CAICT 中国信通院

网络安全产业白皮书

（2017 年）

中国信息通信研究院

2017年9月

版权声明

前　言

十八大以来，党中央高度重视网络安全工作，做出了“没有网络安全就没有国家安全”的重要指示，将网络安全纳入国家安全工作予以部署，开启了网信事业新篇章。2016 年以来，《网络安全法》《国家网络空间安全战略》《“十三五”国家网络安全规划》等一系列重大文件相继发布实施，进一步为网络安全产业健康发展提供了政策保障和法律依托，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。

在此背景下，我国网络安全产业步入快速发展新阶段。2016 年，我国网络安全产业规模达到 344.09 亿元，较 2015 年增长 21.7%。网络安全领域创新活跃，态势感知、监测预警、云安全服务等新技术、新服务不断涌现，以产品为主导的产业格局正向“产品和服务并重”转变。网络安全企业实力有了较大提高，超过 30 家企业年度营收过亿，出现了一批具有产业整合能力的龙头企业。

本白皮书是继《网络与信息安全产业白皮书（2015）》之后，我院第二次发布网络安全产业白皮书。本白皮书重点从规模结构、政府政策、企业发展、技术进展等维度对国内外产业发展进行分析探讨，力求展现网络安全产业发展的新情况、新进展，同时对产业发展趋势进行了展望，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。

目 录

一、网络安全产业的内涵和范畴

（一）网络安全产业范畴的再认识

从网络安全的定义[1]和传统网络安全产业的范围看，网络安全产业主要提供保障网络可靠性、安全性的产品和服务，传统产品形态主要有防火墙、防病毒产品等。随着网络技术的演变与安全形势的复杂化，网络安全也被赋予了新的内涵外延，例如，云计算的广泛应用引入了虚拟化安全、云安全等概念，工业互联网的演进让工业网络安全成为新的焦点。同时，新的安全威胁也进一步拓展了网络安全的范畴，例如利用物联网终端发起攻击、车联网安全等。网络安全产业的范畴将随着网络安全保障需求不断延伸扩展。

从产业发展的时代重要性看，网络安全产业已经成为国家网络安全能力的重要支点。习近平总书记在“4·19”讲话中指出，要“加快构建关键信息基础设施安全保障体系”、“增强网络空间安全防御能力”，国家《网络安全法》提出“国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序”。网络安全产业作为网络安全技术、产品和服务提供者和实施者，承担着国家网络安全防御和保障的历史使命。日益复杂严峻的网络安全形势、国家网络强国战略推进建设迫切要求

[1]国际电信联盟（ITU）对网络安全的定义为：可用于保护网络环境、机构组织以及用户资产的政策、理念、技术等的集合。

创新安全技术、增强综合安全保障能力，发展壮大网络安全产业已经成为维护国家网络空间主权、安全和发展利益的战略选择。

本报告中的网络安全产业范畴主要从国家网络安全、关键信息基础设施保护、打击网络犯罪等网络安全防御角度出发，重点覆盖面向国家关键信息基础设施和重要行业领域、互联网+重点领域、企业级用户的网络安全技术、产品和服务。在网络安全产业规模测算中，未包含产品芯片、元器件等的制造产业、舆情分析产业以及军队、保密、国安等特殊领域产值。

（二）网络安全产品和服务分类

当前，信息网络技术的快速发展，网络安全技术产业不断细分发展，产业结构不断变化完善。同时，软硬件产品的界限愈发模糊，产品和服务的联动更加紧密。在借鉴 IDC 产业分类、PDRR[2]模型和 Gartner ASA[3]自适应安全架构等国际主流网络安全产品和服务的分类方式基础上，结合我国实际，依据主要功能及形态、安全防御生命周期可将我国网络安全产品和服务分为如下类别。

1．依据主要功能及形态分类

（1）网络安全产品

网络安全产品领域可细分为安全防护、安全管理、安全合规、其他安全产品四个类别。其中，安全防护类产品主要包括防火墙、入侵检测和防御、安全网关（UTM）、Web 应用防火墙（WAF）、防病毒、

[2] PDRR: Protection, Detection, Reaction and Recovery

[3] Gartner: Designing an Adaptive Security Architecture for Protection From Advanced Attacks

数据防泄漏等，安全管理类产品主要包括身份识别与访问控制、内容安全管理、终端安全管理、安全事件管理（SIEM）等，安全合规主要包括安全基线管理、安全审计、安全测评工具等。其他类包括未纳入上述分类的行业性较强的安全产品，如僵木蠕检测防护系统等，以及网络安全态势感知平台、大数据分析等新兴技术产品等。

（2）网络安全服务

网络安全服务主要包括安全集成类、安全运维类、安全评估类、安全咨询类四大类别。其中安全集成类主要指信息系统工程项目中的安全集成；安全运维类包括专业运维服务、维保服务等；安全评估包括风险评估、渗透测试、等保评测等；安全咨询类包括教育培训、设计规划等。

2. 依据安全防御生命周期技术能力分类

网络安全防御的生命周期可以分为预测、基础防护、响应、恢复四个阶段，现有网络安全产品和服务可以按其部署位置或部署效果对应于上述阶段。

（1）预测阶段

应用于该阶段的安全产品多为安全基线管理、风险分析及攻击预测类产品，用于在攻击事件发生之前，对业务系统或网络潜在的风险和可能面临的攻击威胁进行分析和预判。

（2）基础防护阶段

基础防护阶段通过部署一系列的访问控制、黑白名单等策略，或

采取隔离、隐藏等手段减少被攻击面来提升攻击的门槛，从策略上加强系统的安全性。

（3）响应阶段

响应阶段是安全手段与攻击者正面交锋的重要阶段，也是大量传统安全产品部署的重点所在，如入侵检测系统、反病毒系统、WAF 等，均作用于响应阶段，对攻击事件进行实时的阻断和防御。

（4）恢复阶段

该阶段的安全产品主要作用于攻击事件发生之后，通过对留存的日志等痕迹进行取证和分析，进行攻击事件的追溯，以及对受攻击系统的修复，包括安全审计、取证溯源等。

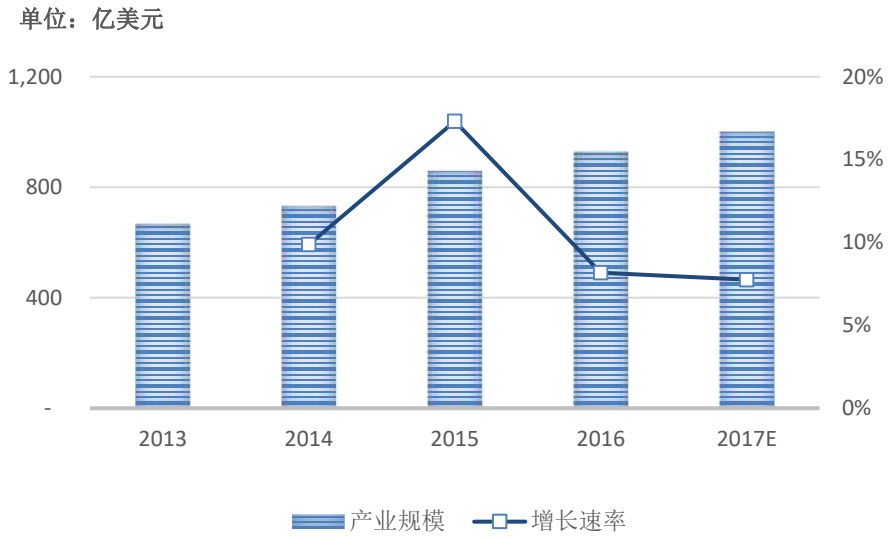
二、国际网络安全产业发展态势

（一）全球产业规模平稳增长，安全服务引领增长

1. 全球安全产业规模稳步增长，区域格局保持稳定

2016 年全球安全产业规模达到 928 亿美元，较 2015 年增长 8.2%，预计 2017 年增长至 1000 亿美元[4]。增速看，全球安全产业增速在 2015 年达到历史高位 17.3%，随后回落至 8%的增长水平。

