CAICT 中国信通院

网络与信息安全产业白皮书

（2015 年）

中国信息通信研究院

2015年12月

版权声明

前　言

当前，发展壮大网络与信息安全产业的需求日益迫切。一方面，国际网络空间的竞争博弈日趋激烈，安全产业是否壮大已经成为衡量国家网络安全综合实力的重要标准。另一方面，“互联网+”融合创新的新业态使得各关键行业和重要系统对网络安全保障的需求不断增加，安全产业已成为网络强国建设的基础保障。新形势下，我国安全产业迎来了发展的关键机遇，也面临诸多挑战。

我院推出网络与信息安全产业白皮书（2015 版），将从产业政策、产业结构、生态环境、技术标准、企业发展等维度对国内外产业发展进行分析探讨，提出进一步推动我国安全产业发展的建议举措，以及产业发展应重点把握的方向和领域，希望与业界分享，共同推动我国安全产业蓬勃发展。

说　明

本白皮书研究范围包括网络与信息安全产品和服务两类。其中，安全产品包括防火墙、入侵检测与防御、统一威胁管理、安全内容管理、安全评测工具、终端安全管理、身份管理与访问控制等；安全服务包括安全集成、安全评估、安全运维、安全培训。

目 录

一、全球安全产业发展趋势.....1
（一）政府发展政策.....1
（二）产业规模结构.....7
（三）产业生态环境.....10
（四）安全技术标准.....15
（五）企业发展经验.....19
二、我国安全产业发展现状.....22
（一）政府发展政策.....22
（二）产业规模结构.....24
（三）产业生态环境.....26
（四）安全技术标准.....30
（五）企业发展现状.....34
三、我国安全产业面临的机遇与挑战.....37
（一）我国安全产业发展的关键机遇.....37
（二）面临的主要问题和挑战.....38
四、促进我国安全产业发展的关键举措.....42
（一）加强安全产业政策引导.....42
（二）优化产业生态环境.....44
（三）技术方向和关键领域.....45
（四）安全企业发展建议.....46
附件：国际安全企业研究.....48
（一）美国典型安全企业研究.....48
（二）创新型安全企业研究.....49
（三）网络安全300强企业中非美国企业研究.....51

一、全球安全产业发展趋势

（一）政府发展政策

政府产业发展政策是扶持网络与信息安全产业的重要手段，国际上的产业相关政策种类涵盖网络安全相关立法、国家网络安全战略、国民经济发展战略、国家网络空间及各关键领域行动计划，具体措施包括：扩大政企合作、加大资金投入等。

1. 美国：政府在安全产业发展中扮演重要角色

美国作为全球领先的网络强国，政府在国家网络安全政策和战略制定方面体现出很强的前瞻性和执行力，在安全企业发展壮大的过程中直接扮演着重要的角色。美国的安全产业促进政策具体呈现以下特点：

一是“促进安全产业发展”已成为美近期网络空间政策普遍涉及的重要领域。美国在奥巴马政府上台之前，网络安全政策制定曾处于“迟缓期”。但近两年，网络安全立法、纲要、行动计划的出台速度大幅提升。虽然美国并无专门针对安全产业的政策，但各类法律、战略等普遍提及加强政府与企业的合作或扩大政府对国产信息产品、服务等的采购，此类规定常被美政府部门或安全企业活用为促进安全产业发展的重要政策。近期美国涉及促进安全产业发展的主要立法、行动计划等简要整理如表 1 所示。

表 1 美国安全产业促进政策

名称	性质	主要相关内容
《提升关键基础设施网络安全行政命令》	行政命令	要求美国联邦政府部门与其安全供应商之间维持良好的信息共享机制
《2013 年边境巡逻员薪资改革法案》（2014 年生效）	法案	提升网络安全专家薪资待遇，提升政府部门和私营机构网络安全人才的收入水平
《2014 年国家网络安全保护法》	法案	奠定联邦政府和私营机构网络安全威胁信息共享的法理基础
《2014 年网络安全框架》	行政命令	加强政府部门和私营机构的合作，发挥安全企业在保障关键基础设施安全方面的重要作用
《2014 年增强网络安全法》	法案	明确企业等私营部门在联邦网络安全研究和发展计划中的作用，加强公私合作
《2014 联邦网络安全研究和发展纲要》	纲要	明确私营部门在联邦网络安全研究和发展计划中的作用，继续加强网络安全保护政企合作
《2015 年网络安全战略》	战略	强调政府与私营部门，尤其是 IT 企业合作的主旨不变

来源：中国信息通信研究院

二是不断加强政企合作，巩固安全企业在维护网络空间安全中的重要地位。美国《2014 年增强网络安全法》要求“相关机构在战略纲要的制定和更新过程中与产业界、学者以及涉及到的利益相关方进行充分的合作”，《提升关键基础设施网络安全行政命令》与《2014 年网络安全框架》中也强调在关键基础设施网络安全保障领域加强企业和政府部门的合作，发挥安全企业的重要作用。这些政策一方面充分响应了企业诉求；另一方面保证了企业参与网络安全保障实践时，与政府部门享有平等地位，企业的技术成果得到充分

保护。

三是持续加大安全产业投入，帮助企业营造良好的市场环境。美国政府近期预算报告显示，美国联邦政府是目前全球网络安全投资最多的政府。预计 2016 年美国联邦政府的信息技术支出预算将达到 863 亿美元，其中用于网络安全的预算额为 140 亿美元，占比 16.2%。美国众议院军事委员会也专门建议国防部将国防预算用于建立新型安全防护技术评估机制，并促进这些新技术的应用。因此，在许多安全企业的发展过程中，美国政府都给予了采购倾斜等实际支持。此外，美国也非常注重网络安全人才培养投入，《2014 年增强网络安全法》明确提出通过设立奖学金、开展竞赛等方式优化安全人才培养机制。2015 年《网络空间行动计划》也要求政府定期对各企业的安全技术团队进行能力培训和测试。

2. 以色列：重视技术能力开发，政府推动产业聚集

以色列目前是仅次于美国的世界第二大网络产品和服务出口国，目前拥有 200 多家相关企业和多个网络安全研发/科研中心，2014 年以色列网络安全软件销售额达 400 亿美元，其安全技术市场份额目前占全球的 5%。以色列的安全产业政策主要呈现以下特点：

一是重视安全企业的技术实力提升。以色列每年遭受大量的网络攻击，因此，以色列政府将“确保本国人民具备应对各类网络安全威胁的能力”作为国家网络战略的核心，将建设网络安全“欧洲主要技术中心”作为技术聚集区的主要建设目标，并多次在网络安全

教育、投资、创新等领域的政策中提及需“维持以色列在技术领域的领导力”。

二是引导企业聚集发展以形成规模效应。以色列政府注重发挥“先进技术园区”在沟通学界、安全企业和国防军队三方面的重要作用，为网络安全领导协同、项目合作、数据共享、资源互补和人才流动提供便利。2013 年以来，以色列着力打造了贝尔谢巴和特拉维夫两个高新技术中心，将安全企业进一步聚集，以便提高各项产业促进政策的实施效率。2014 年，以色列推出了面向高新区网络安全企业的税收减免措施。以色列总理级官员也常视察高新区，并不断加强园区的电力、交通、教育等基础建设，为技术聚集区的可持续发展创造了良好条件。

三是培养和挖掘最顶尖的网络技术专家。以色列 2013 年推行了培养青少年网络精英的新国家法案，计划创建一个“数字铁穹”，保护重要基础设施免受黑客入侵和病毒骚扰。此外，以色列为安全人才的进一步培养提供完善的资金支持，并通过出台优惠政策帮助投资者寻找优质投资项目，设法提高投资回报，以此来吸引欧美的重量级投资机构。

3. 英国：鼓励技术创新，帮助企业拓展海外市场

英国是欧洲传统的网络安全强国，其网络产业的发展水平位于欧盟前列，英国自公布《2011 年英国网络安全战略》以来，网络安全领域产值已超过 60 亿英镑，创造了约 40000 个就业岗位。英国的

网络空间治理策略呈现出“政府干预为辅、行业自治为主”的特点，其安全产业政策体现出以下特点：

一是注重鼓励安全企业开展技术出口和创新。英国制订了详细的计划以利用新兴网络产业，并鼓励企业根据自身切实利益开展网络安全创新。为了实现创新成果的输出和效益最大化，英国还制定了专门的政策以帮助企业向海外销售产品或服务，拓展国际市场。到 2016 年底，英国政府预计将使网络安全出口翻番，到 20 亿英镑；并到 2020 年增加到 40 亿英镑。

二是成立专门机构保障政策落实效果。英国政府为了落实相关政策，加强政府和安全供应商之间的协调，由贸易投资署牵头设立了包括学界、政府和工业界等各界代表的“网络成长伙伴关系”。该伙伴关系致力于获得更多的出口市场，提升英国安全企业在国外市场的竞争力，并通过巴西、印度、海湾国家和东南亚等地的驻外机构收集信息，以了解当地的和区域的网络安全情况、高价值项目和出口风险。同时，英国贸易投资署还积极对外发展双边关系，寻求网络产品和服务的出口机会。

4. 其他国家和地区

日本、澳大利亚、欧盟等国家和地区也出台了相关的安全产业扶持政策，主要围绕明确产业发展方向、加强产业资金投入、加大人才培养力度等方面做出了具体规定。

日本安全产业政策偏重于明确产业发展目标，在《2013 年网络

安全战略》中，将“积极参与国际标准制定，建立工业控制系统评估和认证机制，要求政府部门采购采用尖端技术的产品，实现国内信息安全市场规模翻倍、信息安全人才缺口减半”确立为促进产业发展的主要方向。同时，将“开展公司合作培训计划及技能竞赛以挖掘人才，支持参加国际会议或出国学习以培养具有国际竞争能力的人才”作为人才队伍建设的目标。

澳大利亚安全产业政策注重强化政企合作，在公布的《网络安全战略》中，将“企业-政府伙伴关系”列为重点战略措施，鼓励政府与企业共同促进关键基础设施、网络、产品和服务领域的安全和恢复力。利用 AusCERT[1]加强与私营部门间的可信伙伴关系。通过关键基础设施保护的可靠信息共享网络，与企业进行更广泛的接触，促进一体化网络安全最佳实践途径，促进基于恢复力概念的关键基础设施保护。

欧盟安全产业政策立足于安全意识普及和安全人才培育，其在网络安全战略和“安全网络计划”中提出，“针对专业安全技术人员进行网络安全演练、针对在校学生举行代码编程竞赛等主题活动、针对公共和私营组织进行员工培训、针对所有网络用户开展计算机和移动保护以及隐私保护的宣传等”。力图在强化民众网络安全意识的同时，培育更有利于安全企业生存的市场环境，提升安全企业及从业人员的技术水平。

[1]AusCERT：即 CERT Australia，澳大利亚计算机应急响应中心

（二）产业规模结构[2]

