的一些技术创新。

表 4 数据安全技术创新

技术	简介
企业数字版权管理（EDRM）	Gartner 将 EDRM 描述为用于对某些类型的企业数据强制访问和使用控制的技术，可结合 DLP、文件库、身份和访问管理（IAM）服务等技术，提供更优工具组合。
以数据为中心的审计和保护工具（DCAP）	DCAP 产品和技术特点能够集中监控用户、管理员与特定数据集相关的活动。DCAP 供应商需要通过有机生长和收购来继续增加技术能力，特别是在 UEBA、AI / ML 和区块链技术领域。
数据丢失防护（DLP）	展望未来，终端用户组织有望越来越多地寻求集成的 DLP 功能，而不是全面的 E-DLP 套件。
用户和实体行为分析（UEBA）	UEBA 已完成数据安全产品的集成，这项技术有望成长壮大，技术战略规划者必须建立 UEBA /员工监控能力，以帮助终端用户进一步提升其数据安全状态。
特权访问管理（PAM）	PAM 到 2020 年有望实现复合年增长率为 27%的显著增长，达 22 亿美元。集成 PAM 产品将增强数据安全产品，并向最终用户提供多种功能。
数据脱敏	数据脱敏利用一种旨在防止滥用敏感数据的技术为用户提供虚构而实用的数据，而非真实、敏感的数据，因此用户可以保持其执行业务流程的能力。与加密和令牌化不同，数据脱敏技术中，数据经历单向转换，不可逆，数据不能通过篡改操作被透露。

我国在数据安全领域至今尚未形成体系化的整体解决方案，不同技术流派的厂商仍围绕数据安全保护的不同阶段和视角进行单一方向的产品实践，其主要产品类型和技术方向有：

- 数据库安全方向，包括数据库审计、数据库防火墙、数据库脱敏；

- 数据防泄漏（DLP）方向，包括主机数据防泄漏和网络数据防泄漏;
- 数据加密方向，包括文档加密、磁盘/存储介质加密、应用加密等;
- 数据合规与治理方向，包括敏感数据发现、数据分级、数据脱敏、数据清理等。

未来用户将继续走向数字业务和采用云服务，数据的存储形态将更加多样化，数据的流通也变得越来越频繁，数据价值将逐步放大，数据也将会变得更加危险。随着网络威胁的增加以及数据关键性和价值提升，企业需要对数据的访问、可见性和监控使用更强控制的产品和工具，这也将是未来数据安全的主要内容。

表 5 我国数据安全领域典型企业简介及方案特色

典型企业	企业简介及方案特色
安华金和	安华金和始终专注于数据安全领域，作为国内“数据安全治理”体系框架的提出者，安华金和提供涵盖人员组织、安全策略、流程制定及技术支撑全方位的整体数据安全思路与方案；同时，安华金和作为独立的第三方云数据安全服务商（CDSP）为国内外各大云平台用户提供专业的数据安全保障，包括成为阿里云在数据安全领域的战略合作方。安华金和主营业务方向分为三大部分：围绕数据库安全，安华金和推出全线数据库安全产品及解决方案；推进数据安全治理理念在各行业的方案落地和实践；面向公有云和私有云环境特性，提供云数据安全全线产品，为公有云和私有云用户提供数据安全整体解决方案。

表 5 （续）

典型企业	企业简介及方案特色
美创科技	基于数据泄露的高风险性，美创科技聚焦“敏感数据”，创新实践“零信任”安全理念，围绕数据产生、传输、存储、使用、共享、销毁的全生命周期，构建了以“灯下黑”、“与毒共舞”、“不阻断，无安全”、“知白守黑”为原则的由内到外主动式纵深防御体系，从外部威胁防御、内部风险控制、数据追责溯源、数据共享与交换、终端安全、云安全等多层面，打造了数据库防水坝、数据库审计、数据库透明加密、数据库防火墙、数据脱敏、诺亚防勒索、漏洞扫描、数据防泄漏等一系列市场化数据安全产品，以及安全运营等专业服务，面向多行业提供数据安全全景式解决方案。
世平信息	世平信息致力于智能化数据管理与应用的深入开拓和持续创新，为用户提供数据安全、数据治理、数据共享和数据利用解决方案，经过多年积累，公司形成了强大的数据抽取解析、数据智能识别和数据水印标记专有核心技术，建立了在数据内容识别基础上的敏感信息检查监测与泄露防护功能体系，其研发的数据泄露防护系统可以实现用户信息系统中的数据资产及敏感信息的自动识别，及其在生产（采集）、存储、使用、共享、传输、销毁等生命周期各环节的发现、定位、监控、阻断、溯源、审计等数据泄露风险管控，数据脱敏系统可以对跨部门、跨系统数据共享，开发、测试、运维、分析、培训调用数据及数据外放外发等各类场景中涉及的敏感数据，实现智能发现、自动分类、自动脱敏，并以静态脱敏库或即时逐条返回的形式自动装载还原，消除被共享、调用数据的敏感性，有效降低敏感数据泄露风险。
上海观安	上海观安是以大数据为基础的安全公司，在运营商数据安全、智能制造安全领域拥有雄厚的技术储备，服务于广大运营商、工业企业的网络和信息安全。其数据安全防护产品以数据为保护核心，覆盖传统商用数据库、开源数据库、国产数据库、大数据数据库等多平台的数据防护系统，包含数据运维、数据传递、数据分析、数据共享等多个环节的数据管控套件和解决方案。

（二）云安全

由于云计算的兴起，网络安全市场也开始呈现出与云技术融合的发展态势。随着云环境中的网络攻击变得愈加复杂，在云安全市场上，一些安全技术（如表 6 所示）迅速成为了热点。

表 6 云安全技术热点

技术	简介
微隔离（Micro-segmentation）	在云环境中，数据中心负载的动态化、容器化趋势促发了微隔离技术的兴起。不同于虚拟本地网的粗粒度隔离，微隔离（亦称为“微分段”）是一种针对流量的更细粒度的网络隔离技术。微隔离一般面向虚拟化的数据中心，用于阻止攻击在进入网络内部后进行的横向（东西向）平移。微隔离通常使用策略驱动的防火墙技术或者网络加密技术来实现隔离。
CWPP	CWPP 即云工作负载保护平台，最初是源自主机安全的解决方案。作为一种工具，它自动化了公有云工作负载的安全性，为组织带来了业务的灵活性、风险的降低和成本效率的提升，同时减轻了开发和管理负担。它解决了现代混合数据中心体系架构中，服务器工作负载保护的独特要求。这些体系结构跨越内部部署、物理和虚拟机（VM）以及多个公共云基础设施即服务（IAAS）环境。理想情况下,它们还支持基于容器的应用程序体系结构。随着 CWPP 不断扩展到容器和容器化应用程序领域，CWPP 已经为多云世界的到来做好了准备。
CASB	CASB 即云访问安全代理。根据 Gartner 的说法，CASB 是一个本地或基于云的安全策略实施点。它位于云服务消费者和云服务提供商之间，以便在访问基于云的资源时合并和插入企业安全策略。即使云服务超出了组织的直接控制范围，越来越多的组织转向了 CASB 供应商，以解决云服务风险、实施安全策略和遵守法规。
CSPM	CSPM 即云安全态势管理，对应以前的云基础设施安全态势评估。每个 CSPM 工具包括用于合规性评估、运营监控、开发集成的用例、事件响应、风险识别和风险可视化。在理想的实现中，CSPM 应该持续管理云安全风险。它应该提供检测日志记录和报告，以及云服务配置和与云资源的治理、合规性和安全相关的安全设置。在监控和自动化之间具有互操作性是 CSPM 的一个关键优势。对于处理多云和容器环境的企业来说，知道错误配置是对云安全的最大威胁，CSPM 工具是实现真正的云安全最佳实践的极好步骤。