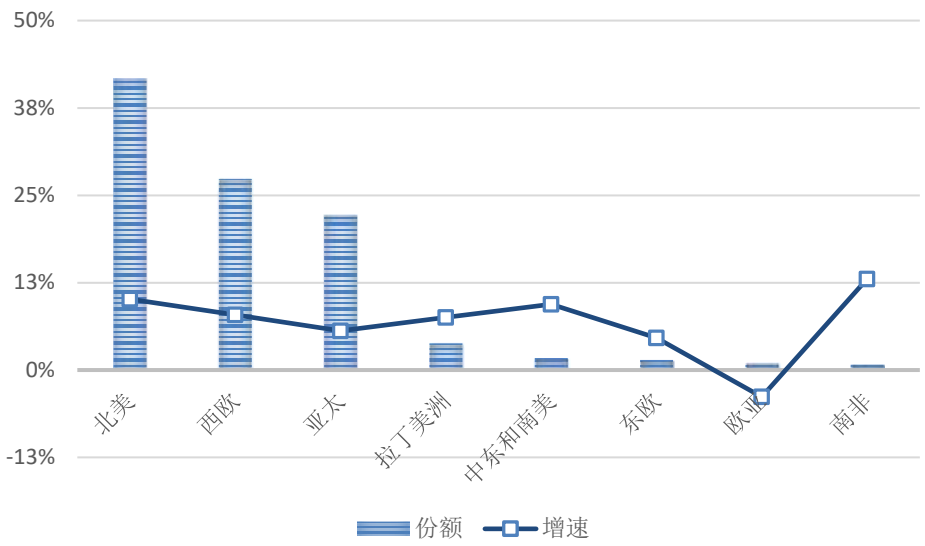
[4]数据来源：Gartner Information Security, Worldwide，2014-2020



数据来源：Gartner Information Security, Worldwide, 2014-2020

图 1 2013-2017 年全球安全产业增长情况

在区域分布方面，北美、西欧、亚太维持三足鼎立态势，合计市场份额超过 90%。其中，美国、加拿大为主的北美地区 2016 年产业规模达到 386.67 亿美元，较 2015 年增长 10.1%，市场规模全球占比 41.67%，牢牢占据全球最大份额；英国、德国、芬兰等 16 个西欧国家 2016 产业规模合计 253.45 亿美元，较 2015 年增长 7.9%，西欧国家市场规模全球占比为 27.31%；日本、澳大利亚、中国、印度等 10 个亚洲国家 2016 年产业规模合计 205.96 亿美元，较 2015 年增长 4.26%，市场规模总和占全球比列为 22.19%，仅次于西欧国家；非洲、东欧、拉丁美洲等其它地区安全产业规模为 81.93 亿美元，占全球比例为 8.83%。



数据来源：中国信息通信研究院（基于 Gartner 数据整理）

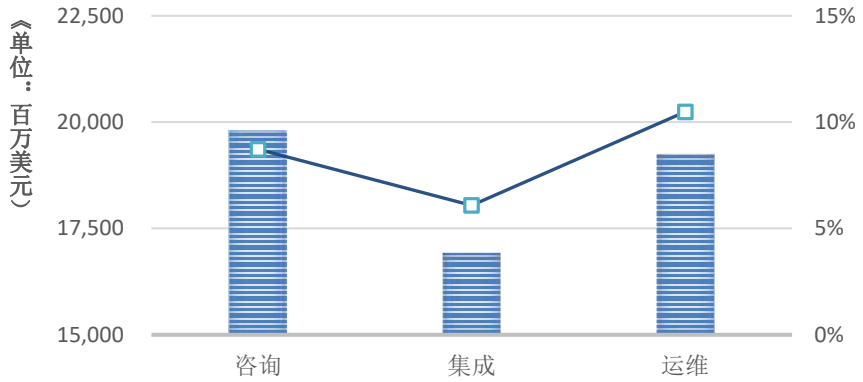
图 2 全球安全产业区域分布和增长情况

2. 安全服务和产品份额总体稳定，安全外包服务、防火墙、安全检测工具、身份识别与访问控制产品引领细分产业增长

2016 年，安全服务与安全产品市场依然保持六四分格局，安全服务增长速度略占优势。安全服务产业规模达到 559.75 亿美元，较 2015 年增长 8.5%；安全产品规模达到 368.26 亿美元，较 2015 年增长 7.7%。

在安全服务领域，安全咨询、安全运维、安全集成市场份额分别为：35.4%、34.4%、30.2%。当前，企业在识别应对高级威胁、内部威胁等方面对于安全专家与工具的协同配合要求不断提升，但企业安全从业人员以及安全专家十分缺乏，进而驱动安全运维服务需求快速增长。特别是，依赖于第三方提供安全服务的安全外包细分市场规模

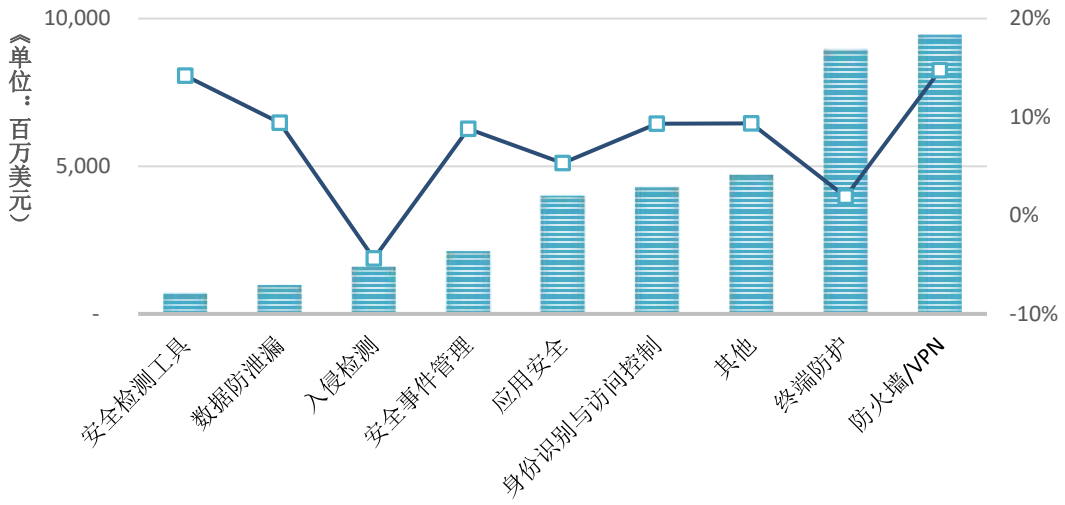
达到 192.5 亿美元，并凭借 11%的增长速度成为安全服务产业的重要增长引擎。