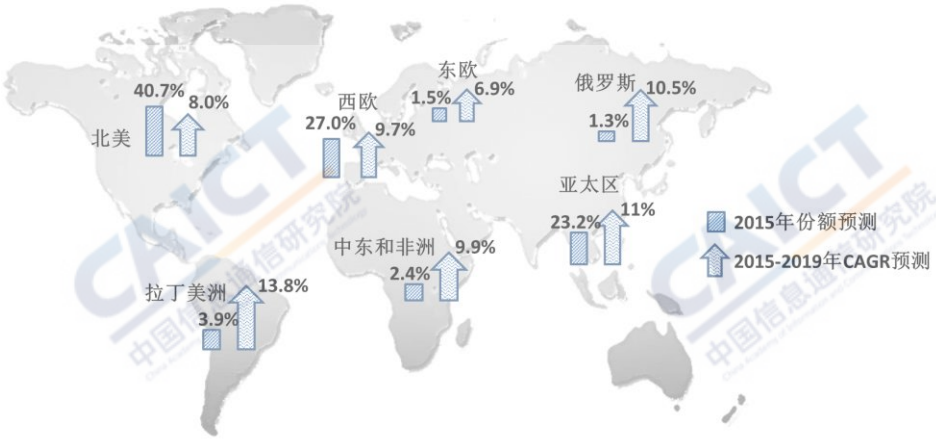
1.全球安全产业规模快速增长，北美市场规模领先

2014 年全球安全产业规模达到 732.67 亿美元，预期 2015 年增长至 833.78 亿美元，2016 年至 2019 年有望保持超过 8%的增长速率。当前，安全产业规模仅占全球 IT 产业规模的 2%，但随着安全产业的高速发展，未来这一占比将有望提升。

从产业规模看，以美国为主的北美地区占据全球市场最大份额，其次是西欧及亚太地区。2015 年，北美地区安全产业规模预计将达到 339.38 亿美元，占全球安全产业规模的 40.7%；英国、德国等西欧国家安全产业规模将达到 225.14 亿美元，占全球比例的 27%；日本、澳大利亚等亚太国家安全产业规模将达到 193.01 亿美元，占全球比例的 23.2%；非洲、东欧、拉丁美洲等其它地区安全产业规模占全球比例低于 10%。

从产业增速看，拉丁美洲和部分亚太新兴地区增速领跑其他地区。2015 年至 2019 年，巴西、墨西哥、阿根廷等拉丁美洲地区的安全产业复合年均增长率（CAGR）将达到 13.8%，中国、印度、泰国等亚太新兴地区达到 13.4%，西欧地区达到 9.7%，北美地区仍将保持 8%的年复合增长率高速增长。

[2]数据来源：基于 Gartner 数据整理，未来 5 年全球 IT 市场增长速度约 2.5%.



来源：中国信息通信研究院（基于 Gartner 数据整理）

图 1 全球安全产业分布及增长情况

2. 安全服务市场态势向好，安全产品市场格局稳定

2014 年，安全产业各细分领域市场份额为：安全服务 58.09%，安全软件 26.92%，安全硬件 14.99%。其中，安全服务产业规模 418.08 亿美元。预计 2015 年安全服务在安全产业中的比重有望进一步提升，达到 61.1%，2019 年达到 64.9%。

安全服务领域，安全咨询、安全运维、安全集成、安全外包的份额分别为：36.8%、3.0%、30.7%、29.5%。其中，安全咨询领域，Deloitte[3]、IBM 和 EY[4]三家企业市场占有率最高，市场份额均超过 10%；安全集成和外包领域由 Dell、IBM、Symantec[5]等企业领军，Trustwave[6]、CenturyLink[7]、Orange Business Services[8]等专业厂商参与竞争。从增速看，安全外包服务增速最快，2014 年达到 14.59%，安全咨询

[3]Deloitte：德勤，Deloitte Touche Tohmatsu Limited（DTTL），安全咨询公司
[4]EY：Ernst&Young，安永会计师事务所
[5] Symantec：赛门铁克，安全公司
[6] Trustwave：面向企业和公共部门提供信息安全性与合规性管理解决方案的全球性供应商
[7] CenturyLink：美国电信运营商
[8]Orange Business Services：Orange（原法国电信）旗下提供企业级综合通信解决方案的分支机构

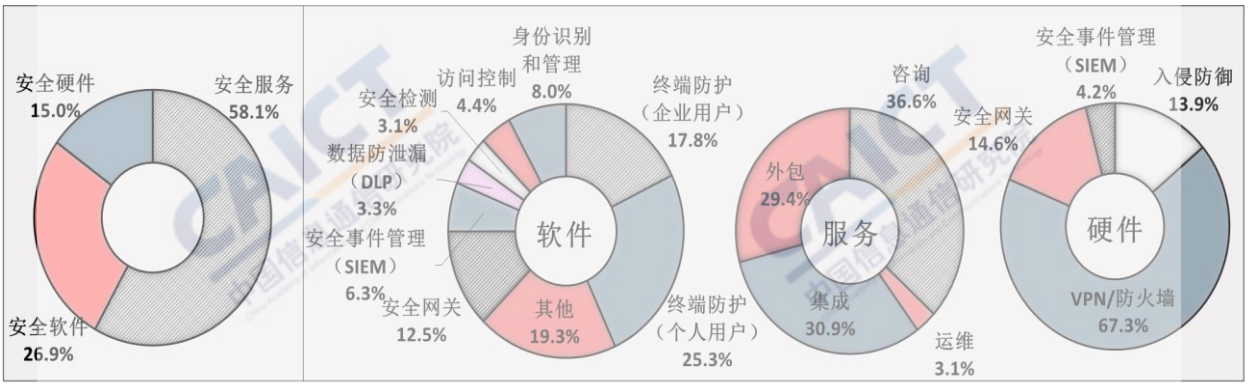
次之，为 8.07%，安全集成与安全运维分别为 6.16%、5.24%。此外，以云服务外包方式提供安全防护能力的云安全服务逐步落地，2015 年，全球基于云的安全服务产业规模将达到 31 亿美元，2017 年预计将达到 41 亿美元。威胁情报服务产业有望保持 60%的年增长率，2018 年产业规模将达到 15 亿美元。

安全软件领域，产业规模达 193.9 亿美元。其中，Symantec、McAfee[9]、IBM、TrendMicro[10]、EMC[11]和 Kaspersky[12]等 6 家企业占据 45%市场份额。以终端防护软件、安全事件管理(SIEM)软件、数据防泄露（DLP）软件和安全网关为代表的基础设施保护类软件占安全软件比重超过 85%；身份识别与访问控制类软件比重超过 10%。

安全硬件领域，产业规模达 115.8 亿美元，Cisco、CheckPoint[13]、Fortinet[14]、Palo Alto Networks[15]、McAfee、Blue Coat[16]和 Juniper[17]等 7 家企业合计占有率超过 50%。以防火墙和入侵防御设备为主的网络安全设备占据安全硬件 62.8%份额；安全网关设备和安全事件管理硬件份额为 17.6%；身份识别与访问控制类硬件份额为 6.6%。预计安全态势感知能力将在安全产品中广泛应用，到 2017 年，超过 30%

[9]McAfee：迈克菲，网络安全和可用性解决方案的供应商
[10]TrendMicro：趋势科技，网络安全软件及服务供应商
[11]EMC：易安信，美国信息存储资讯科技公司
[12]Kaspersky：卡巴斯基，网络杀毒及安全解决方案供应商
[13] CheckPoint：软件公司，网络安全解决方案供应商
[14]Fortinet：飞塔，网络安全设备供应商
[15]Palo Alto Networks：美国安全防火墙和入侵检测系统领先企业，成立于 2005 年，总部位于美国加州
[16]Blue Coat：应用交付网络技术厂商
[17]Juniper：瞻博网络，网络和安全性解决方案供应商

的防火墙将具备安全态势感知能力。



来源：中国信息通信研究院（基于 Gartner 数据整理）

图 **2** 2014 年全球安全产业结构分布

（三）产业生态环境

国际市场上活跃的流动资金、企业间自发形成的协作联盟、此起彼伏的峰会和竞赛、专业的第三方咨询和评价成为安全技术创新、企业跨越式发展的重要支持和推动力量。

1. 灵活健康的融资环境成为创业孵化、企业发展的加速器

一是网络安全创新企业获得国际风险投资机构的密集投资。在过去 5 年中，1208 家互联网安全创业公司在国际市场融资超过 70 亿美金，仅 2014 年一年全球安全产业获得的投资就高达 20 亿美金[18]。从国别看，获得融资的企业中，美国居首，以色列次之。从投资方看，多数企业获得了来自 2 家以上风险投资机构的投资。从领域看，投资聚集于云安全、数据防泄漏、可视化、网络取证等安全热点技术。

[18]数据来源:数据公司 CBInsights

表 2 2015 年部分企业融资情况（单位：百万美元）

企业	国别	领域	2015 年融资情况		总融资额	投资方
Barkly	美国	终端安全	A 轮	12.5	17	New Enterprise Associates (NEA)
BitSight	美国	安全评级	B 轮	23	49	Comcast Ventures、Globespan Capital Partners 等
Checkmarx	以色列	软件应用安全	—	84	—	Insight Venture Partners
CounterTack	美国	大数据分析	C 轮	15	—	TenEleven Ventures、EDBI
CrowdStrike	美国	基于 SaaS 的下一代防火墙	C 轮	100	156	Google Capital. Rackspace
Cryptzone	美国	安全内容管理	B 轮	15	—	Kayne Partners、Medina Capital
SafeBreach	以色列	数据防泄漏	—	4	—	Sequoia Capital、Angel Shlomo Kramer
Twistlock	以色列	虚拟化安全	—	2.5	—	YL Ventures
WireX	以色列	网络取证	—	9.3	—	Vertex Venture Capital、Magma Venture Capital、 Entrée Capital
Ziften	美国	终端可视化	—	24	—	Spring Mountain Capital、Fayez Sarofim

来源：Cybersecurity Ventures,"Cybersecurity Market Report"

二是安全企业上市门槛低、溢价高、融资额大，上市融资的成功案例成为业内最佳示范。以 FireEye[19]为例，虽自 2004 年创立以来净利润持续为负，上市前多年持续亏损上千万美金，但在超高估值预期下，于 2013 年顺利上市，上市首日股票较发行价增长 80%，最

[19]FireEye：火眼，美国网络安全公司

终募集 1.75 亿美元资金，为企业的后续研发投入、市场推广奠定了坚实基础。

2. 自发产业联盟搭建起交流协作、信息共享的桥梁

随着新兴技术的发展，在各领域自发兴起了一批安全产业和技术联盟，联盟成员通力合作，实现信息价值转化增值，增进企业互信互补，有力促进产业协同发展。

一是在推动信息技术标准化及应用方面发挥重要作用。美国威胁信息共享领域的 STIX/TAXII[20]标准得到了包括政府部门、CERT[21]、标准化组织、防病毒厂家、Anti-APT[22]厂家、检测类产品厂家、云安全服务厂家和专业情报厂家等 70 余家机构的支持，共同推动统一规范的威胁信息共享的实现。CSA[23]、Allseen Alliance[24] 等联盟也在云安全、智能制造等领域推动了安全相关标准的制定和应用。

二是搭建威胁信息共享平台。Fortinet、Intel/McAfee、Palo Alto Networks、Symantec 共同组建了 CTA[25]，专注于安全漏洞、恶意软件样本、僵尸网络的控制设施等威胁信息。联盟明确了成员间共享信息的最低要求，对共享数量规模、时效、状态、公开情况严格限制。在苛刻的标准之下，最具实力的安全企业组成互信共享的联盟，成为威胁信息共享实践的重大突破。

