



2019中国 网络安全发展白皮书

赛迪顾问股份有限公司

2019年02月

郑重声明

本报告的著作权归赛迪顾问股份有限公司(简称为“赛迪顾问”)所有。

本报告是赛迪顾问的研究与统计成果，其性质是供客户内部参考的业务资料，其数据和结论仅代表本公司的观点。

本报告有偿提供给购买本报告的客户使用，并仅限于该客户内部使用。购买本报告的客户如果希望公开引用本报告的数据和观点，在事先向赛迪顾问提出书面要求后，必须经过赛迪顾问的审核、确认，并得到赛迪顾问的书面授权。未经赛迪顾问的审核、确认及书面授权，购买本报告的客户不得以任何方式在任何媒体上(包括互联网)公开引用本报告的数据和观点，不得以任何方式将本报告的内容提供给其他单位或个人。否则引起的一切法律后果由该客户自行承担，同时赛迪顾问亦认为其行为侵犯了赛迪顾问的著作权，赛迪顾问有权依法追究其法律责任。

第1章 产业界定 01

02 网络安全产业界定

第2章 产业生态分析 03

04 政策环境

05 安全标准

07 安全事件

08 会议赛事

09 人才培养

10 产业布局

第3章 市场分析 11

12 市场规模

13 市场结构

14 云安全

15 物联网安全

16 移动安全

17 大数据安全

18 工业互联网安全

19 量子通信、商用密码

20 态势感知、威胁情报

21 区块链、人工智能

第4章 投融资分析 22

23 重要事件分析

24 整体态势分析

25 重点领域分析

26 投资轮次分析

27 赛迪网络安全潜力企业榜

第5章 展望新安全 28

29 展望新安全——市场

30 展望新安全——技术



01

产业界定

产业概念界定及产品全景图

从广义上讲，网络安全可以称之为网络空间安全，主要是指包括涉及到互联网、电信网、广电网、物联网、计算机系统、通信系统、工业控制系统等在内的所有系统相关的设备安全、数据安全、行为安全及内容安全。本报告所指网络安全产业主要是针对重点行业及企业级用户提供的保障网络可靠性、安全性的产品和服务。

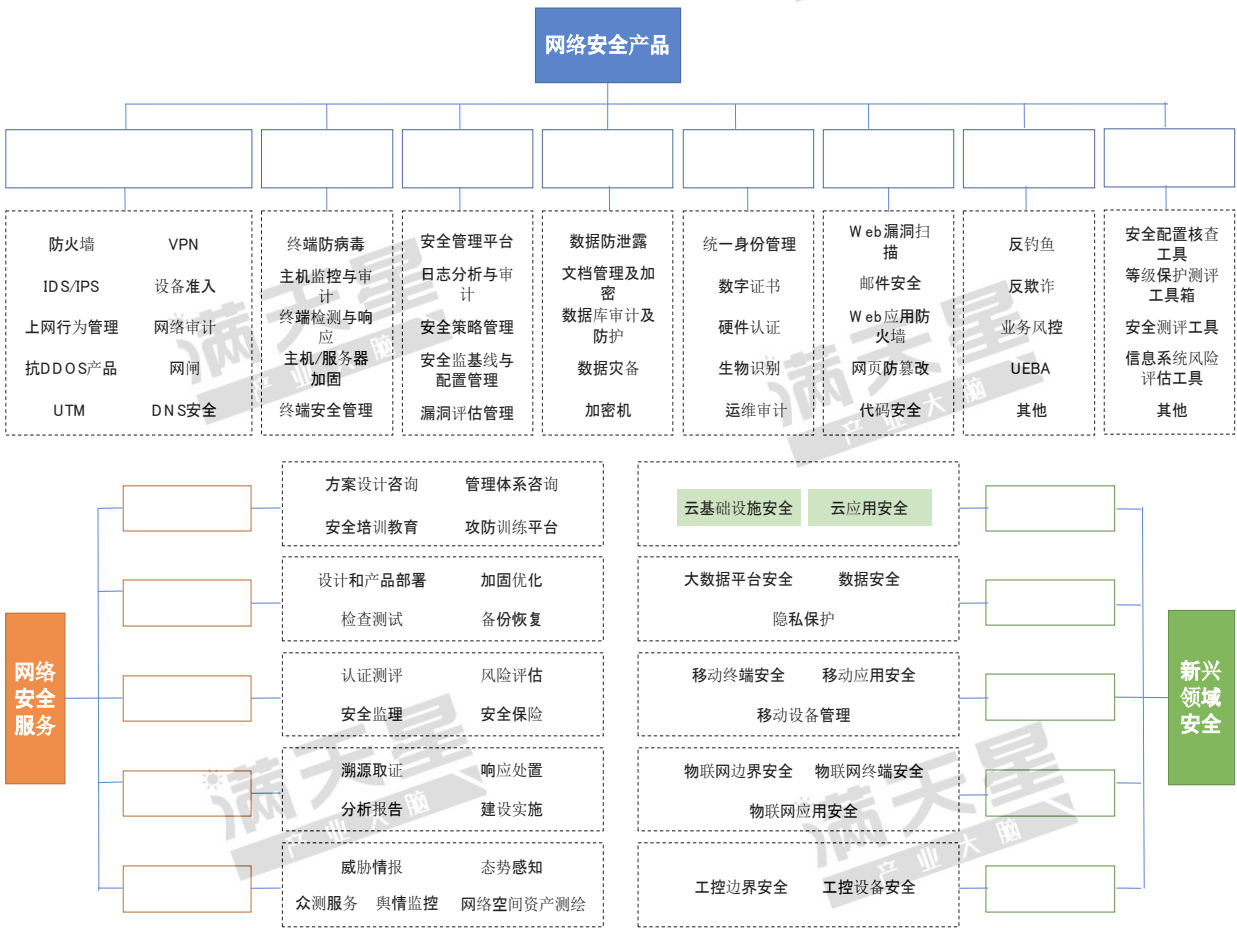
网络安全产业界定

概念界定

随着大数据、云计算、移动互联网、物联网的不断发展，网络的边界越来越模糊，安全形势也越来越复杂化，虚拟空间和实体空间结合的越来越紧密，网络安全的范畴发生了很大的变化。从广义上讲，网络安全可以称之为网络空间安全，主要是指包括涉及到互联网、电信网、广电网、物联网、计算机系统、通信系统、工业控制系统等在内的所有系统相关的设备安全、数据安全、行为安全及内容安全。

网络安全产业主要是针对重点行业及企业级用户提供的保障网络可靠性、安全性的产品和服务。主要包括防火墙、身份认证、终端安全管理、安全管理平台等传统产品，云安全、大数据安全、工控安全等新兴产品，以及安全评估、安全咨询、安全集成为主的安全服务。在网络安全市场规模测算中，未包含芯片及元器件相关制造业、舆情分析、军队、保密等领域的市场规模。

产品全景图



注：

- 网络安全市场中产品众多，并且功能特性相互交叉的情况较多，不同应用领域的产品会形成一定的重合。
- 本文涉及到的网络信息安全产业不包含安全芯片产业链、安全元器件的制造环节、军队及涉密产业等特殊领域。

02

产业生态分析

2018年中网络安全产业生态透视

2018年，网络安全政策逐步落地细化，标准紧密出台，网络安全事件频发，数据泄露事件仍为发生最为频繁的安全事件，网络安全市场的关注度也不断提升，国内安全大赛蓬勃发展、赛事水平持续上升，校企合作加快培育安全人才，全国各地区加快网络安全产业布局，产业集聚效应初显。

政策环境 国内外网络安全政策发展

● 国际

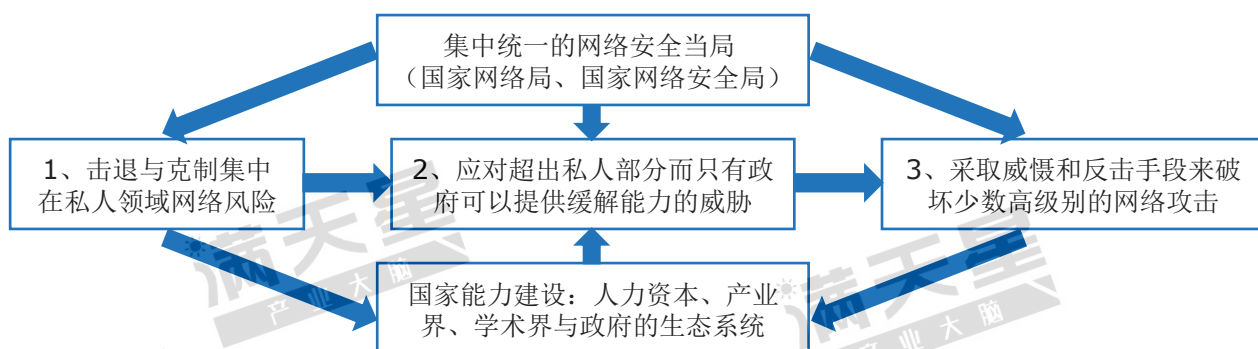
- 美国——在已基本建成的网络安全国家战略政策体系上，强化提升关键基础设施网络安全。

美国通过国土安全部（DHS）“网络安全与基础设施保护局”的重组与重新命名法案，该局将有权指定一名局长直接向DHS部长报告。2018年3月，美国众议院通过《2018DHS网络事件响应小组法案》，帮助保护关键基础设施免于遭受网络攻击；4月，发布《提升关键基础设施网络安全的框架》，该文件就是一份“用于关键基础设施安全风险管控的标准化实施指南”，标志着美国关键基础设施保护领域的重大进步；5月，DHS发布《网络安全战略》，该战略通过评估不断变化的网络安全风险，减少关键基础设施脆弱性，以达到保护关键基础设施的目的。

- 欧盟——提升欧洲整体网络安全水平，加强公民和企业对数字社会的信任程度。

2018年5月，《通用数据保护条例》正式生效，规定了所有欧盟公民所享有的数字生活中的权利，是世界范围内最完善严格的隐私保护规范；10月，欧盟通过《电子证据条例》，允许司法部门直接获取科技企业保存在域外的电子证据；此外成员国还将把《网络与信息安全指令》落实到国家法律中，这将提升公民和企业的网络安全意识，还将协助欧盟机构和成员国的政策制定和实施。

- 以色列——通过加强不同部门间的合作以提升网络安全，维持以色列作为全球网络安全强国地位。



● 国内

- 大数据、工业互联网和个人信息保护是2018年政策法规的重点关注领域。

2017年12月，工信部印发《工业控制系统信息安全行动计划（2018-2020年）》；信息安全标委会于2018年4月发布《大数据安全标准化白皮书（2018版）》，并于5月正式实施《信息安全技术个人信息安全规范》；2018年9月《个人信息保护法》被列入《十三届全国人大常委会立法规划》；10月《贵阳市大数据安全管理条例》正式通过并实施。随着监管法规条例、技术标准的落地，国内网络安全工作愈加有据可查、有法可依。