数据来源：中国信息通信研究院（基于 Gartner 数据整理）

图 3 安全服务市场份额及增长情况

在安全产品领域，防火墙、终端防护、身份识别与访问控制产品位列 2016 年市场规模的前三位，分别占比 25.63%、24.29%、11.62%。



数据来源：中国信息通信研究院（基于 Gartner 数据整理）

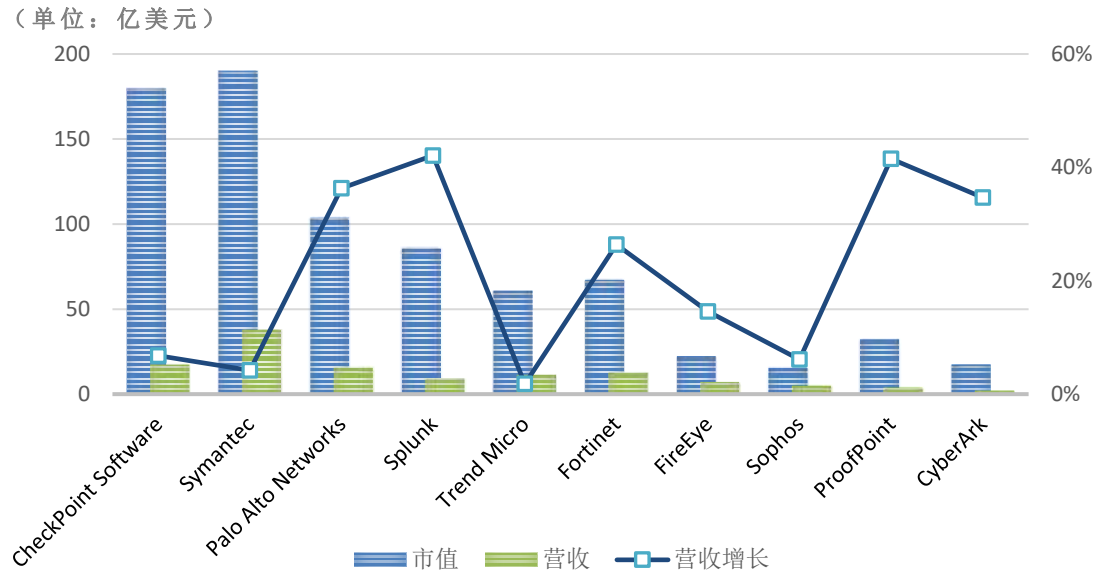
图 4 安全产品市场份额及增长情况

在增速方面，防火墙市场依然保持高位增长，2016 年市场增速达到 14.2%，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。其次是安全检测工具 14.2%，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。而后是身份识别与访问控制产品，增速为 9.3%，驱动因素主要有两方面：一是移动化办公引发的终端和用户管理需求，二是云应用的快速增长。

3. 上市企业营收持续高速增长，发展态势向好

2016 年全球上市安全企业整体表现相对较好，受到网络安全形势利好影响，上市企业市值普遍提升，包括 CheckPoint Software、Symantec、Palo Alto Networks、Trend Micro 等在内的 10 家典型企业平均营收 12.25 亿美元，约合人民币 83.25 亿元，营收平均增长 21.45%，如图 5 所示。



数据来源：中国信息通信研究院整理

图 5 2016 年主要国际上市安全企业公司业绩

（二）主要国家产业政策演进趋缓，进入部署实施期

自 2016 年以来，全球主要国家在安全产业领域的整体政策趋于平缓，新增政策主要集中于强化政府地位、加强地域乃至国际合作等方面，呈现以下三大特点：

1．美国网络安全产业政策方向未变，政府未来仍是助推产业发展的重要力量

美国自特朗普政府上台以来，网络安全政策整体趋于保守，不仅迟迟未发布新版网络安全法案或战略，相关行政令也推迟到 2017 年 5 月 11 日才签署通过。“增强联邦政府网络与关键性基础设施网络安全”行政令是美国涉及安全产业的最新国家政策文件之一，该文件表明了**美国政府未来还将继续成为拉动产业发展的重要力量。**

根据该行政令，美国联邦政府将已知但未得到处理的安全漏洞视为行政部门面临的最严重的网络风险之一，并将使用供应商不再支持的过时操作系统或硬件、未及时安装安全补丁或落实特定安全配置的软硬件视为安全漏洞和隐患的主要来源。该行政令同时要求政府建立一个“现代、安全、更有韧性”行政部门信息技术架构，统筹联邦政府信息技术设施的现代化建设，促进联邦政府的网络防御系统向一体化的云安全技术转移，并要求商务部和国土安全部联合提交加强网络人才培养的计划。此外，为了落实该行政令，美联邦政府将增加 15 亿美元的网络安全总预算。

从行政命令的具体来看，未来美国联邦政府对网络安全产品和服

务的需求还将持续扩大，相关资金倾斜也将不断增多。一方面，这使得政府在未来一段时间内，将成为安全企业和设备供应商主要的潜在客户。另一方面，政府为了提升联邦整体网络安全防御水平，对安全产业的拉动和扶持也将持续加大。目前，华盛顿已超越硅谷成为美国网络安全创新最热门、安全企业最集中的地区之一[5]，这从侧面反映了近年来美国联邦政府和国家安全局等机构倡导的网络安全文化为美安全产业催生了很多的发展机会。

2．欧洲国家安全产业政策层级不断提高，政策重点从偏重市场转向强调国家安全

长期以来，欧盟和欧洲各国的网络安全产业政策主要聚焦于打破区域碎片化，在政策的宏观高度方面，比美等国家略逊一筹。但近年来，**欧洲国家的安全产业政策层级不断提升，在加强人才储备、增强网络安全国家实力等方面的政策不断增加**。

英国在 2016 年底宣布将在未来五年投资约 23 亿美元进行“世界级”的网络安全建设，鼓励英国企业提升技术水平、防范网络攻击，并不断加强政府、企业和学术界的合作。英国在随后发布的新版《国家网络安全战略（2016-2021）》中也提出要大力发展网络安全专业机构，建立世界级的信息保障和网络专业人才力量，打造可信与安全的网络生态系统等。此外，英国在 2015 年启动的网络安全加速器计划（Pre-Accelerator）基础上，进一步组织遴选有潜力的安全企业予以

[5]资料来源：http://www.2cto.com/article/201611/566481.html

培育，制定了涉及市场、用地、资质、融资等方面的一整套扶持方案，目前参与该计划第一期的 7 家企业已融资 270 万英镑，并获得了思科等企业的订单。

法国在去年年底宣布将组建网军部队的同时决定在网络安全防御和研发方面投入 10 亿欧元，主要用来雇佣高水平研究人员和工程师。法国早在 2013 年《国防与国家安全白皮书》中，就计划储备一支民间网络安全防御力量，培养一批在私营企业工作的网络防御专家，以便在必要时可以服务于政府和军队。