由于云服务提供商的存在，网络安全企业在云安全市场中的地位略显尴尬。由于公有云客户对公有云基础服务的依附粘性较强，公有云服务提供商通常会将安全解决方案捆绑在云服务中，客户往往会直接按需购买这些安全服务来解决安全需求，故而网络安全企业能够从公有云安全获得的市场

空间和机会有限。在私有云安全和混合云安全市场，网络安全厂商的参与方式主要有两种，一是为客户提供超融合的软硬件一体化架构方案，并在方案中同时加入云安全产品，二是作为独立提供商，提供云安全整体解决方案。

表 7 我国云安全领域典型企业简介及方案特色

典型企业	企业简介及方案特色
深信服	深信服为用户准备了一套云安全组件，其中包括下一代防火墙（vAF 经纬系列）、SSL VPN（vSSL）、应用交付（vAD）、广域网优化（vWOC）等，无论处于什么样的业务场景、使用何种底层架构及平台，深信服都能安全、灵活、高效地完成云业务交付，让 IT 架构快步走向云化。 私有云安全解决方案可实现虚拟机之间相互隔离和流量可视化，并提供业务负载和多种应用优化功能，保障服务可靠性；保障用户远程安全接入，同时实现业务的 SSL 安全加固；提供了 IPS、WAF、APT 防护等专业的安全功能，为业务系统提供完整的安全防护。
知道创宇	知道创宇云安全云防御平台是知道创宇推出的为了解决互联网时代的企业 Web 系统访问速度慢、安全状态严峻问题的平台产品。目前知道创宇云安全在全国各地部署了数十个大型云计算中心，储备了数百 G 的防御带宽，所有数据中心均部署有腾讯宙斯盾流量清洗设备与知道创宇祝融攻击智能识别引擎，在保证 Web 系统快速访问的前提下，知道创宇云安全一站式的安全加速解决方案，以“零部署”、“零维护”、“云防御”的模式，为客户阻止包括 XSS、SQL 注入、木马、0day 攻击、DDoS 僵尸网络、DNS 攻击等一系列针对 Web 系统的安全威胁。2015 年至今，知道创宇持续推出数十款安全产品，其云安全防御平台由创宇盾、抗 D 保、加速乐、创宇信用等组成，形成了从网站防护到加速，再到品牌线上商业保护的一整套解决方案；在安全监测方面，也形成了从区域资产，到漏洞威胁，再到攻击态势的全面获取能力。

表 7 （续）

典型企业	企业简介及方案特色
山石网科	山石云·格是创新的分布式网络侧微隔离产品，通过专利引流技术、虚机微隔离及可视化技术，能够为用户提供全方位的云安全服务，包括流量及应用可视化，虚机之间威胁检测与隔离，网络攻击、网络应用审计与溯源等，帮助政府、金融、运营商、企业等搭建安全、合规的“绿色”云平台。 山石云·界是专门为云计算环境设计的虚拟化网络安全产品，是可以运行在服务器虚拟机上的纯软件防火墙产品，适用于云计算环境部署，为用户提供下一代防火墙的多种安全防护功能。可结合云管理平台，实现快速部署和便捷管理，可为公有云租户提供独立安全防护，根据业务需求进行安全隔离和流量过滤。
厦门服云（安全狗）	厦门服云（品牌名：“安全狗”）依托云端安全技术和大数据安全分析能力，为用户构建立体式的云安全防御体系，提供私有安全云产品和公有安全云产品，其私有安全云产品云垒·私有云一体化安全管理平台是面向私有化环境、混合云环境推出的一体化云安全平台，可对私有云和公有云资产进行统一安全管理。云垒提供了从宿主机环境、虚拟化资源池到虚拟机系统一体化的纵深安全防御体系，同时提供了一个基于大数据分析的云安全平台，对云环境的管理、安全风险、攻击威胁进行统一分析和安全管控。公有安全云产品则以 SECaaS 为用户提供一站式云安全产品与服务，包括（云）主机安全、Web 应用安全、网站防篡改、抗 DDoS 云服务、安全大数据态势感知等产品。

（三）工控安全

工控系统广泛应用于能源、轨道交通、水利、工业、市政等国家重要行业领域，是事关国家命脉的重要关键基础设施。针对工业控制系统攻击甚至可引发灾难性事故，工控系统已逐渐成为挑起政治争端和武力打击的新兴攻击目标。尤其是自 2010 年“震网”事件以来，工控系统网络安全防护问题成为社会关注的热点。由于现有工控系统在设计之初偏重于功能实现而缺乏足够的网络互联互通规划和网络安全考虑，其大量应用了私有通信协议来进行数据传输交互。而

私有通信协议缺陷及软件安全漏洞在开放网络环境中会逐渐暴露出来，并与传统互联网安全问题相叠加，从而构成了工控系统解决方案的安全性和脆弱性风险。工业网络安全产品和服务的市场正在持续发展和扩大。据统计，目前已有几十家家网络安全企业提供工控安全产品和解决方案，工控安全市场迅速升温。