- 金融行业网络安全政策及标准相继出台。

2018年，中央网信办、证监会、中国人民银行等部门相继发布《关于推动资本市场服务网络强国建设的指导意见》《关于进一步加强征信信息安全管理的通知》《电子商务法》《关于开展支付安全风险专项排查工作的通知》《金融信息服务管理规定》等一系列政策法规，深入落实金融科技风险防控，重点加强金融业关键信息基础设施保护，不断提升金融网络安全水平。

安全标准 国内网络安全标准制定

● 国内标准

➤ 国内信息安全标准化研究虽起步较晚，但近年来信息安全标准制定进展迅速。

- 我国国家信息安全标准自1995年开始制定，至2002年共制定标准19项，全部由国际标准直接转化而来，截止到2014年2月，共发布214条信息安全国家标准。
- 2018年，全国信息安全标准化技术委员会归口的57项国家标准正式发布，将从2019年1月开始陆续实施，标准涉及工控安全、身份认证、加解密、数字签名、物联网安全等方面。
- 2018年1月，信安标委组织召开了人工智能安全标准化研讨会，大数据安全技术、标准和应用实践研讨会，数据安全合规与技术主题论坛，关键信息基础设施安全与实践论坛等。

2018年信安标委归口国家标准发布情况

编号	标准名称	实施时间	编号	标准名称	实施时间
1	《信息安全技术 公钥基础设施 数字证书格式》	2019-01-01	13	《信息安全技术 信息系统安全运维管理指南》	2019-04-01
2	《信息安全技术 证书认证系统密码及其相关安全技术规范》	2019-01-01	14	《信息安全技术 网络安全等级保护测试评估技术指南》	2019-04-01
3	《信息安全技术 密码设备应用接口规范》	2019-01-01	15	《信息安全技术 时间戳策略和时间戳业务操作规则》	2019-04-01
4	《信息安全技术 工业控制系统安全管理基本要求》	2019-01-01	16	《信息安全技术 网络用户身份鉴别技术指南》	2019-04-01
5	《信息安全技术 工业控制系统信息安全分级规范》	2019-01-01	17	《信息安全技术 信息技术产品安全可控评价指标 第1部分：总则》	2019-04-01
6	《信息安全技术 工业控制系统风险评估实施指南》	2019-01-01	18	《信息安全技术 信息技术产品安全可控评价指标 第2部分：中央处理器》	2019-04-01
7	《信息安全技术 工业控制系统现场测控设备通用安全功能要求》	2019-01-01	19	《信息安全技术 信息技术产品安全可控评价指标 第3部分：操作系统》	2019-04-01
8	《信息技术 安全技术 实体鉴别 第6部分：采用人工数据传递的机制》	2019-04-01	20	《信息安全技术 信息技术产品安全可控评价指标 第4部分：办公套件》	2019-04-01
9	《信息技术 安全技术 匿名实体鉴别 第2部分：基于群组公钥签名的机制》	2019-04-01	21	《信息安全技术 信息技术产品安全可控评价指标 第5部分：通用计算机》	2019-04-01
10	《信息安全技术 金融信息服务安全规范》	2019-04-01	22	《信息安全技术 网络安全监测基本要求与实施指南》	2019-04-01
11	《信息安全技术 政务和公益机构域名命名规范》	2019-04-01	23	《信息安全技术 可信计算规范 服务器可信支撑平台》	2019-04-01
12	《信息技术 安全技术 可鉴别的加密机制》	2019-04-01	24	《信息安全技术 数字签名应用安全证明获取方法》	2019-04-01

安全标准 国内网络安全标准制定

国内标准

2018年信安标委归口国家标准发布情况

编号	标准名称	实施时间	编号	标准名称	实施时间
25	《信息安全技术 公民网络电子身份标识安全技术要求 第1部分：读写机具安全技术要求》	2019-05-01	42	《信息安全技术 物联网感知层网关安全技术要求》	2019-07-01
26	《信息安全技术 公民网络电子身份标识安全技术要求 第2部分：载体安全技术要求》	2019-05-01	43	《信息安全技术 物联网数据传输安全技术要求》	2019-07-01
27	《信息安全技术 公民网络电子身份标识格式规范》	2019-05-01	44	《信息安全技术 网络攻击定义及描述规范》	2019-07-01
28	《信息安全技术 ICT供应链安全风险 管理指南》	2019-05-01	45	《信息安全技术 射频识别系统密码应用技术要求 第1部分：密码安全保护框架及安全级别》	2019-07-01
29	《信息安全技术 网络安全威胁信息格式规范》	2019-05-01	46	《信息安全技术 射频识别系统密码应用技术要求 第2部分：电子标签与读写器及其通信密码应用技术要求》	2019-07-01
30	《信息安全技术 基于可信环境的生物特征识别身份鉴别协议框架》	2019-05-01	47	《信息安全技术 射频识别系统密码应用技术要求 第3部分：密钥管理技术要求》	2019-07-01
31	《信息技术 安全技术 带消息恢复的数字签名方案 第3部分：基于离散对数的机制》	2019-07-01	48	《信息安全技术 物联网安全参考模型及通用要求》	2019-07-01
32	《信息安全技术 网络安全等级保护测评过程指南》	2019-07-01	49	《信息安全技术 灾难恢复服务能力评估准则》	2019-07-01
33	《信息安全技术 公民网络电子身份标识安全技术要求 第3部分：验证服务消息及其处理规则》	2019-07-01	50	《信息安全技术 指纹识别系统技术要求》	2019-07-01
34	《信息安全技术 智能卡安全技术要求（EAL4+）》	2019-07-01	51	《信息安全技术 病毒防治产品安全技术要求和测试评价方法》	2019-07-01
35	《信息安全技术 物联网感知终端应用安全技术要求》	2019-07-01	52	《信息安全技术 安全办公U盘安全技术要求》	2019-07-01
36	《信息安全技术 灾难恢复服务要求》	2019-07-01	53	《信息安全技术 密码模块安全要求》	2019-07-01
37	《信息安全技术 网络安全等级保护安全管理中心技术要求》	2019-07-01	54	《信息安全技术 物联网感知层接入通信网的安全要求》	2019-07-01
38	《信息安全技术 网络安全等级保护测评机构能力要求和评估规范》	2019-07-01	55	《信息安全技术 办公信息系统安全管理要求》	2019-07-01
39	《信息安全技术 鉴别与授权 访问控制中间件框架与接口》	2019-07-01	56	《信息安全技术 办公信息系统安全基本技术要求》	2019-07-01
40	《信息安全技术 IPSec VPN技术规范》	2019-07-01	57	《信息安全技术 办公信息系统安全测试规范》	2019-07-01
41	《信息安全技术 电子邮件系统安全技术要求》	2019-07-01			

安全事件 2018仍为信息泄露事件频发的一年

国际

2018年，数据泄露仍为发生最为频繁的安全事件，安全漏洞数量和严重性创下历史新高，黑客攻击、恶意软件等事件也愈发猖獗复杂。

- **VPNFilter木马爆发，全球超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。
- **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。
- **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。
- **瑞士数据管理公司Veeam暴露4.45亿条数据**
- **Veeam存储有超过200GB数据的数据库，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**
- **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。
- **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。
- **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。
- **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，其中包括微博、网易云音乐、QQ音乐、快手等主流应用。

2018年，国内网络安全事件每月都有发生，网络安全态势变得愈发复杂。数据泄露事件频发、攻击愈演愈烈、安全漏洞不断曝光、恶意软件肆意传播……企业与个人安全意识不足、安全投入不够更是加重了网络安全事件所带来的风险和造成的影响。

国内

2018年中国网络安全重点事件

时间	事件	形式
2018年6月	圆通10亿条快递信息遭泄露，并被发到暗网上兜售。	数据泄露
2018年7月	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。	数据泄露
2018年8月	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。	数据泄露
2018年2月	上海某公立医院HIS系统被黑客入侵，遭勒索2亿比特币。	攻击事件
2018年3月	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。	基础设施攻击
2018年1月	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。	安全漏洞
2018年8月	银行、移动支付APP存在短信验证码漏洞，易致资金盗刷。	安全漏洞
2018年8月	台积电感染勒索病毒WannaCry，致17.4亿元人民币损失。	勒索病毒
2018年12月	“微信支付”勒索病毒曝光，10万多台电脑被感染。	勒索病毒

会议赛事 2018网络安全相关会议赛事继续呈爆发态势

会议活动

2018年，网络安全会议活动频频举办，各级会议规模及影响力逐渐增加。据统计，2018年大大小小的安全会议活动有三百多场，会议活动参与度异常火爆，网络安全关注度不断提升。

2018年中国重要安全会议及活动

时间	会议 / 活动	时间	会议 / 活动
4月	4·29首都网络安全日	8月	2018网络安全分析与情报大会
4月	2018西湖论剑·网络安全大会	9月	2018年国家网络安全宣传周
5月	2018 C3安全峰会	9月	互联网安全大会（ISC 2018）
5月	2018宽·窄论坛——智能网络安全交流大会	9月	2018网络安全工程大会
6月	中国网络安全大会（NSC 2018）	10月	2018保密技术交流大会暨产品博览会
6月	2018中国工业信息安全高峰论坛	10月	2018网络安全发展趋势论坛
7月	2018中央企业网络安全与工业互联网交流研讨大会	10月	中科院计算机网络信息中心2018年用户大会暨技术交流
7月	2018中国网络与信息安全大会（CNISC）	11月	2018合肥网络安全大会
8月	2018中国网络安全年会	11月	2018中国（长沙）网络安全·智能制造大会
8月	2018网络安全生态峰会（ISS）	11月	全国网络与信息安全防护峰会（XDef 2018）
8月	互联网安全领袖峰会（CSS 2018）	11月	2018年网络信息安全科技创新技术交流大会

当前，国内安全大赛处于蓬勃发展、赛事水平持续上升阶段，随着网络安全形势的日趋严峻、人才缺口的不断扩大，安全大赛的市场需求仍将持续增加。2018年6月，中央网络安全和信息化委员会办公室、公安部联合发布了《关于规范促进网络安全竞赛活动的通知》，对网络安全竞赛活动提出了多项要求，以推动网安竞赛健康规范发展。