德国政府也于 2016 年底发布了新的网络安全战略，提出加强同欧洲及全球的网络安全信息共享和协作，使用安全可靠的信息技术以及培养联邦政府的网络安全人才等。德国在新战略中还呼吁公共与私营机构之间共享网络威胁与攻击相关信息，并鼓励企业能逐步提高安全意识，更为积极地应对各类网络威胁，保护关键基础设施。

除以上政策措施外，**欧盟还有聚焦于打破区域市场碎片化的政策出台。**欧盟委员会希望欧洲的网络安全企业加强跨境合作，并协助企业开发具有创新性及安全性的技术、产品及服务。欧盟委员会同时提出建立信息通信技术安全产品欧洲认证框架，以进一步解决欧盟网络安全市场的碎片化问题。

3．安全产业国际合作日趋增加，以色列等创新活跃国家成主要合作对象

从近期欧美各主要国家的网络安全产业相关政策来看，**加强国际**

合作成为了未来政策可能重点布局的领域之一。美、英、德等国的相关政策都提到了要加强国际合作，帮助企业“走出去”。

在开展国际合作的具体对象方面，以色列等网络安全创新活跃的国家成为了优先选择。美国在 2016 年底与以色列签署了《高级研究伙伴关系法案》，该法案旨在加强美国与以色列之间在网络安全研究与开发领域的协作进程。美国和以色列在此之前已签署了一份网络安全合作增强法案，促进以色列与美国各企业、大学以及、非营利性组织之间的联合研究与开发工作。除美国外，日本也拟与以色列签署加强网络安全的备忘录，通过强化与拥有高科技能力的以色列企业的合作，来提升日本安全产业的技术能力。

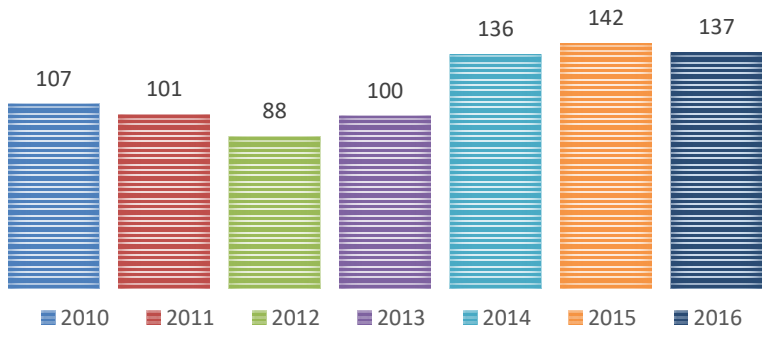
以色列之所以成为各国网络安全合作的优先选择之一，源自其领先的网络安全技术创新孵化能力和产业综合实力。以色列长期以来将发展网络安全产业作为国家战略和“国家经济增长的新引擎”。2016 年，以色列推出了升级版的网络安全产业发展计划“前进 2.0”（KIDMA 2.0）计划。在新计划中，以色列政府针对不同需求，提出了三种产业发展扶持措施：对于从事突破性和颠覆性技术研发的企业，政府每年精选 2～4 家给予持续 4 年的大额补贴，帮助其推进研发；针对急需产品创新和概念验证的企业，政府将给予为期 1 年的资助，帮助其培养一个国内用户或两个国外用户用于验证产品概念；而对于更小规模的网络安全企业，政府要求 3 家以上相关企业自行组合，通过建立研发联合体的方式，打造产业集群，受资助期为 2 年。

以色列目前已成为仅次于美国的世界第二大网络安全产品和服务出口国，拥有 228 家相关企业和数个网络安全研发科研中心。从以色列近年来的发展历程不难看出，创新促进政策对网络安全产业有着显著的拉动作用。

（三）并购、创投市场持续活跃，产业生态圈合作密集

1. 并购活动保持活跃态势，并购热点向中小企业集中

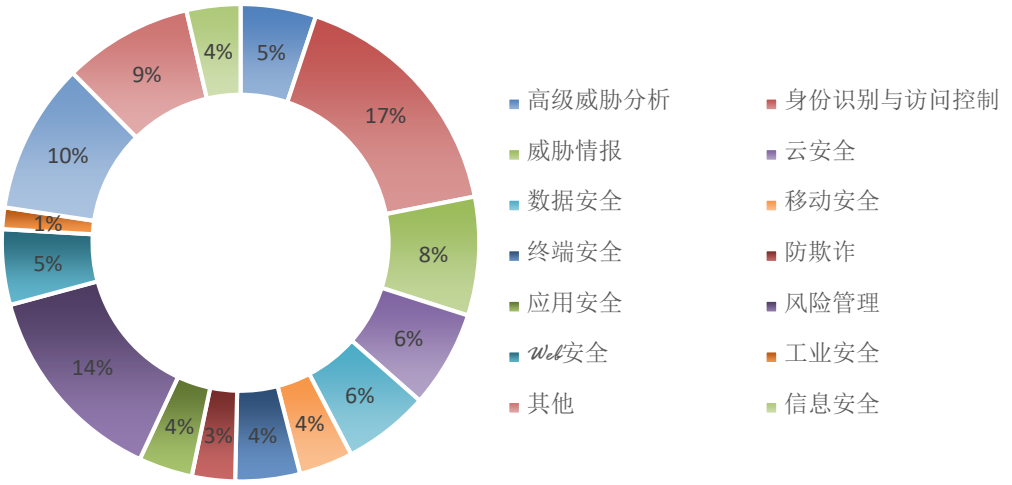
安全领域并购活动数量方面，2016 年全球共完成了 137 起并购活动，较 2015 年小幅下降，但仍处于历年高位水平，如图 6 所示。



数据来源： Momentum Partners

图 6 2010-2016 年全球网络安全并购活动数据

从并购趋势看，**一方面**，并购活动逐渐向中小安全企业集中，被并购企业规模在 5000 万美元以下的达到 105 家，超过并购总量半数以上。受此影响，2016 年国际安全领域并购总金额仅为 194.5 亿元，较 2015 年明显下降。**另一方面**，身份识别与访问控制、风险管理等领域成为并购热点。2016 年，身份识别与访问控制、风险管理、威胁情报领域并购交易数量分别达到 23 个、19 个、11 个，合计占比约 40%。其他新兴领域包括：防欺诈、Web 安全、高级威胁分析等。