表 8 我国工控安全领域典型企业简介及方案特色

典型企业	企业简介及方案特色
卫士通	卫士通公司作为国内知名密码产品、网络安全产品、安全运维服务和行业安全解决方案综合提供商，从 2002 年开始接受国家重要控制系统安全任务，先后承担了财政部国有资本金、科技部“拟态空间安全重大专项工控漏洞挖掘专题”等重大专项。公司围绕工控安全监管侧和防护侧需求，形成了工控安全监管、工控安全防护两大业务体系，重点发展工控协议盲识别与逆向解析、漏洞分析与挖掘、专用密码设计及密码应用、大数据安全分析模型构建四大专业技术；打造了“监评防融”核心产品体系，以及轨道交通、石化、电力、钢铁等重要行业安全解决方案，初步形成规模化发展；并与网信、公安、工信、国防科工等监管部门建立紧密合作关系。
威努特	威努特是一家专注于工控安全的厂商，其产品线丰富，可提供边界安全、主机安全、监测审计、安全评估、安全管理等方面的工控安全产品，支持产品集中管理平台，同时可提供培训、咨询、评估、建设、运维等全流程的安全服务。
六方云	六方云在“工业互联网安全”领域拥有 LinSec 工业信息安全、CSec 云安全、NSec 网络安全、 SSA 态势感知四大产品线，依托人工智能、网络安全、工业控制等领域的技术优势，构建了完整的”安全工厂”解决方案，并基于“AI 基因，威胁免疫”的创新理念，将人工智能技术应用到全线产品中，实现了对未知威胁的有效防范。
长扬科技	长扬科技除了具备工控防火墙、工控网闸、工控监测审计等企业侧防护与审计产品，同时将工控安全数据协同感知与协同处置作为核心技术理念，提供基于人工智能和大数据分析态势感知平台和安全大数据平台解决方案。

（四）安全管理

随着我国产业 IT 应用和信息安全管理水平的不断提高，安全管理的理念越来越受到企业信息安全管理者的重视，面对网络中海量日志和安全告警信息，如何提升安全管理效率、如何辨识真正的安全风险成为摆在信息安全管理者眼前的棘手问题。落地到具体应用和方案上，国内外企业采用了各自不同的技术路线，国外大多采用 SIEM 类产品，在扩展探针、终端代理等新型数据采集方式的基础上，实现广泛的事件收集，并通过融入大数据采集分析和威胁情报、工单自动化运维等特性后实现管理目标。国内则大多以 SOC 产品作为安全管理的具体落地形式，其定位于信息安全产品市场的金字塔顶端，是所有安全产品的集大成者。SOC 的推出并不是取代原有安全产品，而是在这些安全产品之上，面向客户，从业务视角构建一体化的安全管理运行技术集成平台。

在习近平总书记 4·19 讲话、网络安全法中，均明确了以安全态势感知和安全管理的技术路线，具体落地形式可归纳为安全管理产品和安全管理服务两个层面，在产品层面主要包括以满足国家/城市级运营监管要求、用于跟踪区域内整体网络安全态势的态势感知平台级产品和用于满足企业自身安全运营管理需求的 SOC 单一产品，而在服务层面，启

明星辰、安恒信息、绿盟科技等市场头部企业均在积极拓展城市级安全运营服务新业务。

在数据冗杂、变幻莫测的网络空间，面对不断变化的安全威胁，如何提升安全管理检测响应速度和效率是未来企业安全管理的新方向，而从政府和网络安全监管的角度看，未来城市级安全管理配套设施（如城市级安全运营管理中心）的建设将是强化其安全监管力度的必要手段，随着安全管理的应用范围和价值逐步扩大，安全管理产品化向安全运营服务化转型，将会是未来比较明显的发展趋势，也将会带来新的市场机遇和商业模式创新。

表 9 我国安全管理领域典型企业简介及方案特色

典型企业	企业简介及方案特色
安恒信息	AiLPHA 大数据智能安全平台（简称 AiLPHA）是以安恒首席科学家刘博为核心的研发团队创新智造的安全产品，旨在解决传统安全设备无法应对越来越复杂和隐蔽的安全威胁。AiLPHA 以“AI 驱动安全”为核心理念，集成超大规模存查、大数据实时智能分析、用户行为（UEBA）分析、多维态势安全视图、企业安全联动闭环等安全模块。具备全网流量处理、异构日志集成、核心数据安全分析、办公应用安全威胁挖掘等前沿大数据智能安全威胁挖掘分析与预警管控能力。为企业客户提供全局态势感知和业务不间断稳定运行安全保障。致力于让安全更智能，更简单。
奇安信	奇安信态势感知与安全运营平台一方面可基于自有的多维度海量互联网安全数据，进行情报挖掘与云端关联分析，提前洞悉各种安全威胁，并将威胁情报以可机读格式推送到本地系统，供本地威胁检测和分析时使用，另一方面，态势感知与安全运营平台可对本地全量数据进行采集和存储，利用大数据技术在本地进行安全数据分析和威胁溯源。整个设计将遵循发现、阻断、取证、溯源、研判、拓展的安全业务闭环设计，使得用户能通过产品各个功能模块完成威胁处置的全过程。

表 9 （续）

典型企业	企业简介及方案特色
绿盟科技	绿盟科技重点针对异构安全设备的接入与日志的采集、存储，多源日志的关联分析及可视化呈现，脆弱性综合管理，运维处置流程的闭环等需求推出了绿盟企业安全平台。通过主/被动相结合的获取手段，实时采集各类安全设备、网络设备、主机、操作系统、以及各种应用系统的日志信息，通过内置规则或自定义规则的方式进行范式化及存储，极大提高了平台接入设备的覆盖度和操作便利性。除此外，还可提供智能威胁分析及安全治理闭环能力，安全管理人员可以根据实际需要自定义事件关联分析规则，同时对于告警进行便利的处置，在告警关闭后进行事件失效化处置并重新评估安全状态，实现运维处置流程的闭环。同时支持支持联动绿盟远程安全评估系统，进行扫描任务下发和核查结果收集、分析，通过对资产的漏洞、配置基线、弱口令以及网站的持续监控和管理，实现企业资产的脆弱性综合管理工作。
启明星辰	启明星辰新一代安全管理平台 SOC3.0 以大数据分析架构为支撑，以业务安全为导向，构建起以数据为核心的安全管理体系，强调更加主动、智能地对企业和组织的网络安全进行管理和运营。实现对海量安全信息进行全面的收集、整理、分析、审计，并借助智能化的分析手段提取出关键的安全事件；对客户复杂的 IT 系统从业务的角度进行全方位的可用性及性能监测、故障定位和告警；主动地进行事前安全管理，在攻击发生之前就获悉网络的安全态势；对客户重要业务系统进行量化的风险评估；借助量化的分析模型实现全网的安全态势感知；符合并体现了等级保护和信息安全管理体系的要求。

（五）威胁管理

随着信息化程度的不断提升，传统的网络威胁例如病毒、木马、端口等已逐步演变为社会工程、0day、APT 等高级网络攻击方式，传统的安全产品在威胁检测和防御能力上存在明显不足，面对日趋严峻的网络形势，应建立长效的以威胁检测和威胁情报为核心，以威胁分析和威胁猎捕作为辅