---

[20]STIX/TAXII: Structed Threat Information Expression/ Trusted Automated Exchange of Indicator
[21] CERT：Computer Emergency Response Team，美国计算机应急响应中心
[22]Anti-APT ：APT 攻击防御
[23]CSA：Cloud Security Alliance，云安全联盟
[24]Allseen Alliance：物联网 Allseen 技术联盟
[25]CTA：Cyber Threat Alliance，网络威胁联盟

三是合力应对国际网络安全犯罪。由英国政府倡导并支持的ICSPA[26]，联合国际间商业组织、政府机构及 Trend Micro 等安全企业通过国际间的网络安全项目打击网络犯罪，发布数据安全、网络攻击等态势报告，强化网络安全保护意识。

3.论坛峰会成为企业展示、技术交流和人才挖掘的基地

一是展会性论坛成为安全企业的展示平台。由美国 RSA[27]公司组织的 RSA 大会 2015 年吸引了超过 500 家参展企业，这些企业通过发放传单、演讲案例、技术比武等方式，宣传各类新式安全技术产品、安全服务及安全解决方案。

二是技术性峰会成为安全前沿技术交流的沙龙。德国 TROOPERS 论坛为寻求更纯粹的网络安全技术探讨，不允许产品供应商展示和销售。论坛通常邀请来自知名公司的首席信息安全官、IT 审计师、网络安全管理员、安全顾问等欧洲安全圈重量级人物参会，提供精彩的演讲以及与资深专家交流的宝贵机会。

三是攻防结合的黑客竞赛成为安全威胁发布、技术切磋和人才挖掘的宝库。起源于 1996 年 DefCon 全球黑客大会的 CTF[28]赛，发展至今已经成为全球最成熟的竞赛模式之一，每年全球有近 4000 支战队在 DefConCTF 赛中角逐，仅 2015 年就举办积分赛 36 场。除 CTF 外，安全破解、安全防御赛也逐渐兴起，黑客竞赛经过如互联网模

[26]ICSPA：International Cyber Security Protection Alliance，国际网络安全保护联盟
[27]RSA：信息安全解决方案的提供商，被 EMC 兼并
[28] CTF：Catch The Flag，夺旗赛，网络安全技术人员之间进行技术竞技的一种比赛形式

式般的快速迭代日趋成熟，从爱好者的自发切磋行为，演变成为人才展示、培养、选拔的完整机制。

4.第三方研究、咨询、认证机构引领安全技术创新趋势

一是媒体、研究机构等各方的产品评选和企业评比提升了安全企业的市场影响力。例如，仅 2015 年，Lancope[29]就分获了 InfoWorld 2015 技术年度奖、Security of Computer Magazine 英国奖、SANS Institute 最佳高级威胁识别奖、INQUIRER Tech 最佳产品奖、Atlanta Business Chronicle 先导奖等奖项。这些奖项提升了创新产品的知名度，促进了先进产品的推广和应用，增强了企业、尤其是中小企业的市场竞争力。

二是完善的安全产业咨询体系成为安全技术发展的有力向导。IDC[30]、Gartner[31]、Cybersecurity Ventures[32]等机构密切跟踪安全技术趋势、安全市场份额走向，提供覆盖全球安全领域的深度研究报告，评估现状预测未来。Gartner 用技术成熟度曲线和魔力象限形象地展示出安全技术的发展形态、发展轨迹及发展趋势，通过年度 Cool Vendors 评选挖掘新颖的、创新的、具有潜力的、甚至能够改变市场格局的技术或服务，发现技术创新趋势并形成市场需求引导力。

三是独立第三方安全认证机构引领了安全产品的技术优势。例

[29]Lancope：美国流量分析和网络监控领域领先企业，成立于 2000 年
[30]IDC：International Data Corporation，国际数据公司，信息技术、电信行业和消费科技咨询、顾问和活动服务专业提供商
[31]Gartner：信息技术研究和分析咨询公司
[32]Cybersecurity Ventures：网络安全市场调查公司

如，在防病毒领域，英国西海岸实验室的 Checkmark[33]认证、英国的 VB100% Award[34]、德国 AVTest 测试等专业安全认证，引领杀毒引擎技术革新；在云安全领域，CSA 推出 CCSK 和 STAR 认证，推动了基于云的安全构架和保障。这些相对客观、公正、权威的第三方认证，形成了引导安全技术趋势、激励企业持续创新的重要力量。

（四）安全技术标准

信息通信技术的创新应用推动新产品、新业务、新业态、新模式加速涌现，传统安全问题不断向新兴技术领域渗透，新兴安全威胁层出不穷，云安全威胁、数据安全威胁、高级持续性威胁（APT）、未知安全威胁以及智能制造领域安全威胁的有效应对成为全球安全技术与标准发展的重点方向。

1.安全产品与服务加速云端转型，“云化”成为 ICT 技术革命演进方向

云计算的广泛应用驱动云服务高速增长，而云服务特有的虚拟化技术则进一步增加了网络攻击防御的难度。为有效应对云安全威胁，云安全防护技术、云安全解决方案、云安全体系架构等概念应运而生并不断发展。**一是“云模式”引领安全防御技术创新。**通过部署在云端的服务器集群，完成恶意样本分析、篡改特征验证、用户交互反馈等工作，提升原有产品防御能力和云服务场景适用能力。

[33]Check Mark：英国病毒研究机构西海岸实验室针对杀毒软件查毒及杀毒能力的国际认证
[34]VB100% Award：英国著名病毒测试中心 Bulletin 版发给诊断率 100%、误诊率 0%软件产品的奖项

二是综合性云安全解决方案逐渐取代单一产品。结合云服务特性，从虚拟化主机安全、网络安全、数据安全等维度提供体系化的解决方案，突破了单一产品的局限性。**三是云安全三层体系架构成为趋势。**以云基础设施、云网络、云应用构成的三层结构逐渐确立，为用户提供差异化、定制化的安全服务。

2. 数据规模和价值提升，数据安全保障技术亟待突破

大数据技术的蓬勃发展和融合应用，大大加快了网络数据价值的攀升。同时，数据安全威胁加速升级和蔓延，网络数据和用户个人信息面临严峻挑战。因此，数据安全保障体系与数据防泄漏技术产品迎来发展新契机。以数据分类分级为基础，通过敏感信息发现、识别、审计等管理技术，以及数据加密、脱敏、泄露监测等保护技术的全面集成，构建可视化的数据安全统一管理体系成为主流发展方向，技术难点集中在自然语言处理、数据挖掘及聚类分析等方面。

3. APT 攻击愈演愈烈，防御技术成为安全研究热点

以高价值的企业、政府机构以及敏感数据信息为目标，以窃取商业机密，破坏竞争甚至是国家间的网络战争为目的的 APT 攻击正加速蔓延。APT 攻击具有长期盯梢、定点入侵、持续渗透等特点，对传统的基于特征库的被动防御体系提出挑战，以深度沙箱检测、历史数据回溯和关联分析为核心的 APT 攻击实时检测、防御和追溯技术也成为安全领域的研究热点。

4. 应对未知威胁，威胁情报分析和态势感知正当发力

传统依赖边界防御的静态安全控制措施正逐渐被基于大数据分析的智能安全手段所取代，信息安全技术逐渐从被动的事后分析演变为主动的事前防御。以大数据分析为基础的威胁情报分析和安全态势感知技术被认为是应对新型未知威胁的有效途径，并受到国外政府和企业的高度重视。美国联邦政府、国家安全局、国防信息系统局等在联邦范围内推广和实施以情报分析、安全感知、主动防御为核心的科技项目，强化对美国国内重要信息资产的保护，同时感知监控他国网络应用，相关安全企业也致力于研究威胁情报分析和态势感知技术，推进产品化进程。

5. 智能制造引领业态重塑，安全技术创新迎来新战场

随着工业互联网信息化步伐的加快，智能制造成为信息化和工业化深度融合的方向和突破口，而网络安全漏洞的爆发式增长、终端的高度智能化、无线等新技术的应用都给智能制造领域带来了新的安全风险。为此，转换安全防护理念，推动安全技术创新成为解决智能制造安全问题的关键所在。在智能设备领域，在数据采集、传输、分析的不同环节强化安全设计，部署轻量级安全模块，以及依托云端防护成为趋势。在智能系统领域，相关企业纷纷建立体系化的漏洞防护机制，缩短攻击事件响应时间窗口以保障生产，同时，传统的静态安全域划分方式也逐渐被安全域随生产域动态变化的防

护手段取代，IT 与 OT[35]的高度融合促使隔离安全向体系化安全转变，通过综合安全监测、安全审计、风险管理等安全手段提供协同防护。

6. 各国高度重视标准研制，加快新兴领域安全标准布局

近年来，国际安全领域标准体系日渐完善，ISO[36]、ITU-T[37]等标准化组织已发布两百余项安全技术标准[38]，同时加快云计算、物联网、工业互联网等领域布局[39]。此外，围绕国际标准主导权的争夺日趋显性化，世界各国纷纷加强标准研究，争取占据领先优势。美国拥有六百余个政府和非政府的标准制定机构，其中，NIST[40]作为研究安全领域标准的核心机构，定义了超过 450 个常用标准和建议措施，涉及策略规划、风险管理、安全技术等方面，涵盖云安全、工业互联网安全等领域[41]。由于 NIST 是在美国国会授权下代表政府参加标准化活动机构，其标准制定者与标准化活动管理者的双重身份使得其制定的标准和规范在政府和企业间得到了广泛的推广和应用。欧盟设立了 ECMA[42]、ETSI[43]等标准化组织，致力于信息技术产品和系统安全评估框架、电子签名、密码算法、合法监听等方面标准的制定，

[35]OT：Operation Technology，运营技术
[36]ISO：International Organization for Standardization，国际标准化组织
[37]ITU-T：ITU-T for ITU Telecommunication Standardization Sector，国际电信联盟远程通信标准化组织
[38]主要包括 ISO 的 ISO/IEC 15408、ISO/IEC 27000 系列，ITU-T 的 X.500、X.800 系列等
[39]包括云安全相关 ISO 17789、ISO 27017、ITU-T X.1642、ITU-T Y.3600 标准，物联网安全相关 ITU-T Y.2060、ISO 30141 标准，工业互联网安全相关 ISO 13849-1 标准等
[40]NIST：National Institute of Standards and Technology，美国国家标准与技术研究院
[41]以 SP 800 系列安全标准为代表，包括《云计算梗概和建议》、《公有云中的安全和隐私指南》、《增强关键基础设施网络安全的框架规范》等标准和规范
[42]ECMA：European Manufactures Association，欧洲计算机制造联合会
[43]ETSI：European Telecommunications Standards Institute，欧洲电信标准化协会

对数据安全和用户信息保护有着严格的规范和应用；英国 BSI[44]发布的BS7799标准已成为信息安全管理领域的国际标准;作为工业大国，德国也制定了IT基线保护手册、智能电表测量系统等信息安全标准，其DIN[45]已在国家、欧洲和国际层面开展工业4.0相关安全标准化工作；日本的JIS[46]、韩国KISA[47]等标准化机构也以ISO、IEC等国际标准组织为中心，积极推行国内网络与信息安全标准化工作。