数据来源：中国信息通信研究院（基于 Momentum Partners 数据整理）

图 7　2010-2016 年全球网络安全并购技术领域分布

2016 年并购金额较高的 10 个并购案例如表 1 所示。

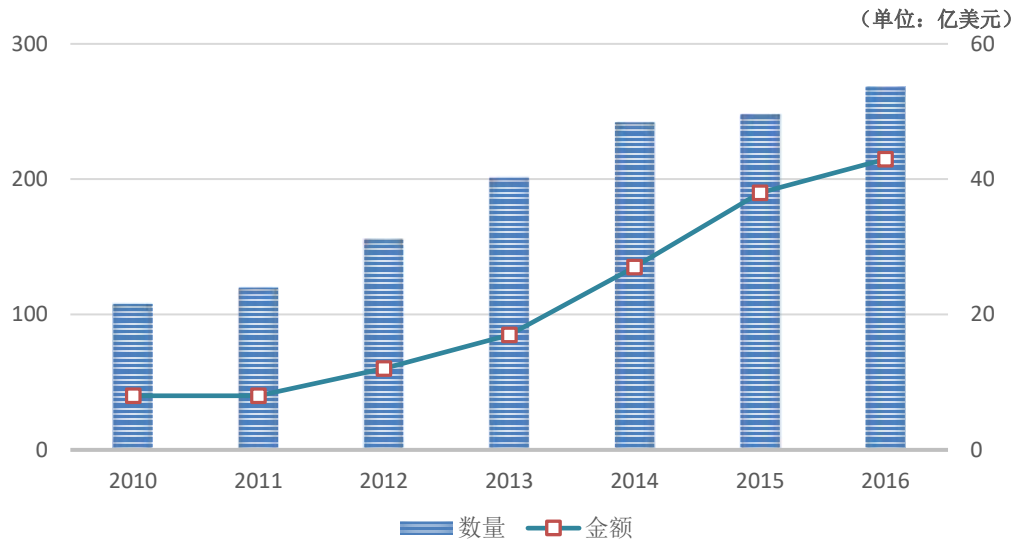
表 1　2016 年网络安全并购典型案例

日期	被收购方	并购方	并购金额（百万美元）
2016.6.12	BlueCoat	Symantec	4722.2
2016.9.7	McAfee	TPG Capital	4200.0
2016.11.20	LifeLock	Symantec	2362.1
2016.12.06	Optiv Security	KKR	1900.0
2016.7.7	AVG Technologies	AVAST Software	1463.0
2016.9.19	Infoblox	Vista Equity Partners	1254.3
2016.6.1	Ping Identity Corporation	Vista Equity Partners	600.0
2016.7.13	Imprivata	Thoma Bravo	488.5
2016.4.18	CSIdentity	Experian	360.0
2016.1.20	iSight Partners	FireEye	275.0

来源：中国信息通信研究院整理

2. 初创企业融资态势良好，以色列势头尤为强劲

2016 年，268 个创新企业收获了 42.95 亿美元的资金支持，企业数量与融资金额再创新高。从融资企业的技术领域分布看，2016 年融资活动超过 20 项的技术领域包括威胁情报、高级威胁分析、数据安全、风险管理、身份识别与访问控制等，与国际安全技术趋势高度一致。



数据来源： Momentum Partners

图 8 2010-2016 年网络安全初创企业融资态势

值得关注的是，以色列网络安全产业在总融资规模、初创企业融资比例等方面势头强劲。2016 年，以色列网络安全企业年共获得 5.81 亿美元融资，占全球网络安全产业融资总和的 15%；在 65 家 2016 年成立的网络安全初创企业中，已有 1/4 成功引入外部投资[6]。同时，跨国公司也在以色列布局扩张，2016 年以色列网络安全融资中有超过 1/3 来自跨国企业，投资者包括德国电信、新加坡 Innov8 Pte 等。

[6]数据来源：PitchBook,why 15% of the worlds investment in cybersecurity go to Israel.

中国企业也加入了以色列投资大军，例如华为收购了 HexaTier Ltd.，提供数据库安全解决方案。

3. 产业生态圈合作密集，大型企业平台效应逐渐显现

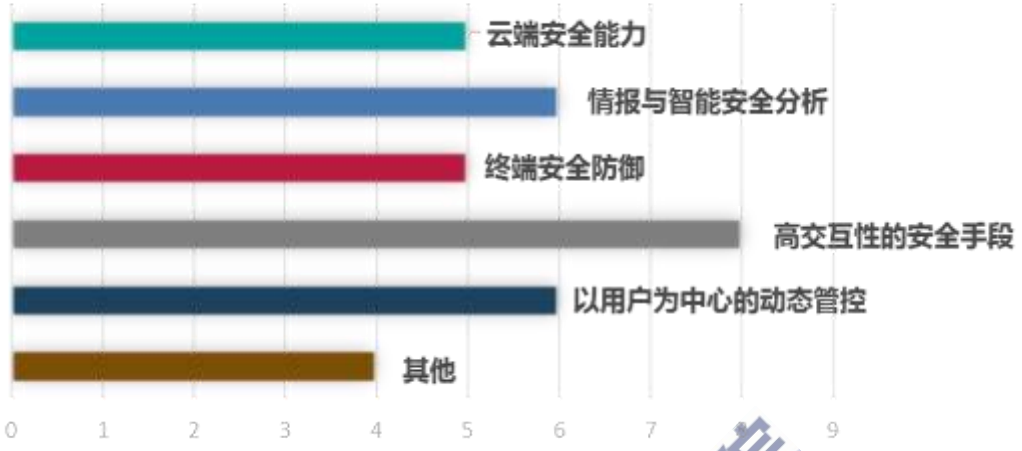
网络安全领域的协同理念已经由威胁情报共享延伸至更广维度，大型平台企业积极搭建安全生态，成为网络治理和秩序构建的核心平台，促进产业协同升级。例如，成立于 2012 年的工业互联网安全企业 Bayshore Networks，已经与 SAMSUNG、Cisco、BAE Systems 等巨头建立战略合作伙伴关系，合作厂商包括 Amazon、Splunk、Vmware、Arista 等 8 家。类似的，成立于 2013 年的云安全企业 Evident、威胁分析企业 Protectwise 分别将产品集成到 Amazon、Splunk 以及 Palo Alto、Phantom 等平台。

（四）网络安全技术加速创新迭代

信息通信技术的变革发展和新型安全威胁的不断出现驱动了全球网络安全技术的加速迭代创新。云安全、威胁情报等新兴安全产品和服务逐步落地，自适应安全、情境化智能安全等新的安全防护理念接连出现，为国际网络安全技术发展不断注入创新活力。

从国际权威机构聚焦的热点趋势上看，作为全球安全技术发展趋势的重要风向标，Gartner 和 RSA 对技术发展的趋势预测在不同程度上影响了国际安全产业的转型与持续发展。从近几年 Gartner 发布的技术发展趋势预测和 RSA 大会上各厂商讨论的热点议题看，国际上逐渐将安全技术发展的关注点聚焦在云端安全能力、以用户为中心的

动态管控、高交互性的安全手段、终端安全防御以及情报与智能安全分析等领域。



来源：中国信息通信研究院

图 9 2015-2017 年国际安全热点技术

从国际网络安全企业技术和产品布局上看，国际网络安全技术在云安全、安全行为分析、攻防交互性技术、终端安全防护、安全智能等相关领域中聚焦解决实际安全问题，呈如下发展趋势：

1．多点推进，发展云端安全能力

随着 IT 基础设施的虚拟化和业务的云化，大量企业开始向云端迁移。根据 Gartner 的预测，以云服务外包方式提供安全防护能力的云安全产业规模将在 2017 年达到 41 亿美元，到 2018 年，51%的企业应用服务将托管在云上。届时，**云服务使用者与提供商之间的安全认证、设备和行为的识别、敏感数据共享等安全技术将成为刚需。** BlueCoat、CipherCloud、Netskope、Skyhigh 等云安全领域国际领先技术厂商都已率先对云访问安全代理、软件定义安全、远程浏览器技

