CAICT 中国信通院

中国网络安全产业白皮书

（2018 年）

中国信息通信研究院

2018年9月

版权声明

本白皮书版权属于中国信息通信研究院，并受法律保护。转载、摘编或利用其它方式使用本白皮书文字或者观点的，应注明“来源：中国信息通信研究院”。违反上述声明者，本院将追究其相关法律责任。

前　言

坚实的网络安全产业实力，是网络空间繁荣稳定、保障有力的前提和基础。习近平总书记在全国网络安全和信息化工作会议上强调，要树立正确的网络安全观，积极发展网络安全产业，做到关口前移，防患于未然，对新时代我国网络安全产业发展提出更高要求。

近年来，网络安全产业步入发展的崭新阶段。产业规模快速增长，2017年我国网络安全产业规模达到439.2亿元，较2016年增长27.6%，预计2018年达到545.49亿元。企业数量明显增加，从事网络安全相关业务的企业数量达到2681家，上市安全企业（含新三板）近百家，超过120家安全创新创业企业获得融资支持。产业层次逐渐丰富，安全龙头企业纵深发展，专业创新厂商深耕前沿领域，IT运营商、设备商积极推动网络安全应用实践，夯实关键信息基础设施安全保障。

本白皮书是我院第三次发布网络安全产业白皮书，延续了从规模结构、政府政策、企业发展、技术进展、人才培养等维度对国内外产业进展跟踪分析，同时结合热点趋势，重点对身份管理与访问控制、可管理安全服务、云安全、威胁情报服务、“人工智能+安全”五个领域进行了分析预测，最后对产业发展前景进行了展望，希望为关注网络安全产业发展的企业、政府机构以及相关单位提供参考和帮助。

在本白皮书的研究过程中，得到以下单位的支持协助，在此表示感谢：北京启明星辰信息安全技术有限公司、上海观安信息技术股份

有限公司、北京神州绿盟信息安全科技股份有限公司、杭州安恒信息技术股份有限公司、北京天融信网络安全技术有限公司、亚信科技(成都)有限公司、360企业安全集团、深圳市腾讯计算机系统有限公司、北京微智信业科技有限公司、杭州默安科技有限公司。

CAICT 中国信通院

目 录

一、网络安全产业总体形势

（一）网络空间安全形势日趋复杂严峻

近年来，网络空间安全形势快速变化，国家级博弈更为凸出、攻防对抗更为激烈、数字经济安全保障要求不断提升，网络安全形势演变对网络安全产业发展产生深刻影响。

1. 国际网络空间竞争博弈进入深水区

自 2015 年美国战略核心从“全面防御”调整为“攻击威慑”以来，各国在网络空间主导权、话语权争夺更加激烈。**一是**国际网络空间规则制定进程“道阻且长”。2017 年 4 月，七国集团首次统一网络安全外交立场，发布《网络空间国家责任宣言[1]》，重申关于动网和动武、自卫权的观点。2017 年 6 月，在联合国信息安全政府专家组（UNGGE）会议上，美及其盟友力图将《武装冲突法》引入网络空间，与其他国家存在严重分歧，最终 25 国代表未能就网络空间行为规范形成共识。**二是**网络军事力量建设步入强体系、扩规模、提能力新阶段。美国于 2017 年 8 月将网络司令部升格为一级作战司令部，其下属的 133 支网络任务部队已具备作战能力；美国国防部在 2018 年 7 月发布 4580 万美元的采购计划，拟开发武器系统“网络航母”，辅助网络部队执行情报侦察、网络攻击等行动；“2019 财年国防授权法案”明确了网络威慑的路径和战略对手，给予美国防部发起军事网络行动授权。英国在 2017 年首次在联合军事行动中使用了网络攻击、

[1] G7 Declaration on Responsible States Behavior in Cyberspace，http://www.g8.utoronto.ca/foreign/170411-cyberspace.html

干扰等网络能力。以色列在 2017 年 12 月将国家网络安全局和国家网络局合并成立国家网络指挥部，并拟增加网络安全预算至国内生产总值（GNP）的 0.2-0.3%。日本拟发布新版《中期防卫力量整备计划》，将在 2019 年至 2023 年间，新设统筹太空及网络空间专业部队的司令部，增强自卫队“网络防卫队”的规模和能力。

2. 网络攻击智能化、自动化、武器化趋势蔓延

人工智能等新技术的应用、网络武器泄露的延续效应，正在逐渐转变网络攻击的逻辑和手段，“攻防不对等”形势更为严峻。**一是**攻击技术越发先进智能。人工智能等新技术以及社会工程理念驱动网络攻击智能化发展，攻击手段在潜伏性、隐蔽性、定向性、自主性、融合性等方面能力日益增强，智能分析使得快速绕过多重防御手段成为可能。**二是**自动化攻击时代悄然来临。根据安全公司 Distil Networks 发布的《2018 恶意机器流量报告[2]》，2017 年全流量中 21.8%为恶意机器流量，较上一年增长 9.5%，其中，高级别恶意机器流量（Advanced Persistent Bots，APBs）占比高达 74%。相对于一般的恶意流量，高级别恶意机器流量通过使用模拟器、伪造流量器环境、变换 IP 地址等方式，实现更好的隐蔽性，通过机器实施的自动化攻击日益成为主流。**三是**网络武器研发和利用提速，潜在危害影响加深。2017 年 5 月，WannaCry 勒索病毒爆发，全球 150 多个国家、20 多万台电脑受到影响，累计损失高达数十亿美元，展示了网络武器的空前威力。

[2] 2018 Bad Bot Report，https://resources.distilnetworks.com/white-paper-reports/2018-bad-bot-report

WannaCry 勒索病毒利用的微软操作系统安全漏洞“永恒之蓝”，是方程式组织（Equation Group）为美国中央情报局开发的专用工具。目前，美国中央情报局掌握的千余种网络武器或已泄露，并向不可控的方向发展。这一事件，一方面将进一步催化全球网络武器研发进程，美国将加强网络武器研发和列装以进一步扩大与其他国家的技术“代差”，其他国家则将对标美国的网络武器储备展开研发竞赛，力求抢占网络攻防高地；另一方面，网络武器攻击范围广、速度快、破坏性大，行动隐蔽性好、效费比高、非对称性强等特点，也将激发各种黑客组织、恐怖主义势力加速对网络武器的融合利用，成为威胁网络空间安全的严峻风险。

3. 数字经济发展对网络和数据安全提出更高要求

当前，新一轮数字化浪潮已经到来，全球数字经济蓬勃发展，成为驱动经济增长的新引擎和世界各国竞争的新高地，与此同时，网络安全的基础保障作用和发展驱动效应日益突出，成为关系数字经济发展的根基所在。一是数字基础设施建设加速安全威胁传导渗透，催生了融合领域网络安全保障新需求。随着传统产业数字化、网络化、智能化转型步伐加快，网络安全风险逐渐向智慧医疗、金融科技、车联网、工业互联网等融合新兴产业蔓延。例如，在医疗领域，今年 1 月，美国医疗机构 Hancock Health 遭到勒索软件 SamSam 攻击，支付 5.5 万美元赎金；8 月，勒索病毒 Globelmposter 来袭，多家大型医院中招。在金融领域，2 月，日本加密货币交易所 CoinCheck 遭到非法入

侵，黑客窃取了价值 5.3 亿美元的数字货币，导致比特币市场震荡；8 月，继荷兰三大银行 1 月遭受 DDoS 攻击后，西班牙央行遭受 DDoS 攻击致使网站和业务瘫痪。**二是**数据作为数字经济的根本要素，安全形势不容乐观。互联网平台汇聚海量用户数据，随着数据价值的不断提升，用户个人信息泄漏和非法利用、数据非法跨境流动等风险不断增大，各类恶性事件频发。根据 Verizon 发布的 2018 数据泄露报告，2017 年全球发生的 53000 件网络安全事件中，有 2216 起确认数据泄露。2018 年 3 月，剑桥分析[3]公司非法获取脸书（Facebook）上超过 5000 万用户数据，并通过定向推送影响大选事件曝光，再次敲响大数据安全警钟。**三是**数据经济的安全监管面临挑战。一方面，数字经济下新业态丰富、市场主体众多，具有跨界融合等特点，给传统监管体系带来新的挑战。同时，新兴技术快速应用引发新的安全风险，例如人工智能核心算法不透明，存在恶意操纵导致不正当竞争风险；区块链技术应用暴露多重风险，目前尚未形成覆盖全生命周期的监管思路。

（二）主要国家强化网络安全技术产业投入布局

1. 持续细化提升网络安全保障要求

近年来，各国政府不断细化完善网络安全政策和标准体系，着力提升整体网络安全防御水平，为安全产业的发展提供新的动能。特朗普政府延续了奥巴马政府对网络安全的重视态度，2018 年以来，美国相继发布了多份网络安全相关政策文件，进一步强化网络安全政策指

[3] Cambridge Analytica

导，包括：商务部国家标准与技术研究院（NIST）《提升关键基础设施网络安全的框架》、能源部《能源行业网络安全多年计划》、国土安全部（DHS）《网络安全战略》、国家安全电信咨询委员会（NSTAC）《网络安全“登月”计划》等。英国政府内阁办公室于 2018 年 6 月发布实施网络安全最低标准（Minimum Cyber Security Standard）[4]，从识别、保护、检测、响应和恢复五个维度，提出了一套网络安全能力建设的最低措施要求。标准的强制效力将驱动英国政府部门、非政府公共机构、承包商等相关单位加大网络安全保障投入，提升安全防护能力。

2. 加大网络安全领域国家投入力度

近年来，各国在网络安全领域的国家级投入强势增长，在有力支撑国际战略政策落地的同时，也为产业发展注入强心剂。2018 年美国网络司令部将在政府网站安全、主动防御、实地运营、反恐和基础设施抵御力、身份识别管理等 5 个方向加大投入，总预算达 15.13 亿美元；美国“2019 财年国防授权法案”将网络安全预算大幅增加至 300 亿美元，将从推进技术发展、扩大采购权限、强化政企合作、支持人才培养、创建试点项目等方面提升国家网络安全能力。英国《国家网络安全战略》（2016-2021）提出，英国政府将投入 19 亿英镑强化网络安全能力。以色列创新局将联合以色列经济和工业部、国家网络局启动为期三年的产业发展计划，包括对有全球影响力的技术、有突破

[4] 来源：https://www.gov.uk/government/publications/the-minimum-cyber-security-standard

性研发潜力的网络安全企业提供资金支持等，投资 9000 万新谢克尔（约 2443 万美元）。德国国防部长和内政部长在 2018 年 9 月宣布，将在未来五年投入 2 亿欧元组建网络安全与关键技术创新局，机构定位类似于美国国防部高级研究计划局（DARPA），主要致力于推动自主网络安全技术创新。

3. 指引网络安全技术产品创新方向

美国、德国等多国通过制定发布指南性文件，引领网络安全技术创新发向。2018 年 3 月，美国国土安全部科学技术局（Science and Technology，S&T）发布《2018 网络安全部技术指南》《2018 网络安全部组合指南》[5]两项指南文件。其中，《2018 网络安全分部技术指南》是第三次发布，提供 70 多种技术解决方案以及市场转型方案指导，涵盖移动安全、身份管理、DDoS 防御、数据隐私、网络取证等前沿技术领域；《2018 网络安全部组合指南》系统介绍了 S&T 支持的网络安全研发项目，涉及关键信息基础设施、身份管理和数据隐私、执法支撑、移动安全等 13 个领域，并提供了技术转化方案和 DHS 硅谷创新计划指南。德国教育和研究部计划到 2020 年共投入 1.8 亿欧元对重点网络安全研究项目提供支持。例如，IUNO 项目集合了包括大型企业、中小企业、应用企业、网络安全公司和科研机构的来自业界和学界 21 个合作伙伴，为网络和数据安全提供解决方案。

4. 支持网络安全技术产品出口

[5] 来源：https://www.dhs.gov/science-and-technology/news/2018/03/12/news-release-st-announces-release-new-cybersecurity-research

英国、以色列等国将网络安全作为对外贸易的重点领域，继续致力于扩大网络安全技术产品出口。以英国为例，2016 年，英国 800 家网络安全企业出口贡献总额达到 15 亿英镑。为进一步支持和促进产业发展，打造充满活力的网络安全产业生态，英国于 2018 年 3 月发布《网络安全出口战略》。根据战略，英国国际贸易部（DIT）将利用其全球办事处，与其他政府部门、贸易和商业专家、学术界、工业界和行业领先机构开展密切合作，提供定制化优惠方案和对接平台，促进和资助网络安全国际贸易和投资。

（三）网络安全创新技术服务进入实质部署应用期

1. 数字化浪潮驱动身份管理与访问控制技术智能化发展

云计算、物联网等 IT 技术发展、数据资产的价值攀升和数据合规要求趋紧，驱动身份管理与访问控制[6]技术创新和市场繁荣。2017 年，身份管理与访问控制市场规模为 47.26 亿美元，较 2016 年增长了 9.15%[7]。网络融合生态以及指数级增长的设备、平台、应用数量以及外部连接等，加速身份管理与访问控制技术创新和理念变革。**一是**身份管理技术理念向身份治理转化，应对多模型、多应用、复杂结构的集中化管理成为趋势。IBM 、One Identity 等厂商推出身份治理工具（IGA），提供动态控制引擎，处理复杂且交叠化的策略，通过集中化管理方式有效识别符合策略的访问。**二是**单点登录（SSO）、多因子

[6] 身份管理与访问控制：Identity and Access Management, IAM，通过对网络中每个用户和其访问权限的有效管理，确保用户活动合规，从而避免非授权访问、身份欺诈等导致数据泄露风险