（五）企业发展经验

以美国为首的西方发达国家高度重视支持安全企业发展，安全企业凭借领先的技术、高效的协作模式牢牢占据网络空间优势地位，呈现出如下发展趋势。

1.IT厂商、安全厂商通过兼并收购加速产业链布局

2014 年至今，安全领域并购活动近 50 笔，IT 巨头、安全巨头活跃在第一线。一方面，Palo Alto Networks、AVG Technologies[48]、Splunk[49]等知名安全企业不断兼并初创型企业以获取知识产权、及时跟进技术。另一方面，Microsoft、Google 等 IT 巨头通过并购增强安全技术实力。兼并收购成为安全企业快速发展的重要途径，也是当前全球产业界实现资源和技术互补、打造综合竞争实力的普遍选择。

---

[44] BSI：British Standards Institute，英国标准协会
[45]DIN：German Institute for Standardization（Deutsches Institut für Normung），德国标准化学会
[46]JISC：Japanese Industrial Standards Committee，日本工业标准调查会
[47]KISA：Korea Information Security Agency，韩国互联网络振兴院
[48] AVG Technologies：捷克安全公司，主要从事计算机安全软件业务
[49]Splunk：企业数据软件公司，全球第一家上市的大数据分析公司

表 3 2014 年—2015 年部分企业投资并购情况（单位：百万美元）

收购方	国别	被并购方	国别	领域	金额
Raytheon	美	Blackbird Technologies	美	监视、安全通信	420
Raytheon	美	Websense Inc	美	Web 安全、数据安全、内容安全	1900
BAE Systems	英	SilverSky	美	云安全	232.5
Gemalto	法	SafeNet	美	数据保护	890
IBM	美	Lighthouse Security Group	美	身份识别/访问控制	—
AVG Technologies	荷	Location Labs	美	移动安全	220
Singtel	新	Trustwave	美	可管理安全服务	810
Lookingglass	美	CloudShield	美	威胁情报	—
EMC	美	CloudLink	加	云安全	—
GTT Communications	美	MegaPath	美	可管理安全服务	152.3
Microsoft	美	Aorato Ltd	以	应用防火墙	—
Microsoft	美	Adallom	以	云安全	320
F-Secure	芬	nSense	丹	安全咨询、评估	—
Opera Software	挪	SurfEasy	加	VPN	—
AVG Technologies	荷	Privax	英	隐私服务	—
Splunk Inc	美	Caspida	美	威胁检测	190

来源：Cybersecurity Ventures,“cybersecurity market report”

2. 安全技术授权成为优化产品和解决方案的重要方式

为完善其网络威胁防御系统解决方案,Cisco 获得 Lancope 的授权，使用其明星产品 StealthWatch 优化威胁识别方式；Webroot[50]取

[50]Webroot：英国安全软件公司，反病毒软件领域领导厂商之一

得了 Sophos[51]的 AntiVirus with AntiSpyware 病毒查杀引擎授权，并将该引擎与自主研发的 Spy Sweeper 一同整合到其反病毒软件中。

3.赴美融资成为创新型中小安全企业的优先选择

中小型安全企业是专业领域技术创新的重要主体，分析 2015 年 RSAC Innovation Sandbox[52]入围企业成长路径，即使是成立时间不足 3 年的初创公司，都能够得到世界顶级风险投资动辄百万美金的资金支持。西方发达国家也充分发挥多元化市场资本运作机制，引导天使基金、社会资本投资于网络与信息安全创新型企业，鼓励创新企业上市融资。

4.非竞争企业间的技术、方案合作不断拓展深化

Palo Alto Networks 与 VMware[53]、Citrix[54]、Splunk 等虚拟化、大数据分析公司建立了战略合作伙伴关系，同时与 ForeScout[55]等初创公司、Symantec 等安全巨头以及 ARISTR[56]等非安全企业加强合作。寻求更广范围、更多形式的合作成为安全企业迅速扩充实力的重要方式。

---

[51]Sophos：英国安全软件公司

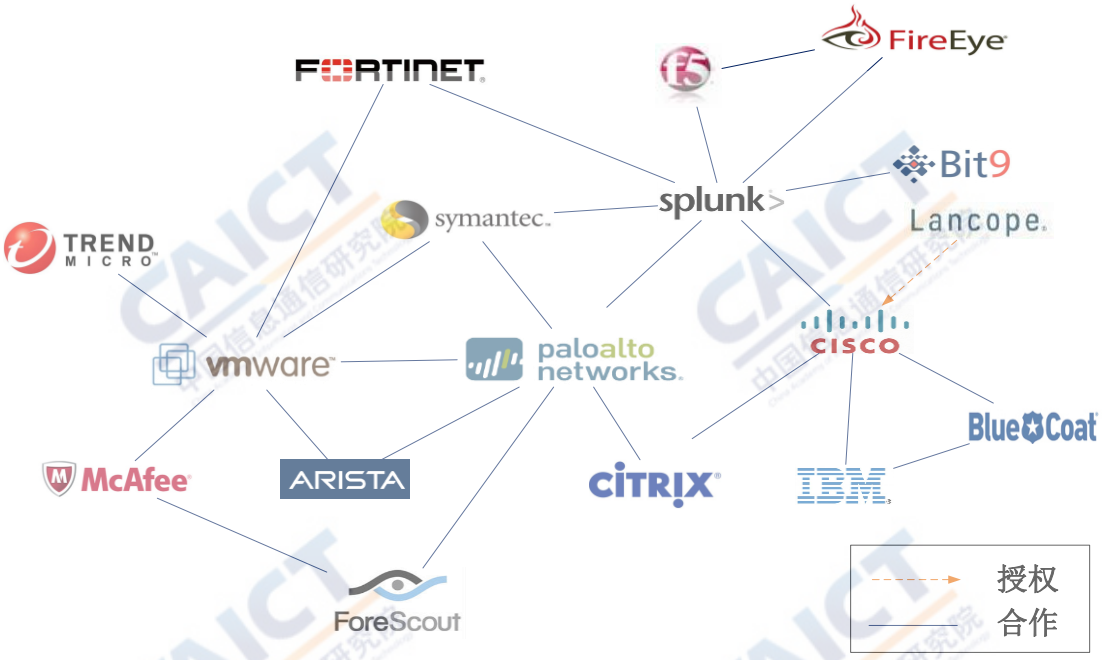
[52]Innovation Sandbox：可译为创新沙盒，是由 RSA 大会组织开展的、评选最具创新价值的企业产品活动。这一活动已经成为安全产业技术创新和投资的风向标，自“创新沙盒”活动开展以来，每年的赢家都在获胜后的一年内成功获得投资，并发展成为业界领跑者

[53]VMware：威睿，美国虚拟化解决方案的领导厂商

[54]Citrix：思杰，美国虚拟化网络和云服务领域领导厂商

[55]ForeScout：威胁动态识别和访问控制技术领先企业，成立于 2000 年，总部位于美国加州，研发中心位于以色列

[56]ARISTR：美国云计算网络设备提供商，2004 年成立，2008 年上市，其创始人曾担任 Cisco 资深副总裁



来源：中国信息通信研究院

图 3 企业间技术授权和产业协作示意图

二、我国安全产业发展现状

（一）政府发展政策

随着我国网络与信息安全工作的重要性不断提升，安全产业发展成为近年来政策扶持的重要领域，我国政府明确要求安全与发展同步建设，扶持中小安全企业创新成长，推动安全产业发展。

1. 将发展安全产业作为网络与信息安全建设的重点

安全产业已成为近来网络与信息安全政策制定着力考虑的主要方面。我国《信息安全产业“十二五”发展规划》成为推动信息安全产业向体系化、规模化、特色化、高端化方向发展，做大做强信息安全产业的指导文件。在《工业和信息化部关于开展电信行业网络安全试点示范工作的通知》中提出在电信行业遴选网络安全优秀

实践案例，并促进先进技术和经验的行业推广应用。试点示范工作将网络与信息安全企业纳入了参与单位的范畴，起到了促进安全企业与基础电信企业开展合作的作用。已公布的《网络安全法（草案）》也明确提出“国家促进网络安全技术和产业发展”，并要求国务院和省、自治区、直辖市人民政府“统筹规划，加大投入，扶持重点网络安全技术产业和项目”。

2. 将保障安全作为新兴技术领域发展的根基

我国近几年发布的新兴技术领域发展指导性文件均将保障安全作为基本原则或重点任务。国务院发布的《关于积极推进“互联网+”行动的指导意见》将“完善互联网融合法律法规和标准规范，增强安全意识，强化安全管理和防护，保障网络安全”作为“互联网+”行动的原则之一；《关于推进物联网有序健康发展的指导意见》要求加强物联网重大应用和系统的安全测评、风险评估和安全防护工作，保障物联网重大基础设施、重要业务系统和重点领域应用的安全可控；《促进大数据发展行动纲要》要求切实加强关键信息基础设施安全防护，做好大数据平台及服务商的可靠性及安全性评测、应用安全评测、监测预警和风险评估；《中国制造 2025》提出应加强智能制造工业控制系统网络安全保障能力建设，健全综合保障体系。

3. 将安全企业纳入新兴产业扶持政策的受惠对象

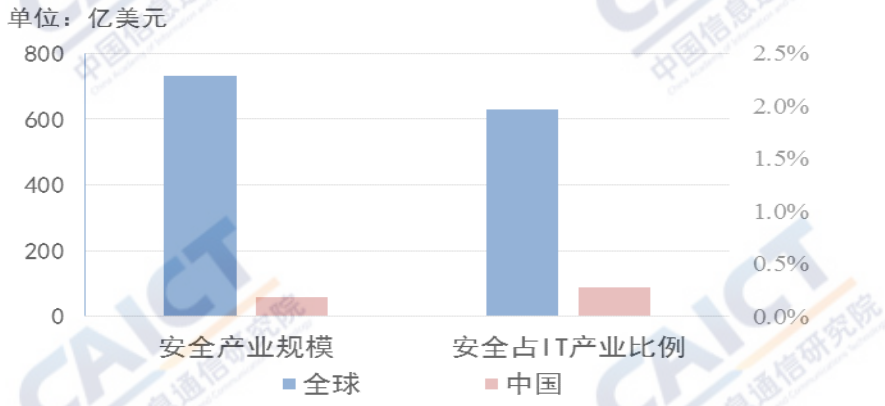
我国近来发布的产业扶持类政策，基本都涉及鼓励企业进行技术创新、促进新兴产业企业发展以及为中小企业营造良好市场环境

等内容。例如：《“十二五”国家战略性新兴产业发展规划》将新一代信息技术产业列为国家战略性新兴产业，提出加快信息安全关键设备的研发和产业化，直接促进了信息安全关键设备生产企业的发展。此外，国家出台的一系列税收优惠政策，包括高新企业税收优惠、双软企业税收优惠、技术开发免缴增值税、专利申请费用减免等，也全面覆盖到安全产业，为安全企业创新发展提供激励和优惠。

（二）产业规模结构

1. 国内网络安全产业规模持续扩大

根据中国信息通信研究院统计测算，2014 年国内安全产业规模约为 393.7 亿元。从调研企业数据看，企业营收较 2013 年增长超过 15%。根据工信部 2014 年电子信息产业统计公报数据，2014 年我国信息产业总规模达到 14 万亿元，安全产业占信息产业比重为 0.28%，相较 2010 年 0.14%有明显提升[57]。