术等进行商业化和产品化，推出了各自的云安全解决方案和部署模型，提升云端的安全可视性、合规性、数据安全和威胁保护能力。

2．用户行为的深度挖掘逐渐成为安全分析的新中心

作为网络流量分析的补充和升级，行为分析一直是网络安全分析领域的热点。用户行为分析以用户作为分析的中心，通过定义不同的属性实体如终端、网络、应用、账号等，从多个维度关联分析用户行为。自 2014 年以来，用户行为分析市场增速明显、并购频繁，Splunk、Securonix、Interset、Exabeam、Niara 等厂商已推出成熟度较高的相关产品，而人工智能、高级机器学习等先进技术的兴起（如表 2 所示），有望推动安全行为分析利用更多安全实体的行为信息及实体间的关联关系，给行为分析提供智能化的决策模式，使分析结果更加准确，提高安全威胁检测的有效性。

3．虚拟化助推交互性的主动防御技术发展

以网络伪装、主机伪装、服务伪装等技术为核心的动态防御是从军事领域延伸到网络安全领域的对抗防御概念。早期依赖沙箱、蜜罐等技术在虚拟环境中捕获恶意代码并分析其入侵过程，随着虚拟化技术的逐渐成熟和落地，高交互性的攻防技术不断发展。Shape、Morphisec、JunmoSoft 等前沿技术厂商推出了基于移动目标防御、多态防御概念的产品，**对网络、应用、终端和数据的伪装，诱骗攻击者实施攻击**。尤其针对通过特征识别实施攻击的各种自动化攻击工具，可隐藏真实目标，触发攻击告警，与攻击者进行主动对抗。

表 2 已应用人工智能/机器学习的国际网络安全企业

企业名称	相关产品概述	投资额（百万美元）	投资方
Tanium	利用自然语言处理，实现实时的终端可视化管理，企业可通过网络收集数据和更新终端信息	295	Executive Press; Andreessen Horowitz; Nor-Cal Invest
Cylance	应用人工智能算法预测、识别和阻止恶意软件，减少零日攻击	177	Khosla Ventures; Fairhaven Capital; Citi Ventures
LogRhythm	在合规自动化、增强的 IT 智能的基础上，提供威胁情报和分析，快速检测、响应和控制威胁	126	Access Venture Partners;Siemens Venture Capital; Exclusive Ventures
Darktrace	结合行为分析和高级数学，自动化地检测异常行为	107	SoftBank Group; Samsung Ventures; Ten Eleven Ventures
Sift Science	基于实时的机器学习的防欺诈解决方案	54	Union Square Ventures; Spark Capital; SV Angel
Exabeam	利用已有日志数据分析用户行为，快速检测高级攻击，管理事件优先级，并指导有效的响应	35	Aspect Ventures; Icon Ventures; Norwest Venture Partners
E8 Security	提供智能和分析软件，及大数据平台，实现长期数据留存和回溯分析	22	Allegis Capital; March Capital Partners; Strategic Cyber Ventures
CyberX	通过分析工业网络中的操作数据，检测异常行为	11	FF Venture Capital; Flint Capital; GlenRock Israel
Interset	利用行为分析保护制造、生命科学、高新技术、金融、政府、航空、国防和证券行业的关键数据	10	In-Q-Tel;Anthem Venture Partners; Telesystem

来源：中国信息通信研究院

4．设备和智能终端侧安全检测和响应技术持续升温

终端发展的多样化、智能化和海量化使得安全问题在终端使用场景中被逐步放大，而**仅靠拦截已逐渐无法应对新形势下的安全挑战**。RSA 总裁 Amit Yoran 指出，当前仅有 10%的安全预算被用在安全检测和响应技术上，而到了 2020 年，该比例将上升至 60%。目前，终端安全检测和响应、内存保护、漏洞利用阻断等终端防御技术正在不断涌现，以针对性的保护终端系统，并快速地对攻击进行响应。Symantec、Kaspersky、Trend Micro 等传统终端安全厂商都在不断推出自己的终端安全检测和响应产品，完善终端安全解决方案。同时，Carbon Black、CrownStrike、CounterTack 等一批专注于终端恶意行为拦截的新兴终端安全厂商正在积极推动该领域的产品和技术创新。

5．安全情报驱动安全智能从概念走向落地

国际安全威胁情报市场逐渐兴起，据 IDC 预测，到 2018 年，威胁情报安全服务市场规模将增长到 14 亿美元，复合增长率达到 12.4%。随着企业对威胁情报系统的普遍部署，**威胁情报本身也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**，旨在构建全面的预测、基础防护、响应和恢复能力，防御不断演变的高级威胁。此外，未来将有更多企业建成安全数据仓库，支持全要素融合的安全监测与情报分析，安全架构的重心将从防护向持续普遍性的监测响应以及自动化、智能化的安全流程转移。Symantec、FireEye、iSight Partners、Phantom 等传统和新兴安全厂商也持续在威胁情报、安全智能、安全自动化等方面推出了各自的平台和产品。

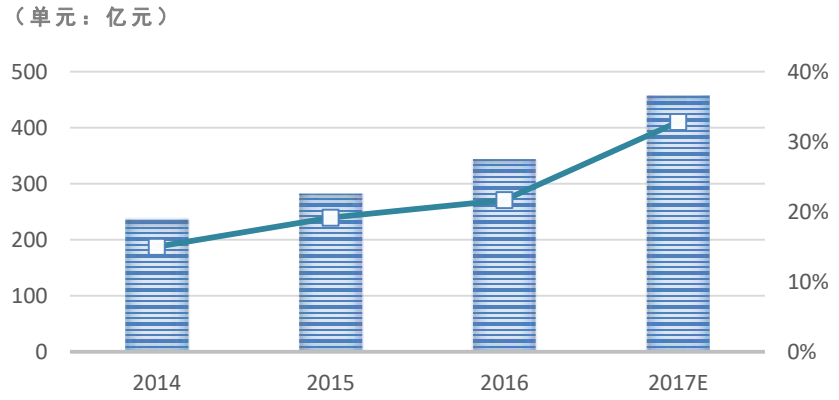
三、我国网络安全产业发展进入崭新阶段

（一）我国产业规模迅猛增长，产业各方协同发力

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。

1. 国内网络安全产业规模高速增长，安全服务领域创新活跃

随着政策的持续利好，近年来国内网络安全产业快速发展。根据中国信息通信研究院统计测算[7]，2016 年我国网络安全产业规模约为 344.09 亿元，较 2015 年增长 21.7%，预计 2017 年达到 457.13 亿元。



来源：中国信息通信研究院

图 10　2014-2017 年国内网络安全产业规模及增长情况

新形势下，产品和服务的联动更加紧密，安全服务逐渐从配合产品的辅助角色，转变成为安全产品发挥最佳效用的必要条件。网络安全产业正由产品主导向服务主导转型，态势感知、监测预警、云安全服务等新技术新业态层出不穷，网络安全技术密集化、产品平台化、