助研判手段、对新兴网络威胁进行全方位和全生命周期的监测和防御体系，并提供四个核心能力输出（如图 15 所示）。

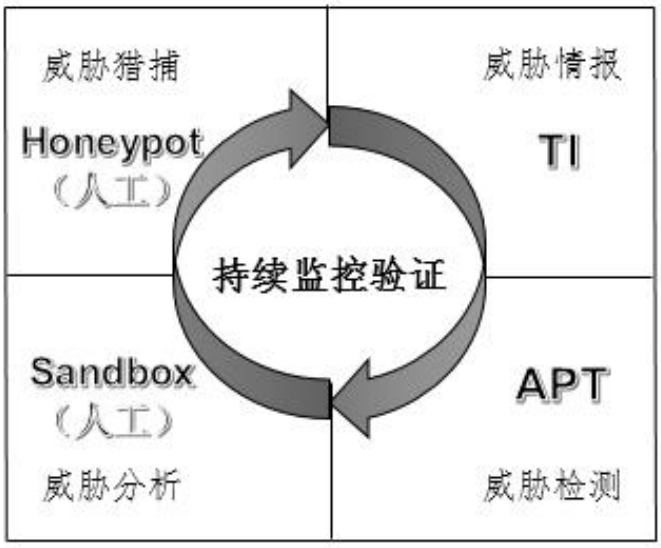


图 15 威胁管理的四大能力

从我国情况来看，基于传统特征库检测技术的 IDS 产品在检测 APT 攻击时有着明显的局限性，其依赖签名的检测机制无法识别 APT 惯用的 0day 漏洞攻击行为，而基于会话的实时检测技术亦无法实现以攻击链视角来追踪和溯源可能长达数月的攻击过程。从国外情况来看，主流厂商则普遍采用了无签名检测和保护技术，辅助以高级沙盒来进行恶意代码检测、仿真和机器学习等技术来实现高级威胁检测和预警，并由此形成威胁情报数据，亦可用于验证威胁检测体系的有效性，最终构建良性的威胁管理闭环。

表 10 我国威胁管理领域典型企业简介及方案特色

典型企业	企业简介及方案特色
亚信安全	亚信高级威胁发现系统 TDA 是一款 360 度的高级威胁检测产品，可掌握全网络的流量来侦测并响应高级威胁与未知威胁。TDA 采用三层式的侦测方法，第一层是静态分析，第二层是动态分析及行为侦测，第三层是事件关联，目的就是为了发掘隐匿的攻击活动。其独特的侦测引擎加上定制化沙箱动态模拟分析，能快速发掘并分析恶意文档、恶意软件、恶意网页、违规外连、勒索软件以及传统防护无法侦测到的内网攻击以及定向式攻击活动。 亚信高级威胁分析系统 DDAN 提供定制化沙箱分析用以增强亚信安全及第三方安全产品的威胁防护能力。DDAN 可以为网络安全产品、Web 和邮件安全产品及服务器与终端安全产品提供集中的动态沙箱分析，可疑威胁对象通过产品联动的方式自动提交给 DDAN 进行分析。 亚信安全高级威胁回溯分析系统 TRA 是一个集成大容量存储的高性能数据包采集与智能分析软硬件一体化平台，凭借其大容量存储能力，存储超过 6 个月的网络全流量，为网络回溯取证提供依据。TRA 可以分布式部署在网络的关键节点，对物理网络和云网络做全流量采集分析；亦可以以关键应用为目标，定向收集网络流量，实现对应用的网络访问性能、系统访问性能、应用相应性能等关键性指标的智能分析。
中睿天下	中睿天下专注于攻击溯源十五年，将多年一线攻防实战经验，应用于网络安全领域，基于攻击链（Kill Chain），中睿天下在攻击路径的每一个环节设置有效的检测和防御措施，全面覆盖形成安全防护闭环，实时监测发现威胁，并还原溯源攻击过程，实现精准防护目标，其攻击溯源解决方案从攻击者视角出发，以强大的威胁发现能力、智能研判能力，和还原溯源能力，解决了传统安全产品存在的“检测率低、误报率高、效率低”等问题，其基于攻击溯源技术提供集威胁发现、威胁处置和攻击溯源等于一体的综合解决方案，可以帮助用户知己知彼，有效应对各类未知威胁。
默安科技	幻阵是默安科技自主研发的一款基于欺骗防御的高级威胁狩猎与溯源系统。该系统从攻击视角出发，根据攻击者行为和资产状态，实时构建动态沙箱，可在不同网络环境中自动化部署沙箱、伪装代理、漏洞、诱饵等形成动态蜜网，实现对攻击者的全链路欺骗，同时在攻击者必经之路上构造陷阱，从而混淆其攻击目标，精确感知并溯源攻击者行为。它通过云密网将攻击隔离，保护企业内部真实资产，构成了企业至关重要的一道安全屏障。

（六）终端安全

近年来 IT 信息化不断发展，数据加密、5G 商用、移动和物联网终端等新技术和新应用不断涌现，在万物互联和万物感知中对数据传输进行加密将逐渐成为现实。据 Gartner 预测，未来超过 80%的企业流量将被加密，而在 5G 的未来，网络接口将支持至少 20Gbps 传输速率，核心网用户面将继续下沉靠近终端。预计到 2030 年，全球移动通信设备总数将达到 1000 亿量级，数据流量较 2010 年增长约 20000 倍，移动终端和 IOT 终端产品也将加速从消费领域向服务领域和工农业领域渗透。面对以上 IT 技术和应用的不断革新，传统边界安全防护的效率将逐步减弱。目前市场上几乎所有可用的边界防护设备（例如防火墙），在面对加密数据和大规模网络流量检查时都存在明显的性能瓶颈，深度包检测和响应时间大幅增加，因此网络安全也呈现了新的发展趋势。安全战场已经逐步由对核心与主干的防护，转向网络边缘终端的管理和保护。终端安全俨然已成为了企业信息安全保障工作的重要环节。

随着终端安全理念的日益火热，我国终端安全技术的发展也呈现出多元化趋势，各大安全企业陆续推出了各具特色的终端安全解决方案，以满足特定场景下的个性化需求，其主要技术包括：以终端防病毒为基础、通过融和终端安全检