[7] 数据来源：Gartner

身份验证（MFA）等走向成熟，自适应能力以及对复杂环境的兼容性成为技术博弈焦点。自适应能力将提升风险识别准确性的重要手段，基于用户行为实施持续性的身份验证，可以避免风险提示过多导致的用户频繁响应。云计算、工业、IOT 等复杂环境则为新兴厂商提供机遇，特别是在物联网认证领域，目前 IETF 下的 ACE 研究组正在研究基于 OAuth2.0 的认证机制，以解决设备资源约束问题。**三是**特权账户管理[8]（Privileged Access Management，PAM）逐步升温。咨询机构 Forrester 认为，80%的数据泄漏都与特权账户凭证被窃取有关；安全企业 One Identity 的调查显示，54%的受访者仍采取纸质、电子表格等管理特权账户，57%的受访者反馈未能实现对特权账户的全面监控。随着特权账户重要性不断提升，预计这一市场有望在未来 3-5 年迅速扩大。CyberArk、IBM、Cisco 等厂商围绕特权凭证安全保护和监测、特权账户行为审计、安全预警及响应等推出了平台和产品。**四是**区块链、生物识别等技术发展将推动身份管理与访问控制迈入新的阶段。目前将区块链技术应用于身份管理和访问控制领域的实践正在展开。SecureKey 推出了基于 IBM 区块链的数字身份网络。Shocard 将区块链技术融入 IAM 和单点登录解决方案。生物特征识别能力的提升则为身份识别提供了更多选择，通过提取用户行为的特殊特征，例如触摸压力、操作顺序等替代指纹、口令等认证方式。

[8] 特权账户是指具有较高权限的“超级账户”，这些账户一旦泄露，特权账户使攻击者可全面控制企业的 IT 基础架构，禁用安全控制功能，窃取保密信息、实施金融欺诈并中断业务运营

2．可管理安全服务[9]迎来发展新机遇

网络安全领域的攻防对抗持续激烈，同时网络安全专业人才愈发稀缺，使得越来越多企业倾向于选择可信赖的安全企业提供专业安全运维服务。根据 Gartner 数据，2017 年可管理安全市场规模达到 103 亿美元，较 2016 年增长 9.5%，超过同期全球安全市场增长率。可管理安全服务呈现如下特点：**一方面**数据本地化需求强烈，区域化运营企业受青睐。GDPR 生效以来，数据本地化存储和分析需求更为强烈，IBM、Symantec 等在全球具备多个区域化运营中心（SOC）、能够满足数据安全监管新政的企业优势日益凸显；同时，本地化的中小型厂商通过更为灵活而定制化的服务、较强的“可信任”度，成功占据了一定的市场份额。**另一方面，**电信运营商发挥渠道和流量优势，形成业务发展和安全互为补充的良好局面。BT、AT&T、Verizon 等电信运营商提供网络、云计算服务等 IT 外包服务，为其在可管理安全服务领域的拓展市场提供了渠道优势，安全能力的补充也使得 IT 外包服务更为一体化、完整化。在安全能力方面，运营商具备骨干级别的网络安全监测能力，特别是 DDoS 攻击防御领域，成为其他厂商不具备的独特优势；有力的第三方合作伙伴关系和丰富的威胁信息来源帮助电信运营商提升了威胁发现和分析能力，进一步增强了用户粘性。

3．云安全技术加速拓展和应用

[9] 注：可管理安全服务（Managed Security Services, MSS），也称安全托管服务，是由专业厂商提供的安全运维服务，包括如安全事件监测和分析、漏洞扫描、应急响应等。可管理安全服务的提供商通常称作 Managed Security Services Provider，MSSP。

云安全市场规模的持续快速增长和云安全事件的日益频发驱动安全技术创新应用。根据 Gartner 数据，2017 年云安全市场规模达到 49.07 亿美元，相比 2016 年增长 21.64%。应对多云环境、强化风险控制、数据安全合规等成为云安全热点领域。**一是**云访问安全代理（CASB）市场竞争加剧。云访问安全代理在用户和云服务商之间建立起安全屏障，通过实施加密、访问控制、行为监控、审计隔离等不同层次的风险管理和安全策略，保障云应用和数据安全。Gartner 预测到 2020 年，60%企业将使用云访问安全代理技术产品管理云服务。目前，主流厂商均已推出云访问安全代理产品，将同 Bitglass、Symantec、Skyhigh（McAfee 2018 年收购）、Netskope 等先发厂商展开激励角逐。**二是**云工作负载保护平台（CWPP）功能多样化拓展。在负载分割、流量可视化、系统监控、应用管理、漏洞和配置管理等能力基础上， Trendmicro、Tripwire、Dome9 、Stackrox 、vArmour、HyTrust 等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 等能力扩展以及在多云环境的适配。**三是**云计算服务商逐步开拓云安全市场。最为典型的是亚马逊 AWS。自 2006 年诞生以来，AWS 一直将生态建设作为其发展的重要引擎，在安全方面也采取了生态合作伙伴路线，其应用市场（Marketplace）提供来自 TrendMicro、Palo alto、Cisco、Sophos 等近 300 个厂商的 819 款安全产品和服务，给予用户丰富的选择空间。但 2015 年以来，AWS 相继推出了 16 款商业化云安全产品和服务，包括身份管理与访问控制、

云原生目录服务、应用程序身份管理、智能威胁检测服务、自动化安全评估等[10]，积极拓展云安全市场，致力于“云+安全”的一体化解决方案。

4．威胁情报技术服务逐步走向落地

威胁情报技术推动了传统的事件响应式的安全思维向着全生命周期的持续智能响应转变。借助威胁情报，企业能够从网络安全设备产生的海量告警中解脱出来，以更为智能的方式掌握最新的网络安全事件、重大漏洞隐患、典型攻击手段、潜在危险领域等信息并及时启动预警、响应、应急等工作。Gartner 预测，到 2020 年，15％的大型企业将使用商业威胁情报服务。近年来，IT 和安全企业在威胁情报领域布局持续不断，2018 年也有多笔交易。例如，L3 technologies 并购 Azimuth Security[11]与 Linchpin Labs[12]，增强全球威胁追踪、事件响应和安全分析能力;Splunk 以 3 亿欧元收购 Phantom Cyber[13]，打造自适应安全能力；Verizon 并购 Niddel，开辟威胁情报业务线。威胁情报服务落地模式日益清晰，四种主流模式逐渐成型：**一是**提供威胁情报门户和威胁情报源。Blueliv、Flashpoint 和 Group-IB 等企业汇聚自身资源和多种开源情报建立了开放的威胁情报查询平台，可支持 IP、网站、关键字等多种模式情报查询。**二是**提供威胁情报平台服务。LookingGlass、Anomali 和 ThreatConnect 等厂商推出了用于日常运营

[10] 来源：https://aws.amazon.com/cn/
[11] 注：澳大利亚安全公司
[12] 注：加拿大安全公司
[13] 注：美国安全公司

的威胁情报平台，支持攻击阻断、战略决策和流程改进，实现对威胁情报进行全生命周期[14]的管理。**三是**提供威胁情报一体化分析服务。例如 FireEye，Group-IB 和 LookingGlass 等企业能够将威胁情报能力融入到综合技术解决方案中，提供例如针对暗网和深网监控分析等定制化服务以及 MRTI[15]外的其他服务。**四是**威胁情报与安全产品的融合。例如，威胁情报与安全运营中心（SOC）、安全事件管理产品（SIEM）等结合。

5．人工智能将成为重塑网络安全防御模式的主导力量

伴随着人工智能技术成熟和应用拓展，网络安全逐渐成为人工智能应用的最活跃领域之一。据 CB Insights 统计，目前国际上已有 80 余家应用人工智能技术的安全公司，其中自动化终端防护厂商 Tanium 和智能预测分析厂商 Cylance 市值超过 10 亿美元。美国将投入 20 亿美元支持人工智能技术应用，其中网络安全是重点方向之一。人工智能、深度学习等技术可以优化数据挖掘、行为识别和风险预测，提供更为自动化、智能化的安全感知和响应，驱动安全防御理念变革升级。目前，Skycure、Darktrace、Authbase、CyberFog 等一大批创新技术企业积极推动将人工智能技术应用于身份管理、网络欺诈防护、异常行为分析、移动安全、物联网安全等领域。但与此同时，人工智能在攻击自动化、网络诈骗等方面应用引发新的安全风险，亟需关注。

[14] 注：全生命周期包括收集，处理，分析和传播

[15] 注：MRIT 是指可机读威胁情报，包括失陷检测 IOC（技术指标器）情报、文件信誉和 IP 情报三种类型

（四）网络安全人才全球紧缺态势加剧

1. 网络安全岗位需求快速增长，呈现全球范围短缺局面

从全球上看，网络安全岗位需求快速增加，人才短缺形势日益突出。国际咨询机构预测，2019 年网络安全岗位缺口将在 100-200 万，而到 2021 年缺口将达到 350 万个[16]。网络安全岗位需求增长加剧了网络安全人才短缺态势。针对信息领域的调研显示，墨西哥、澳大利亚等国家 88%的受访企业存在网络安全人才短缺，美国、日本、法国等其他 6 个国家也均不低于 75%。在全球市场供不应求的环境下，围绕网络安全人才争夺将更趋全球化、白热化。

数据来源：McAfee，Hacking the Skills Shortage

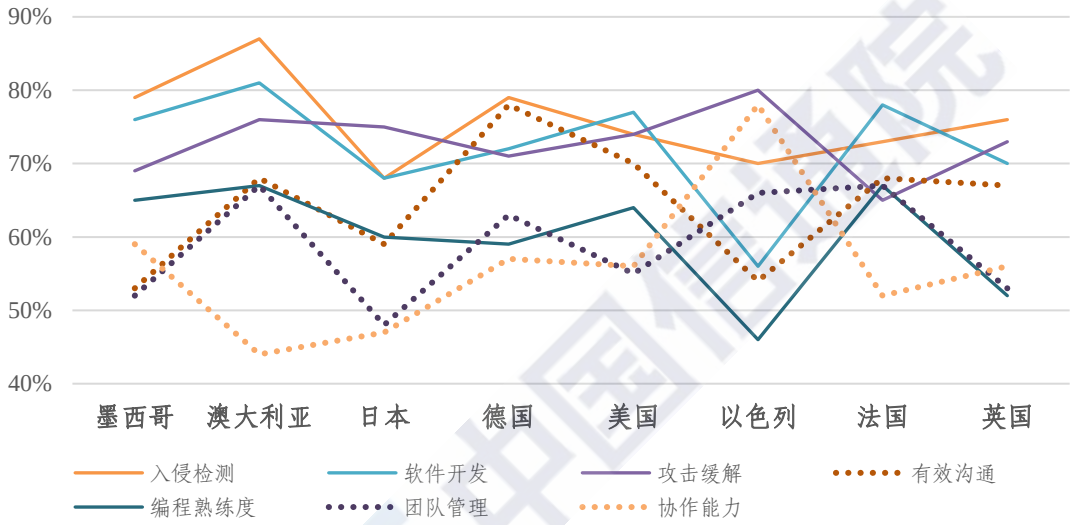
图 1　国际主要国家网络安全人才短缺程度

2. 入侵检测和安全软件开发技能最为稀缺，技术能力较管理能力更受重视

根据对美国、日本、英国、以色列等 8 个国家调查显示，入侵检测和安全软件开发的技能最为稀缺，其中入侵检测平均稀缺程度达到

[16] 数据来源：Cybersecurity Ventures

75.8%，其次是安全软件开发 72.3%。综合看，以入侵检测、软件开发、攻击缓解、编程熟练度为代表的技术能力相较团队建设、沟通、协作等管理类技能更为缺乏，这一方面表明技术能力是网络安全对抗的关键因素，掌握网络安全技能的从业人员是行业稀缺资源；另一方面也揭示出网络安全技术能力相较管理能力更难获取和提升。



数据来源：McAfee，Hacking the Skills Shortage

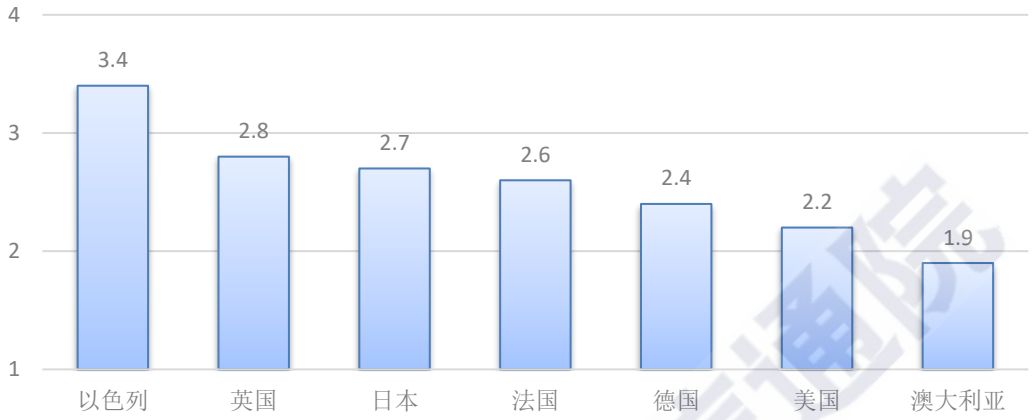
图 2 网络安全人才技能需求程度

3. 网络安全从业人员薪酬持续走高，达平均工资 2.7 倍

网络安全人才的全球性、大幅度短缺，引发了网络安全职位薪酬的快速提升。根据 Robert Walters 调查显示，2018 年网络安全从业人员薪资涨幅将达到 7%。同时，网络安全岗位薪资水平远超其他 IT 岗位。根据对美国、日本、英国、以色列等 8 个国家调查显示，网络安全从业人员薪资约为企业平均工资的 2.7 倍[17]。例如，美国网络安全

[17] 数据来源：OECD

从业人员薪资水平较其他 IT 岗位高出 6500 美元，溢价 9%；薪酬最高的岗位是网络安全架构师，年薪高达 23.3 万美元，高于首席信息安全官（CISO），这也侧面印证了网络安全技术能力相对管理更为稀缺。