[7]测算以国内近百家安全企业调研数据为基础，按照细分市场分类测算方式进行估算，并参考样本企业平均增长率对产业规模进行了修正。

产业服务化等特征不断显现。

2．重点城市加快产业布局，产业集群效应逐渐显现

为抓紧网络安全产业发展机遇，打造国家网络安全产业区域高地，成都、武汉、上海等重点城市不断加快产业布局，引导企业、科研、人才等资源集聚。四川省《信息安全产业发展工作推进方案》提出 2020 年实现安全产业规模 1100 亿目标，而成都作为四川网络安全产业重地，制定出台一系列促进产业发展的重要举措，如 2016 年 4 月投资 130 亿建设“成都国家信息安全产业基地”；连续 3 年给予安全示范应用企业、公共技术平台、产学研用创新机构以及专业技术人员提供补助等。成都的积极布局，吸引了国际国内安全巨头相继设立研发基地，也使得成都在安全技术研发和产业发展方面走在全国前列。

武汉则致力于打造网络安全领域的中国硅谷。2016 年 9 月，武汉正式启动国家网络安全人才与创建基地建设。2017 年 3 月，武汉市政府发布了《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，例如，对教学实验设备的购置给予总额不超过 1 亿元的补贴，对网络安全基地内企事业单位和机构新引进的产业领军人才个人给予 50 万元至 200 万元的奖励补贴等。

上海市以创建具有全球影响力的科技创新中心为契机，加快网络安全产业发展布局。2016 年，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，为互联网经济发展

保驾护航。截至目前，已有百余家安全企业在上海落户发展，多家安全企业成功在新三板挂牌，同时上海也在网络安全人才教育、网络安全公共平台建设等方面取得积极进展。

3．网络安全人才培养上升法律和战略高度，高校企业共同发力

中央对网络安全人才培养问题高度重视，安全人才培养、交流、培训、考核等纳入法律范畴。2016 年，习近平总书记在“4·19”讲话中对网络安全人才问题做了重要论述。2017 年 6 月正式实施的《网络安全法》中，有三处明确涉及网络安全人才工作。第三条提出，国家“鼓励网络技术创新和应用，支持培养网络安全人才”。第二十条明确，“国家支持企业和高等院校、职业学校等教育培训机构开展网络安全相关教育和培训，采取多种方式培养网络安全人才，促进网络安全人才交流”。第三十四条要求，关键信息基础设施的运营者要定期对从业人员进行网络安全教育、技术培训和技能考核。《网络安全法》首次以法律形式强调要加强网络安全学历教育和职业培训，将有力推动各方面参与、支持网络安全人才培养工作。

互联网企业、安全企业与高校携手，通过联合研发、共建学院、资金支持等创新模式，共同致力于网络安全人才培养。**一是**企业与科研院所共同研发具有学术前瞻性的市场化、实用化的科研项目成果。例如，中国信通院与阿里巴巴集团成立安全创新中心，通过标准制定、产业研究、测试技术研发等方面深度合作，加强安全技术能力和创新成果输出，增进社会服务能力；北信源和北京邮电大学成功建立联合

实验室；360 与北京大学联合共建“数据可视分析联合研究中心”，与西安电子科技大学联合共建“系统安全与大数据联合实验室等。**二是**企业与高等院校通过联合共建网络安全研究院、实训基地等方式，着力培养高层次、具备实战对抗能力的网络安全精英人才。例如，360 与武汉大学联合共建“国家网络安全研究院”、与北京航空航天大学合作建立汽车信息安全研究院；阿里云与成都信息工程大学、贵州理工学院等高校联合共建大数据学院，专注大数据人才培养。

（二）网络安全重大政策助力产业打造竞争优势

随着我国《网络安全法》的实施和网络安全相关规划的不断推进，相关政策也为安全产业的发展提供了新的契机和更有力的支持。

1.《网络安全法》为安全产业进一步发展打开了空间

《网络安全法》共有 7 章 79 条，规定的基本制度包括：关键信息基础设施保护制度、网络产品检测认证制度、国家安全审查制度、数据安全和个人信息保护制度、实名登记制度以及监测预警和应急处置制度等。其中，涉及安全企业权利与义务的条款主要集中于基础设施保护与网络安全防护、加强数据安全和用户信息保护、应急处置与威胁监测等方面。

《网络安全法》确立了网络安全保障在整个信息化建设中的核心和关键地位，对遏制网络安全威胁、推动网络安全标准化工作、促进网络安全技术和产品开发等都具有重要意义。**一方面，**《网络安全法》为产业的未来发展指明了方向，使安全企业的产品和服务开发、网络数据和知识产权保障等有法可依，为各企业发展壮大、走向国际提供

良好的产业环境；**另一方面**，《网络安全法》中关于安全认证、审查、检查等的规定能有效促进企业提升网络安全意识，加大网络安全投入；并促进金融、能源、电信等关键行业加大对网络安全产品和服务的采购、部署，进一步提升安全产业规模的增长率，为中小企业、初创企业等的发展营造良好的产业生态。

2．科技专项为安全产业提供资金投入支持和发展方向指导

随着技术创新在产业发展中的重要性不断凸显，涉及网络安全的科技专项不断增加，客观上增加了对安全产业的投资和对安全技术发展方向的指引。2016 年，网络安全正式纳入了国家重点研发计划，定位于逐步推动建立起既“与国际同步”又“适应我国网络空间发展”、“自主”的网络空间安全保护、治理和网络空间测评分析技术体系。

2017 年“网络空间安全”重点专项总体目标是：聚焦网络安全紧迫技术需求和重大科学问题，坚持开放发展，着力突破网络空间安全基础理论和关键技术，研发一批关键技术装备和系统，逐步推动建立起与国际同步，适应我国网络空间发展的、自主的网络空间安全保护技术体系、网络空间安全治理技术体系和网络空间测评分析技术体系。包括了网络与系统安全防护技术研究、开放融合环境下的数据安全保护理论与关键技术研究、大规模异构网络空间中的可信管理关键技术研究、网络空间虚拟资产保护创新方法与关键技术研究、网络空间测评分析技术研究等 5 个创新链，共部署 47 个重点研究任务，实施周期为 5 年，国拨经费总概算为 3.99 亿元。

重点专项依托众创空间和科技企业孵化器拓展了企业的创新渠道，未来还将进一步支持企业、龙头骨干院校和青年人共同建造专业化众创空间，对安全企业创新网络安全技术、开发高新技术产品有着鼓励和促进作用。