安全大赛

2018年中国重要网络安全赛事

时间	会议 / 活动	时间	会议 / 活动
4月	“强网杯”全国网络安全挑战赛	9月	“巅峰极客”网络安全技能挑战赛
4月	“360企业安全春秋杯”网络安全技术大赛	9月	“网鼎杯”网络安全大赛
5月	百度国际网络安全技术对抗赛（BCTF）	9月	2018年工业信息安全技能大赛
5月	“红帽杯”网络安全攻防大赛	10月	2018全国网络安全等级保护测评能力验证与攻防比赛
7月	2018年CNCERT恶意代码分析引擎比赛	10月	GeekPwn（极棒）2018国际安全极客大赛
7月	2018全国大学生信息安全与对抗技术竞赛	10月	“护网杯”2018年网络安全防护赛
7月	2018年WCTF世界黑客大师赛	11月	“天府杯”2018国际网络安全大赛
8月	2018中国网络安全技术对抗赛	11月	2018年军工网络安全攻防演练活动
9月	“蓝帽杯”全国大学生网络安全技能大赛	11月	XCTF网络攻防联赛
9月	2018年全国大学生网络安全知识竞赛	11月	腾讯信息安全争霸赛（TCTF）
9月	2018“黄鹤杯”RHG机器人网络安全大赛	12月	2017-2018全国高校信息安全铁人三项赛

人才培养 全球范围内网络安全人才仍是稀缺资源

高校

网络安全人才培养速度远跟不上快速发展的网络安全市场，市场缺口达到90%以上，因此，国家、高校、企业必须联合培养网络安全专业人才。

➤ 网络空间安全一级学科设立

- 2015年，教育部决定在“工学”门类下增设“网络空间安全”一级学科，全国共有160多所高校开设信息安全或网络空间安全专业；
- 2016年共有清华大学、北京交通大学、北京航空航天大学、北京理工大学、上海交通大学、哈尔滨工业大学等29所高校获得网络空间安全一级学科博士学位授权点。

➤ 积极探索实战型人才培养新模式

- 校企合作、联合育才：已经有近半数的高校开展校企合作育才实践，北航、北邮、哈工大等多所高校分别与360企业安全、绿盟、永信至诚、安恒等成立校企联合实验室；
- 网络安全大赛也日益受到重视，大学生网安竞赛举办频繁，每年均吸引大量学子参加。

截至2020年，中国网络安全人才需求量将达到160万人，每年网络安全专业毕业生人数仅为1万人，巨大的需求缺口需要通过专业的安全人才培训机构填补。

企业

➤ 构建人才实训基地，加强从业人员在职培训

- 蓝盾股份、美亚柏科、永信至诚等国内领先安全人才培训企业都在安全教学、实战训练、攻防演练等方面加以布局，全方位加强应用型人才培养。

➤ 人才供需集中于“北、深、上”

- 从地域范围来看，北京、深圳、上海、广州、杭州这五个城市是网络安全人才需求量最大的城市，北京、深圳、上海、西安、成都是求职者数量最多的城市。

国际

随着网络安全逐渐成为制约网络安全健康发展的瓶颈，世界各国已清楚认识到加强网络安全最关键的是人才，美国、欧盟等国家纷纷加强网络安全人才培养。

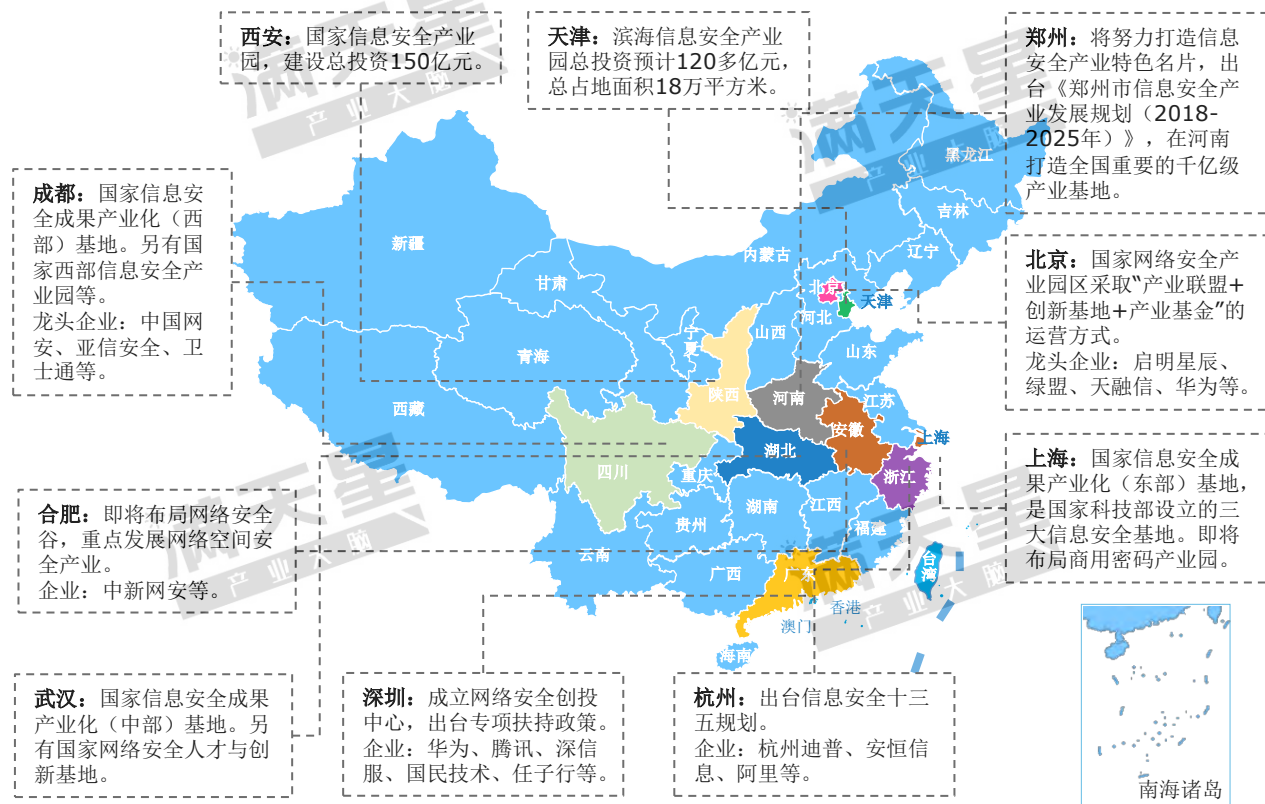
➤ 美国

- 拥有众多网络安全专业实力较强的高校，包括加州大学伯克利分校、麻省理工学院、斯坦福大学等，同时不断加强网络安全实验室建设，推进高校网络安全人才培养；
- 拥有世界权威的网络安全职业培训认证资质，包括国际注册信息系统安全师（CISSP）、国际注册信息系统审计师（CISA）等。

➤ 欧盟

- 通过建立认证培训方案，提升网络安全从业人员技能水平；加强研究生教育，扩展具有深度网络知识的专家库；
- 欧盟各成员国在欧洲网络和信息安全局（ENISA）的支持下，从2013年起每年组织一次网络安全月活动，以提升欧盟公民的网络安全意识。

产业布局 安全产业园成为发展重要载体



各地区加快网络安全产业布局，产业集聚效应初显

- 到2020年，北京市将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；
- 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）基地将集聚人才、技术和资源，促进产业成果转化；
- 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；
- 信息安全产业被四川省确定为五大高端成长型产业之一，四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；
- 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；
- 杭州先后发布并实施了《杭州市计算机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，助力网络安全产业持续发展。

03

市场分析

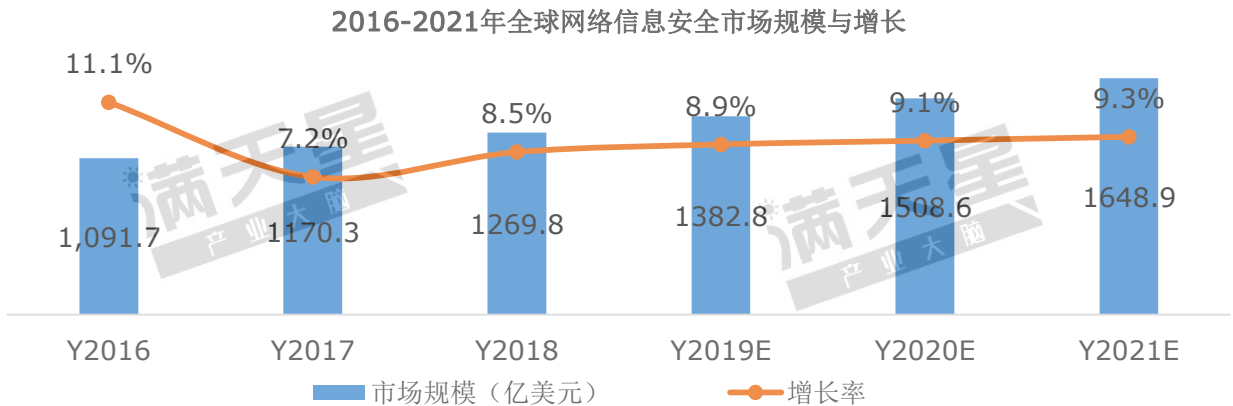
网络安全市场规模及热点分析

网络安全市场继续保持稳步增长，技术创新不断涌现，政府部门、重点行业在网络安全产品和服务上的投入持续增加，网络安全市场依然保持较高的发展势头。新兴领域安全逐步成为市场增量，随着5G与物联网的成熟建设，未来物联网安全、工业互联网安全等市场将迎来爆发。量子通信、商用密码、区块链安全等安全新技术也将快速发展。

市场规模

网络安全投入依旧是全球经济发展关注焦点之一

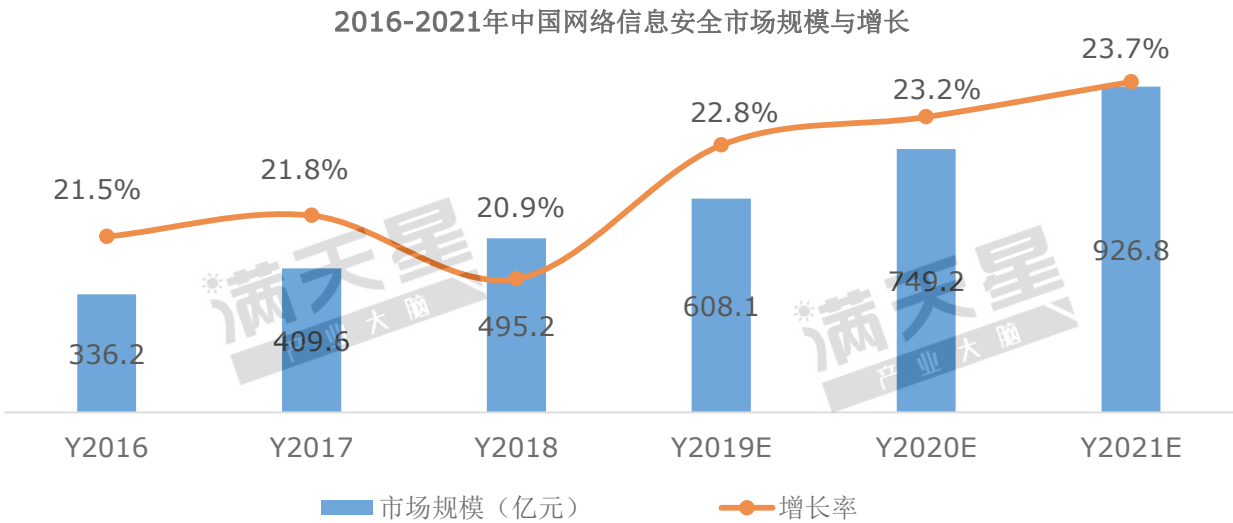
随着全球经济增长，数据安全和隐私问题将越来越重要。2018年，全球许多知名企业都遭遇了重大泄露事件，欧盟在2018年出台了一般数据保护条例，对个人信息保护及其监管达到了前所未有的高度，其他国家也正在讨论制定类似数据保护条例。赛迪顾问预测，未来几年中，随着5G、物联网、人工智能等新技术的全面普及，网络安全市场依然会保持稳定上涨的趋势，到2021年，全球网络信息安全市场将达到1648.9亿美元。