数据来源：McAfee，Hacking the Skills Shortage

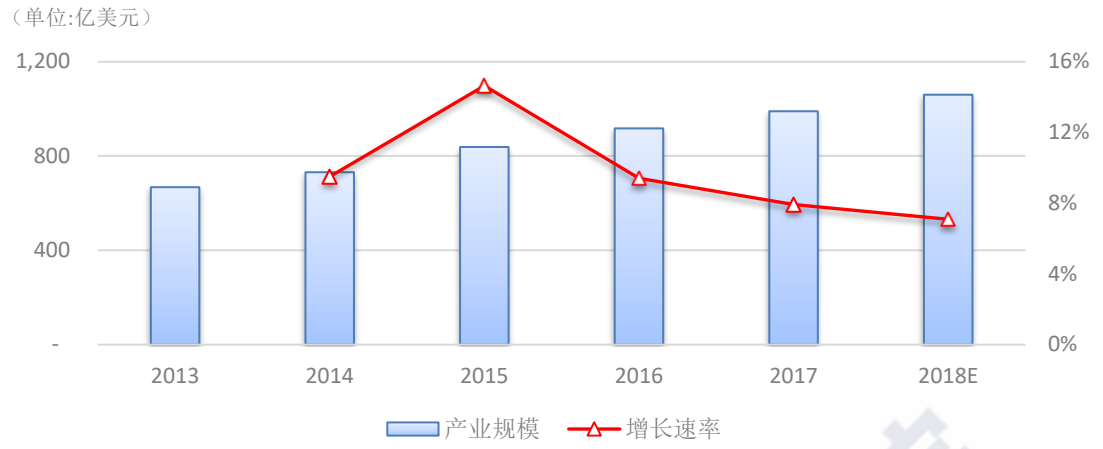
图 3 网络安全专业人员的薪酬溢价比例

二、国际网络安全产业年度发展情况

（一）全球网络安全产业规模稳步增长

2017 年全球网络安全产业规模达到 989.86 亿美元，较 2016 年增长 7.9%，预计 2018 年增长至 1060 亿美元[18]。从增速上看，全球安全产业增速在 2015 年达到历史高位 17.3%，随后回落至逐年 8%的增长水平。

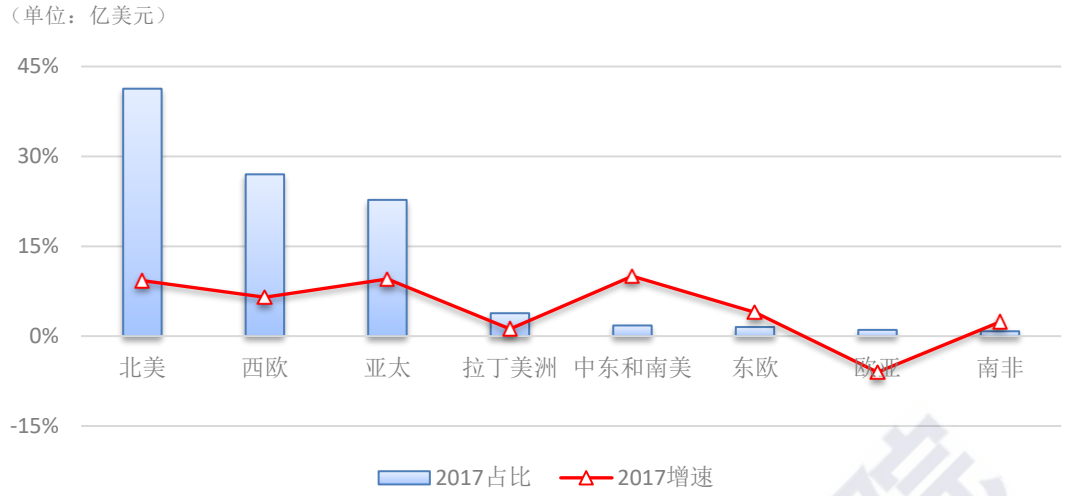
[18] 数据来源：Gartner Information Security, Worldwide，2015-2021



数据来源：Gartner

图 4 2013-2018 年全球安全产业增长情况

在区域分布方面，北美地区全球主导地位巩固；西欧地区保持稳定增长，规模位列全球第二；亚洲地区增速领先，规模位列第三。其中，美国、加拿大为主的北美地区 2017 年市场规模达到 408.76 亿美元，较 2016 年增长 9.24%，全球占比为 41.29%，牢牢占据全球最大份额；英国、德国、芬兰等 16 个西欧国家市场规模合计 267.29 亿美元，较 2016 年增长 6.5%，全球占比为 27%；日本、澳大利亚、印度等 10 个亚太国家产业规模合计 225.08 亿美元，较 2016 年增长 9.53%，全球占比为 22.74%，仅次于西欧国家，增速位于全球第一；非洲、东欧、拉丁美洲等其它地区安全市场规模为 88.74 亿美元，全球占比为 8.97%。

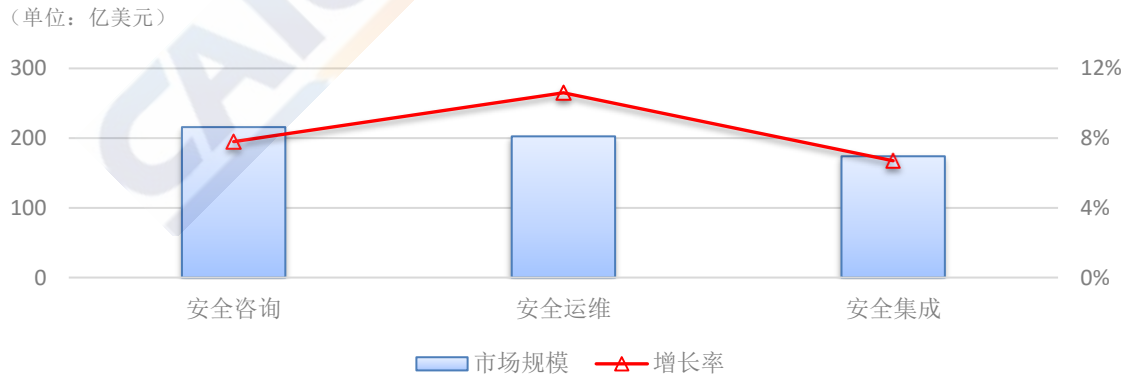


数据来源：中国信息通信研究院（基于 Gartner 数据整理）

图 5　全球安全产业区域分布和增长情况

（二）安全服务和产品市场格局总体稳定

安全服务市场与安全产品市场继续保持六四分格局，安全服务增长速度略占优势。2017 年安全服务市场规模达到 592 亿美元，较 2016 年增长 8.3%。其中，安全咨询、安全运维、安全集成三个细分市场份额分别为：21.8%、20.4%、17.6%，如图 6 所示。



数据来源：中国信息通信研究院（基于 Gartner 数据整理）

图 6　安全服务细分市场份额及增长情况

安全咨询服务市场规模达到 216 亿美元，相比 2016 年增长 7.8%。

安全咨询服务将面向行业纵深发展，以行业特点为核心，从技术、运维、管理、策略等方面提出更为针对性的安全技术与管理咨询服务，满足多样化的咨询服务需求。**安全运维**服务市场规模达到 203 亿美元，相比 2016 年增长 10.6%，成为安全服务产业的重要增长引擎。从全球范围来看，安全运维服务发展迅速，全球已有超过 2 万家在行业领军企业和政府机构正在使用安全运维管理服务，特别是北美、欧洲等发达地区，安全运维服务市场已较为成熟。随着安全人才技能短缺、技术复杂性和威胁形势持续加深，安全运维服务市场规模增长有望持续。**安全集成**服务市场规模达到 174 亿美元，相比 2016 年增长 6.7%。美国、日本、欧盟占据了全球安全集成服务 80%的市场份额。随着以政府、金融、电信等重要行业为主导的产业格局面向企业、家庭应用为主导的新格局转型，安全集成服务面临着全新的挑战与机遇。

2017 年全球网络安全产品市场规模达到 398 亿美元，较 2016 年增长 7.3%。其中，市场份额最高的三类依次是防火墙、终端防护、身份管理与访问控制：防火墙市场规模为 108.01 亿美元，占比 27.17%；终端防护市场规模为 92.87 亿美元，占比 23.33%；身份管理与访问控制市场规模为 47.26 亿美元，占比 11.87%。

数据来源：中国信息通信研究院（基于 Gartner 数据整理）

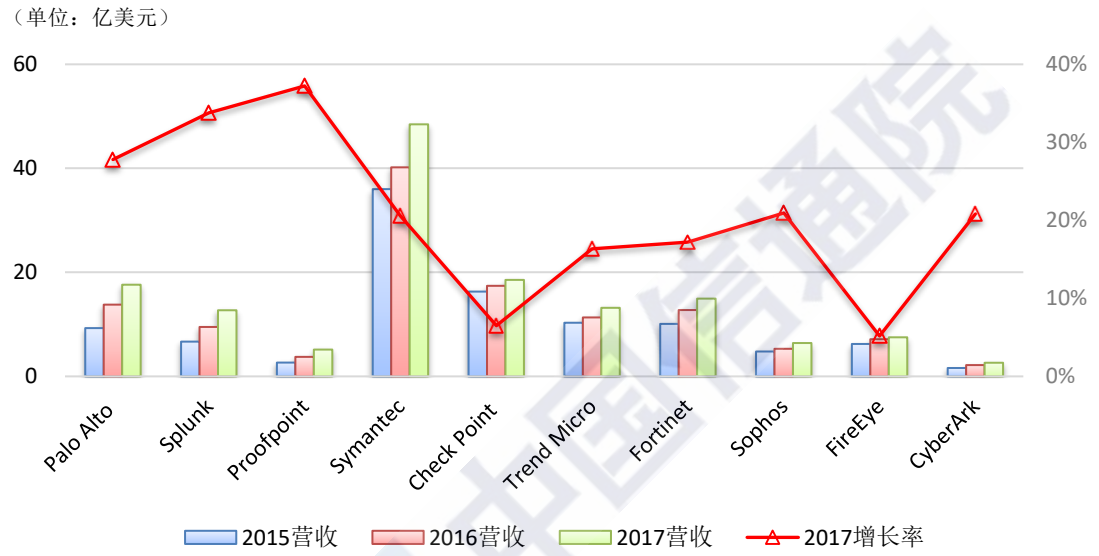
图 7　安全产品市场份额及增长情况

增速方面，排名前三的网络安全产品分别是防火墙、安全检测工具以及身份管理和访问控制。其中，防火墙市场增速达到 15.8%，主要是受益于数据中心等大规模网络的部署、大型企业集中化管理以及传统产品升级需求。安全检测工具市场增速为 13.9%，基于内部风险的安全事件频发，进一步引发了网络安全隐患排查的需求，企业日益重视通过有效工具和手段以识别、评估内部风险和脆弱性。身份管理与访问控制产品市场增速为 13.6%，驱动因素包括：移动化办公引发的终端和用户管理需求以及云应用的快速增长，市场对网络入侵风险缓解技术的需求持续上升等。

（三）上市企业发展态势总体良好

1. 企业营收持续高速增长

2017 年全球上市安全营收持续增长，包括 CheckPoint、Symantec、Palo Alto Networks、Trend Micro 等在内的 10 家典型企业平均营收 14.94 亿美元，约合人民币 100.87 亿元，营收平均增长 21.99%，如图 8 所示。

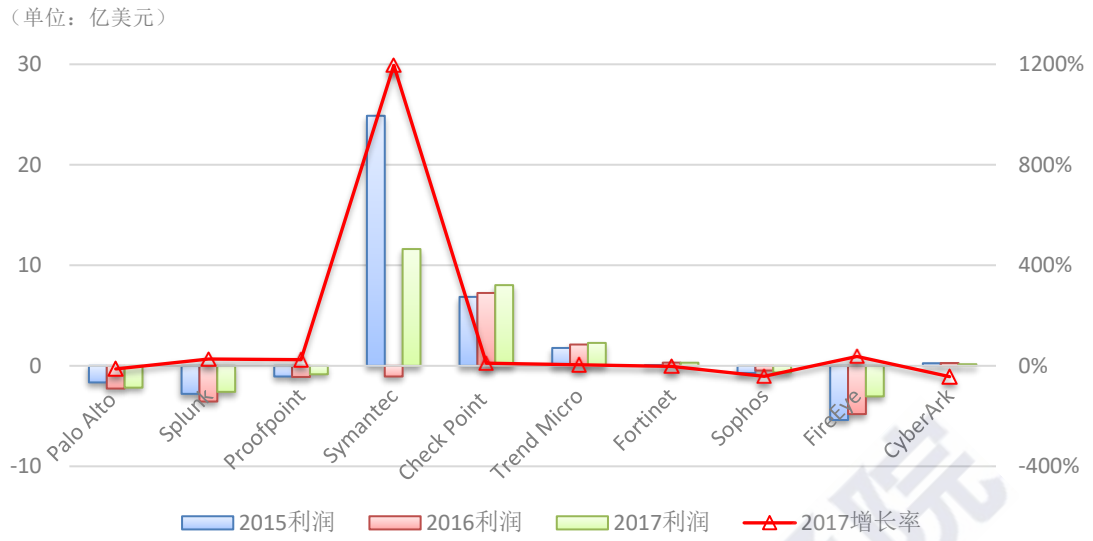


数据来源：中国信息通信研究院（基于 wind 数据整理）

图 8 2015-2017 年主要国际上市安全企业营收情况

2. 亏损态势总体得到缓解

在净利润方面，大部分企业的亏损势头得到缓解，少部分企业开始盈利。2017 年 10 家典型企业平均净利润为 1.31 亿美元，相比于 2016 年平均亏损 0.23 亿美元，企业净利润情况明显好转，如图 9 所示。