来源：中国信息通信研究院

图 4 中国安全产业规模与全球安全产业规模对比

[57]安全产业占信息产业比例：2010 年为 109.6/78000=0.14%；2014 年为 393.7/140000=0.28%

2. 政府、金融、电信、能源等重点行业领域应用领先

我国政府、金融、电信、能源四大行业领域安全市场需求强烈，2014 年市场份额合计超过 60%。随着网络安全日益受到重视，国家关键信息基础设施的安全保障要求不断加强，带动重点行业和领域安全市场快速增长。同时，伴随智慧城市、“互联网+”、智能制造等发展规划的逐步推进，制造、医疗、旅游等领域安全市场日渐兴起。

3. 安全产品与服务市场维持七三分格局

2014 年我国安全产品产业规模达 277.9 亿元，占比 70.58%。安全防火墙、身份管理与访问控制、统一威胁管理、安全内容管理产品占据市场主要份额。由于资产管理、采购制度等传统规则约束，安全产品仍以软硬件结合产品为主导，纯软件产品仅在病毒查杀、访问控制等终端安全领域占据优势。

安全服务产业规模达 115.8 亿元，占比 29.42%。其中，安全评估、安全集成占安全服务市场份额的 90%。随着 IT 虚拟化的转型和云服务理念的渗透，安全服务市场份额有望进一步提升。同时，安全人才数量难以满足快速增长的市场需求，安全攻防人才、IT 运维人员的安全知识和技能培训有望驱动安全培训市场繁荣。

表 4 我国安全细分产业规模

类别		规模（万元）
安全产品	防火墙	681058
	入侵检测和防御	182125
	统一威胁管理	291866
	安全内容管理	336417
	安全评测工具	69960
	终端安全管理	208060
	身份管理与访问控制	402341
	安全平台	257000
	其他安全产品	350000
安全服务	安全集成	567440
	安全评估	337126
	安全运维	224803
	安全培训	29000
总计		3937195

来源：中国信息通信研究院

（三）产业生态环境

1. 企业创业孵化与上市融资取得积极进展

随着创投机构将目光移向安全领域、安全企业开展前瞻性产业布局、产业基金的相继成立、一批企业上市形成行业示范，我国安全产业融资环境正不断优化完善。

一是创业投资机构、安全企业担起产业孵化重任。北极光创投在安全领域投资布局近 10 年，2007 年投资山石网科，后者目前成为国内统一威胁管理领域领导者;2011 年投资移动安全公司信歌互联，已被百度收购；2012 年投资安全宝，已被腾讯全资收购；2015 年投

资云计算提供商云杉网络、威胁情报公司微步在线等企业。启明星辰、绿盟等老牌安全企业近年来也相继投资多家初创企业，为中小企业创新成长提供资金支持。

二是在严苛的上市条件下，我国安全领域已有超过 20 家企业成功上市融资。在主板市场，亿阳通信、航天信息、东软集团等企业上市；在中小板市场有启明星辰、卫士通上市融资；在创业板市场，有北信源、蓝盾股份、立思辰、拓尔思、美亚柏科、任子行、绿盟等企业上市。在新三板市场，天融信、上讯信息等企业新近挂牌成功。

三是安全产业发展基金相继成立，加速产业孵化。2015 年 8 月，中国互联网发展基金会在北京正式挂牌，基金会由国家互联网信息办公室主管，将致力募集资金、促进国际交流合作、开展专业培训等。11 月，工业和信息化部、国家安全生产监督管理总局、国家开发银行、中国平安签署《促进安全产业发展战略合作协议》，拟组建千亿规模安全产业发展投资基金，对有明确发展潜力的安全细分领域进行启蒙，助推安全产业发展。

2. 各领域安全产业联盟相继成立作用初显

近年来，我国相继成立了多个安全产业联盟，将安全领域的专家、企业、院校及相关机构紧密联系在一起。

一是区域性产业联盟推动地方项目工程安全建设、技术交流和金融合作。中国数字信息与安全产业联盟联合山西相关企业机构，

开展技术交流、项目讨论等；中关村网络安全与信息化产业联盟目前成员单位已突破 80 家，联盟设立了政策指导委员会、企业移动计算工作组(EMCG)、金融创新服务平台等机构推动相关安全标准制定、技术交流和联盟企业间的融资合作。

二是新兴领域安全联盟推动产品与安全同步研发应用。例如，工业控制系统信息安全产业联盟联合 24 家工业企业、安全企业、院校和其他机构共同推动工业控制系统安全，多次举办工业控制系统信息安全峰会，促进工业控制系统安全技术与产品的研发和应用。

三是企业发起的事实联盟打造全新安全业态。阿里推动建立的云安全生态圈目前召集了包括安恒、Array Networks[58]、深信服、山石网科在内的 14 家国内外知名安全企业参与,在阿里云平台提供近 20 款安全应用，以云生态为牵引，调动企业云安全产品研发应用。

3. 国内网络安全攻防赛事日渐兴起

自 2014 年至今，各类网络安全竞赛如雨后春笋般拔地而出，国际黑客竞赛热潮已全面涌入中国。

一是各大网络安全峰会均将黑客竞赛作为大会的重要环节。例如,2015 中国计算机网络安全大会设立了《中国网络安全攻防大赛》环节，设计渗透测试、漏洞分析、漏洞修复、安全防护等实战项目，普及安全基础知识，强化人才技能培养。

二是专业安全赛事成为安全技能展示、学习、交流的重要平台。

[58]Array Networks：SSL VPN 领域的市场领导者，汉鼎亚太和美国风险投资合伙人共同投资的私营公司

中国通信企业协会通信网络安全专业委员会联合中国国防邮电工会全国委员会举办的“通信网络安全管理员技能大赛”，得到工信部和全国总工会的支持，参与人数超过 5000 人。全国网络安全技术对抗赛（XCTF）在全国范围内设立多场次巡回选拔赛。福建、江苏、陕西等各地通信管理局组织开展了年度网络安全技能大赛。百度顶尖网络安全大赛（BCTF）和阿里巴巴安全技术竞赛（ALICTF）设立了校园巡展和宣讲环节，将人才的培养与挖掘渗透至校园。

三是攻防演练成为企业安全能力展示、产品宣传的重要舞台。例如，百度云加速产品发布会组织了由云服务提供商、基础电信企业、相关机构共同参与的 DDoS 攻防实战演练，在逾 10 分钟的演练时间内，攻击流量峰值达 1Tbps，刷新了全球 DDoS 攻击最大流量的历史记录，以真枪实弹的场景演练博引眼球。

4. 安全咨询机构增多，评价机制初步形成

网络安全热潮推动产业咨询需求攀升，安全研究日渐兴起，同时安全产品和技术认证在类别和范围上进一步拓展。

一是安全产业研究逐渐成为安全领域研究机构的重点业务。例如，咨询平台安全牛 2015 年 10 月推出了第一期“中国网络安全企业 50 强”，依据销售收入、人员规模、技术水平、申请专利数量、参加重要技术演讲和攻防赛事次数等指标对国内安全企业进行分类排名，为国内外行业和机构了解中国安全企业基本情况提供参考。

二是行业管理机构、相关单位密集开展产品测评和资质认证。

从认证性质看，部分认证为强制性认证，如公安部安全专用产品销售许可证；部分为非强制性认证，如互联网安全研究中心 Web 防火墙认证。从认证领域看，涉及政府、电信、军工等行业领域。从认证范畴看，主要以针对安全企业和安全产品的测试和认证为主。

表 5 我国安全产业相关认证情况

机构	资质名称
中国信息安全测评中心	1) 信息技术产品安全测评证书—EAL3 认证系列信息技术产品自主原创测评证书 2) 信息安全服务资质证书 3) 信息安全风险评估资质证书
中国信息安全认证中心	1) 中国国家信息安全产品认证证书（3C）
国家保密科技测评中心	1) 涉密信息系统产品检测证书 2) 涉密信息系统集成资质
国家密码管理局	1) 商用密码产品品种和型号证书 2) 商用密码产品销售许可证 3) 商用密码产品生产定点单位证书
公安部	1) 计算机信息系统安全专用产品销售许可证
中国人民解放军信息安全测评认证中心	1) 军用信息安全产品认证证书
互联网安全研究中心	1) WEB 应用防火墙认证证书

来源：中国信息通信研究院

（四）安全技术标准

我国网络与信息安全产业经过多年发展，通过与国际企业与机构的合作交流、学习和引进国际先进的技术和产品、紧跟国际安全产业发展趋势，目前在网络与信息安全相关产品研发和标准制定方面都取得了一定成果。

1. 云基础设施逐步落地，云安全问题受各界关注

随着各主流云基础设施在国内建设完毕，相关的云安全问题也在国内各界引起关注。在发改委组织实施的国家信息安全专项中，明确涉及了云操作系统安全加固、高性能异常流量检测和清洗等云安全技术与产品。北京、上海、深圳、杭州等各地政府先后开展云计算创新发展试点示范工作、建设各级云计算中心，助力我国云计算及云安全技术的发展创新。各学术机构和高校积极参与各类国家专项、863 计划等云安全相关科技项目，在云数据隐私保护、云计算环境中恶意行为检测、云安全追责管控等方面展开研究。阿里云、华为、奇虎 360 等国内企业与 CSA 密切合作，加强云安全相关技术和产业的互助交流，在防火墙、入侵检测、病毒防护等方面也推出了相应的云安全解决方案。

2. 数据安全形势严峻，信息泄密防护受到重视

近年来，用户敏感信息泄露事件在国内频频发生，给企业信誉、经济等方面带来了巨大的损失，政府和企业对数据安全防护以及安全产品的自主可控提出了前所未有的严格要求。在此情况下，启明星辰、绿盟、天融信等国内企业纷纷推出 DLP 系统，与国外 DLP 系统更关注防范外部窃密事件相比，由于我国数据安全管理制度不完善、内部人员泄密概率较大、泄密者易逃脱法律制裁，我国 DLP 系统更注重对内部泄密事件的防范。

3. APT 攻击常态化，防御手段寻求新发展方向

近年来，我国境内受 APT 攻击影响的主机数急剧上升，攻击范

围从传统信息网络蔓延到工控网络、移动互联网等其他信息系统。目前，360、翰海源（被阿里巴巴收购）、安天、知道创宇等国内安全企业纷纷展开对 APT 攻击防御技术的研究，依托恶意代码检测、入侵检测、蜜罐、大数据分析等技术对 APT 攻击各阶段进行跟踪和分析，加强对 APT 攻击检测和防御产品的研发。

4. 威胁情报分析和安全态势感知技术研究已经起步

受国内外重大安全事件影响及国外安全企业启发，我国逐渐意识到建设以基础数据为核心的主动防御体系是应对未知威胁的重要途径，并于 2012 年起开始针对木马僵尸网络、移动互联网恶意程序等安全威胁的情报分析和态势感知平台建设。随着抵御未知威胁攻击在国内受到高度重视，国家 863 计划、国家信息安全计划以及国家自然科技基金项目中均引入了安全态势感知相关的内容。此外，国内多家企业也开始着手建立威胁情报分析和态势感知系统，部分已实现产品化。

5. 重点扶持工业互联网发展，全面开展相关安全产品和技术研究

随着两化融合的深入推进，我国网络攻击威胁也逐渐向工业互联网领域渗透，针对重要信息系统、基础应用和通用软硬件的攻击事件频发，同时，工控系统漏洞引发的安全风险也向互联网、智能终端泛化演进。国内企业目前已针对工业网络安全防护网关、工控防火墙、工控现场安全基线及行为监管等工业网络安全防护产品开