数据来源：赛迪顾问 2019，2

中国网络安全市场规模持续稳步增长

2018年，网络安全政策法规持续完善优化，网络安全市场规范性逐步提升，政企客户在网络安全产品和服务上的投入稳步增章，2018年市场整体规模达到495.2亿元。随着数字经济的发展，物联网建设的逐步推进，网络安全作为数字经济发展的必要保障，其投入将持续增加，赛迪顾问预测，到2021年网络信息安全市场将达到926.8亿元。



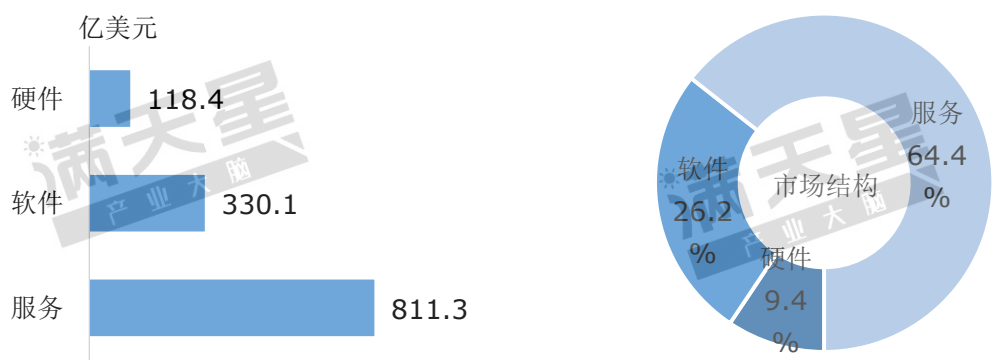
数据来源：赛迪顾问 2019，2

市场结构

全球网络安全市场依然以安全增值服务为主

随着网络攻击行为日趋复杂，防火墙、IDS等传统网络安全设备并不能完全阻挡恶意的网络攻击，构建全面的安全防护体系和制定完善的安全管理策略显得尤为重要，风险评估、安全管理咨询、安全应急响应、安全托管服务的作用越来越受到用户重视。在全球市场中，网络安全市场以提供订阅化服务为主，2018年，以安全服务市场份额最大，占市场的64.4%；软件市场规模为330.1亿美元，占整体市场的26.2%。

2018年全球网络信息安全市场产品结构

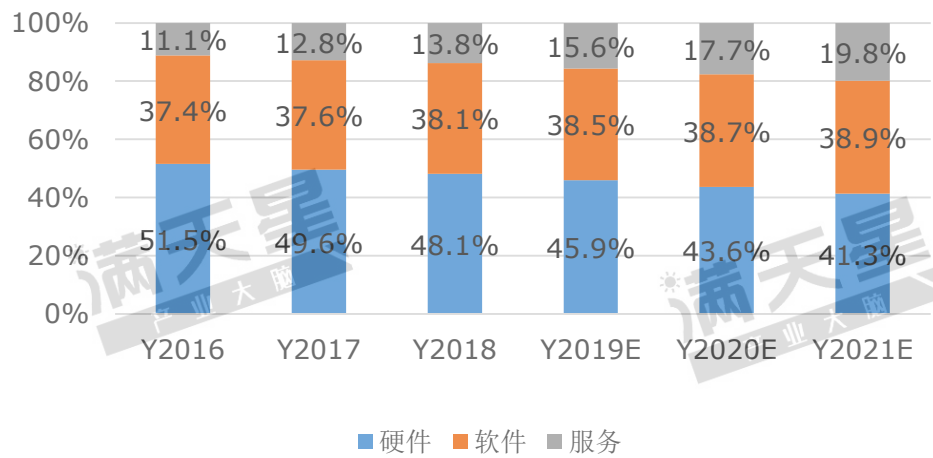


数据来源：赛迪顾问 2019，2

中国网络安全市场持续向服务化转型

在网络安全产业发展过程中，大多数是由合规需求驱动的，而近年来的灾难性攻击表明网络风险是重大威胁，企业开始把安全视为一项重要的商业风险，并且更看重网络安全服务的持续性。随着虚拟化及云服务理念的渗透，网络安全盈利模式将由软硬件产品向服务逐步转移。

2016-2021年中国网络安全市场结构



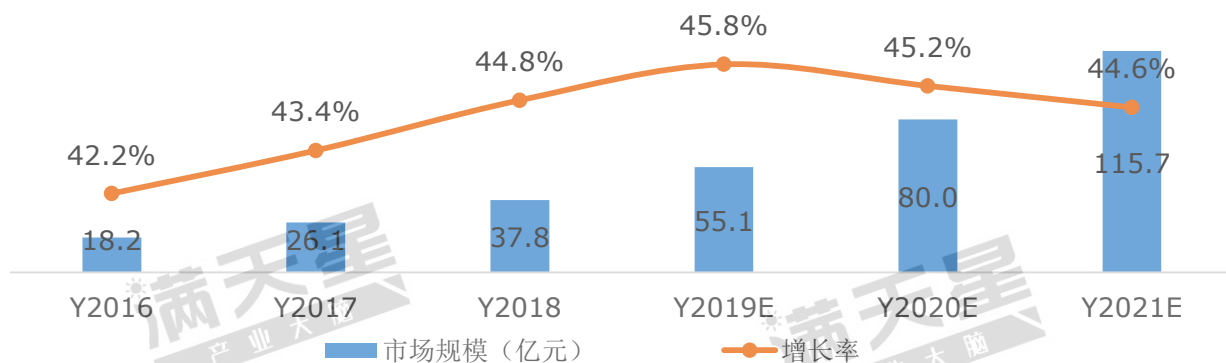
数据来源：赛迪顾问 2019，2

云安全

云安全市场规模

2018年，随着云计算产业的快速发展，云安全成为服务商和用户关注的焦点。虽然中国云安全市场目前仍处于起步阶段，但整体的市场规模会随着云计算市场规模的增长而快速崛起。2018年，中国云安全市场规模达到37.8亿元，增长率为44.8%。

2016-2021年中国云安全市场规模与增长



数据来源：赛迪顾问 2019，2

云安全市场特点



云计算——虚拟架构安全

➤ 纵深防御体系成为应对公有云安全威胁的重要手段

- 公有云的典型场景是多租户共享，但和传统IT架构相比，意味着可信边界的弱化，威胁的增加。因此，通过轻量级病毒防护、流量控制防火墙等多层防护构建基于云的纵深防护体系，联动大数据智能分析，实现智能联动精确抵御安全风险，全面防护云平台的数据安全。

➤ 云安全资源池、云工作负载保护平台等重点领域布局加速

- 结合安全服务链技术，将安全服务化，用户可以根据业务的安全策略需求，自定义安全访问路径，构建以软件定义安全为核心的云安全资源池；
- 众多厂商积极推动云工作负载保护平台在容器安全、微隔离、态势感知、EDR等能力拓展以及在多云环境的适配。

➤ 公有云安全防护领域发展态势持续向好，领域生态初步成型

- 阿里云云盾集成了DDoS防御、Web安全防御、主机安全防御等功能，借助云计算提供SaaS化安全服务，已积累了数十万规模用户；腾讯云提供主机安全、移动安全、业务安全以及应急响应支持等产品服务；蓝汛、网宿等企业也相继在云WAF、DDoS防御等领域发力，并积极利用大数据资源增强威胁情报能力。

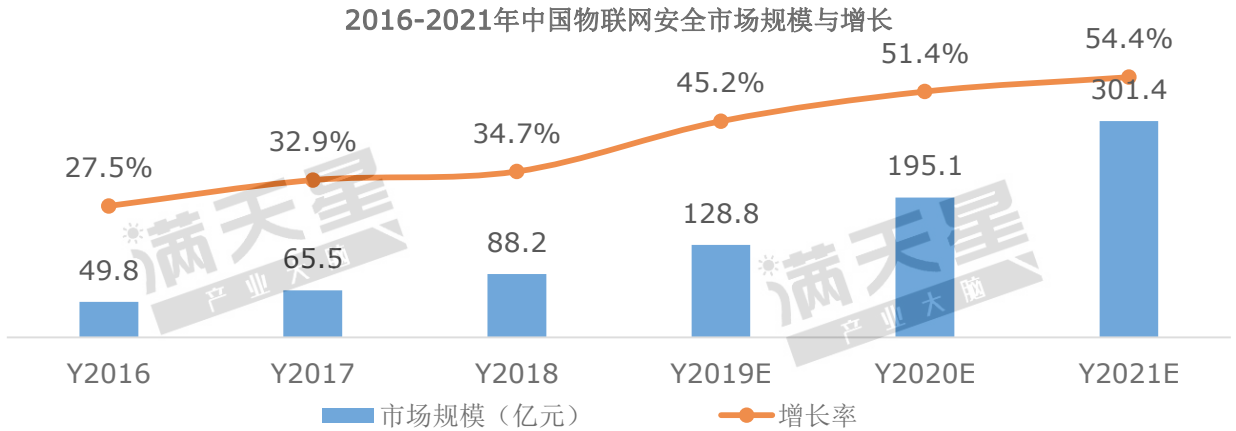
典型厂商



物联网安全

物联网安全市场规模

在“互联网+”时代，物联网发展迅猛，正加速渗透到生产、消费和社会管理等各领域，物联网设备规模呈现爆发性增长趋势，万物互联时代正在到来。物联网给我们的工作和生活带来便携的同时，也带来了风险。物联网安全事件从国家、社会、个人层出不穷，物联网设备、网络、应用面临严峻的安全挑战。物联网安全将成为万亿规模市场下的蓝海“潜力股”，2018年，我国物联网安全市场规模达到88.2亿元，增速达到34.7%。