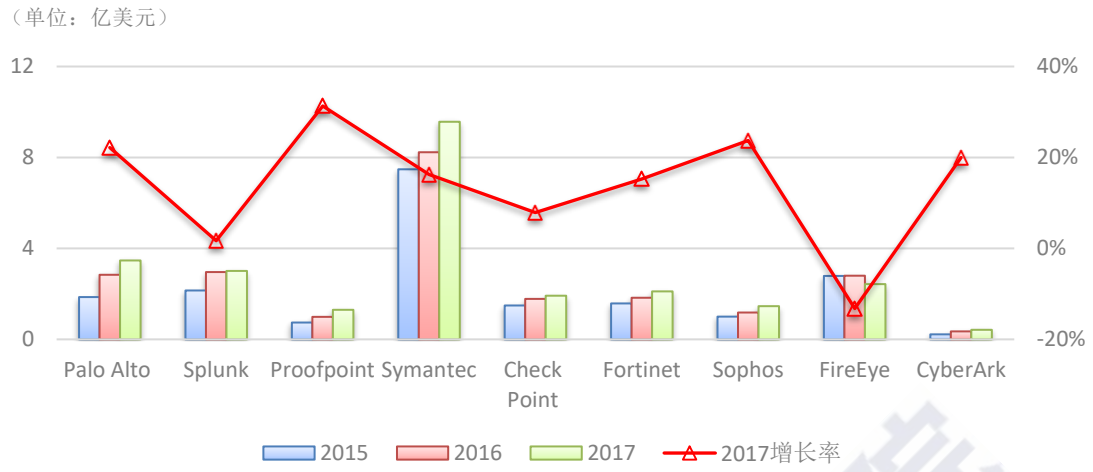
数据来源：中国信息通信研究院（基于 wind 数据整理）

图 9　2015-2017 年主要国际上市安全企业净利润情况

部分企业在布局长远的同时，营业成本大增，影响企业利润。以 Proofpoint 为例，2017 年该企业的营业收入为 5.15 亿美元，而支出达到 5.85 亿美元，维持“入不敷出”局面。营业支出总额较 2016 年的 4.61 亿美元增加了 26.9%，其中，研发费用为 1.3 亿美元，增加了 31.31%；营业费用为 4.41 亿美元，增加了 25.28%，主要原因是用人成本持续走高。一方面，2017 年员工总数为 2047 人，增长 30.13%，另一方面，员工平均薪酬普遍增加。此外，该企业在 2017 年完成了 2 起并购活动，共花费 1.7 亿美元，用以提升自身威胁情报技术，预计未来盈利情况将得到进一步的改善。

3. 企业研发投入稳步增长

企业研发投入持续三年增长，2017 年上市安全企业的平均研发投入为 2.85 亿美元，相比去年的 2.55 亿美元，增长了 11.76%；企业平均研发投入增长率为 13.91%，保持高位水平。



数据来源：中国信息通信研究院（基于 wind 数据整理）

图 10 2015-2017 年主要国际上市安全企业公司研发投入及增长率[19]

4. 企业上市步伐保持稳定

据不完全统计，2017 年至 2018 年 9 月，国际上已有 5 家网络安全产业实现上市融资。其中，2017 年上市的 3 家企业 Okta、Forescout、SaiPoint 技术领域均为身份管理与访问控制，反映出市场对身份管理与访问控制领域的前景看好。

表 1 2017 年至 2018 年 9 月国际安全企业 IPO 情况

日期	企业名称	技术领域	募集资金（亿美元）
2018.07	Tenable	风险管理	2.33
2018.03	Zscaler	云安全	1.79
2017.11	SailPoint	身份管理与访问控制	1.60
2017.10	Forescout	身份管理与访问控制	1.08
2017.04	Okta	身份管理与访问控制	1.74

数据来源：中国信息通信研究院根据公开资料整理

[19] Trend Micro 未披露研发费用。

（四）并购和创投市场保持高度活跃态势

1. 并购活动热度不减，交易数量创历史新高

2017 年国际网络安全产业的并购活动达到了创纪录的 178 起，交易数量增长了 12.66%；交易总额为 206 亿美元，保持历史高位水平，仅较 2016 年小幅回落。

数据来源：Momentum Cyber

图 11 2010-2017 年全球网络安全并购活动数据

IT 巨头、私募和安全厂商共同在网络安全领域并购活动中扮演重要角色。例如，军工企业 Thales 以 69 亿美元收购数字安全领军企业 Gemalto 成为 2017 年金额最高的并购案例，并购后，Thales 数字安全领域业务规模扩大到 42 亿美元，位列全球第三。私募股权公司 Thoma Bravo 以 16 亿美元收购网络安全和数据保护解决方案提供商 Barracuda Networks，加速其安全平台及存储解决方案的推广应用。安全企业 Proofpoint 以 2.25 亿美元收购了 SaaS 提供商 Wombat Security Technologies，升级了自身高级威胁保护功能。2017 年已披露并购金

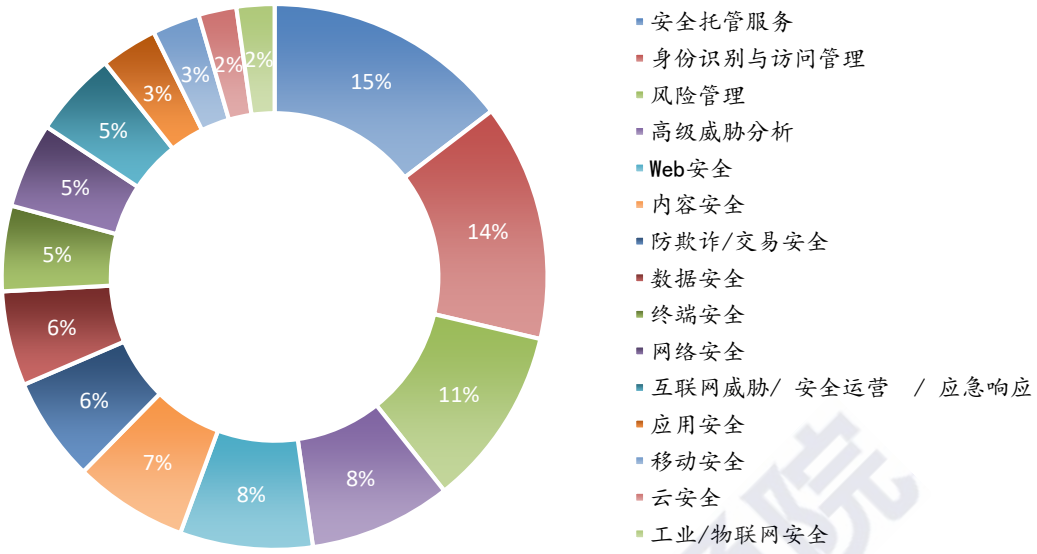
额较高的 10 个并购案例如表 2 所示。

表 2 2017 年已披露金额较高的网络安全并购案例

日期	被收购方	并购方	技术领域	并购金额（百万美元）
2017.12.18	Gemalto	Thales	数字安全	6885
2017.11.30	Barracuda	Thoma Bravo	数据保护	1600
2017.11.02	Gigamon	Elliott	数据保护	1329
2017.01.03	Landesk	Heat Software	安全服务	1150
2017.08.03	Symantec Website Security	Digicert	安全认证	950
2017.05.17	Veracode	CA Technologies	云安全	614
2017.11.07	Blackduck	Synopsys	应用安全	548
2017.11.17	Argus	Continental	安全服务	约 400
2017.09.25	Gigya	SAP	安全服务	350
2017.03.17	BlueCat	MDP	云安全	325

来源：中国信息通信研究院根据公开资料整理

从并购的技术领域来看，可管理安全服务成为了最热门的选择。该市场的并购数量为 26 起，比 2016 年的 19 起增加了 36.84%，市场占比来到了 15%。这一趋势反映出市场对可管理安全服务的认可：一是降低成本，包括人员配置、产品、场地等成本需求；二是全天候监控服务，有效识别安全风险，第一时间提供解决方案；三是提供趋势分析，包括专业的安全趋势分析，按月、季、年提供安全分析报告等。

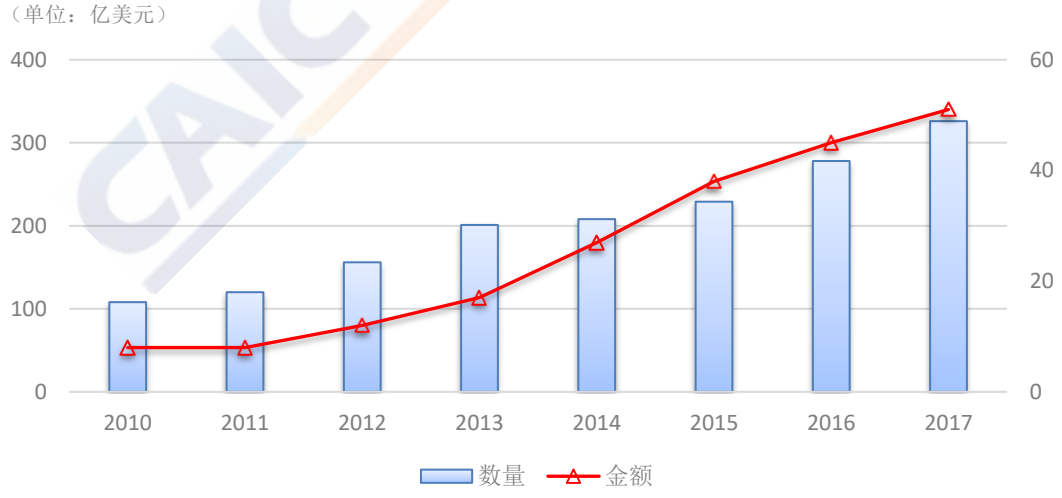


数据来源：Momentum Cyber

图 12　2017 年全球网络安全并购领域

2. 初创企业融资态势良好，国际融资活动再创记录

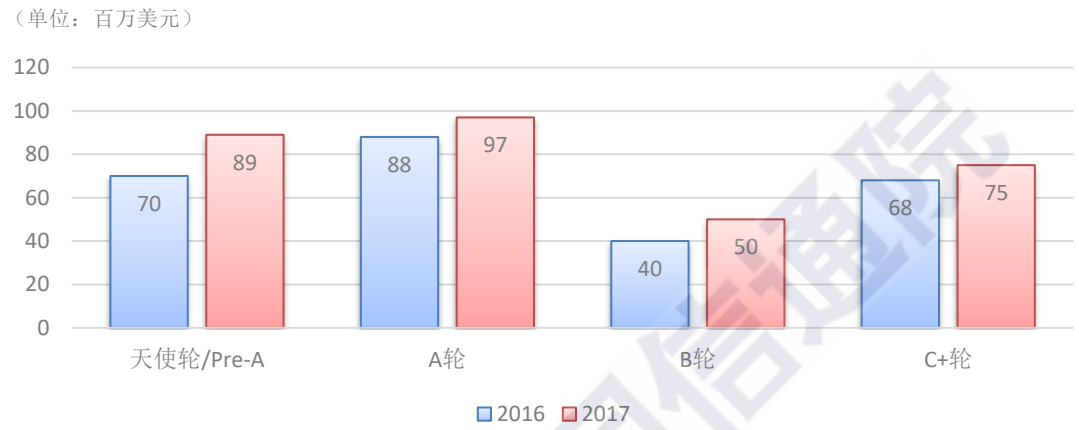
2017 年，国际网络安全产业的融资活动数量与融资金额再创新高。融资活动达 326 起，增长 17.27%；交易总额为 51 亿美元，增长了 13.33%，如图 13 所示。



数据来源：Momentum Cyber

图 13　2010-2017 年网络安全初创企业融资态势

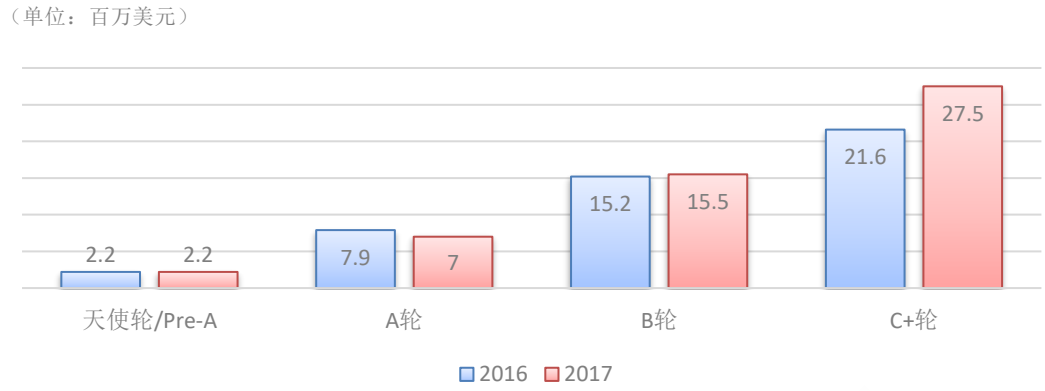
从融资轮次分布看，2017 年共有 89 家的企业位于天使轮阶段，相对于 2016 年增加了 27.1%；处于 A 轮的企业有 97 家，较 2016 年增加了 10.2%；有 50 家企业处于 B 轮阶段，相比于 2016 年增加了 25%；位于 C+轮的有 75 家，比 2016 年增加了 10.3%，如图 14 所示。



数据来源： Momentum Cyber

图 14 2016 与 2017 年网络安全初创企业融资态势对比

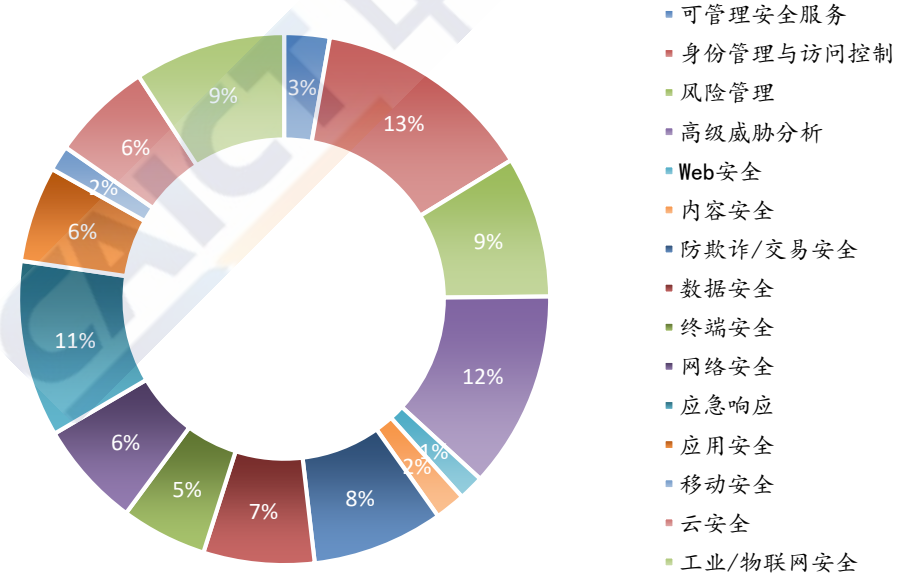
从平均交易规模上来看，2017 年天使轮阶段平均交易规模为 220 万美元，与 2016 年持平；进入到 A 轮的企业，平均交易规模为 700 万美元，较 2016 年 790 万美元下降了 12.86%；位于 B 轮的企业平均交易规模为 1550 万美元，相较于 2016 年 1520 万美元增加了 1.97%；而处于 C+轮的企业平均交易规模为 2750 万美元，比 2016 年的 2160 万美元增加了 27.31%，如图 15 所示。