展技术研发和产品应用，同时构建智能制造工业控制系统网络安全保障体系，加强接入控制管理和外包服务管理等配套举措。

6. 标准制定全面推进，国际地位有所提升

我国安全标准研制工作虽起步较晚，但在各行各业的积极参与下，安全标准化工作全面推进，国际地位也有所提升。**一是国内标准组织、企业、研究机构积极投身标准化工作，协力推进安全标准制定。**目前 TC260[59]已发布了安全标准 140 余项，CCSA[60]发布或起草的通信领域安全标准共计 230 多个，涉及信息安全技术与机制、信息安全管理、信息安全评估以及保密、密码和通信安全等领域。**二是紧跟国际发展趋势，积极开展新兴领域安全标准研究。**随着新技术新应用的兴起与发展，有关云计算、物联网、工业控制系统安全、移动互联网、智慧城市等领域的安全标准化工作已经开始启动，目前已发布了多项云安全国家标准，正在进行物联网安全框架设计、工业控制系统安全架构等标准研制，初步构建了新兴领域安全标准体系框架。**三是国际标准研制地位提升，逐渐发挥主导作用。**近年来，我国政府、产业界、学术界日益重视国际标准研制工作，参与人数与提交文稿数量逐渐增多，由我国主导完成的国际安全标准在数量上以及涉及领域上均有所突破。以 2014 年 ITU-T SG17 会议为例，在全部 63 篇提案文稿中，我国占 23 篇，最终被采纳 19 篇，涉

[59]TC260：全国信息安全标准化技术委员会
[60]CCSA：China Communications Standards Association，中国通信标准化协会

及电信业务安全、云计算安全、泛在网安全、身份管理、对象标识应用技术以及安全应用技术等内容。2013 年我国主导研制的云计算安全标准《云计算安全框架》获批成为国际标准，2015 年智能制造总体标准《工业物联网背景下的智能制造概述》在 ITU-T 立项，我国在国际安全标准领域的话语权逐步提升。

表 6 新兴技术领域主要国内外厂商

新兴领域安全技术		国外厂商	国内厂商
云安全	流量分析、恶意样本分析、虚拟化安全等	趋势科技、迈克菲、卡巴斯基、Cisco、英特尔、EMC、亚马逊、谷歌等	阿里、腾讯、百度、华为、山石网科、杭州安恒、网康科技、
数据安全	数据加密、自然语言处理、数据挖掘与聚类分析等	赛门铁克、迈克菲、趋势科技、RSA 等	启明星辰、天融信、绿盟科技、神州泰岳、时代亿信、明朝万达、中国软件、中电长城网际、上海观安、360、亿阳、鼎普等
APT 攻击检测与防护	网络流量分析、恶意样本分析、关联分析、网络及终端取证等	FireEye、Bit9、趋势科技、RSA 等	360、阿里（瀚海源）、安天、知道创宇、绿盟科技、金山安全等
威胁情报分析及安全态势感知	爬虫技术、关键字匹配、威胁数据分析、机器学习、可视化、社会工程学等	戴尔、赛门铁克、迈克菲、FireEye、RSA 等	360、阿里（瀚海源）、知道创宇、安天、微步在线等
智能制造安全	兼容协议、轻量级设备、攻击识别、基础防护等	GE、西门子、英特尔、AT&T 等	和利时、浙大中控、四方继保、南京自动化、三维力控、北京亚控；绿盟、启明星辰、天融信、中科网威匡恩网络等

来源：中国信息通信研究院

（五）企业发展现状

国内安全企业实力稳步提升，在国内外上市的数量已达二十余家，营业收入达 97.14 亿元。国内安全企业发展态势总体良好，呈现出如下发展特征。

1.传统安全企业加速投资并购，丰富产品线并弥补市场空白

近三年，国内安全企业频繁开展投资并购等行为。2014 年启明星辰通过斥资 4 亿余元收购书生电子、合众数据、安方高科等企业，弥补了市场空白，扩大了市场占有率，进一步提升了公司业务规模和盈利能力。2014 年绿盟科技以 4.98 亿元收购亿赛通 100%股权，填补在数据安全和网络内容安全管理领域的技术不足。同时，传统安全企业利用渠道优势不断丰富自身的产品线，如启明星辰、绿盟科技等安全厂商通过不断丰富自身的产品线，拥有横跨防火墙/UTM、入侵检测管理、网络审计、终端管理、加密认证等技术领域的产品，努力将自身打造成为安全领域的综合提供商。

表 **7** 国内传统安全企业在网络安全领域主要投融资情况

投资方	被投方	投资/收购价格	时间
启明星辰	书生电子	9180 万元收购 51%股份	2014 年
	合众数据	1.78 亿元收购 51%股份	2014 年
	安方高科	2.22 亿元	2014 年
绿盟科技	金山安全	投资 4450 万元	2015 年
	亿赛通	4.98 亿元收购 100%股权	2014 年
	安华金和	970 万元收购 25%股权	2014 年
	深之度	2000 万元收购 10%股权	2014 年
	剑鱼科技	出资 441 万元设立北京剑鱼科技公司	2014 年
	敏讯科技	990 万元收购 55%股权	2014 年
卫士通	三零盛安	1.53 亿元收购 93.98%股权	2014 年
	三零瑞通	2 亿元收购 94.41%股权	2014 年
	三零嘉微	1.28 亿元收购 85.74%股权	2014 年
北信源	中软华泰	1 亿元收购 100%股权	2014 年
美亚柏科	江苏税软	6.2 亿收购 100%股权	2015 年
	新德汇	2.6 亿收购新德汇 49%股权	2015 年
	武汉大千	3315 万元收购 51%股权	2015 年

来源：中国信息通信研究院

2. 国内互联网龙头企业加强在安全领域的布局，缔造更安全的互联网生态

2015 年阿里巴巴收购国内安全公司翰海源，增强阿里云的防护体系，同时吸纳国内外网络安全专家。腾讯公司 2014 年新成立了信息安全研究部门“玄武实验室”，2015 年投资安全公司知道创宇，并与启明星辰联手推出专门的企业安全产品。百度在今年 4 月份宣布完成对安全宝的收购，加强云防护体系建设。奇虎 360 积极布局 APT、态势感知领域，2014 年 4 季度安全营收达 2000 万美元，同时在硅谷设立了风险投资公司，在生物识别、大数据、智能硬件、家庭安全应用等多个领域前瞻布局。为有效保护自身业务和生态伙伴的安全，互联网企业不断加大安全投入，建设一张更安全的互联网。

表 8 国内互联网企业在网络安全领域主要投融资情况

投资方	被投方	投资/收购价格	时间
阿里巴巴	翰海源	—	2015 年
	新加坡 V-Key 公司（移动安全、加密技术）	1200 万美元	2014 年
腾讯	知道创宇	—	2015 年
	Keen Teem	—	2014 年
百度	安全宝	—	2015 年

来源：中国信息通信研究院

3. 小型企业发挥技术优势，聚焦于细分专业领域

目前，国内小型安全企业纷纷发挥自身优势，走以专补缺、以小补大，专精致胜的成长之路。例如，部分企业专注于提供技术授权，面向其他安全厂商提供杀毒引擎等；部分企业在运营商、金融等领域深耕，贴合该类市场特殊需求，定制产品和服务，并占据市

场优势；也有一批新兴技术企业出现，提供 APT 攻击检测防御、安全威胁态势感知等高新技术。国内安全市场正呈现出“百花齐放、百家争鸣”的态势。

三、我国安全产业面临的机遇与挑战

（一）我国安全产业发展的关键机遇

我国网络与信息安全意识与重视程度不断提升，政策环境逐步优化、市场需求稳步增长、技术产品加速创新、安全人才保障有力，安全产业迎来发展的关键机遇。

多项加强网络安全技术研发、推进产业发展的法律法规和政策措施密集发布，为网络安全产业的发展提供了良好的政策保障。2015 发布的《网络安全法（草案）》被视为助推中国网络安全产业发展的“强心剂”;《信息安全产业“十二五”发展规划》等政策措施的发布为组织实施信息安全产业化专项、加强行业网络安全工作、推进安全产业持续健康发展了提供指导性规划。此外，“互联网+”时代的到来和网络强国战略的推进为安全产业促进政策的出台和实施营造了良好的契机。

国内市场需求逐步扩大，经济发展驱动安全产业繁荣。“互联网+”融合创新的新业态使得各关键行业和重要系统对网络安全保障的需求不断提高，安全产业已成为网络强国安全领域建设的重要基础。政府、企业甚至个人对于网络安全的投入不断增加，安全产品和服务的需求进一步扩大，安全产业步入高速发展的战略机遇期。国际网

络安全产业占 IT 产业比重达到 2%，而我国目前仅为 0.28%，具有巨大市场容量和发展空间。

对新技术新业务发展的及时跟进推进了我国在新兴领域网络与信息安全技术服务实力的加速发展。云计算、大数据、移动互联网、物联网、工业互联网等新技术、新应用和新模式的出现，对网络安全提出了新的要求，拓展了安全产业的发展空间。新技术、新应用和新模式在国内外市场的全面开拓将加快国内网络安全技术创新速度，催生云安全、工业互联网安全等新的网络安全应用领域，为国内企业与国际同步发展提供了契机。

“网络空间安全”国家一级学科正式获批，加快网络空间安全高层次人才培养，为安全产业健康发展提供人才保障。网络安全工作的性质决定了其对人才的需求是多层次、复合型的，一级学科的设立会更有利于网络安全人才的培养和网络安全人才队伍建设，使我国网络安全核心技术做到真正的自主创新和自主可控。总体而言，政府部门、行业组织、企业、应用部门、科研院校等各方均在协力助力安全产业发展，我国网络与信息安全产业有望实现跨越式发展。

（二）面临的主要问题和挑战

我国网络与信息安全产业在政府政策、产业环境、技术标准、企业发展等方面仍面临巨大的问题和挑战。

从政府政策角度看，我国已发布了大量安全产业促进政策并取得了一定的成效，但在政策的深度、广度和落实效果上，与国际强

国尚存在一定差距。**一是安全产业扶持政策未能详细阐述国家具体需求，日常指导性不强。**美、以等安全产业强国发布的产业政策对政府需求的阐述较为具体细致，明确界定产品或服务应满足的技术参数或解决方案。与此相比，我国政策仍存在“大方向号召多，具体需求少”的问题，难以为企业日常运营提供实质性引导。**二是顶层政策覆盖领域有限，对促进产业发展的重要措施涉及不够。**欧美普遍将政企合作、人才培养等作为国家政策着力布局的关键领域。反观我国，目前对于通畅政企合作渠道、开展面向产业的技术竞赛等外国普遍重视的政策手段目前并没有直接规定。不利于安全产业经济地位和从业人员综合素质的提升。**三是尚未形成企业解读、落实政策的有效机制，政策的针对性和实际收效不匹配。**我国与欧美各国在安全产业政策数量、针对性方面差距并不显著，但英美等国的安全企业对于国家政策的关注度、解读能力和适用水平较我国远为突出。经调研，我国部分企业关注重点集中在行业采购政策层面，对国家宏观顶层政策了解不足，尚不善于从政策中援引规定为自己拓展业务或争取其他合法利益。企业对政策贯彻能力的不足直接影响了我国产业政策的实施效果。