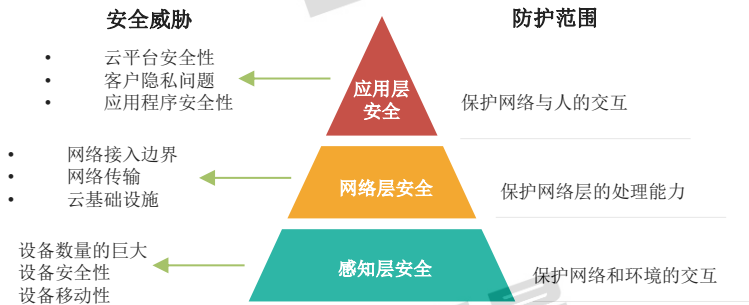


数据来源：赛迪顾问 2019，2

物联网安全市场特点

物联网安全防护是要实现物联网的感知层、网络层及应用层的安全问题。应用层安全主要涉及云平台安全性及客户隐私问题，要实现大数据安全以及对已有的安全能力的集成。网络层安全涉及到网络传入和基础设施以及边界安全的问题，应用层及网络层主要是基于传统的IT安全系统，大都可复用传统的网络安全防护技术。感知层的安全涉及到大量终端，是从终端感知节点到网关节点之间的安全问题，与传统安全技术不同，是未来关注重点。

物联网感知层功能单一，计算能力弱，缺乏安全防护能力，针对物联网终端的安全问题，一方面是终端设备生产环节就加入安全芯片和防护措施，另一方面增加物联网安全网关，实现对终端的安全防护。



物联网安全热点领域主要在车联网安全、智能家居安全、智能终端安全等。
典型厂商

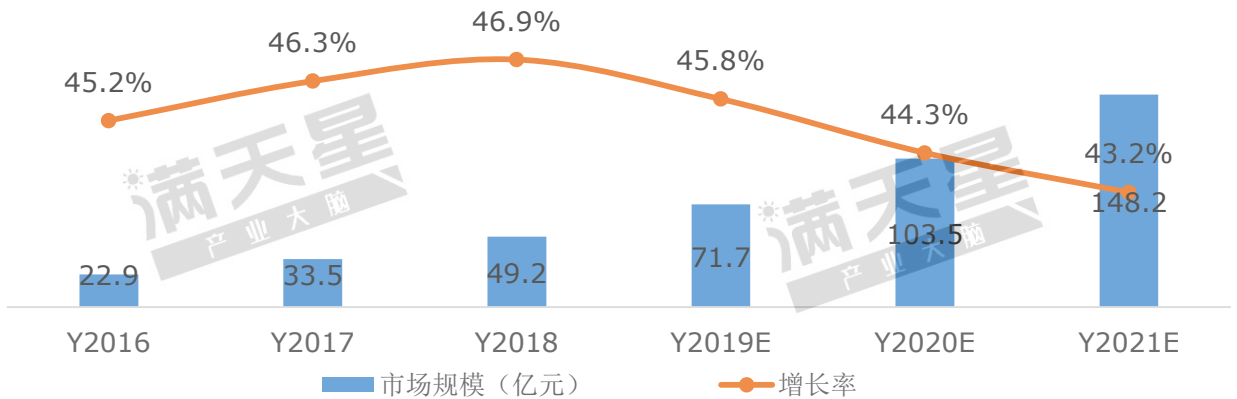


移动安全

移动安全市场规模

随着移动互联网的快速发展，移动互联网市场规模和用户数量持续高增长，移动电子商务、移动支付、社交网络等应用快速发展，而由此引发的信息安全问题也愈发突出。同时，由于移动互联网自身具有一定的特性，拥有独特发展方式与传播能力，更使得网络安全问题越来越受到人们的关注。近几年，我国移动安全市场呈现较强的增长趋势，2018年市场规模达49.2亿元，同比增长46.9%。

2016-2021年中国移动安全市场规模与增长



数据来源：赛迪顾问 2019，2

移动安全市场特点

随着移动互联网的发展及智能手机的普及，网络欺诈从PC端转移至移动端，近年来手机安全问题越来越严峻，各种网信犯罪层出不穷，严重威胁个人和企业的信息安全。

- 移动安全要以数据为核心，减少设备相关性
在移动设备中，数据的载体是应用，应用的载体是设备，数据传输的通道是网络，因此需要保护移动终端、应用及内容安全，实现以数据为核心的终端安全管理。此外，由于移动设备的可变性，移动安全管理过程中需减少设备相关性。
- 移动安全一定要保护最终用户的隐私
移动设备涉及到大量个人隐私，企业管理个人设备一定是会受到阻碍，因此移动安全必考虑解决如何保护最终用户的隐私，才能顺利推广使用。
- 移动支付飞速增长，移动金融安全不容忽视
近年来，全球移动支付高速发展，其中以支付宝、微信支付等为首的中国移动支付事业发展飞速。面对移动支付安全问题和漏洞的不断爆出，移动金融安全已经成为综合性的问题，不能单独由一个金融机构、支付类厂商或者安全服务提供商解决。

典型厂商

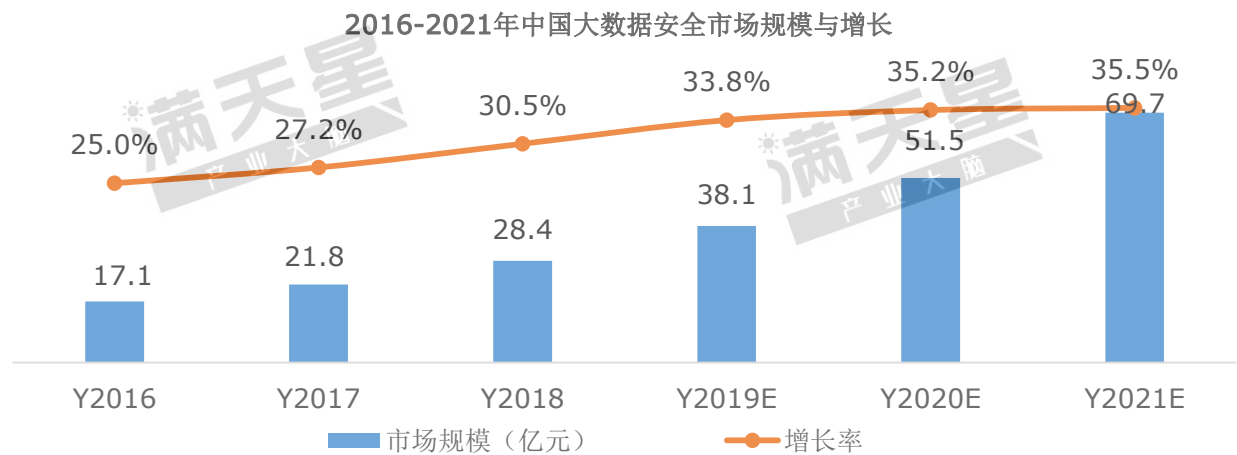


大数据安全

大数据安全市场规模

大数据安全是用以搭建大数据平台所需的安全产品和服务，以及大数据场景下围绕数据安全展开的大数据全生命周期的安全防护。大数据安全主要包括大数据平台安全、大数据安全防护和大数据隐私保护，产品主要包含大数据系统安全产品、大数据数据发现、大数据管理运营、敏感数据梳理、大数据脱敏、应用数据审计、大数据审计等。

近年来，中国大数据安全市场规模持续高速增长，受政策和各类数据泄密事件影响，市场规模快速上升。2018年的总规模达到了28.4亿元。随着大数据安全市场的成熟，年均增长率将逐步提高。当前，大数据安全业务已经被各大传统安全企业纳入未来企业战略布局重点和重要商业化盈利点。



数据来源：赛迪顾问 2019，2

大数据安全市场特点

- 大数据安全观念和技术落后于大数据发展
 - 密文计算技术的研究处在理论阶段，运算效率未达到实际应用的需求；
 - 数据血缘追踪技术未获得足够的应用验证，产业化仍需要一段时间；
 - 数字水印技术无法满足大数据环境下大量、快速更新的应用需求。
- 传统数据安全无法满足大数据安全需求
 - 大数据安全涉及到数据全生命周期的防护，需要从“以系统为中心的安全”转换到“以数据为中心”的安全思路上来；
 - 大数据场景下，企业内部组织结构不完善、内控制度不健全也会导致数据的泄露；
 - 数据复杂度大幅增加，数据存储形式、使用方式和共享模式均发生变化，无法适应大数据时代下的安全防护需求。

典型厂商



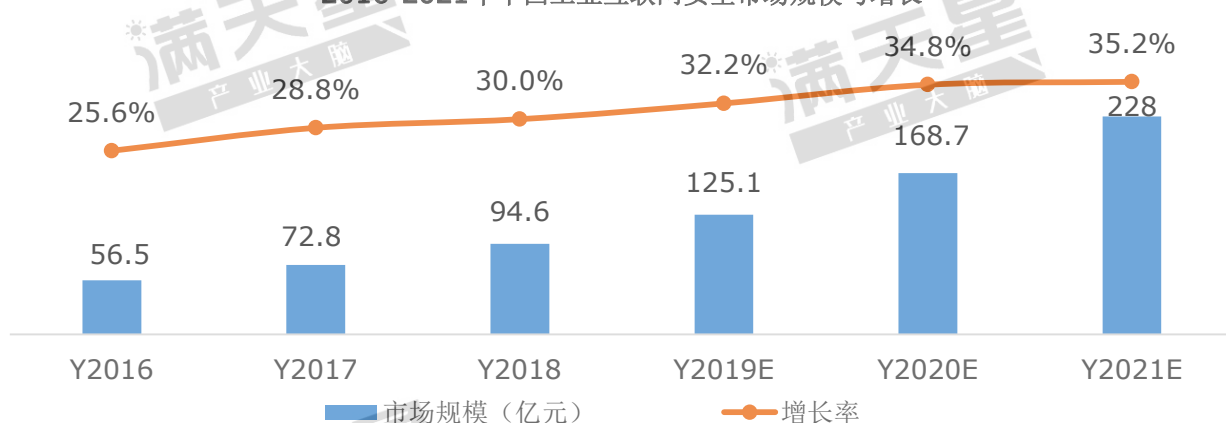
工业互联网安全

工业互联网安全市场规模

由于工业互联网推动企业IT和OT融合，因此工业互联网安全是工业生产安全和网络空间安全相融合的领域，包含了工业数字化、网络化、智能化运行过程中的各个要素、各个环节的安全，主要体现在工业控制系统安全、工业网络安全、工业大数据安全、工业云安全、工业电子商务安全、工业APP安全等。

2018年，对制造、通信、能源、市政设施等关键基础领域的攻击事件频频发生，受到攻击的行业领域不断扩大，造成后果也愈加严重，工业互联网安全的市场关注度随之提升。随着智能制造和工业互联网推进政策的不断出台，政府及企业开始逐步重视对工业互联网安全的投入，工业互联网市场具有较快的增长率。据赛迪顾问统计，2018年，中国工业互联网安全市场达到94.6亿元。

2016-2021年中国工业互联网安全市场规模与增长



数据来源：赛迪顾问 2019，2

工业互联网安全市场特点

根据《网络安全法》中关于关键信息基础设施安全技术措施“同步规划、同步建设、同步使用”的具体要求，需在工业互联网设计、建设、运维等全生命周期开展安全防护工作。我国工业互联网企业多采用传统信息安全防护技术，尚无面向工业互联网OT侧安全的专用防护设备，整体安全解决方案还不成熟，工业互联网平台数据安全风险隐患凸显。