数据来源：Momentum Cyber

图 15　2016 与 2017 年网络安全初创企业融资各阶段对比

从融资的技术领域来看，热门领域正在发生变化。其中，数据安全领域融资数量明显回落，由 2016 年的 32 起下降为 2017 年的 22 起，降幅为 45%；身份管理与访问控制领域则由去年的 25 起上升到今年 44 起，增幅达到了 76%。



数据来源：Momentum Cyber

图 16　2017 年网络安全融资热点领域分布

（五）网络安全人才培养进入深水区

1. 美国：加大网络安全人才培养投入

美国国家标准与技术局（NIST）调查显示，美国网络安全职位缺口将近 35 万。政府担忧由于私营部门的网络安全人员待遇较高，会使得许多政府的高技能网络防御人才转向私营部门。为此，美国政府在 2017 年投入 6200 万美元用以招聘和留住网络安全人才。该预算还被用来扩大 CyberCorps 计划，包括：为希望将来在政府部门从事网络安全工作的美国人，提供网络安全培训与奖学金；为学术机构制定网络安全核心课程；加强国家网络安全卓越中心提供网络安全解决方案的能力；为加入联邦政府的网络安全专家提供免息贷款；通过“全民计算机科学行动计划”等项目，对网络安全教育进行投资。

2. 英国：加强青少年和女性网络安全从业者培养

2017 年 2 月由政府通信总部(GCHQ)组建的国家网络安全中心(NCSC)是英国网络安全人才培养工作牵头部门。该中心成立以来，高度重视网络安全领域的人才队伍建设，特别是注重对青少年和女性两个群体的发掘和培养。对于青少年，英国于 2017 年 7 月份启动“网络学校计划”，将投资约 2000 万英镑，选取 14 至 18 岁的青少年培训网络安全课程，计划到 2021 年前培养至少 5700 名网络安全人才。对于女性，该中心于 2017 年 3 月组织了 Cyber First Girls 比赛，以团队参赛的形式，通过技术测试、事件模拟等比赛形式，发掘 13 至 15 岁女性中的网络技能强者；同时也为重返网络安全技术职位的女性提供

针对性的指导和帮助。

3. 欧盟：举办暑期学校、安全月等丰富活动

2018 年 6 月，欧盟下属电信委员会宣布通过《网络安全法案》，将欧洲网络与信息安全局（ENISA）升级为一个永久性的欧盟网络安全机构，在安全人才培养方面赋予其更多职责。目前，欧洲网络与信息安全局已经建立了多样化的人才培养活动机制，通过网络安全教育、培训、竞赛等平台，推动欧盟网络安全人才发展。**一是**组织年度“暑期学校”活动。2018 年的暑期学校将于 9 月在希腊举行，主题为“应对来自复杂安全风险的挑战”，将有包括法兰克福歌德大学、Hellas[20]和 Deutoe[21]在内的 10 家高校、安全机构及企业参与。暑期学校自 2013 年启动以来，已向欧盟各成员国输送了约 1200 名安全人才。**二是**举办欧洲网络安全月。2017 年 10 月第五届欧洲网络安全月召开，此次活动由欧洲网络与信息安全局、欧盟通信网络、内容和技术总局(DG CONNECT)和欧洲刑警组织欧洲网络犯罪中心(EC3)合作举办，在欧洲各地举办了会议、培训课、研讨会和在线课程等 530 多项活动，同比增长超过 15%。**三是**举办年度网络安全挑战赛。在欧洲网络与信息安全局的支持下，2017 欧洲网络安全挑战赛由西班牙国家网络安全研究所举办，大赛汇聚了来自 15 个国家的参赛队伍。

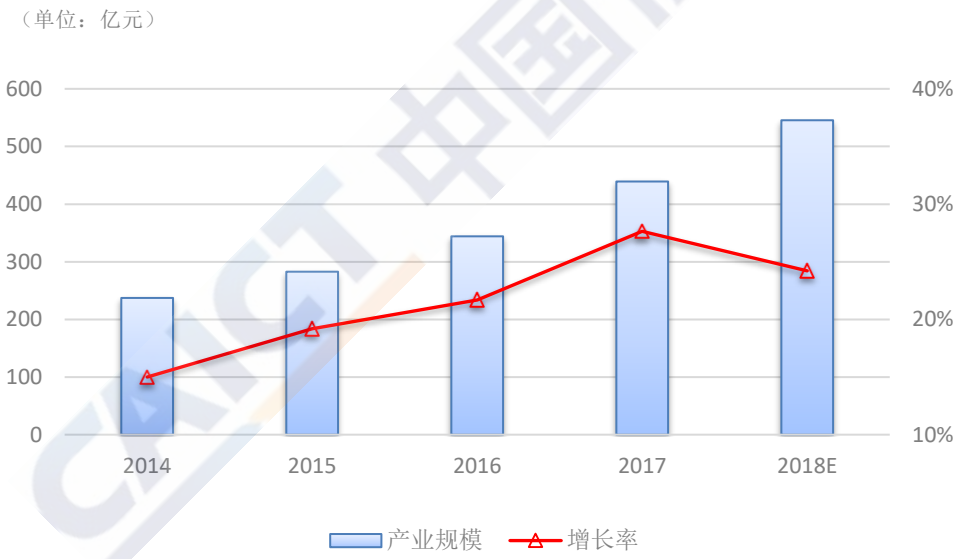
[20] Hellas：德国网络安全研究机构
[21] Deutoe：德国网络安全解决方案提供商

三、我国网络安全产业年度进展

（一）我国产业规模快速增长

国家网信工作持续发力，为网络安全技术创新、网络安全企业做大做强提供了宝贵机遇，也为网络安全产业发展创造了更为优越的政策环境，国内网络安全产业进入发展黄金期，近三年来产业增长率不断走高，产业规模迅速扩大。

根据中国信息通信研究院统计测算，2017 年我国网络安全产业规模达到 439.2 亿元，较 2016 年增长 27.6%，预计 2018 年达到 545.49 亿元，如图 17 所示。



来源：中国信息通信研究院

图 17 我国网络安全产业规模增长情况

据不完全统计，2017 年我国共有 2681 家从事网络安全业务的企业，其中北京、广东、上海企业数量最高，分别为 957 家、337 家和 279 家，呈现高度集聚态势，如表 3 所示。

表 3 我国网络安全企业区域分布 Top10

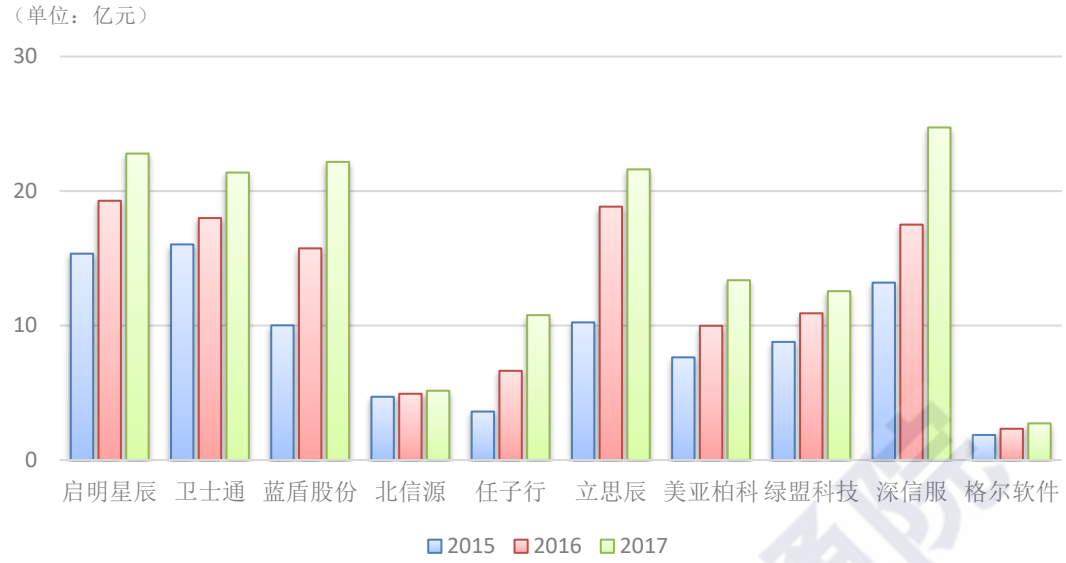
区域	企业数量	占比
北京	957	35.70%
广东	337	12.57%
上海	279	10.41%
江苏	143	5.33%
四川	133	4.96%
浙江	117	4.36%
山东	110	4.10%
福建	90	3.36%
湖北	72	2.69%
辽宁	69	2.57%

数据来源：中国信息通信研究院网络安全产业开放平台

（二）安全企业发展态势总体良好

1. 主板/创业板上市企业业绩再创新高

2017 年国内上市安全企业总体表现稳定，企业营收持续三年增长。10 家上市安全企业 2017 年平均营收规模为 15.72 亿元，其中启明星辰、卫士通、蓝盾股份、立思辰、深信服 5 家企业营收超过 20 亿元，如图 18 所示。

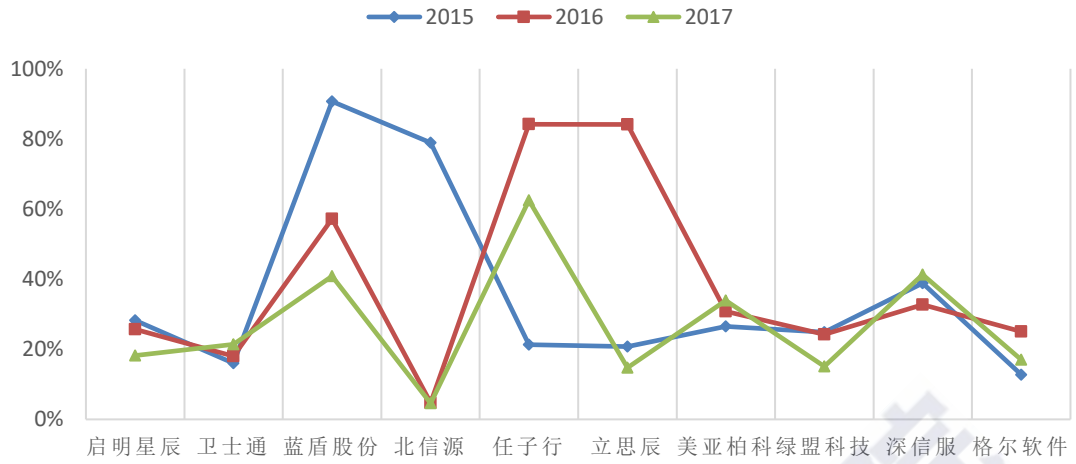


来源：中国信息通信研究院基于公开资料整理

图 18 2015-2017 年国内上市安全企业营收情况[22]

10 家典型上市安全企业 2017 年平均营收增长率为 26.98%，超过了国际企业 21.99%的平均增长速度；但营收增幅普遍有所回落，较 2016 年 38.05%的平均增速,下降了 11.07%。这主要是企业受逐步向服务转型、行业竞争加剧和网络安全政策实施不及预期的影响。随着国家政策催化和网络攻击行为愈发频繁，预计未来企业营收增速仍会维持在较高位水平。2015-2017 年营收增长情况如图 19 所示。

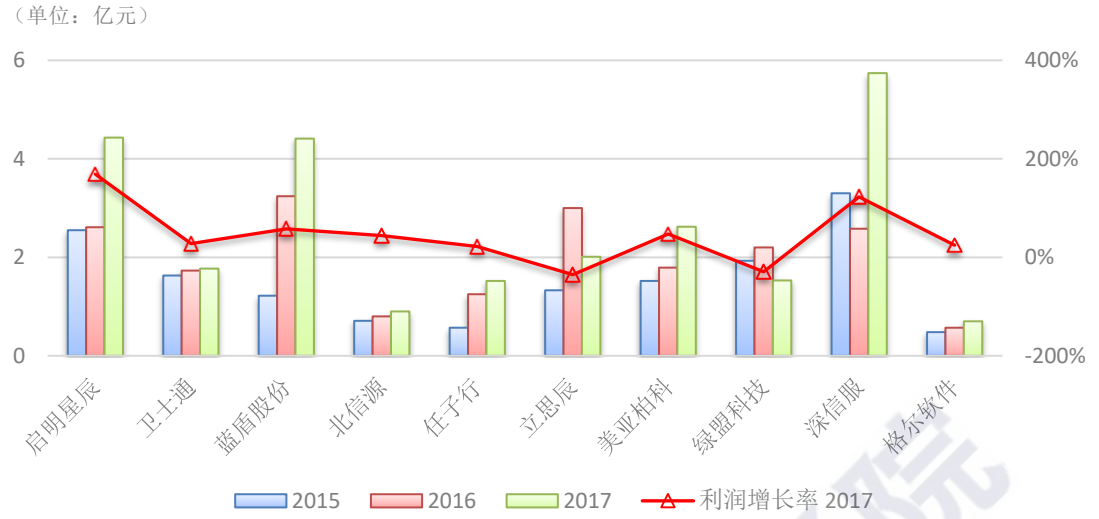
[22] 部分上市企业安全业务占比较低，故未纳入作为典型企业分析。



来源：中国信息通信研究院基于公开资料整理

图 19　2015-2017 年国内上市安全企业营收增长情况

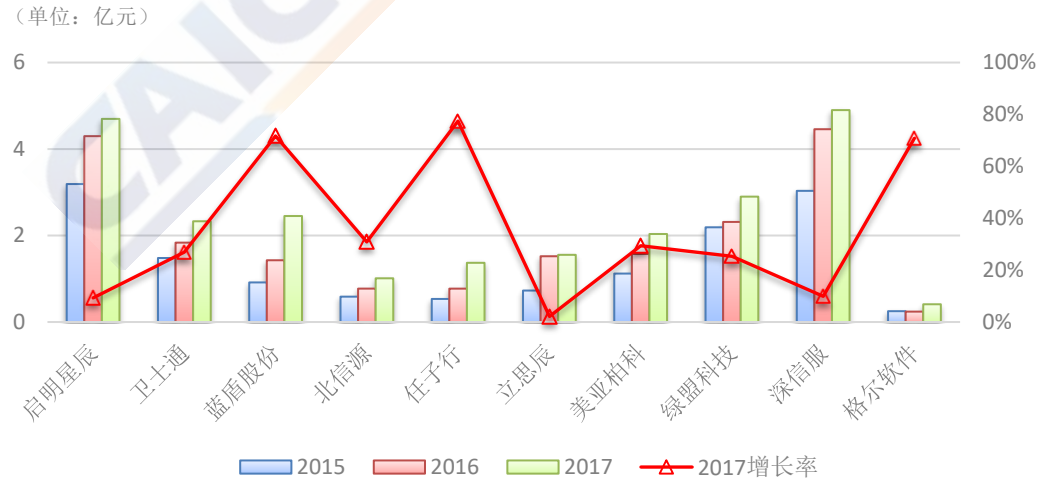
安全企业盈利能力不断提高。10 家上市安全企业 2017 年平均净利润为 2.56 亿元，较 2016 年增长 22.86%，净利润稳步增长。其中，有 3 家企业净利润超过 4 亿元：一是深信服，净利润共计 5.74 亿元，净资产收益率（摊薄）为 32.95%，较上年增加了 11.68%；二是启明星辰，净利润共计 4.43 亿元，净资产收益率（摊薄）为 14.41%，较上年增加了 2.50%；三是蓝盾股份，净利润共计 4.41 亿元，净资产收益率（摊薄）为 10.39%，较上年增加了 1.35%。10 家上市安全企业的 2015-2017 年净利润及增长情况如图 20 所示。