测与响应技术而形成的融合方案；将网络数据防泄漏技术延伸至主机层面形成的主机数据防泄漏方案；针对云环境下主机和服务器的微隔离和 CWPP 保护方案。

表 11 终端安全领域技术热点

技术	简介
EDR	以检测（Detection）和响应（Response）做为主要技术环节，可满足持续监控和响应高级威胁的需求，它是端点安全技术的一个子集，专注于通过正确的洞察力提供正确的端点可见性，以帮助安全分析师发现，调查和响应跨越多个端点的高级威胁和攻击活动,在 IT 端点部署轻量级代理采集终端信息并上传中心数据分析平台，通过大数据、机器学习、威胁情报、UEBA 等新兴技术实现对终端安全态势的研判分析，是针对日渐多变的网络攻击、零日攻击等新兴威胁的主动性防御机制。EDR 与其他端点保护平台（EPP）（如防病毒（AV）和反恶意软件）的不同之处在于，其主要关注的不是通过在端点上预先执行检查来抵御威胁。
防病毒	重量级客户端的部署形式，依靠对已知病毒和威胁的特征比对来识别端点潜在威胁。它是常见的端点防护手段。
主机 DLP	主机数据防泄漏方法主要以主机数据资产为中心，在统一平台之上依据主机数据的特点，灵活采用加密、隔离、内容智能识别等多种不同技术手段，例如正则表达式检测（标示符）、关键字和关键字对检测、文档属性检测、精确数据比对 (EDM)、指纹文档比对 (IDM)、向量分类比对 (SVM)等多种检测方法，防止在各种具体应用场景下主机数据的泄露和扩散。
EMM	一套实现企业员工安全使用手机、平板等移动终端进行移动化工作的技术平台与管理方法。EMM 通过移动信息化技术和管理手段，针对企业移动信息化建设过程中涉及到的企业移动设备、应用、信息等内容提供信息化管理的解决方案与服务。面向移动终端领域的 EMM 包括移动设备管理(MDM)、移动应用管理(MAM)、移动内容管理(MCM)等平台产品。
MDM	移动设备管理，提供从设备注册、激活、使用、淘汰各个环节进行完整的移动设备全生命周期管理。MDM 能实现用户及设备管理、配置管理、安全管理、资产管理等功能，还可以提供全方位安全体系防护，同时对移动设备、移动 APP、移动文档三方面进行管理和防护。

在未来很长的一段时间里，终端威胁仍将是信息安全的最大潜在威胁，终端安全保护也将成为未来网络安全防护的

重要手段和措施。其面临的技术挑战将包括：面对新兴的终端安全威胁（例如采用新恶意软件变种、0Day 攻击手段，以电子邮件、浏览器、应用程序作为入口向端点渗透）时，企业如何抑制威胁扩散，解决端点设施的脆弱性；如何将终端安全技术与 IT 基础架构深度融合以降低目前高额的实施成本与复杂性；在人员和设备复杂多变的情况下，如何提高端点可视化能力，以确定不可见或无法管理的端点设施的安全有效性和漏洞状况。

表 12 我国终端安全领域典型企业简介及方案特色

典型企业	企业简介及方案特色
安天	安天智甲终端防御系统（IEP）是安天研发的面向政企客户的端点综合安全防护软件，产品为办公机、服务器、虚拟化节点、移动设备、国产专用计算机、各类自助终端、工控上位机等各类端点场景提供多层次、全周期的动态防护能力。智甲产品内置安天自主研发的下一代威胁检测引擎，基于黑白双控模式的安全策略，有效支撑终端检测与响应（EDR）。智甲具有恶意代码查杀、实时主防监测、勒索病毒增强防护、溢出攻击和横向系统防护等综合威胁防御功能；融合主机防火墙、终端管控、外设管控、漏洞扫描、集中补丁修复等管理功能；支持对 Rootkit、感染式病毒、宏病毒等内网顽固威胁的有效处置，结合安天独家的高级威胁追溯包服务，可以实现全网威胁追溯。
天融信	天融信终端威胁防御系统（EDR）是一款集终端威胁检测、防御和响应于一体的下一代终端安全防护产品。系统可以通过病毒族群基因特征匹配和动态沙箱行为分析技术识别恶意软件未知变种，有效的防御未知威胁攻击。同时，系统结合终端加固、行为管控、全网一体化管理技术，构建完善的终端防御体系，实现全面预防、有效检测。为了能够有效应对安全事件，系统可利用微隔离、主动防御机制及时、高效地响应处置安全威胁，及时止损。系统可与其他安全设备联动进行协同响应，自动处置，形成立体防护能力，为用户提供主动、动态、自适应的安全保障。

表 12 （续）

典型企业	企业简介及方案特色
北信源	主机安全类产品致力于内网终端安全管理，除传统的 Windows 操作系统的终端外，主机安全类产品已经全面覆盖多种自主国产终端、虚拟化终端、移动终端和工控终端等。主机安全产品包括主机监控审计与补丁分发系统、金甲防线、防病毒系统、虚拟化综合审计系统等。随着安全管理理念的升级，内网安全产品从合规管理逐步扩展成为包括主机防护、行为合规监管和终端安全运维的新一代终端安全管理体系，为用户提供多位一体、统一管理的解决方案。

（七）身份与访问管理

在网络环境改变和攻击复杂度的影响下，原来可信的网络不再安全，已经变得不可信任。零信任网络（亦称零信任架构）模型的主要目的就是守护动态网络边界，阻止威胁在网络内部传播。该模型由研究机构 Forrester 的前首席分析师约翰·金德维格（John Kindervag）于 2010 年创建，现已成为 IT 安全在国际上流行的一种替代架构。一些企业也开始尝试在身份认证与访问管理中采用零信任网络架构，以防止敏感数据外泄，提高抵御网络威胁的能力。

表 13 身份认证与访问管理技术热点

技术	简介
多重身份验证（MFA）	有些组织正在从双因素身份转变为三因素身份验证。多因素身份验证(MFA)结合了用户所知道的信息(比如，密码)、用户拥有的东西（如，智能手机、令牌）以及属性（生物特征：如，面部识别、虹膜扫描或指纹传感器；行为特征：如步态识别）。MFA 通常是一个分阶段的过程，如果检测到了风险，则要求用户提供额外的识别因素。它通常与基于风险的身份验证配对。

表 13 （续）

技术	简介
上下文感知的访问控制模型-CaRBAC（基于策略）	它预先确定了一个基于各种属性的事件及其结果。例如，如果 IP 地址未列入白名单，则可能会被阻止。或者，如果没有表明设备受管理的证书，则上下文感知网络访问控制可能会升级身份验证过程。
基于风险的身份验证（RBA）	基于风险的身份验证根据当前风险配置文件动态地将各种严格级别应用于身份验证过程。风险越高，认证过程对用户的限制越严格。在用户可以访问公司的信息资源之前，用户的地理位置或 IP 地址的更改可能会触发其他身份验证要求。
API 安全	API 流量监控和身份认证技术的结合，目标是 API 流量可视化，以及基于 AI 的行为识别模型快速检测、阻断威胁和违规行为，并使用欺骗或者蜜罐的环境来识别真正的黑客攻击。
用户行为分析（UBA）	UBA 技术检查用户行为模式，并自动应用算法和分析来检测可能表明潜在安全威胁的重要异常。UBA 与其他安全技术不同，后者专注于跟踪设备或安全事件。UBA 有时也与实体行为分析组合在一起，称为 UEBA。
特权账号管理（PAM）	PAM 则是将身份认证与访问管理的原则和操作，简单应用到“超级用户”账户和管理凭证上，主要用于后台管理。Gartner 建议先对高价值、高风险的系统实施 PAM，监控对其的访问行为。国内对应产品为堡垒机，目前国内企业也在纷纷增强特权账号全生命周期管理能力。