➤ 工业互联网技术将从单点防御向纵深防御转变

工业互联网新技术新模式带来新的安全挑战，我国工业互联网安全产业亟待从“应急响应”转变为“持续响应”，需要建立多点防御、联合防御，与产业界合作开展防御响应。

➤ 企业级工业安全运营与监测将成为工业互联网安全建设重点

全球领先的工业互联网企业均在组建IT&OT融合的信息安全管理团队，建立企业工业安全运营中心，对整个工业控制系统进行安全监测和安全运营。

典型厂商



量子通信

在量子通信领域，我国量子保密通信应用建设进程加快，已初步形成量子保密通信产业生态体系，通信网络建设在全球处于领先地位，量子保密通信已经从基础研究开始向产业化大步迈进。

- 2017年9月29日，世界首条量子保密通信干线——“京沪干线”正式开通。
- 2017年以来，“宁苏干线”和“武合干线”等一批项目开始建设。
- 2017年11月，国家发改委规划在京津冀、长江经济带等重点区域建设量子保密通信骨干网及城域网，形成量子保密通信骨干环网。

产业链	上游	中游	下游
产业链环节	<ul style="list-style-type: none">量子保密通信核心器件制造商（光子源、光子探测器等）量子保密通信设备制造商（网关、交换机等）	<ul style="list-style-type: none">量子保密通信传输网络建设（光纤搭建、基础设施、网络设施等）量子网络运营与应用（量子通信网络运营、服务提供商等）	<ul style="list-style-type: none">量子保密通信行业应用（金融、军事、政务、商务等）
参与厂商			

商用密码

我国商用密码在密码算法、密码芯片和技术标准的研制上取得了突出成果，密码算法SM2、SM3、SM4、SM9已顺利成为国际标准，全国商用密码产品生产单位已近800家，已经形成了从密码算法到芯片到产品再到应用的完整产业链。



关键信息基础设施应当依照法律、法规的规定和密码相关国家标准的强制性要求使用密码进行保护，同步规划、同步建设、同步运行密码保障系统。2018年，中共中央办公厅、国务院办公厅印发《金融和重要领域密码应用与创新发展规划（2018-2022年）》，上海等地已经根据国家工作规划制定了当地相关的商用密码工作规划，金融和关键领域商用密码应用将成为热点。

- 金融领域
- 基础设施网络
- 数字经济
- 信息惠民密码应用
-

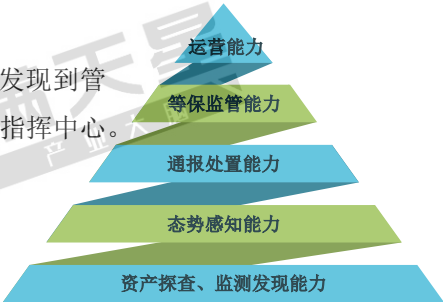
应用层	行业应用	金融	政务	工业控制	交通	通信	能源	其他	检测、测评、法律、法规、标准、保障层
	通用应用	安全电子邮件系统	电子印章系统	安全公文传输	权限管理系统	桌面安全防护	其他		
支撑层	密码服务	对称密码/公钥密码服务			咨询	培训	其他		
	密码产品	软件	芯片	模块	板卡	整机	系统		
资源层	应用技术	量子技术	云计算	大数据	人工智能	工业控制	物联网	其他	
	密码算法及协议	随机数生成算法			身份认证及密钥交换协议			其他	
		对称密码算法			公钥密码算法			杂凑算法	

态势感知

2018年，公安、网信、工信、政府等行业领域加快建设网络安全态势感知平台，加强关键信息基础设施保护与监测，全天候全方位感知网络安全态势。

态势感知平台可以为客户提供从底层的企业资产探查、监测发现到管理层的运营、分析及响应处置能力，构建主动防御体系的智慧指挥中心。

- 深度融合大数据和人工智能技术
- 系统可以动态扩展和云化
- 可以提供精准预测和防御处置建议



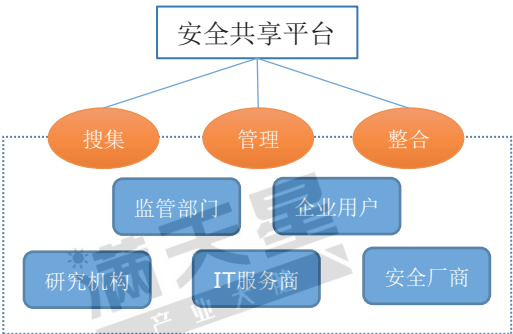
- 监管类行业态势感知——公安、网信等
 - 国家级态势感知平台，实现情报分析、统一指挥、溯源研判、通报响应等；
 - 各省市地级单位态势感知系统，感知地域整体态势、实现日常监控及案事件处理等；
- 关键信息基础设施保护类态势感知——电力、运营商、金融、大型央企、智慧城市等
 - 总部单位负责系统安全运营，安全检测、通报预警及态势感知；
 - 各下级单位形成安全运营，感知本单位态势，安全监测上报及协同防护等。



威胁情报

- 威胁情报作为网络安全的能力输出，有利于优化风险应对，及时响应处置，完善企业纵深防御体系。
 - 威胁情报可主动感知态势，发现新的攻击面；
 - 威胁情报提升检测能力，便于应对高级威胁；
 - 威胁情报有利于准确、快速判定，保障安全事件可以及时处置响应。
- 建设威胁情报共享平台，提升威胁情报能力，形成威胁情报生态体系，构建主动防御体系。

- 单一厂商无法提供全面准确的威胁情报，情报生产需要形成从厂商到行业用户的生态；
- 情报产生效用，需要从情报的采集、立即分析到响应处置一系列环境，需要多种安全能力支撑，需要情报生态的建立；
- 情报分析和研究，需要情报大数据支撑，建立情报共享平台，从而研究新的安全技术。



区块链+网络安全

在数字化转型浪潮的推动下，全面数字化识别成为未来的必然趋势，区块链作为记录并验证数字行为的一种技术，无论是保护数据完整性，还是利用数字化识别技术来防止设备免受DDoS攻击，都可以发挥关键作用。区块链技术其实可以为我们的数字服务构造更加值得信任的基础设施。

应用区块链可以解决很多网络安全问题，典型应用场景有：

- **利用身份验证保护边缘设备。**利用区块链来保护（工业）物联网设备的安全，并提升现有设备的验证、数据流和记录管理的安全性。
- **提升保密性和数据完整性。**区块链数据完整性服务有提供了全面的审计、兼容和可信赖数据服务来允许开发人员利用区块链平台来进行技术实现。
- **保护隐私信息。**使用区块链来保护社交媒体聊天软件的隐私通信数据。
- **可能取代PKI。**大多数PKI实现都依赖于集中的第三方证书颁发机构（CA）来发布、撤销和存储密钥对，在区块链网络中发布密钥可以消除第三方安全风险，并允许应用程序验证其他通信程序的合法身份。
- **构建更安全的DNS。**在区块链技术的帮助下，可以构建更加安全且受信任的DNS基础设施。
- **缓解DDoS攻击。**去中心化“记账”系统可以帮助用户抵御流量超过100Gbps的DDoS攻击。



人工智能+网络安全

随着网络攻击增多，危害程度上升，网络安全专业人才严重不足；“0 day攻击”等新型攻击形式日渐增多；攻击技术迭代的速度不断加快。因此，网络安全急需提供自动化解决方案，众多厂商开始讲人工智能与机器学习用于理解和响应来自网络和服务器的海量数据，进行自动化流量检测及行为分析等，区分系统或网络中的恶意行为。

➤ 人工智能要与其他算法相融合

- 传统的基于规则的方法在某些场景仍然十分有效
- 基于规则、特征、统计的方法要和AI形成互补的关系

➤ 人工智能要有持续进化的能力

- 人工智能算法要能够持续的检测新型威胁，需要不断被训练，靠的是不断的加入新的数据，以及攻防专家也需不断对算法和模型进行调优

➤ 人工智能与人要形成互补

- 在实践当中，攻防专家、数据科学家、安全服务专家应当与AI进行通力合作
- 攻防专家识别出安全问题，数据科学家对问题进行建模，安全服务专家对AI识别的结果进行过滤和反馈，实现AI的真正落地



04

投融资分析

网络安全投融资态势年度观察

从近几年的投融资案例金额来看，呈现出逐年上涨的态势，尤其是2018年投融资金额大幅上涨。网络安全、数据安全与云安全仍然是2018年市场关注的热点。随着全球安全态势越来越严峻，安全创新技术的演进，安全初创企业会不断涌现，网络安全行业依旧会受到投融资市场的持续关注。

重要事件分析 2018年网络安全领域投融资及并购持续升温

国际

2018年，全球网络安全融资并购事件频发，最大并购金额达到24亿美元，并购总体规模达到300亿美元，并购活动多发于美国，占比达到90%以上。

2018年，国外网络安全领域融资活动依然频繁，呈现出天使轮融资金额愈来愈大、企业IPO上市步伐持续稳定、初创公司融资金额稳步上升等特点，2019年对网络安全公司的大额投资活动仍将继续，IPO和并购市场热度仍将继续火爆。

热门领域包括区块链安全、云安全、IoT安全、数据安全等。

2018年全球网络安全领域重要投融资及并购事件

投融资及收/并购事件	金额	业务领域
思科并购Due Security	24亿美元	云安全
AT&T收购AlienVault	16亿美元	威胁检测
Blackberry收购Cylance	14亿美元	AI安全
Checkmarx Ltd.收购Custodela	1亿美元	软件安全架构
Thoma Bravo收购Barracuda	16亿美元	区块链安全
Vdoo完成A轮融资	1300万美元	物联网安全
Twistlock完成C轮融资	3300万美元	容器安全
Toka完成天使轮融资	1250万美元	网络安全防护
Opaq完成B轮融资	2250万美元	安全架构评估
Ledger完成B轮融资	7500万美元	区块链安全
Netskope完成F轮融资	1.69亿美元	云安全