来源：中国信息通信研究院基于公开资料整理

图 20 2015-2017 年国内上市安全企业净利润及增长情况

在研发投入方面，2017 年国内 10 家上市安全企业的平均研发费用为 2.37 亿元，相较于去年的 1.92 亿元，增长了 23.43%。增速方面，2017 年 10 家企业的平均研发投入增长率为 35.37%，保持快速增长，如图 21 所示。

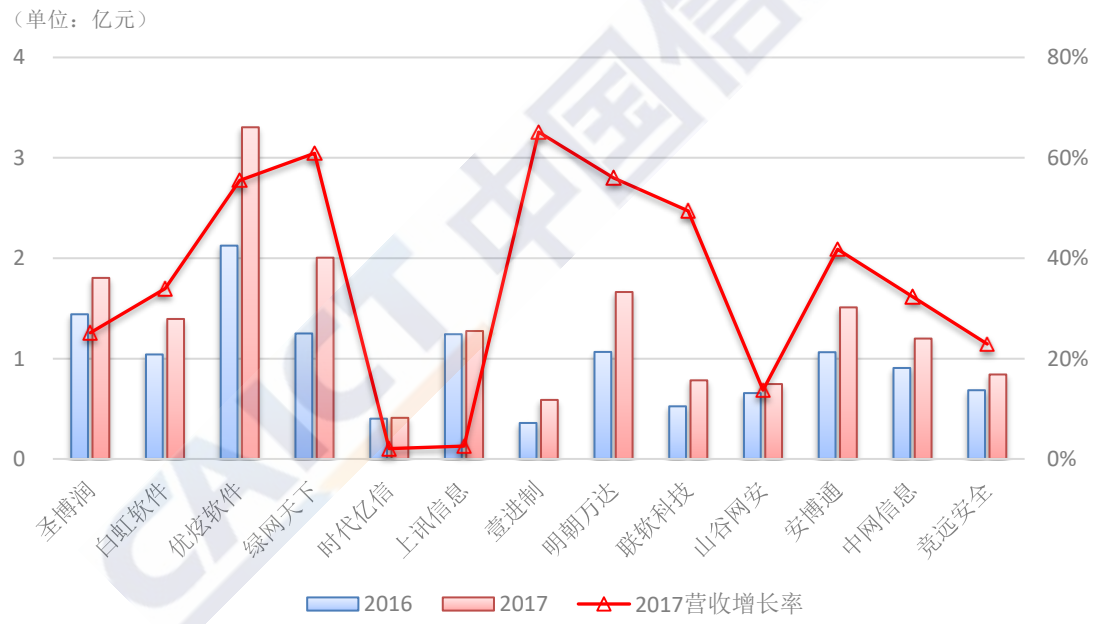


来源：中国信息通信研究院基于公开资料整理

图 21 2015-2017 年国内上市安全企业研发投入及增长情况

2. 新三板挂牌企业发展呈现两极分化

一方面，部分企业发展态势向好。69 家样本企业[23]2017 年平均营收达到 0.97 亿元，其中 13 家企业营收增长超过 50%；在净利润方面，盈利超过 30%的企业达到了 31 家，占所有样本企业的 45%。部分样本企业 2016-2017 年营收及增长情况如图 22 所示。**另一方面**，也有小部分企业选择退市。同质化产品服务的激烈竞争、技术水平市场认可度不高、企业市场占有率下降等因素共同作用，导致安达通、安宁创新、海加网络等企业黯然退出。



来源：中国信息通信研究院（基于 wind 数据整理）

图 22 2016-2017 年部分国内新三板挂牌安全企业营收增长情况

[23]统计范围包括：点景科技、圣博润、白虹软件、优炫软件、闽保股份、绿网天下、高士达、意畅科技、远望信息、时代亿信、上讯信息、信大捷安、宝利明威、国舜股份、创谐信息、万联网络、壹进制、明朝万达、七洲科技、中宇万通、思智泰克、圣目股份、虎符科技、信元网安、安信华、网博科技、盛邦安全、永信至诚、以太网科、海天炜业、天锐股份、峰盛科技、海加网络、联软科技、山谷网安、高正信息、安达通、瑞星信息、浪潮创新、奔凯安全等 69 家企业。

（三）我国网络安全企业发展特点及趋势

1. 联盟、协作共同体相继成立，企业间合作日趋紧密

一是大型 IT 厂商推进安全联盟建设，打造协同联动的网络安全防御生态。2018 年 3 月，华为联合天融信、微步在线、远江盛邦等厂商成立安全商业联盟，旨在通过创新架构深度整合联盟伙伴优势产品，实现终端、网络、应用等层面协同联动，构建全网协同立体防御体系。8 月，腾讯携手卫士通、立思辰等 15 家上市企业，成立 P16 上市企业协作共同体，将深化沟通合作，在应对网络安全威胁、加强基础设施建设、掌握关键核心技术、引领网络安全产业的发展和生态环境的构建发挥重要作用。**二是**云安全成为企业间合作的重点领域。浪潮与天融信、瑞星等安全企业携手共建云安全，例如天融信虚拟化安全防护系统、瑞星虚拟化系统安全软件实现与浪潮云海服务器系统兼容。

2. 军民融合步入深水区，军民携手维护国家网络安全

自 2015 年军民融合上升为国家战略以来，我国网络安全领域的军民融合路径日益明确，合作不断加深。截至目前，已有超过 30 家网络安全企业与军队有关部门开展了广泛而深入的合作。**一是**安全企业积极投身于军民融合网络安全保障。例如，安天科技成立网络民兵分队，为国家重大任务提供安全解决方案，强化应急保障支撑能力；高维数据提出网络安全军民融合新理念，推出了安全通信、安全存储、溯源取证等符合军队需求的安全解决方案。**二是**军民联手开展网络空间安全军民融合创新。360 集团在军队指导下创建了“网络空间安全

军民融合创新中心”，将推动探索网络民企参军“需求主导”模式、构建军民网络安全“共建共享”模式和完善网络装备技术“研用一体”模式。

3. 借力“一带一路”，我国安全企业探索“走出去”

“一带一路”战略的实施为网络安全企业提供了拓展国际市场的新机遇。例如，启明星辰亮相 GITEX2017，重点面向中东地区展示推广包括下一代防火墙、UTM、WAF、SIEM/SOC 等国际版本的安全产品及解决方案。美亚柏科面向“一带一路”有关国家提供安全领域专业培训服务，并推广了优势技术产品。绿盟科技中标马来西亚运营商项目，其集合 NTA 攻击检测、ADS 流量清洗和 ADS-M 集中管理的抗 DDoS 解决方案经历国际竞争而更趋成熟。观安信息与联合国亚太地区经济与信息化人才培训中心合作设立国内首个培训基地，为“一带一路”沿线国家提供专业安全培训，年度培训人次超过 200 人。

（四）安全产业生态环境建设持续推进

1. 投资机构持续助力安全企业融资活动

我国网络安全领域投资活动持续活跃态势。根据中国信通院统计数据，目前国内已获得融资企业已达到 135 家，参与网络安全领域投资企业 100 家。**一是**大型安全企业引领网络安全创新技术培育。360 企业安全集团及其创投基金，面向应用安全、云安全、移动安全、数据防泄漏、工控安全、车联网安全等领域培育挖掘有潜力的创新企业，目前已累计投资超过 10 亿，惠及近 40 个初创企业。**二是**专业投资机

构、产业基金等继续发力布局。国科嘉和[24]聚焦应用安全、大数据安全和云安全等领域，2017 年相继投资了炼石网络、瀚思安信、迅达云等网络安全企业，目前已披露的投资金额达到 2.3 亿元，被投企业分布在 Pre-A 轮至 B+轮的各个融资阶段。中国互联网投资基金[25]正式起航，2018 年 8 月完成对恒安嘉新等企业的首批投资。苹果资本专注于全球网络安全产业项目投资，国内已投项目包括安全宝、长亭科技、数字联盟等，同时正在筹建 10 亿规模的成长期安全基金。

2. 网络安全企业上市步伐明显加快，融资更为便利

2018 年 4 月，中央网信办和中国证监会联合印发《关于推动资本市场服务网络强国建设的指导意见》，支持符合条件的网信企业利用资本市场做大做强。受政策利好影响，网络安全企业步入上市快车道。例如，迪普科技于 2018 年 7 月过会，拟募资 4.63 亿元。迪普科技成立于 2008 年，专注于网络安全和应用交付领域。2017 年的主营业务收入为 6.16 亿元，净利润为 1.47 亿元。中新网安于 2018 年 1 月披露招股说明书，拟在创业板上市。中新网安成立于 2002 年，主要从事网络安全软硬件产品的研发、生产和销售以及网络安全服务。中新网安 2017 年实现营业收入 2.66 亿元，同期净利润为 5864.38 万元。

[24] 国科嘉和成立于 2011 年，是由中国科学院国有资产经营有限责任公司直接管理的一级投资平台。国科嘉和目前管理两支人民币创投基金、一支人民币并购基金、一支美元创投基金以及政府专项基金等多支基金，管理总金额达数百亿人民币。

[25] 中国互联网投资基金是经国务院批准、由国家网信办和财政部共同发起的国家级投资机构，战略出资企业包括中国工商银行、中国农业银行、中信国安、中邮人寿、中国移动、中国联通、中国电信等，基金规划总规模达 1000 亿元人民币。

3. 国家级网络安全产业园加快建设，打造世界一流产业集聚中心

一是武汉国家网络安全人才与创新基地进入实质性建设阶段。2018 年上半年，国家网安基地新增签约项目 12 个，协议投资 352 亿元，新增注册企业 16 家。在网安基地，正在建设的还有与网安学院相关的 5 个项目，包括展示中心、国际人才社区、网安基地一期基础设施、中金武汉超算（数据）中心以及启迪网安科技孵化园，投资总额约 216 亿元。截至目前，武汉国家网络安全人才与创新基地目前已签约项目 32 个，协议投资 2350 亿元，注册企业 53 家，注册资本 56 亿元。**二是**北京国家网络安全产业园区即将挂牌。2017 年 12 月，工信部、北京市正式启动国家网络安全产业园区（北京）建设，拟打造国内领先、世界一流的网络安全高端、高新、高价值产业集聚中心，到 2020 年，依托产业园区拉动 GDP 增长超过 3300 亿元，北京市网络安全产业力争达千亿规模，打造不少于 3 家年收入超过 100 亿元的骨干企业。各大网络安全产业园的建设，将形成一个巨大的开放式平台，加快我国网络安全产业形成产业聚集和产业链条，助推我国网络安全产业的持续发展。**三是**天津滨海信息安全产业园迎来首批企业入驻。该产业园总投资 45 亿元，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，打造成为产值超百亿元的国家网络安全产业综合基地。预计三年内，该产业园可培养数家上市企业，新增专利 200 项，培养专业人才 1000 名，实现产值 100

亿元以上。目前已有北信源等 17 家企业入驻。**四是**中国电科（成都）网络信息安全产业园获得增资。2018 年 4 月，产业园获得增资，目前总投资将超过 500 亿元。该产业园增资将有助于进一步为大数据安全、云安全等新兴产业发展提供保障，同时加强网络安全产业合作。

（五）多渠道促进网络安全人才队伍建设

1. 各地政府出台网络安全人才相关政策

自《关于加强网络安全学科建设和人才培养的意见》发布以来，各地政府积极响应，纷纷出台网络安全人才队伍建设政策文件。**一是**武汉市政府出台《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》，文件对人才安居政策、生活住房补贴和建立人才奖励机制等方面做出了明确规定，着力引进、培育网络安全领域高层次人才和团队。**二是**成都市政府先后出台包括《信息安全专项资金补贴》在内的 10 余项网络安全人才培养支持政策，并与四川大学、电子科技大学、中国网安等知名校企合作开展复合型网络安全人才培养计划，增强网络安全科研人才队伍力量。

2. 网络安全竞赛如火如荼展开

近年来，网络安全竞赛在我国各地如火如荼举行，竞赛形式和内容日益丰富，影响力持续提升。**一是**重点行业立足安全保障需求展开技能挑战。工业和信息化部、中华全国总工会指导，中国信息通信研究院、中国通信企业协会与中国国防邮电工会全国委员会在京联合举办了“2017 第二届通信网络安全管理员技能大赛”。在赛制上，设立