身份认证与访问管理的主要应用场景及价值包括 IAM/4A 和堡垒机/PAM。其中，IAM 可确保授权的员工、合作伙伴和客户拥有适当的资源访问权限访问业务系统。IAM 自动化的管理入职，离职，管理角色，身份验证，访问管理等流程，对用户行为进行审计，并提供报告。堡垒机/PAM 则是将身份认证与访问管理的原则和操作，简单应用到“超级用户”账户和管理凭证上，主要用于后台管理。我国堡垒机应

用较为广泛，堡垒机侧重解决运维审计问题，但目前我国堡垒机厂商也在增强特权账号全生命周期管理能力。

表 14 我国身份认证安全领域典型企业简介及方案特色

典型企业	企业简介及方案特色
格尔软件	格尔软件是国内较早研制和推出公钥基础设施 PKI（Public Key Infrastructure）平台的厂商之一，公司拥有全系列信息安全产品、安全服务和解决方案的提供能力，产品包括：“安全认证网关”、“可信边界安全网关”、“无线安全网关”、“电子签章系统”、“安全即时通系统”、“网络保险箱”、“终端保密系统”、“签名验证服务系统”、“局域网接入认证系统”等产品”。其政府行业统一认证解决方案可以实现 PC 端、移动端跨屏互动，B/S 与 C/S 应用状态共享，多个 APP 登录联动。并采用高强度密码算法的安全协议技术，保障登录令牌的传输与存储。可以扩展支持多种认证方式，包括数字证书，一次性口令，生物特征识别等。解决了复杂应用环境下，不同应用，不同客户端，不同 APP，不同平台的统一认证问题。
芯盾时代	芯盾时代基于信息安全、人工智能、身份认证等多维技术驱动，依托于坚实的企业服务能力，目前已拥有具有自主知识产权的多因素认证、统一身份管理、人工智能反欺诈、零信任安全等 4 个产品系列，公司已为政府、金融、互联网、运营商等行业提供了数十种业务安全解决方案，覆盖金融账户及交易安全、企业用户安全管理、智能风控反欺诈、用户和实体行为分析等领域。 芯盾时代持续自适应安全平台（ECP），对账户持有者采取“零信任”的态度，在用户操作系统的全周期内，持续的通过规则引擎对前端采集的信息进行风险评估，根据风险值自动匹配认证方式。解决了账号拖库、撞库、账户共用等账号安全问题，可以最大化的确保账户使用者身份的可信度。ECP 同时支持多种独立于业务系统的认证方式，可快速增加新型认证方式。 芯盾时代身份管理与访问控制 Identity and Access Management (IAM)对企业复杂的账号和权限体系进行统一治理，提供统一账号目录服务和授权服务，让管理更加科学高效。 芯盾时代开创性的将身份认证迁移到人的“所持”--移动端，支持二维码、APP 一键登录、动态口令、临时授权码、短信认证、语音认证、人脸识别、声纹识别、密码、微信认证等多种认证方式。

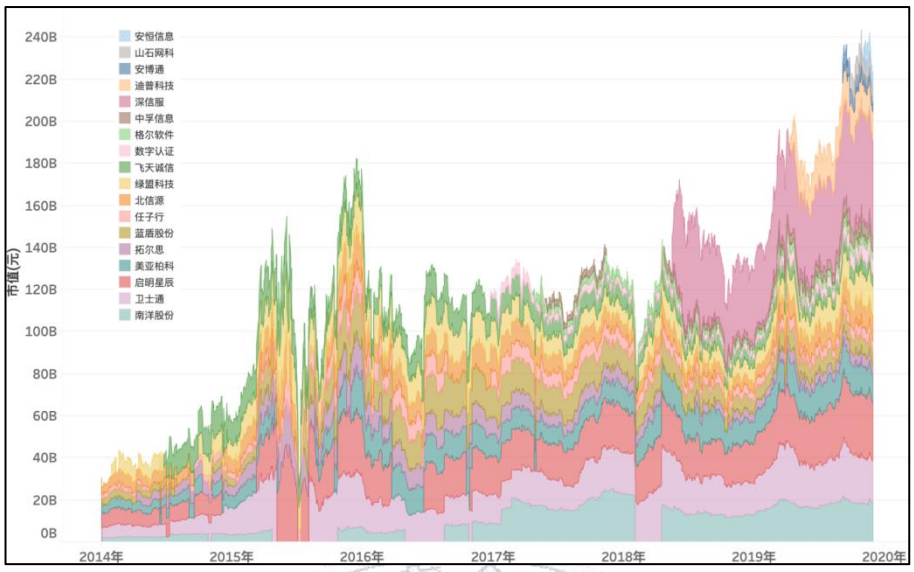
表 14 （续）

典型企业	企业简介及方案特色
九州云腾	九州云腾是一家专门针对云计算与移动应用的下一代统一身份认证和管理的解决方案提供商。公司专注于解决国家机构、事业单位、各类企业机构的员工、合作方以及其服务对象、客户等人群在访问私有云、公有云、内网自有业务、互联网及移动互联网业务等多种复杂应用场景下的身份认证及业务安全问题。 九州云腾的产品分为生成令牌 IPG 和 解析令牌 SPG 两类。IPG 产品线支持多租户、分级管理，其模块包括 SSO、UD、PS、STS、MFA、SM2 密码控件。SPG 产品线用于取代 VPN，起到堡垒机作用，其模块包括 API、RP。所有产品模块均可独立工作，模块化部署，实现按需供给。

四、我国网络安全资本市场分析

（一）我国网络安全企业资本市场表现

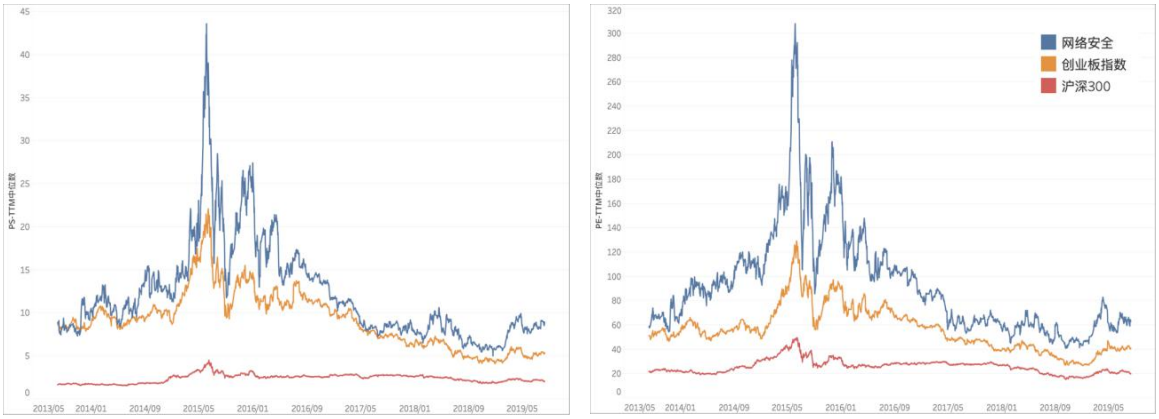
从 2015 年牛市过后，经历了三年多时间的市场下行周期。2018 年下半年上市网络安全企业（不含三六零）整体市值跌到了 1200 亿以下，网络安全公司估值水平达到历史低点，部分企业估值水平创历史新低。随后市场热度快速回升，不到半年的时间，上市网络安全公司完成了估值修复过程。深信服 2018 年 5 月上市，上市后受到市场青睐，最高市值突破 500 亿元。迪普科技 2019 年 4 月上市，上市后最高市值突破 170 亿元。科创板开启后，安博通、山石网科和安恒信息先后完成 IPO。在这些企业的推动下，网络安全企业整体年内市值增长 60%以上，突破 2000 亿元大关。如图 16 所示。