从产业环境角度看，我国产业生态环境呈现优化趋势，但在融资环境、第三方机构作用、产业协作等方面，我国与国际环境仍存在巨大差距。**一是国内安全企业的融资渠道少、成本高、耗时长、融资金额有限。**虽然创投机构已将目光移向安全领域，少数产业基

金相继设立，一批企业上市融资形成示范效应，但仍难以满足企业创新和发展的融资需求。而在天使基金和风险投资方面，由于整体市场规模和企业营收规模不高，对风险投资机构吸引力不强，当前涉足安全领域的投资机构屈指可数，尚未形成支撑推动安全技术孵化、企业培育的融资环境。**二是产业第三方声音微弱，创新技术的产业化和市场推广艰难。**国际上，第三方咨询和评价机构引领企业创新和技术趋势。反观我国，第三方机构针对安全市场、企业、产品、技术的报告稀少，产品服务采购方基本将市场份额作为主要采购依据，因而中小企业在采购中长期处于劣势，市场拓展停滞不前。**三是行业协会和产业联盟的行业影响力和凝聚力不足，行业内低价竞争等不良竞争行为频现。**欧美等发达国家以产业联盟、产业论坛为平台增进产业协作，在引导安全技术发展趋势、扩大安全市场需求方面形成巨大影响力。与之相比，我国企业参与协会和联盟的热情虽高，但通常缺乏一致的目标，同时受到竞争关系影响，不仅在推动技术发展和威胁信息共享方面的深度合作有限，还出现在竞标时恶性压低价格、在失标后对企业发动流量攻击等行为。**四是认证制度缺乏统筹管理，认证和许可已经成为安全市场的隐性准入门槛。**国外安全领域相关认证多是针对新兴技术，用以鼓励创新，由行业第三方开展，不具有强制性质。对比之下，我国安全领域的认证和许可多是出于安全保障的目的，而非对技术先进性、产品成熟度进行评判，部分为强制性的准入许可。认证时间长、费用高、种类多、

投入大、重复认证与反复认证等问题凸出，已经成为市场发展的严重障碍。

从技术与标准角度看，我国安全技术和标准领域取得积极进展，但与国际先进水平对比，在技术先进性和创新性，标准全面性和主导力等方面仍相对落后。**在基础安全技术领域**，我国入侵检测、病毒查杀、防火墙、安全网关、认证与加密、漏洞扫描、统一威胁管理等技术产品相对成熟，部分已接近或基本达到国际先进水平，但在流量检测分析、基础性漏洞挖掘、数据保护等方面存在较大技术差距，威胁特征库、病毒样本库等知识库建设仍有待完善。**在新兴安全技术领域**，虽然我国已积极在新兴领域前瞻布局，但云安全产品、数据防泄漏、APT 攻击检测防御、威胁情报收集和分析、智能制造安全防护等方面多为刚刚起步，数据挖掘、关联分析、机器学习、智能感知等技术能力不足，成熟产品种类少、产品适用性有待检验。**在标准研制方面**，我国已全面开展安全标准基础研究、国际标准化跟踪研究和专项研究，但与发达国家相比，管理类、系统类、跨领域安全标准研究仍有待加强，国家网络与信息安全标准体系有待完善。此外，网络与信息安全相关标准文件法律效力不足，制度标准落实力度不足。

从企业角度看，2015 年全球网络安全 500 强企业中，美国企业有 380 余家，英国 20 余家，以色列 16 家，我国仅有安天（95 名）、

山石网科（184 名）、安恒信息（314 名）、Vkansee[61]（412）4 家入围，排名相对靠后，整体差距明显。**一是缺少具有国际竞争力和影响力的龙头安全企业。**在企业规模方面，Symantec、TrendMicro 等安全巨头市值达到数十亿乃至数百亿美元，我国净利润超过 1 亿元的安全企业仍屈指可数，与行业巨头存在巨大差距。**二是国内安全企业并未形成差异化竞争优势。**目前国内企业从产品技术到服务范围和水平都很难拉开档次。此外，一些企业为快速抢占市场，通过 OEM 途径扩充产品线。长期看，采用 OEM 模式不仅威胁企业技术创新和企业声誉，还将对我国网络基础设施安全构成潜在威胁。**三是产品和服务创新乏力。**在低价中标的市场机制下，国内企业愈发重视市场销售推广，而忽视产品和服务创新的内在源动力。**四是安全人才快速流失。**由于薪酬和福利等吸引人才的条件不足，传统安全企业的大量人才流入国外企业或者 BAT[62]等互联网公司，顶尖安全专家日益匮乏。

四、促进我国安全产业发展的关键举措

（一）加强安全产业政策引导

一是加强政策引导与落实。以政府采购为引导，推动形成产品与服务均衡理念，调整采购中最低价中标规则，以产品的服务质量预算等作为衡量标准，避免“低价中标”引发安全服务市场“劣币

[61]Vkansee：由中国航空工业集团公司投资，专注于指纹识别技术的创业公司
[62]BAT：百度、阿里、腾讯

驱逐良币”效应。统筹优化安全产品和服务认证管理，确定国家权威认可的安全资质名单池，取消企业导向性资质认证，破除束缚市场发展的制度性瓶颈。同时，以《网络安全法》的出台实施为契机，制定推动政策落实的具体方案，如在“互联网+”、智能制造、智慧城市的建设中，明确安全投资占项目建设投资的最低比例，要求工程验收前需由专业机构对网络与系统安全进行评估，切实增强网络安全保障能力。开展关键基础设施安全防护示范工程，发掘行业网络安全优秀实践案例，促进先进技术和经验的推广应用。加强安全政策宣贯，提高政策的实效性，调动安全企业参与各类政策落实项目或工程的积极性。

二是引导安全创新。顺应大众创业、万众创新的产业氛围，鼓励安全企业开展技术创新。激发中小企业发展活力，鼓励大企业打造开放平台，构建更具包容性的产业发展生态系统。引导建设区域性安全产业基地，促进产业集聚发展。加强对安全企业创新成果的知识产权保护，营造良好的创新氛围。

三是加强金融扶持。强化中央财政资金引导，集中力量支持网络安全核心关键技术攻关、产业链构建、重大应用示范建设。将安全产业纳入国家政策性基金支持范围，发挥产业引导、技术创新支持作用。发挥原有税收政策对安全产业的导向作用，适当扩大原有税收优惠政策适用范围，惠及更多服务类、硬件类安全企业。

四是优化人才培养。创新人才选拔和培养机制，利用网络教育、

技术竞赛、产业与高校、科研院所及其他行业联合等方式，培养创新型、复合型人才，打造多层次的人才梯队。加大人才发展资金投入，设立安全人才奖学金，提升突出人才的薪资水平和待遇，促进人才向安全产业汇聚。促进产业发展与人才培养的良性循环，以产业发展带动人才培养，以人才培养推进产业升级。

（二）优化产业生态环境

一是优化安全产业融资环境。加快构建完整的资本市场融资体系，吸引天使投资、风险投资等投向安全产业，加快安全技术和企业孵化速度，促进创新成果产业化。加大安全企业进入资本市场融资支持力度，鼓励符合条件的企业在创业板、新三板等上市挂牌。

二是营造公平竞争市场环境。树立底线思维、红线管理理念，营造创新为先、质量为先、信誉为先的发展环境。开展企业网络安全第三方认证，从安全产品和服务使用方角度客观衡量安全保障工作实效，在提升企业网络安全工作的主动性和全面性的同时，加强企业对安全服务采购的重视，提升对安全服务质量的要求。加快安全服务相关标准制定，确立安全服务评价规则，遏制低价竞争。

三是推动举办国家级、地方级、行业级、企业级不同层次的安全盛会和技能竞赛。围绕安全领袖、技术发展、企业创新等不同主题举办国家级安全盛会和竞赛，将其与国家网络空间安全的实际需求有机结合，进行针对性的规划和设计，传达国家安全意志。推动地方政府、行业平台、相关企业组织安全盛会和竞赛活动，促进知

识与技术交流，促进安全人才培养。

四是充分发挥安全产业咨询平台和行业力量。鼓励政府智库、新闻媒介、咨询机构密切跟踪安全技术产品发展趋势，关注中小企业创新，定期发布安全产业、技术、人才等方面研究报告和评论，秉持独立第三方的专业性与公正性，开展年度安全产品、技术评奖活动，提高新兴技术企业品牌影响力，提升领先安全产品知名度。充分发挥行业协会、产业联盟等机构平台作用，推动建立政府主导、多方参与的安全产业社会信用体系，推动安全产业持续健康发展。

（三）技术方向和关键领域

一是加强基础安全技术能力攻关。加快提升基于基础网络架构、应用协议等的漏洞挖掘、深度渗透检测、攻击检测发现、溯源取证、漏洞修复等基础安全能力。重点建设脆弱性漏洞库、恶意代码库、攻击规则库、协议行为特征库、软件补丁库、标准信息库等安全知识、安全资源库。加快防火墙、入侵检测/防御等网络与边界安全类产品，病毒查杀、身份管理与访问控制、内容安全管理等终端安全类产品的创新和应用。

二是加强面向云计算、大数据、智能制造等新兴领域的安全技术的研发应用，提升网络威胁的感知、预警和防御能力。

1. 云计算领域

加快虚拟化安全、多用户数据安全、安全中间件、数据备份与恢复等关键技术的研究及产业化，提升对云计算核心软硬件的自主

研发能力，加强等级保护、云安全认证、安全测试与评估等云安全服务的创新及应用推广。

2. 大数据分析领域

重点依托大数据分析平台实现对威胁情报的外防和内控，对外建立情报共享驱动防御体系，实现安全情报再分析;对内将机器学习作为首选方案，开展对已渗透进系统内部的恶意代码的异常行为检测。加强全局安全态势感知能力，及时掌握大规模安全事件进展、影响，并快速处置。突破内容感知、智能沙箱、异常检测等技术，加快 APT 攻击检测和防御产品的研发。

3. 智能制造等新兴信息网络领域

重点开展对智能设备、工控系统的风险评估，对业务系统协议、业务逻辑、脆弱性进行技术分析，提取安全需求并制定安全框架，加强智能制造领域漏洞扫描工具、防火墙及 APT 防护类产品的研发。

（四）安全企业发展建议

一是以兼并收购、战略合作为途径打造龙头企业集群。兼并收购、战略合作是安全企业快速发展的重要途径，也是当前全球产业界实现资源和技术互补、打造综合竞争实力的普遍选择。安全企业应打破恶性竞争循环，寻求更广范围、更多形式的合作，通过跨国兼并重组、购买技术和专利，强化企业盈利能力和产业链控制能力，形成技术优势突出、业务能力综合、能够支撑国家战略的龙头企业。

二是打造自主的“专精特新”的技术产品布局。安全产业具有

技术性和专业性极强的特点，网络安全依赖于最先进的技术和产品来实现可持续发展，这就使得安全技术和产品的创新能力成为企业做大做强的重要基石。安全企业应将技术创新作为企业发展的源动力，着力发展安全可控核心关键技术,形成技术优势；同时，密切跟踪新技术新业务安全，加速研发推广云安全产品和服务，开展新技术新业态安全前瞻研究。