了实际攻防对抗、团队协作防御等环节；在竞赛环境上，新增设了大数据系统、IoT 等真实操作环境。竞赛共有 6000 余名行业选手参与，为网络安全保障工作持续有效开展起到积极的促进作用。**二是**业界携手促进网络安全人才技能提升。2018 年 8 月，国家网络与信息安全信息通报中心、国家密码管理局商用密码管理办公室支持，永信至诚主办，中科院信工所、清华大学、百度等单位联合协办的“网鼎杯”网络安全大赛拉开序幕。在赛制上，线上预选赛采用 CTF 解题模式，线下半决赛及总决赛采用 AWD 攻防对抗模式展开。大赛共吸引 7000 多支战队、21000 多名选手参赛。

3. 网络安全从业人员在职培训成果突出

网络安全人才稀缺也带动了网络安全培训市场蓬勃发展。有关机构、行业协会、安全企业等积极开展面向党政机关、事业单位和相关企业开展网络安全意识和技能培训，提升网络安全在职人员职业素养和技能水平，为网络安全工作提供必要的人才支撑。截至 2018 年 1 月，我国 CISP 持证人数[26]约为 2.5 万人；CISSP 持证人数[27]共计 2038 人，相较于 2017 年的 1372 人增加了 48.54%。网络安全从业人员在职培训体系的建立和完善，一方面将加快网络安全高端人才培养；另一方面将推动网络运维、软件开发等相关人员向网络安全人员转型，不断提升员工整体安全能力。

[26] 数据来源：北京汇哲信安知识分享平台
[27] 数据来源：https://www.isc2.org/en/About/Member-Counts

四、重点细分领域发展进展

结合国内外网络安全产业结构增速、投融资热度、技术布局进展等，2018 年白皮书重点对身份管理与访问控制、可管理安全服务、云安全、威胁情报服务、人工智能安全五个领域进行了跟踪分析。

（一）身份管理与访问控制领域活力涌现

1. 现状：大型厂商持续深耕，创新企业开拓前沿领域

身份管理和访问控制技术作为基础性安全技术，在网络安全体系中具有重要作用。我国身份管理与访问控制市场发展较早，上海格尔、吉大正元等专业领域厂商以及天融信、亚信安全等综合型厂商均在这一领域开展了多年深耕。主要产品分为两类：一是动态口令、数字证书等强认证技术产品，另一类是以集中管理为理念，集成帐号、认证、授权、审计功能为一身的 4A 管理平台等多种形态的产品。近年来，国内也出现了一批专注于身份管理与访问控制的创业公司问世，聚焦于云身份认证、单点登录等新兴技术领域，包括派拉软件、深圳竹云、上海硅孚、九州云腾等，如表 4 所示。

表 4 国内身份管理与访问控制领域创新企业

企业名称	创立时间	技术领域/特点
派拉软件	2008	使用 Docker 微服务架构，支持 SAML、OAuth、CAS 等主流协议，提供基于 Restful API 的服务；具备 IT 身份、BYOD、IoT 等多种身份接入以及企业应用、云应用、移动应用等身份管理能力；在单点登录（SSO）领域具备优势。
深圳竹云	2009	一是通过风险引擎、数据交互等提升智能分析能力；二是在云环境下的应用拓展，提供 IDssS 身份安全管理平台、云安全审计平台等。

续表 4 国内身份管理与访问控制领域创新企业

企业名称	创立时间	技术领域/特点
上海硅孚	2010	聚焦于身份治理领域，提供包含用户/组织机构、账号推送、群组、岗位、系统配置、审计等管理功能的智能身份管理产品，实现用户身份数据账本化管理。
九州云腾	2014	专注于“云大物移”领域统一身份认证管理；使用 Docker 微服务架构，采取 OpenID Connect 机制，支持 Fido 等 10 多种开发者认证协议。
国民认证	2015	深耕多模式生物识别技术领域，支持指纹、虹膜、声纹等多种生物识别技术；基于 FIDO+国际标准，推出了跨平台、跨设备、多认证方式的 AaaS 服务模式。
芯盾时代	2015	专注于移动安全认证领域，推出了多因素身份认证（MFA）、统一身份管理（IDaas）、智能行为认证（IPA）、物联网身份管理（IoTAM）、安全咨询服务(SCS)等产品和服务。
Authing	—	致力于云端身份认证服务;支持主流第三方 OAuth 配置接入;基于 HTTPS、JWT、MD5、SHA256、Salt 和非对称加密的安全身份认证；探索区块链技术应用。

数据来源：中国信息通信院根据公开资料整理

2. 展望：迎接数字经济发展新机遇

IT 技术的演进、数字经济的发展为身份管理与访问控制市场提供了崭新机遇。一是云计算、物联网、微服务、DevOps、移动计算等技术的发展，对身份管理和访问控制技术提出了新的更高要求。在管理对象方面，逐渐从“人”向设备、物、服务等对象扩展，鉴别这些对象的合法性和鉴别人变得同等重要；在技术实现方面，从单一、静态向多维、动态方向发展，基于风险的自适应能力需求日益迫切；在应用场景方面，从单点、独立向整个组织统一化、跨组织跨域方向发展，同时在支持传统的 IT 架构基础上，兼容私有云、混合云、公用

云等复杂环境。**二是**大数据、机器学习、人工智能等新一代信息通信技术快速发展，推动身份治理和威胁分析智能化升级。机器学习、威胁情报等技术的采用，使得内部威胁、欺诈行为等依靠传统基于规则难以发现的行为，有了被发现和识别可能。**三是**“互联网+”、大数据、信息消费等一系列重大政策推进实施，推动数字经济日渐繁荣，保障数字安全的基础上实现数据有序高效流动成为企业关注的焦点，市场对身份管理与访问控制的期待包括安全和合规、快速极简部署、良好交互体验、提升管理效率等。**四是**身份管理与访问控制与业务紧密结合的属性，造就国内厂商场景化发展优势。身份管理与访问控制解决方案需要对企业业务架构和应用系统的深刻理解，涉及应用整合、数据库&中间件、API 管理、开发拓展等各方面。特别是，高度集成的业务架构，多样化的开发者认证协议增加了打通业务实现对接的复杂度。国内身份管理与访问控制厂商可以通过与系统集成方、平台提供方开展合作，开展基于场景化的产品开发，并降低对接成本。

（二）可管理安全服务领域有望升温

1. 现状：服务价值和市场认可进展缓慢

总体看，我国可管理安全服务市场发展相对缓慢。**一方面**，相对“远程服务”，国内更为青睐“驻场运维”模式。目前，大部分网络安全专业厂商均具备 7*24 小时运营中心，提供网络威胁检测、分析、响应、处置等多种能力，但主要为相应安全产品的增值性服务，以及提供威胁情报等，尚难以成为独立的服务形态，因而市场规模十分有

限。现对于国外安全产品、服务一揽子外包服务，国内市场普遍更为倾向于本地驻场的安全运维模式，依靠本地的安全网络安全管理平台等产品和驻场运维人员，实现对本地网络设备、网络安全设备流量和日志等的采集处理、深度分析和事件处置。在安全分析需要依靠云计算技术实施的情况下，倾向于选择以私有云方式提供服务，以更好保障安全。**另一方面**，具备渠道优势的网络运营商提供的服务类型、服务深度等仍有待拓展。例如，中国电信推出的云堤高防是行业内标杆型产品，目前可提供 5000G 运营商级 DDoS 防御能力。但除了高防产品外，电信可管理安全服务仅覆盖反钓鱼、DNS 域名安全和 Web 网站安全等领域，服务类型有待进一步拓展。此外，尚未推出类似国外安全运营中心提供的一体化的、基于用户侧网络设备和安全设备等的安全运维模式，服务模式亟待进一步创新。

2. 展望：理念、政策等现实约束仍是最大挑战

相对于发展稳定、成熟的国际市场，我国可管理安全服务市场仍面临重重阻碍。现有政策标准中“本地化”要求，使得可管理安全服务面临“合规”难题。同时，主流认知也较难转变。一方面，设备级别的“远程管控”面临“依赖外部，更不安全”的担忧，另一方面，随时在岗的“驻场”模式无论技术能力如何，在响应方面似乎更为可靠。未来发展方向上，基于 SaaS 的云端服务和基于链路的增值服务前景相对明朗。**一是**基于 SaaS 的云端可管理安全服务模式逐步被接受。云计算普遍应用以来，用户对云计算的托管模式逐渐熟悉信任，

带动了安全观念的转变，云安全托管相对易于接受。同时，云计算与传统 IT 架构的差异，一定程度上加大了安全能力建设难度，促进用户更倾向于依靠专业的安全厂商和团队。**二是**基于服务链路的安全能力有望成为新的增长点。电信运营商提供的 DDoS 攻击防御已经得到市场的普遍认可，未来服务类型有望进一步拓展，包括威胁预防、事件监测、防御溯源等；云服务提供商、CDN 厂商则将借助已有计算、加速服务等渠道和资源优势，在数据安全、终端安全、应用安全等领域开展可管理安全服务的创新实践。此外，针对重大活动保障等特殊、临时性可管理安全服务需求逐渐增加。

（三）云安全领域生态初步成型

1. 现状：云安全发展态势持续向好

随着云计算在我国的推广普及，云安全市场逐步打开局面。**一是在公有云领域，**云平台厂商强化自身安全能力布局和输出。阿里、华为、腾讯等云服务巨头均建立了较为完备的云安全能力体系，可提供覆盖网络、主机、应用、业务、数据、管理、服务等一揽子安全产品和服务，如表 5 所示。同时，阿里云、华为云、腾讯云也建立了与 AWS Marketplace 相似的云市场，分别上线了 243 个、126 个、132 个第三方安全产品和服务，涉及云堡垒机、日志审计安全分析、云数据库审计、Web 安全评估服务等多种服务类型，建立了“自主”与“第三方”并存的生态格局。由于公有云市场主要为中小型企业，而且受到互联网免费经济和“免费安全”思维习惯影响，目前我国用户对第三方云

安全产品认可度仍十分有限。例如，在阿里云市场，近半年成交量超过50笔的第三方云安全产品仅有7个，且基本全部为免费产品。

表 5 国内部分云服务厂商安全能力介绍

类别		阿里云	华为云	腾讯云
网络安全	DDoS 防御	10T+带宽，单点1000G+	5T+带宽，单IP 最高 600G	5T 带宽，单点最高 900G
	云防火墙	✓	—	—
主机安全	主机安全	安骑士，功能包括：安全配置核查、漏洞管理、入侵防护、端口管理、日志管理等	HSS，功能包括：资产管理、漏洞管理、入侵检测、基线检查等	云镜，功能包括：密码破解拦截、异常登录提醒、木马文件查杀、高危漏洞检测等
应用安全	WEB 应用防火墙	✓	✓	✓
	网站威胁扫描	✓	✓	✓
	其他	爬虫风险管理	—	—
业务安全	内容安全	✓	—	✓
	其他	风险识别、实人认证、游戏盾	—	业务防控；移动安全
数据安全	数据加密服务	✓	✓	✓
	数据库审计	✓	✓	✓
安全管理	态势感知	✓	✓	✓
	密钥管理	✓	✓	—
	堡垒机	✓	✓	—
	SSL 证书管理	✓	✓	—
安全专家服务	安全专家服务	先知，包括：安全众测、等保、应急响应、漏洞扫描、培训、评估、代码审计、网站安全监测、安全加固、保障、演练等	ES，包括安全咨询、渗透测试、应急响应、等保合规等	SES，包括安全体检、安全监测、应急响应、渗透测试、安全加固、等保等。

数据来源：中国信息通信研究院根据公开资料整理

二是在私有云、混合云领域，安全专业厂商积极布局，围绕云安全监测、防护、管理等需求，提供一揽子安全解决方案。例如，亚信

安全推出了服务器深度安全防护系统以及虚拟安全管理中心；新华三聚焦云安全合规，推出了云平台安全架构设计与部署、云安全测评、云服务安全审核测评等服务支撑；安恒推出了天池云安全运营平台，可提供监测、防御、审计、态势感知等安全能力；山石网科推出了虚拟化防火墙和微隔离产品，分别提供租户级、业务系统的隔离与南北向防护以及提供云计算环境内虚机间东西和南北向安全防护。

2. 展望：政策利好驱动云安全发展再上新台阶

政策引导持续加码、安全合规需求增强有望助推我国云安全市场快速发展。**一是**云计算产业的政策导向增强，形成对云安全市场的带动力。2018 年 7 月，工信部印发《推动企业上云实施指南（2018-2020 年）》（以下简称《实施指南》）。这是继 2015 年 1 月国务院印发《国务院关于促进云计算创新发展培育信息产业新业态的意见》以及 2017 年 4 月工信部印发《云计算发展三年行动计划（2017－2019 年）》后，又一项促进云计算产业发展的重大政策。《实施指南》提出“到 2020 年，全国新增上云企业 100 万家，形成典型标杆应用案例 100 个以上，形成一批有影响力、带动力的云平台和企业上云体验中心”的发展目标，将对整体行业发展起到重要的拉动作用。特别是，《实施指南》全文 20 次提到“安全”，并明确提出“使用**云上主机安全防护、网络攻击防护、应用防火墙、密钥/证书管理、数据加密保护**等安全服务”，在强化云安全至关重要性的同时，也为增强云安全提供了细化的方向指引。**二是**安全合规需求进一步强化。包括我国《网络安全

法》及配套法规、欧盟 GDPR 等在内的安全合规要求日益明确，对于数据安全、业务运行安全等的合规投入将进一步增加。**三是**云安全事件频发有望增强云安全投入意愿。2018 年 3 月，亚马逊 AWS 存储桶泄露 50.4GB 数据；7 月，腾讯云发生故障导致创业企业数据丢失；同月，新西兰云储存托管平台 Mega 上午登录凭证泄露；8 月，亚马逊 AWS 配置错误导致域名注册机构 GoDaddy 数据泄露。受云安全事件影响，在政务、金融等关键领域的云安全投入有望增加。