数据来源：巨潮资讯网

图 16 2014-2019 年我国上市网络安全企业市值动态

我们对网络安全与资本市场主要指数估值水平对比（如图 17 所示），发现网络安全整体估值水平显著高于创业板指数，也高于沪深 300 指数，可见资本市场对网络安全概念的青睐，资本也更愿意给予网络安全企业较高的溢价。我们还对上市网络安全企业主要估值指标的历史数据做了分析，行业 PS-TTM 中位数为 9.2，PE-TTM 中位数为 65.8，当前网络安全企业估值总体处于历史中位水平（以上数据仅具备统计学意义，仅供参考，不作为投资建议）。另外，我们还能够看到网络安全企业整体估值中枢的波动与产业主要指数几乎同步，说明网络安全企业市值与资本市场热度关系紧密。



数据来源：巨潮资讯网

图 17 我国网络安全板块与市场主要指数估值水平对比

（二）我国网络安全企业 IPO 动态

2018 年以后，深信服和迪普科技先后在深交所创业板成功上市。随着科创板政策落地，网络安全资产证券化大潮拉开序幕。2019 年至今，已有 7 家网络安全企业申报科创板，其中安恒信息、安博通、山石网科已成功登陆上交所科创板。恒安嘉新、连山科技和光通天下终止了 IPO 申请。白山云目前处于中止状态，待披露最新财务数据后将重启上市进程。由于科创板与主板、中小板和创业板相比营收利润要求相对较低，且推行注册制，发行定价更贴近市场，成为了网络安全企业登陆资本市场的第一选择。科创板具备的这些特性让一些中等规模网络安全企业上市成为可能，这也打通了创业者和早期投资者的退出通道。

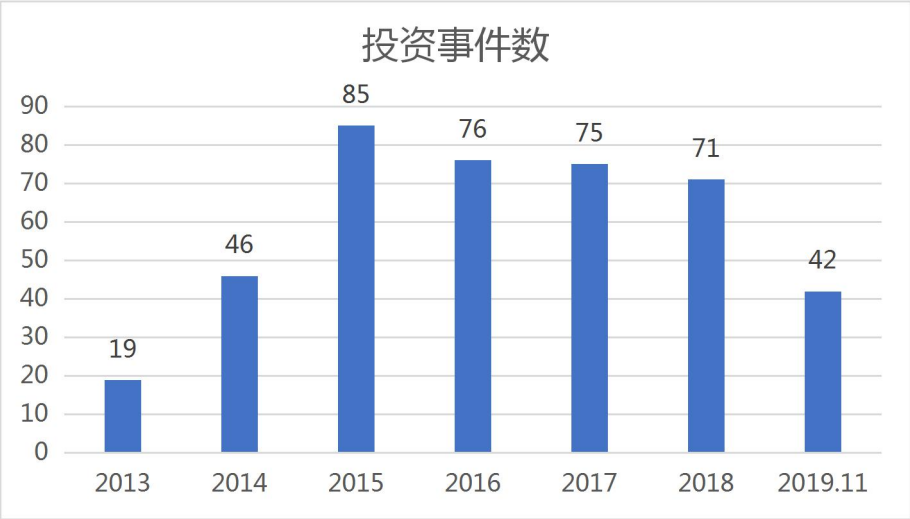
表 15 2018 年至今网络安全企业创业板上市进程情况汇总

企业名称	当前状态	板块	上市时间	发行市值	最新市值
深信服	上市	创业板	2018 年 5 月	120.3 亿	464.6 亿
迪普科技	上市	创业板	2019 年 4 月	44.9 亿	133.4 亿
安博通	上市	科创板	2019 年 9 月	29.1 亿	46.1 亿
山石网科	上市	科创板	2019 年 9 月	38 亿	64.9 亿
安恒信息	上市	科创板	2019 年 11 月	41.9 亿	75.6 亿
恒安嘉新	终止	科创板	n/a	n/a	n/a
连山科技	终止	科创板	n/a	n/a	n/a
光通天下	终止	科创板	n/a	n/a	n/a
白山云	中止	科创板	n/a	n/a	n/a

数据来源：数说安全基于证监会官网数据整理，截止日期 2019 年 11 月 30 日

（三）我国网络安全产业投融资情况

2018 年由于资本市场环境因素影响，一级市场对网络安全领域投资热度略有减弱，全年投融资事件有 71 起，相比前几年略有下降。2019 年一级市场投资热度显著下降，截止 11 月发生的投融资事件数量仅有 42 起，而且获投的早期项目比例也明显下降。根据我们对投融资事件的梳理发现，与前几年相比一级市场投资偏好发生显著变化，早期项目获投比例大幅减少，中后期项目获投比例大幅增加。初创企业融资较为困难，未来一段时间内将更加考验创业企业自身经营能力，业务创造现金流将成为企业生存的关键。



数据来源：数说安全根据公开资料整理，截止 2019 年 11 月

图 18 2013-2019 年我国网络安全领域投融资事件

从融资金额角度来看，2018 年至今融资额度处于亿元以上的融资事件有 20 起，千万级以上融资事件数量超过 50 起，千万级项目仍是一级市场的主流。2019 年虽然融资事件数量减少，但我国网络安全公司融资总额再创新高，截止 11 月融资总额已超过 70 亿元。近两年网络安全企业获得投资总额相比前几年大幅提升，主要是由于深信服、迪普科技、安博通、山石网科和安恒信息上市，奇安信等具备上市条件的公司获得了大额融资，由此可见，资本更加青睐退出确定性强的投资标的。从细分市场角度来看，数据安全、工控安全、身份认证、云安全是市场上热点投资领域。其中数据安全领域热度最高，全知科技、数篷科技、安华金和、中安威士、中安星云和杭州美创等相关标的企业均成功获得了融资。数据安全的概念比较模糊，各家企业的解决方案差异性也是比

较大，数据安全市场还不够清晰。工控安全最近几年快速升温，市场上出现了众多工控安全厂商，各家企业方案上差异较小，已出现同质化现象。威努特、六方云和天地和兴等获得了融资。