三是积极开拓国内和国际市场，打造经典案例，形成品牌效应。安全企业应注重产品和服务质量，积极寻找市场需求，不断提升用户体验，建立良好品牌口碑。一方面，努力开拓国内政府市场，密切跟进政府政策，加强政企合作，强化对政府的支撑保障；另一方面，加强全球市场和研发资源的统筹布局，在海外设立研发机构和开拓市场，提升企业国际化发展的水平和层次。

四是重视企业文化和人才建设。一方面，安全企业应重视企业文化建设，帮助员工树立正确的安全观，增强团队凝聚力。另一方面，应加强人才队伍建设，完善人才的培养机制，着力培养攻防等重要技术领域的高水平实战型人才；完善人才的激励机制，健全技术入股、股权、分红权、期权等多种人才激励形式。

附件：国际安全企业研究

（一）美国典型安全企业研究

表 9　典型企业介绍

企业名称	成立时间	技术领域	企业背景	获得荣誉	合作伙伴
Lancope	2000 年	流量分析和网络监控，提供可视化网络安全隐患检测	由约翰·科普兰教授在佐治亚理工学院成立；2010 年，曾担任 AirDefense 公司 CEO 的迈克·波茨加盟 Lancope 并担任总裁兼 CEO	1）InfoWorld 2015 技术年度奖；2）SC Magazine 英国奖；3）SANS Institute 最佳高级威胁识别奖；4）INQUIRER Tech 最佳产品奖；5）Atlanta Business Chronicle 先导奖	Cisco、Barracuda、Chenk Point、HP
FireEye	2004 年	提供 APT 检测和防御产品、威胁情报	成立于美国，早期得到美国中央情报局下属投资机构 In-Q-Tel 投资，2013 年上市	1）SANS Institute2014 年最佳产品评选中获得高级威胁检测和威胁情报奖；2）2015 年 4 月，多向量虚拟引擎和动态威胁情报云平台取得美国国土安全部《培育反恐技术法案（2002）》认证	Palo Alto Networks、Bit9、ACE Group、HP、
Palo Alto Networks	2005 年	提供防火墙产品，集成传统防火墙和入侵防御系统的全部功能，具备机器学习、可视化、外部情报支持和智能升级等特性	成立于美国创始人 Nir Zuk 曾担任 Check Point、NetScreen 的工程师，他是第一代安全状态检测防火墙和第一代入侵防御系统的主要开发者	1）2009 年 Gartner“下一代防火墙”	VMware、Citrix、Splunk Symantec、ARISTR
Norse	2010 年	提供实时准确的攻击情报、实施攻击拦截、揭示隐藏漏洞以及跟踪新出现的全球安全威胁	成立于美国，创始人兼 CEO Sam Glines 是曾就职于埃森哲担任高级经理。得到具有 80 亿资金规模的风投 Oak Investment Partners 投资	1）2014 年 Gartner 安全情报领域“Cool Vendors”	

来源：中国信息通信研究院

（二）创新型安全企业研究

表 10　典型创新企业介绍

企业	成立时间	技术路线	企业背景	获得荣誉	合作伙伴
Waratek	2009 年	提供面向 Java 应用的安全防护软件，可实现应用程序在运行时自我防护、虚拟补丁、可视化零日攻击检测、取证等功能	总部位于爱尔兰都柏林，在伦敦、纽约、东京等地有办事处。公司获得了红杉国际为首的 50 家国际投资者支持	1）2015 RSA 创新沙盒安全产品 TOP10；2）2015 SIIA SODiE 最佳产品；3）2013 Gartner Cool Vendor；4）2013FinTech Innovation Lab 创新奖	IBM、Oracle、Red Hat、Microsoft Azure、Amazon Web Services
Ticto	2000 年	提供基于群体识别的可视化身份认证产品	公司位于比利时布鲁塞尔，创始人曾担任比利时邮政执行董事，麦肯锡合伙人，是 Certipost 的创始人并持有相关专利	2015 RSA 创新沙盒安全产品 TOP10	布鲁塞尔航空公司、比利时核能研究中心、网络安全公司 Cordell、WILLEMEN 集团等
Vectra Networks	2011 年	提供大数据安全分析平台，可提供基于自身流量传感器的数据挖掘、基于机器学习的异常检测以及可视化分析	由 Mark Abene 等人于美国创立，获得 Khosla Ventures、Accel Partners、IA Ventures、AME Cloud Ventures 共计 1780 万美元注资	1）2015 Gartner Cool Vendor；2）2015 InfoSecurity Products Guide 企业级安全金奖、下一代安全银奖、最佳安全服务铜奖；3）2015 Cyber Defense Magazine 网络安全解决方案先锋奖；4）2015 RSA 创新沙盒安全产品 TOP10；5）2014 Computer Tech Review 最具价值安全产品	Riverbed Networks 、Aruba Networks、Banic 等
FortScale	2012 年	提供大数据安全分析平台。基于操作系统、各类应用日志分析，专注于检测内部攻击，具备基于个体和却组的双重异常判断准则	Idan Tendler 和 Yona Hollander 于以色列创立，目前总部设在美国洛杉矶，公司先后获得 SWARTH GROUP、INTEL CAPITAL、BLUMBERG CAPITAL 投资，共计 1200 万美元	1）2015 Cyber Defense Magazine 最佳创新解决方案奖；2）2015 RSA 创新沙盒安全产品 TOP10；3）2015 Info Security Products Guide 企业级安全卓越奖	2015 年加入 CISCO Solution Partner Program

企业	成立时间	技术路线	企业背景	获得荣誉	合作伙伴
SecurityDo	2012年	提供大数据关联分析产品，可对数据进行全索引，实现多源异构数据关联，提供TB级数据、秒级响应的查询性能	由McAfee前执行官Chris Jordan及其同事Kun Luo创立	2015 RSA创新沙盒安全产品TOP10	与Lumenate进行授权合作
Cybereason	2012年	提供大数据威胁检测平台，可实现终端行为数据采集，大数据平台进行实时关联分析和异常行为挖掘	由以色列军队退役网络安全专家成立，前期投资者包括Tumblr, Upworthy, Twitter, Oculus VR, and Foursquare。2015年得到2500万美元的融资，为首的是Spark Capital，战略投资者包括洛克希德马丁公司	2015 RSA创新沙盒安全产品TOP10	
Sentinelone	2013年	提供终端安全威胁检测平台，可实现基于行为的终端实时安全检测，利用云端情报中心共享异常行为相关特征	由Intel, McAfee, Checkpoint, IBM and the Israel Defense Forces在加州投资成立，2015年引进Palo Alto Networks市场副总裁。2014年融资得到Accel Partners, Data Collective, Granite Hill Capital Partners, Tiger Global Management, UpWest Labs, and the Westly Group等企业支持，2015年又获得250万美元融资	1）2015 RSA创新沙盒安全产品TOP10；2）2015 Computer Tech Review最具价值安全产品；3）2014 CRN十大安全创业企业；4）AVTest英国最佳商用杀毒产品	
Nexdefense	2012年	提供工业网络异常检测系统，可针对已知和未知威胁进行检测	由Michael Sayre、Michael Assante、Derek Harp等人创立，2014年获得240万美元的融资	1）佐治亚州创新企业Top 10；2）2015 RSA创新沙盒安全产品TOP10	美国能源部、伯特立能源联盟、爱达荷实验室

来源：中国信息通信研究院

（三）网络安全 300 强企业中非美国企业研究

表 11　网络安全 300 强非美国企业列表

序号	企业名称	榜单排名	国别	技术领域
1	AVG Technologies	6	荷兰	防病毒软件、互联网安全软件
2	BT	10	英国	安全和风险管理解决方案
3	Trend Micro	13	日本	服务器、云和内容安全
4	NuData Security	14	加拿大	在线欺诈检测
5	DFLabs	17	意大利	应急事件响应
6	F-Secure	22	芬兰	网络安全防护
7	Codenomicon	24	芬兰	应用安全测试工具
8	Gemalto	27	法国	数字身份管理
9	CyberArk	28	以色列	安全威胁检测与防护
10	Kaspersky Lab	32	俄罗斯	防病毒解决方案
11	Thales	34	法国	IT 安全解决方案
12	Check Point Software	39	以色列	统一威胁管理
13	Brainloop	63	德国	文件安全管理
14	WinMagic	66	加拿大	全磁盘加密软件
15	Checkmarx	68	以色列	软件开发安全
16	i-Sprint	75	新加坡	身份管理与访问控制
17	Clearswift	78	英国	数据安全
18	Business Risk Intelligence	85	德国	威胁情报和威胁态势感知
19	ESNC	89	德国	SAP 应用安全
20	CenterTools Software	91	英国	终端安全解决方案
21	Antiy Labs	95	中国	防病毒引擎和解决方案
22	Cryptomathic	96	丹麦	云、移动和网络安全
23	Seculert	100	以色列	基于云的恶意软件防护
24	Bwise	102	荷兰	IT 监管、安全合规
25	AhnLab	104	韩国	互联网安全解决方案
26	Sophos	106	英国	防病毒，恶意软件检测
27	SurfRight	112	荷兰	恶意软件检测和防护
28	Avira	114	德国	防病毒，安全软件
29	itWatch	119	德国	终端安全，数据安全
30	Wontok	122	澳大利亚	防欺诈技术
31	Spam Titan	123	爱尔兰	邮件安全
32	Silobreaker	132	英国	网络分析和威胁情报
33	Bitdefender	134	罗马尼亚	防病毒和终端安全
34	cryptovision	137	德国	密码和身份认证

序号	企业名称	榜单排名	国别	技术领域
35	CloudLink	161	加拿大	云安全和数据加密
36	Above Security	172	加拿大	安全服务
37	Rohde & Shwarz	173	德国	加密和 IT 安全
38	Secunia	174	丹麦	脆弱性和补丁管理
39	SENTRIX	193	以色列	WEB 应用安全
40	TrulyProtect	196	芬兰	软件应用安全
41	Swivel Secure	197	英国	基于风险的认证
42	ENCODE	198	希腊	IT 安全和数字安全
43	TrapX Security	199	以色列	威胁检测和防护
44	Skycure	202	以色列	移动设备安全
45	Aujas	207	印度	信息风险管理服务
46	Qosmos	211	法国	实时数据安全
47	Modulo	221	巴西	IT 监管、安全合规
48	Quintessence Labs	231	澳大利亚	数据安全
49	PrimeKey Solutions	232	瑞典	PKI 和数字签名解决方案
50	Napatech	233	丹麦	网络安全管理
51	Herjavec Group	234	加拿大	信息安全服务
52	VU Security	236	阿根廷	身份认证和欺诈防护
53	Riscure	237	荷兰	安全产品测试实验室
54	Protected Networks	239	德国	身份管理与访问控制
55	CoSoSys	243	罗马尼亚	数据安全
56	Smoothwall	250	英国	统一威胁管理
57	Link11	263	德国	DDOS 缓解方案提供商
58	Keypasco	276	瑞典	多因素认证
59	Light Cyber	277	以色列	预测漏洞检测
60	Messageware	292	加拿大	微软交换安全

来源：Cybersecurity Ventures,“cybersecurity TOP 500”

致　谢

在本白皮书的研究过程中，得到安天实验室、迪普科技、知道创宇、阿里巴巴、启明星辰、绿盟科技、天融信、安恒信息、神州泰岳、任子行、安域领创、华三通信、恒安嘉新、深信服、联软科技、安络科技、山石网科、汉柏科技等企业大力协助，在此一并表示感谢。

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、62303621

传真：010-62304980