（四）我国威胁情报市场平稳起步

1. 现状：威胁情报落地模式持续探索

在勒索软件等网络攻击实时性更强、规模更大、爆发更频繁的背景下，威胁情报价值逐渐显现。威胁情报立足更高纬度，识别分析攻击及危害性，提升安全防御智能化、自动化。2015 年以来，我国的威胁情报市场逐步发展。**一是**龙头企业建立威胁情报中心，提升自身安全能力。例如 360 威胁情报中心，依托云端大数据技术自动化处理和人工运营配合，提供多种类型的威胁情报服务；绿盟威胁情报中心（NTI），利用多源情报清洗与归并技术、大数据关联分析技术等关键技术实现情报自动化处理，助力构建立体协同防御生态。**二是**专注于威胁情报领域的创新企业逐渐涌现。例如，微步在线（ThreatBook）相继推出了威胁情报搜索引擎、情报社区、以及在线新建威胁检测平台、威胁情报分析和管理平台等产品和服务；天际友盟借助本地安全情报中心（SIC）实现与客户本地、云端平台对接，提供给多源情报

和管理服务。**三是**产业联盟等搭建威胁信息共享平台。中国互联网网络安全威胁治理联盟汇聚国内 90 余家企业，强化互联网网络安全威胁情报共享和协作。天际友盟、云盾科技、思睿嘉得等企业发起成立烽火台安全威胁情报联盟，通过天际友盟 RedQueen 平台，实现威胁情报的交互。

表 6 我国部分威胁情报平台介绍

项目名称	成立时间	主要产品/服务	特点
360 威胁情报中心	2015	ALPHA 提供威胁研判分析、文件信誉、失陷检测、云沙箱等产品和服务，可基于可视化和智能建模的自动化关联分析，挖掘关联对象和攻击事件。	汇集包括失陷检测 IOC、IP 信誉、文件信誉、文件的动静态分析数据、攻击者和病毒家族情报库等多维度情报数据。
绿盟威胁情报中心	2016	NTI 支持客户名称、事件名称、IP、域名、漏洞、文件 Hash 等情报查询；利用多源情报清洗与归并、互联网资产画像、关联分析等技术，提供关联情报追踪溯源、攻击者画像定位等。	NTI 提供互联网资产类、威胁类、漏洞类、热点资讯类情报，数量已达数亿。
微步在线	2015	提供威胁检测平台（软/硬件/API）、情报管理平台 TIP、恶意软件分析平台、情报社区、MDR 安全服务、OneDNS 等产品和服务。	TIP 可对多源情报进行统一存储、检索、对比，实施对情报产生、使用、静默、消亡的全生命周期管理，实现单点感知全网联动。
天际友盟	2015	提供情报订阅、情报平台 SIC、以及云端溯源、监控类品牌保护、关停类品牌保护等情报增值服务。其中 SIC 安全情报中心支持多元情报获取解析、数据信誉评价、数据聚合、告警管理、设备协同等。	在 SIC 基础上，可集成基于流量的检测（Ada）和本地威胁溯源（Alice）两个增强功能，提升威胁检测、预警、分析与取证能力。

数据来源：中国信息通信研究院根据公开资料整理

2．展望：威胁情报迈向产品应用新阶段

一是《网络安全法》为信息共享提供了法律依据。《网络安全法》第三十九条提出“促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享”，将网络安全信息共享上升为法律要求，将加速威胁情报体系建设。**二是**威胁情报标准加快制定，助力交换标准的统一。当前，国内外已经出现了 CybOX、STIX 和 TAXII 等多种威胁情报标准，由于各大厂商采用的标准不同，跨平台、跨系统、跨设备的对接协作难以实现，制约了威胁情报的应用推广。目前国家标准《网络安全威胁信息表达模型》等情报共享技术规范正在加快制定，提出网络安全威胁信息的基本框架，将有助于统一情报表达、促进情报共享。**三是**威胁情报与安全产品相结合将成为发展趋势。目前我国威胁情报的应用场景主要集中在安全事件的检测防御、攻击溯源以及应急响应，例如通过威胁情报阻断攻击，溯源分析查获证据，辅助事件处置等。威胁情报应用对于高级技术人员的依赖，极大限制了威胁情报的应用领域和效果发挥。而通过将威胁情报与入侵检测、防御等安全能力结合，例如将威胁情报能力集成到企业安全管理平台，可以一定程度降低人工参与度和参与门槛，同时改变企业安全产品各自为营、海量告警、处置效率低等现状，实现更高效的监测预警、更有效的防护联动，将成为威胁情报落地的重要方向。**四是**行业威胁共享平台建设，有望形成对威胁情报市场的带动力。开放和合作是威胁情报技术发展的必然趋势。中国信息

通信研究院将联合相关机构共同建威胁信息共享平台，聚合电信和互联网行业力量，共同加强威胁情报信息的共享，围绕关键信息基础设施保护、重大网络安全事件处置等工作打造紧密联动的生态合作链。

（五）人工智能与网络安全加速融合

1. 现状：“人工智能+网络安全”迈向产品应用阶段

伴随人工智能技术的快速发展，国内厂商日益重视人工智能与网络安全深度融合，积极推动机器学习、深度学习等人工智能技术在网络安全领域落地应用，助力提升网络安全风险预测、攻击防御等全方位能力。**一方面，**用户行为分析成为“人工智能+网络安全”落地的重点方向。人工智能技术通过IP、指纹、信誉库、历史行为等多维度关联分析，更为精准的对用户网络行为进行画像、评估风险点；应用知识图谱技术，将用户各类行为进行归类、聚合，筛选出具有某一共性的关联图，对未发生的威胁进行感知和预测；提供更为智能化的决策模式，突破了传统安全技术的局限。例如，腾讯利用人工智能技术强化网络运行、金融结算等特定场景中的用户行为分析，实现对恶意代码的监测与防御、网络谣言治理、有害信息鉴别等；安恒信息借助人工智能技术分析、跟踪并智能判定用户异常行为，实现对隐蔽威胁、未知攻击和0day攻击等网络攻击的检测和预警；观安信息基于机器学习和深度学习，通过无监督的异常检测算法对页面和用户进行快速检测，发现Webshell、XSS等异常页面和恶意扫描等异常行为。**另一方面，**人工智能技术对于数据分析实时性、准确性的提升，也激发了

厂商在身份识别、数据保护等领域的应用探索。平安科技以深度学习为基础，结合数据挖掘、生物特征识别等技术，通过采集面部信息等生物特征识别用户身份；默安科技利用机器学习算法，主动分析建立访问者信誉库，生成风险策略模型，提升对云安全威胁的感知力、防御力；墨云科技利用人工智能、机器学习等方式对用户的数据进行持续性安全验证；赛猊腾龙利用人工智能技术，对用户终端、存储和网络中的敏感数据进行发现、监控和保护。

2. 展望：人工智能将加快驱动网络安全技术革新

近年来，我国政府、产业界对人工智能技术发展和应用的重视程度不断提升，为人工智能发展提供了良好环境，也将进一步加速人工智能与网络安全的融合，引发网络安全领域的技术革新浪潮。**一是**人工智能将加快信息和情报流动的闭环构建。人工智能将推动传统的事件响应式的安全思维向着全生命周期的持续智能响应转变，构建全面的预测、基础防护、响应和恢复能力，实现威胁情报精准的发现、决策和处置。**二是**人工智能将推动未知威胁监测技术演进升级。依靠人工智能对流量、行为等的统计和关联分析，及时发现偏离正常行为模式的攻击或异常，将提升未知威胁检测和拦截效率。**三是**推动对于复杂攻击识别由专家模型向智能模型转变。人工智能应用将促进将持续积累专家经验转化为模型，提升 APT 等复杂攻击的智能预警能力。此外，尽管人工智能与网络安全融合进程加快，但人工智能技术本身带来的安全风险仍不容忽视，如自动化的编写分发恶意软件、可扩展

攻击的智能僵尸网络等。最大程度的发挥人工智能在网络安全领域的价值，需要正视其技术本身安全风险，及时做好安全风险应对，推动人工智能安全发展和应用。

五、我国网络安全产业前景展望

（一）国家意志和国家行动为产业发展注入强心剂

近年来，党中央高度重视网络安全。十九大报告指出，网络安全等非传统安全是人类面临的共同挑战之一，要坚持总体国家安全观，加强国家安全能力建设，坚决维护国家主权、安全、发展利益。习近平总书记在全国网络安全和信息化工作会议上强调，没有网络安全就没有国家安全，就没有经济社会稳定运行，要树立正确的网络安全观，积极发展网络安全产业，做到关口前移，防患于未然。网络安全新理念新思想新战略为网络安全工作提供了根本遵循，网络强国、数字中国、智慧社会等的建设为网络安全发展创造了宝贵机遇，同时，国家级产业基金、科技创新专项、重点产业园区以及一系列支持网信企业做大做强、优化完善产业生态的政策举措逐步落地实施，为激发企业活力、促进产业高速优质发展铺就了沃腴的土壤。预计到 2020 年，将有一系列细化丰富的产业发展扶持政策出台，产业发展重心和方向更为明确、发展信心和步伐更为坚定。

（二）关键信息基础设施领域仍是产业核心带动力

一方面，关键信息基础设施日益成为网络攻击的重点目标，安全防护能力建设需求迫切。美国防部、德核电站、印度外交部以及以色

列电力局等关键信息基础设施的攻击事件层出不穷，造成严重危害后果，也为我国敲响警钟。特别是，以社会工程为代表的攻击新理念、以网络武器为代表的攻击新工具、以自动化为代表攻击新方式将极大改变攻防博弈格局，增强关键信息基础设施安全防护能力迫在眉睫。另一方面，《关键信息基础设施安全保护条例》实施在即，网络安全“三同步”、检测评估、应急处置等细化要求将有效指导和规范关键信息基础设施保护实践。在两方面的作用下，预计未来 1-2 年，政府、金融、电信、能源、交通、教育、医疗、工业等领域网络安全投入意愿将进一步增强，特别教育、医疗、工业领域网络安全保障需求增长突出，在网络威胁监测预警、网络安全态势感知、网路数据和用户信息保护、突发事件应急响应以及安全合规等方面需求迫切。

（三）细分领域助力网络安全服务市场打开新局面

国际上安全服务连续多年占据安全市场的六成份额，而我国服务市场占比不足三成，“重产品轻服务”“劣币驱逐良币”等问题凸出，安全服务市场发展缓慢且艰难。近年来，随着网络安全事件频发和政策标准落地，应急服务、合规服务等服务市场发展态势逐步向好，为提升安全服务的价值认知、开辟服务市场空间起到一定助益作用。**一是**事件调查、应急响应、溯源处置等服务推动对安全服务价值认可。攻防是长期持续性对抗，本质是人与人的较量。在网络安全事件调查、应急处置等服务中，服务人员长期从事网络安全工作积累的对安全威胁的敏锐发现能力、对安全情报的分析利用能力、对安全事件的快速

响应能力得以充分体现。从而让企业在解决燃眉之急的同时，更加认可安全服务的价值和采购安全服务的必要性。**二是**合规性检查服务需求日益增多。等保 2.0 系列标准推动《网络安全法》中对于等级保护要求落地，企业自查和合规需求逐渐增多，合规性检查服务日渐兴起。有关行业组织、联盟等加大对检查服务机构、人员的管理，网络安全服务市场行为逐渐走向规范。

（四）以应用为核心成为安全技术创新支持新思路

自 2015 年起，电信和互联网行业践行“揭榜挂帅”思路，创新性的开展了网络安全试点示范工作，以实用性、创新性、先进性、可推广性为原则，以部门推荐、专家评审为依据，遴选并推广优秀技术手段项目[28]。3 年来，共收到项目申报 300 项,从中遴选出试点示范项目 130 项,入选项目企业投资总额达 16.6 亿元,在促进行业网络安全威胁监测预警、数据安全、域名保护等技术能力提升的同时，搭建了应用场景展示、供需对接交流的平台。电信和互联网行业实践为产业支持政策提供了新思路：**一是**强化“应用价值导向”，给予实用价值高、技术理念新、需求贴合好的“真”技术以支持，同时建立考察评估机制，加强持续管理，确保项目真实有成效。**二是**将关键信息基础设施保护需求与网络安全产业发展相结合，以产业创新带动能力升级，以能力建设驱动产业发展，有效发挥网络安全产业“关口前移”作用。预计未来，立足实际需求，以应用为核心的技术创新支持模式有望得

[28] 来源：http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057729/c5740828/content.html

到复制推广，在支持力度、支持方案、运作模式等方面有望进一步优化，更好支撑技术创新需求。

（五）网络安全产业生态协同开创产业发展新基调

网络安全整体、动态、开放、相对、共同的特性，要求技术、产业以协同为理念发展创新。近年来，呼吁产业协同、生态共建的声音日益增多，“强强联合”屡见不鲜，产业协会、联盟、协作体等相继成立，产业生态建设方兴未艾。未来产业协同的发力点，将主要聚焦在安全架构创新、情报共享、防御联动等方面：**一是**探索新型网络安全架构理念。科研院所、相关企业联合推进拟态安全等虚拟化异构安全体系、可信计算体系等技术体系架构创新应用，打通基础研究和技术创新衔接的绿色通道，力争以基础研究带动应用技术群体突破。**二是**促进威胁情报共享共用。威胁情报具有天然的共享属性。随着国家、行业、产业多层次的情报共享体系的逐步建立，威胁情报标准化规范化共享有望实现，从而打破安全厂商“各自为战”的防御局面，促进整体安全能力的共同提升。**三是**构建协同联动的网络安全防线。网络安全事件、应急处置、追踪溯源等需求持续增加，将加速厂商间有效的防御联动机制建立。

（六）职业教育和培训成为应对人才紧缺的关键点

当前，网络安全人才短缺已经成为全球面临的共同难题。美国、欧洲等相继采取了学科教育与职业教育并重的理念加快人才培养。例如美国明确了网络安全人才技能分类，指导职业发展的路径；欧盟网

络安全月开展持续性培训活动，助力从业人才技能提升。从我国看，一方面，目前我国网络安全学科教育年度培养规模约 1 万人左右，远不能适应日益加剧的网络安全人才缺口需要，另一方面，从业人员普遍在知识储备、技能等方面存在短板，难以适应网络安全新形势要求。重要行业和领域网络安全运维保障、监管执法等人才短缺、技能不足等问题日益严峻，亟需通过职业教育和培训补齐缺口。预计随着我国网络安全人才培养体系完善，政策重点将有望向职业教育和培训方面发力，相关机构已经在积极探索网络安全职业资格、能力认定等制度和标准框架，网络安全人才培训教育市场迎来新的增长点。

CAICT 中国信通院

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62304839、62300128

传真：010-62304980

网址：www.caict.ac.cn