2018年，国内网络安全领域企业总融资金额已达72.1亿元人民币，数倍于往年。云安全、移动安全、数据安全、工控安全与身份认证均为热门投资领域。

国内

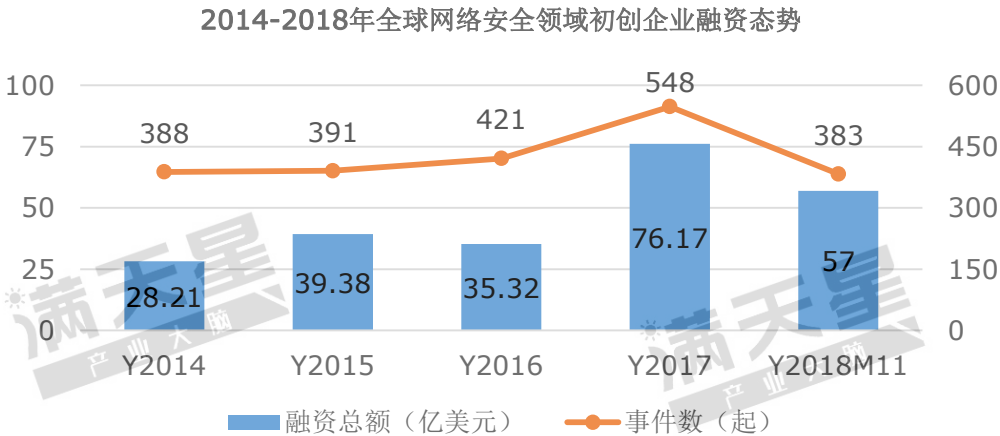
2018年中国网络安全公司重要融资事件

企业名称	融资金额	业务领域	企业名称	融资金额	业务领域
360企业安全	12.5亿元	全安全行业	芯盾时代	1.2亿元	身份安全
深信服	12亿元	网络安全、云安全	顶象技术	亿级	在线业务安全
白山云科技	3.3亿元	业务安全	安赛科技	1亿元	下一代IDS
壹进制	2.7亿元	容灾备份/数据安全	威努特	1亿元	工控安全
红芯	2.5亿元	安全浏览器	美创科技	亿级	数据安全
白山云科技	2.4亿元	云WAF	光通天下	1亿元	抗DDos
青藤云安全	2亿元	云主机防护	势必可赢	近亿元	身份认证
指掌易	2亿元	移动安全	天地和兴	8000万元	工控安全
DataVisor	亿级	业务安全	中睿天下	8000万元	攻击溯源
长亭科技	亿级	应用安全	椒图科技	8000万元	主机加固
安华金和	亿级	数据库安全	云杉网络	7500万元	流量分析
极御云安全	1.4亿元	云安全	四叶草安全	6700万元	应用安全
观安信息	1.3亿元	大数据安全	圣博润	6004万元	安全防护

整体态势分析 2018年中国网络安全领域投融资市场分析

01. 全球网络安全领域投融资态势良好

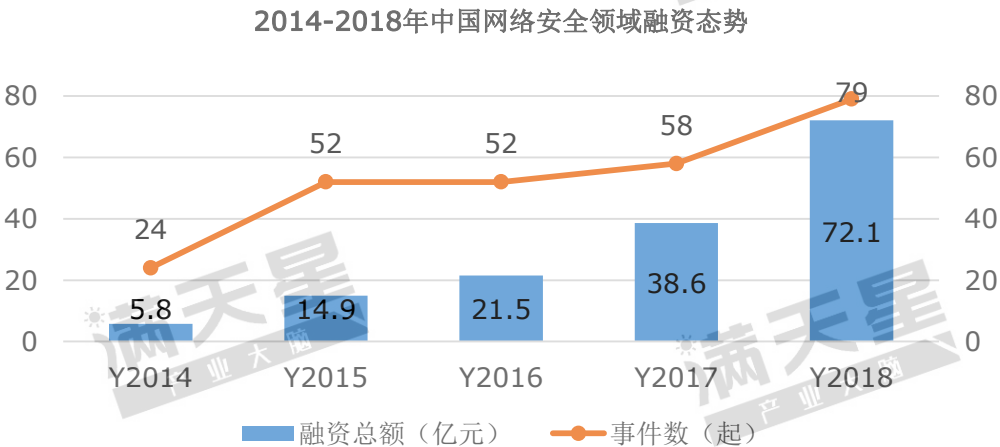
自2014年开始，全球网络安全投融资事件数逐年增长，交易金额持续上扬。截至2018年11月，全球网络安全领域初创企业投融资交易383起，共计57亿美元。随着全球安全态势愈发严峻，安全技术的持续创新，安全初创企业将会不断涌现，网络安全行业依旧会受到投融资市场的持续关注。



数据来源：CBINSIGHTS 2019, 2

02. 中国网络安全领域投融资金额和事件数均大幅增加

从近五年的中国投融资金额和交易数量来看，呈现出逐年上涨的态势，尤其是2018年二者均大幅增长。单笔融资金额不断上涨，亿级融资20起，千万级融资44起，百万级融资2起，这些都标志着2018年中国网络安全领域投融资依旧保持较高的市场热度。



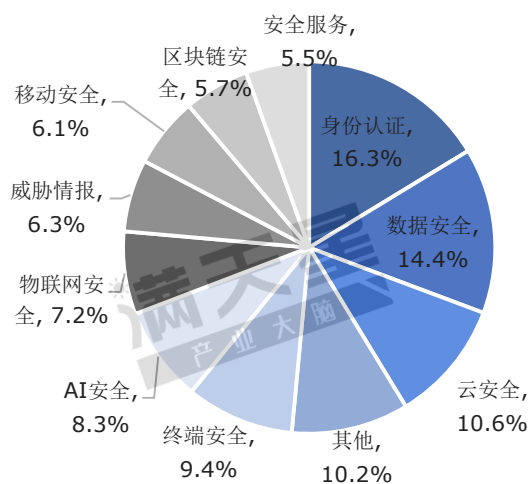
数据来源：赛迪顾问 2019, 2

重点领域分析 2018年中国网络安全领域投融资市场分析

03. 数据安全与云安全成为网络安全投融资重点领域

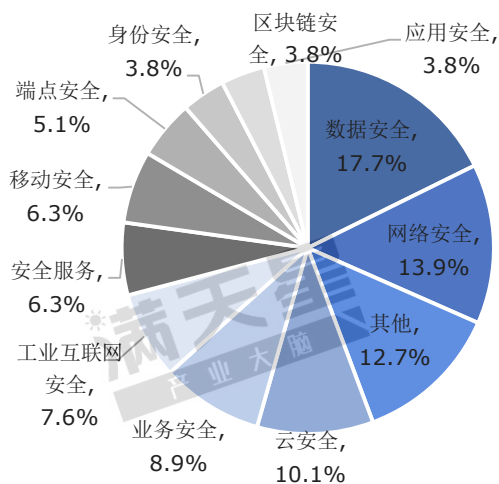
从细分领域来看，投融资事件主要集中在数据安全、云安全、工业互联网/物联网安全、移动安全等领域。全球数据安全领域重大投资交易超过40起，国内数据安全领域投融资也如火如荼，包括观安信息、中安威士、美创科技、云屏科技、安华金和等都在2018年获得数千万元融资。

2018年全球网络安全融资事件数量领域分布



数据来源：赛迪顾问 2019，2

2018年中国网络安全融资事件数量领域分布

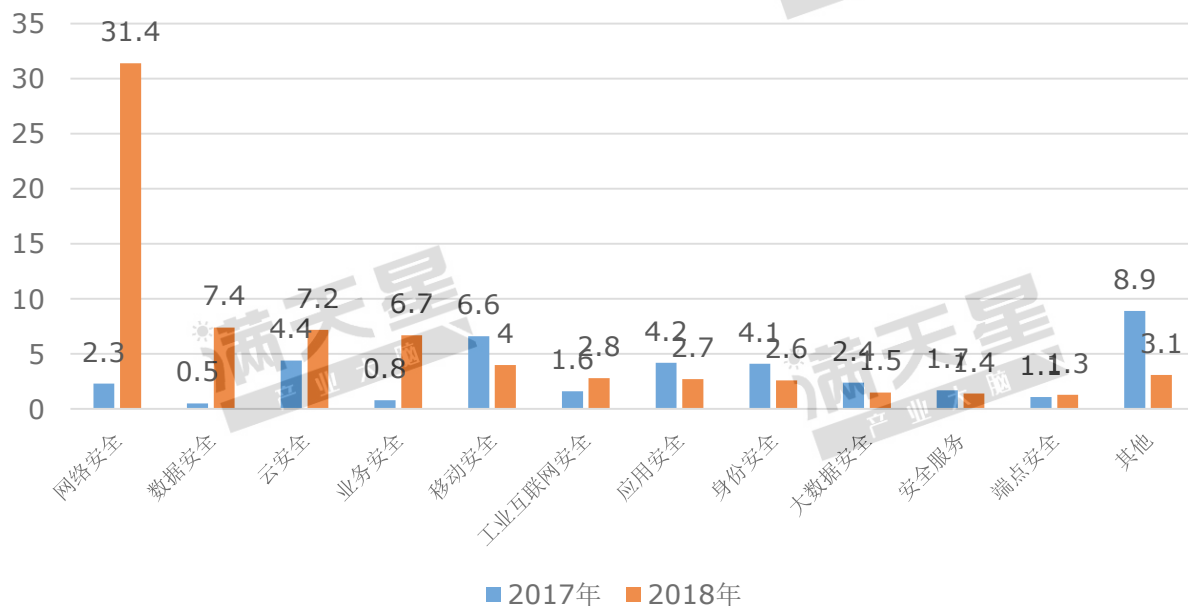


数据来源：赛迪顾问 2019，2

04. 网络安全与数据安全领域投融资金额较上年增长明显

对比2017年，网络安全、数据安全、云安全、业务安全领域融资金额均有不同程度的上涨。深信服IPO融资12亿元、360企业安全Pre-B轮融资12.5亿元致使网络安全领域2018年融资金额增长明显，人工智能等热点技术在数据安全、云安全、业务安全领域不断创新应用，导致上述领域也愈发受到资本市场青睐。