表 16 2018-2019 年我国网络安全企业亿元级融资情况

时间	公司名称	轮次	金额	投资方
2019 年 11 月	微步在线	C 轮	亿元级	高领资本、星路资本
2019 年 11 月	安恒信息	IPO	7.6 亿	公开发行
2019 年 10 月	天地和兴	C 轮	2 亿	毅达资本、广州基金、松禾资本
2019 年 9 月	山石网科	IPO	9.5 亿	公开发行
2019 年 9 月	奇安信	Pre-IPO	15 亿	未披露
2019 年 9 月	万里红	战略投资	9.5 亿	湘财证券、格力电器、新湖中宝-新湖控股
2019 年 9 月	安博通	IPO	7.3 亿	公开发行
2019 年 7 月	瑞数信息	C 轮	1 亿	君联资本
2019 年 5 月	竹云科技	B 轮	亿元以上	东方富海、达晨创投、子于资本
2019 年 5 月	迪普科技	IPO	4.5 亿	公开发行
2019 年 4 月	四叶草	B 轮	亿元以上	蚂蚁金服
2019 年 1 月	奇安信	B 轮	9 亿	未披露
2019 年 1 月	芯盾时代	C 轮	3 亿	宽带资本、云锋基金、红点创投
2019 年 1 月	漏洞盒子	B+轮	1 亿	同创伟业、国发创投、云栖基金
2018 年 12 月	山石网科	战略投资	亿元以上	奇虎 360、博彦科技、同心基金
2018 年 11 月	奇安信	Pre-B 轮	12.5 亿	IDG 资本、中信建投资本、国投创合
2018 年 11 月	安华金和	C 轮	亿元以上	德联资本
2018 年 10 月	指掌易	B 轮	2 亿	高成资本、长安资本、苹果天使 APU
2018 年 9 月	美创科技	B 轮	亿元以上	英华资本、普华资本、东方福海
2018 年 5 月	深信服	IPO	12 亿	公开发行
2018 年 4 月	白山云	C+轮	2.4 亿	富禾投资、德威资本、金晟资产等
2018 年 2 月	青藤云安全	B 轮	2 亿	红杉资本中国、宽带资本

表 16 （续）

时间	公司名称	轮次	金额	投资方
2018 年 2 月	顶象技术	B 轮	亿元以上	嘉实资本、晨兴资本、东证资本
2018 年 2 月	观安信息	B 轮	1.3 亿	上信投、联新资本、张江集团等
2018 年 1 月	芯盾时代	B+轮	1.2 亿	云锋基金、昊翔资本、红点创投
2018 年 1 月	安赛科技	A 轮	1 亿	腾讯投资、奇虎三六零

数据来源：数说安全根据公开资料整理

五、我国网络安全产业发展展望

（一）客户安全能力跃升将对网络安全产业提出更高要求

长久以来，“合规”是很多甲方用户的核心需求，这我国网络安全产业也是主要依赖合规来驱动发展。合规是基础，但是在攻击者攻击手段多样化，攻击技术复杂化的背景下，客户所面临的安全风险仅通过合规来保障是不够的。

近年来，网络安全的红蓝对抗为人们安全观念和意识的转变带来了契机，红蓝对抗正在驱动网络安全从追求”合规”到追求”效果”的转变。随着红蓝对抗在各行业的展开，越来越多的组织的社会责任开始提升，真正产生了一些客户自身对网络安全的需求，即在保证“合规”的基础上，要防止遭受攻击威胁，保证业务服务的连续性。这种真实存在的安全需求正在转化为促进网络安全产业升级的巨大驱动力。

同时，随着云计算、物联网、移动互联网的普及，安全场景也在极大地扩展和丰富，网络安全建设不仅需要有效的

网络安全产品，更需要专业的安全服务。客户对安全咨询、技术服务、产品集成、安全运维、教育培训的需求将会进一步放大。随着网络安全整体解决方案的完善，将会有越来越多的客户希望获得融合了网络安全产品和服务的安全整体解决方案，来提升安全竞争力。

（二）场景逐渐固化和技术微创新将引导网络安全产业进入平稳发展期

网络安全技术和 IT 技术具有相伴相生性，随着近几年云计算、移动互联网、物联网等 IT 技术的逐渐成熟和应用场景逐渐固化，我们可以预见，与之对应的网络安全新概念和新技术的提出速度将逐渐趋于收敛，网络安全产业将随之进入一轮平稳发展期，这个阶段更考验企业的工程能力。

平稳发展中也会伴随着一些网络安全技术的微创新，改进传统网络安全产品，帮助其适应新场景下的安全需求，延长某些类型网络安全产品的生命周期。同时，在微创新的过程中，也可能会有一些原来场景适用的技术、产品被合并，但场景不会消亡。

未来，我们认为在数据安全、终端安全、安全管理、身份认证与访问管理等热点领域，将会有越来越多的技术微创新出现。

（三）网络安全市场竞争格局演变中将渐呈稳态

根据前面的分析数据推测，未来三年，我国网络安全整体市场仍会保持 20%左右的增速。随着市场空间不断扩大，网络安全市场中将出现新面孔。新进入者可能来自大型互联网公司，甚至是电信运营商，网络安全企业的概念将由此变得模糊，为数众多的企业的网络安全基因发生变化，将不再是“纯正”的网络安全企业。同时，网络安全的市场结构也在发生着改变，主要表现在传统网络安全市场增量趋势逐渐开始出现放缓的迹象，新兴应用场景（如，云计算、移动互联网和物联网）下的网络安全市场将出现高速增长。

新兴应用场景将加剧网络安全领域的碎片化趋势，但市场份额将逐渐集中在一些头部企业手中，网络安全产业将呈现明显的分层结构。国家队或者准国家队，大型网络安全企业，创新型网络安全企业和网络安全服务型企业将形成完整的产业生态，共同为提升我国整体网络安全水平付出努力。

（四）资本助力网络安全企业成长，也是头部企业竞争的重要手段

近年，网络安全产业创投领域活跃，资本对网络安全标的青睐有加，业内企业也开始拥抱资本。很多初创企业拿到了投资后快速成长，成为网络安全产业中不可忽视的新势力。随着科创板大幕拉起，一批符合条件的网络安全企业正

在 IPO 路上，未来在二级市场上将能够看到越来越多的网络安全企业。上市企业经营管理更加规范，公司治理能力加强，企业的融资渠道更多，这些将成为企业加速发展的重要基础。

过去几年里，头部企业之间除了在业务层面的竞争之外，也在资本市场上展开较量，通过对初创企业的投资并购，进行网络安全能力整合，构建产业生态。国资、互联网企业、大型网络安全企业频频出手，在资本维度布局展开竞争，争夺产业的战略制高点。资本将对产业整体竞争格局产生重要影响，资本运作也将成为网络安全企业竞争的重要手段。