2017-2018年中国网络安全融资金额领域对比（单位：亿元）

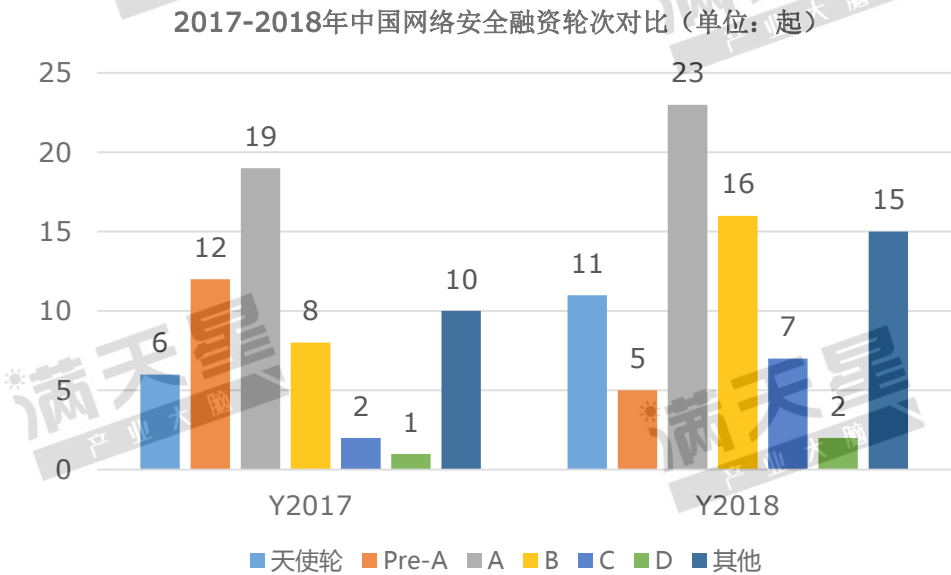


数据来源：赛迪顾问 2019，2

投资轮次分析 2018年中国网络安全领域投融资市场分析

05. A轮融资数量仍然保持最多优势

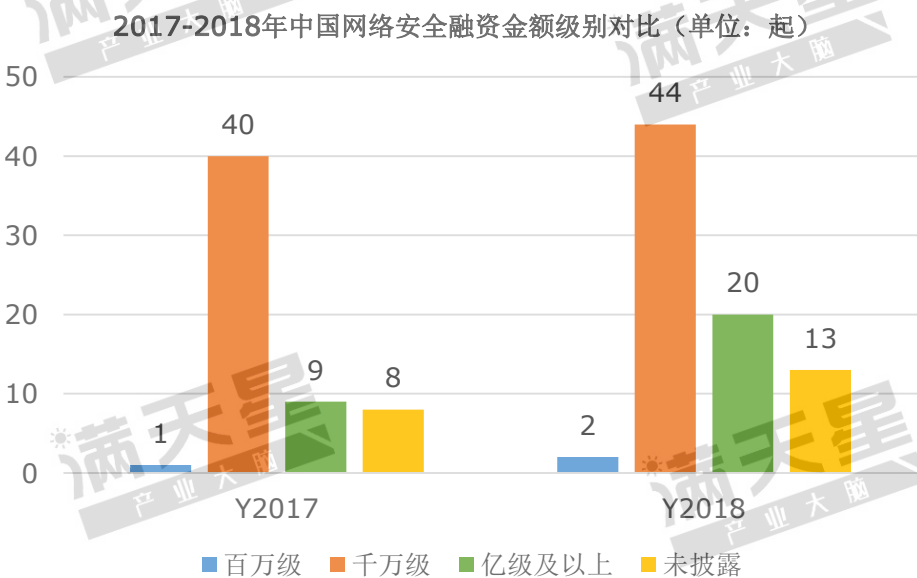
2018年，A轮融资数量依旧高于其他轮次，达到23起，B轮、C轮融资数量增长较快，共增长13起，天使轮仍然受到较高关注。



数据来源：赛迪顾问 2019，2

06. 网络安全领域投融资金额主要集中在千万级

2018年，各金额级别融资数量均有不同程度增长，尽管融资金额亿级及以上的数量增长较快，但是千万级仍然为全年融资主力，占半数以上。



数据来源：赛迪顾问 2019，2

赛迪网络安全潜力企业榜

赛迪网络安全潜力企业排行榜通过建立评判指标体系，从经营情况、技术创新、融资热度、市场吸引力、产品能力、商业模式、竞争优势等多个维度进行定量与定性相结合的评比，最终经过专家打分，对中国未上市的网络安全企业进行排名对比，评选出赛迪网络安全最具潜力的前80强企业。

2018年赛迪网络安全潜力企业榜80强

排名	企业简称	主营业务	排名	企业简称	主营业务
1	360企业安全	综合安全	41	美创科技	数据安全
2	亚信安全	综合安全	42	上讯信息	终端安全
3	安恒信息	综合安全	43	同盾科技	风控反欺诈
4	山石网科	综合安全	44	卫达安全	动态防御
5	迪普科技	综合安全	45	安全狗	云安全
6	恒安嘉新	综合安全	46	志翔科技	大数据安全
7	中新网安	网络安全	47	默安科技	云安全
8	知道创宇	云安全	48	数字观星	大数据安全
9	安天	智能安全	49	安赛科技	下一代IDS
10	梆梆安全	移动安全	50	四叶草安全	应用安全
11	安博通	网络安全	51	盛世光明	上网行为管理
12	永信至诚	安全培训	52	海天伟业	工控安全
13	明朝万达	数据安全	53	力尊信通	应用安全
14	爱加密	移动安全	54	长亭科技	应用安全
15	优炫软件	数据安全	55	杰思安全	终端安全
16	威努特	工控安全	56	溢信科技	内网安全
17	信安世纪	身份认证	57	华盖科技	安全防护
18	瀚思科技	大数据安全	58	火绒安全	终端安全
19	通付盾	云安全	59	势必可赢	身份认证
20	微步在线	威胁情报	60	东翼科技	APT攻击
21	安华金和	数据库安全	61	兰云科技	安全管理
22	圣博润	终端安全	62	安点科技	工控安全
23	盛邦安全	Web安全	63	派拉软件	身份安全
24	国舜科技	业务安全	64	中睿天下	溯源取证
25	芯盾时代	身份安全	65	观数科技	大数据安全
26	指掌易	移动安全	66	有云信息	WAF
27	青藤云安全	自适应安全	67	网思科平	终端安全
28	天懋信息	大数据安全	68	竞远安全	安全服务
29	上海观安	大数据安全	69	数美时代	大数据反欺诈
30	天空卫士	数据安全	70	墨云科技	云安全
31	交大捷普	安全防护	71	斗象科技	众包安全测试
32	山谷网安	安全服务	72	天际友盟	威胁情报
33	众人科技	身份认证	73	卓识网安	安全测评
34	天地和兴	工控安全	74	九州云腾	云安全
35	科来	网络流量分析	75	世平信息	数据安全
36	亿赛通	数据安全	76	联软科技	访问控制
37	顶象技术	业务安全	77	杭州邦盛	金融反欺诈
38	炼石网络	云安全	78	威胁猎人	业务安全
39	椒图科技	云安全	79	盛华安	态势感知
40	白山云科技	业务安全	80	长扬科技	工控安全

数据来源：赛迪顾问 2019，2

05

展望新安全

中国网络安全发展趋势分析

在数字化转型浪潮推动下，网络安全将持续增加投入，市场关注度将持续上升。在万物互联的推动下，工控及物联网的安全产品市场迎来爆发点。重点企业开始探索海外市场，实现市场增量。从技术上将，网络安全产品和技术呈现自动化、平台化、服务化和融合化的趋势，提升产品技术能力，创新产品商业模式。

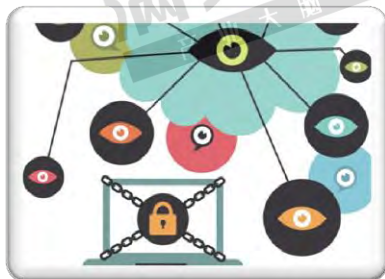
展望新安全——市场

中国网络安全与信息化建设投入占比逐年提升



2019年,《网络安全等级保护条例》《国家关键信息基础设施安全保护条例》《商用密码法》等网络安全领域重要政策法规将陆续出台,将为网络安全市场增长提供强势合规性驱动。另外,数据泄露的频发导致中小企业自身安全意识也在不断提升,这将间接促使企业愈加重视安全投入。交通、能源、制造等行业也开始加大网络安全投入,从而保障业务安全,推动业务发展。由此看出,中国网络安全与信息化建设投入将逐年提升。

市场范围不断扩展,增量市场日益延伸



随着5G落地、企业上云步伐的加速,网络安全与云计算、大数据、物联网等新兴技术的融合也愈发深入,物联网安全、云安全、工业互联网安全市场潜力巨大,未来三年三者复合增长率均达到30%以上,高于网络安全整体市场规模增速。此外,网络安全龙头厂商也在积极布局欧、美、日等发达国家与一带一路沿线国家市场,通过加强各国家区域安全合作,形成网络安全体系生态。企业开始不断寻求增量市场,网络安全市场范围不断扩展。

网络安全市场集中度将会不断提升



随着云服务的发展以及网络安全行业运营服务模式转型,网络安全对公司的产品、技术和综合服务能力要求将大幅提升,行业竞争门槛提升,市场份额将不断集中。国内的龙头企业也将通过并购创新型企业不断的抢占市场,与其他的安全厂商拉开距离。当然,网络安全领域特殊的市场需求也会允许中小型企业不断提升自身技术能力,在其专精领域存在及发展壮大。

构建安全可控的信息技术体系



当前,国内已经形成了以“国产CPU+基于开源Linux的国产操作系统”的自主生态,但是上下游各环节协同不够,自主生态并不完备,仍有漫长的路要走。未来着力方向需整合资源,形成核心技术发展合力;前瞻布局,抢占下一代信息技术发展至高点;创新驱动,突破产业链关键环节;应用牵引,培育核心技术产业生态。

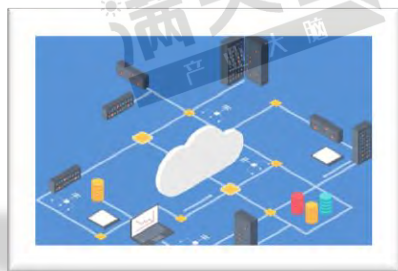
展望新安全——技术

自动化：安全数据实现自动化智能分析及响应



对海量安全数据进行攻击画像、威胁建模、情报匹配等自动化分析，形成完整威胁杀伤链可视化溯源，从而提升威胁发现与处置效率。从传统安全问题的人工处理分析到利用智能化技术自动从海量信息中寻找可疑数据，进行人工智能分析评判，分析人员快速判断结果是否正常，最后将新威胁迅速进入情报体系，并进行自动化响应处置。

平台化：多层面打造能力平台，多维协作构建完备安全体系



通过将威胁情报、态势感知、云安全、统一认证、安全大数据分析等安全能力平台化，从不同维度对安全数据进行深加工，并以接口方式对外提供能力，从而对业务系统、安全工具以及外部系统进行支撑，加深安全对业务的深度融合与互补，最终形成平台经济效益。

服务化：创新商业模式，开拓安全服务新阶段



由于网络形态的转变、用户需求方式的转变，网络安全领域开始寻求商业模式的创新，网络安全产品加速向包括云安全在内的服务形态转型。安全云服务化、安全驻场运维服务、第三方安全独立运营、情报订阅及高级安全分析服务、仿真模拟市场等都成为服务化转型的新模式。

融合化：加速新技术融合，创新安全防护方法



传统的网络安全技术开始与新技术进行融合，加速技术创新，寻求安全防护新方法。利用区块链的去中心化和不可篡改性创新安全业务场景，利用数字化识别技术来防止设备免受DDoS攻击，都可以发挥关键作用。量子技术作为保密通信的创新模式，我国已初步形成量子保密通信产业生态体系，已经从基础研究开始向产业化大步迈进。



扫描下载更多报告

满天星·产业知识分享平台

☎ 010-88559043

🌐 www.mtx.cn

覆盖行业 100+ 个

产业数据 1000 万+ 条

汇聚专家 1000+ 位

研究报告 10000+ 本

注册会员 100 万+人