3．各类网络安全规划推进实施对安全产业的拉动作用不断凸显

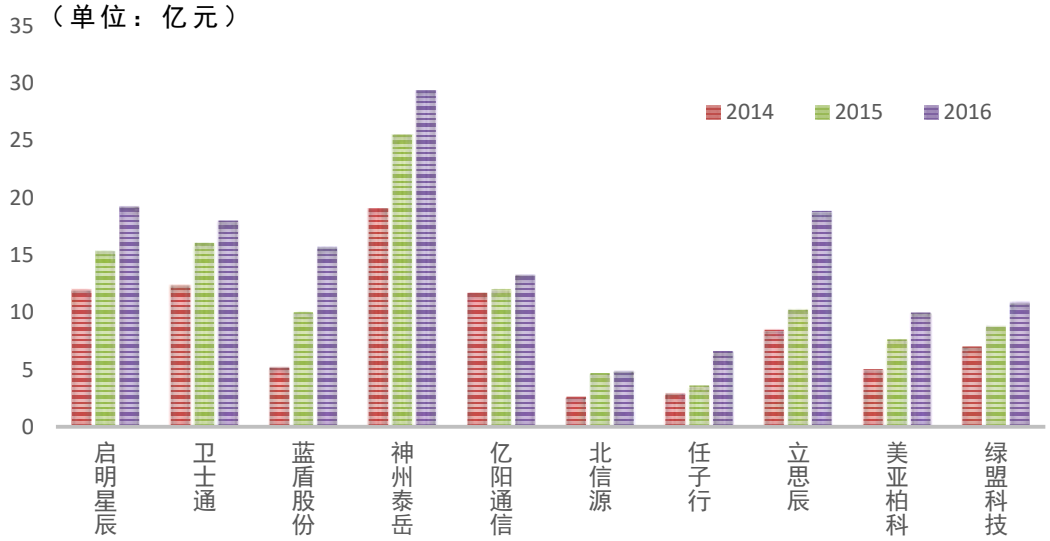
我国已进入十三五规划深入推进时期，随着各类规划、指南的进一步实施，有效拉动安全产业的措施也不断增多。**《“十三五”国家信息化规划》**在“防范安全风险，夯实发展新基石”这一主攻方向中提出“提升网络安全保障能力”，要求落实网络安全责任制，促进政府职能部门、企业、社会组织、广大网民共同参与，共筑网络安全防线。在主要任务“建立统一开放的大数据体系”中，提出要“注重数据安全保护。推进数据加解密、脱密、备份与恢复、审计、销毁、完整性验证等数据安全技术研发及应用”。在主要任务“健全网络安全保障体系”中提出要“建立政府和企业网络安全信息共享机制”，“强化网络安全科技创新能力”，“加快推进安全可靠信息技术产品创新研发、应用和推广，形成信息技术产品自主发展的生态链”，“建立有利于网络安全产业良性发展的市场环境，加快培育我国网络安全龙头企业”。此外，**《信息产业发展指南》**也提出要“推动信息安全技术和产业发展”，“推动信息安全产品和服务的研发和产业化应用。充分发挥政府引导作用，加快培育骨干企业，发展特色优势企业，打造结构完整、层次清晰、竞争有力的产业格局”。

以上政策措施与促进安全产业发展直接相关，可为安全企业的未来发展提供直接指导。此外，工业和信息化部近年来为了落实《网络安全法》等重大政策，开展了网络安全试点示范工作，为企业提供了研发、应用、交流、学习网络安全先进技术和最佳实践的良好平台。

（三）安全企业业绩再创新高，产业阵营逐步扩大

1．我国安全企业整体发展态势良好，营收增幅显著

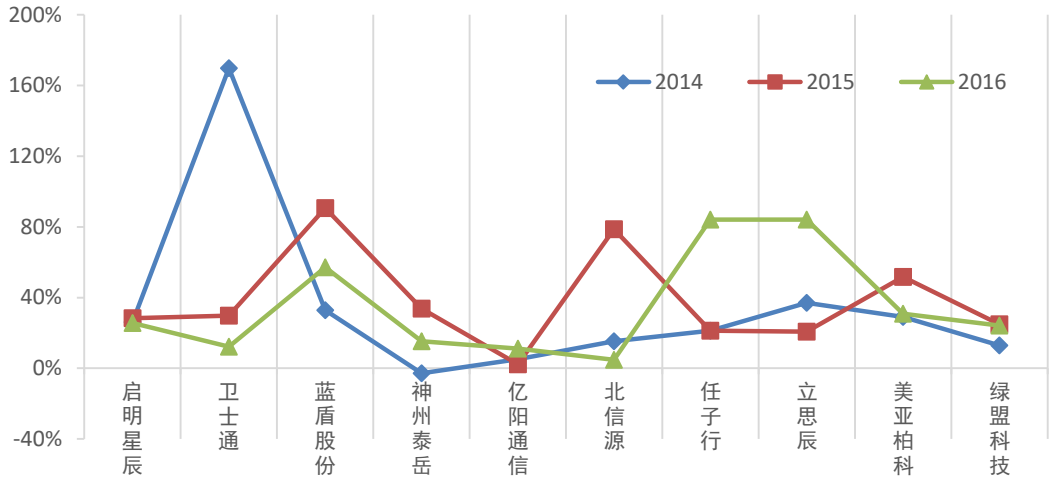
国内安全企业 2016 年总体表现良好，稳步成长壮大的同时营收增幅明显。从上市企业营收情况规模看，10 家上市安全企业 2016 年总营收规到 146.95 亿元。2014-2016 年国内上市安全企业营收情况如图 11 所示。



来源：中国信息通信研究院

图 11　2014-2016 年国内上市安全企业营收情况

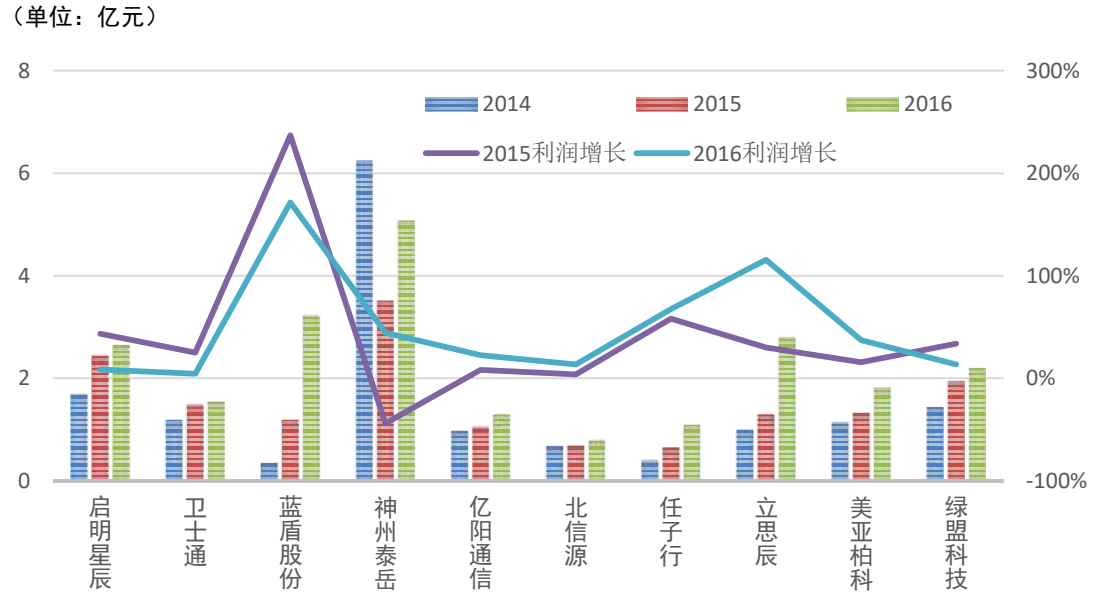
在营收增长方面，10 家上市安全企业 2016 年平均营收增长率 34.94%，超过国际上市的安全企业 21.45%的增长速度。2014-2016 年营收增长情况如图 12 所示。



来源：中国信息通信研究院

图 12　2014-2016 年国内上市安全企业营收增长情况

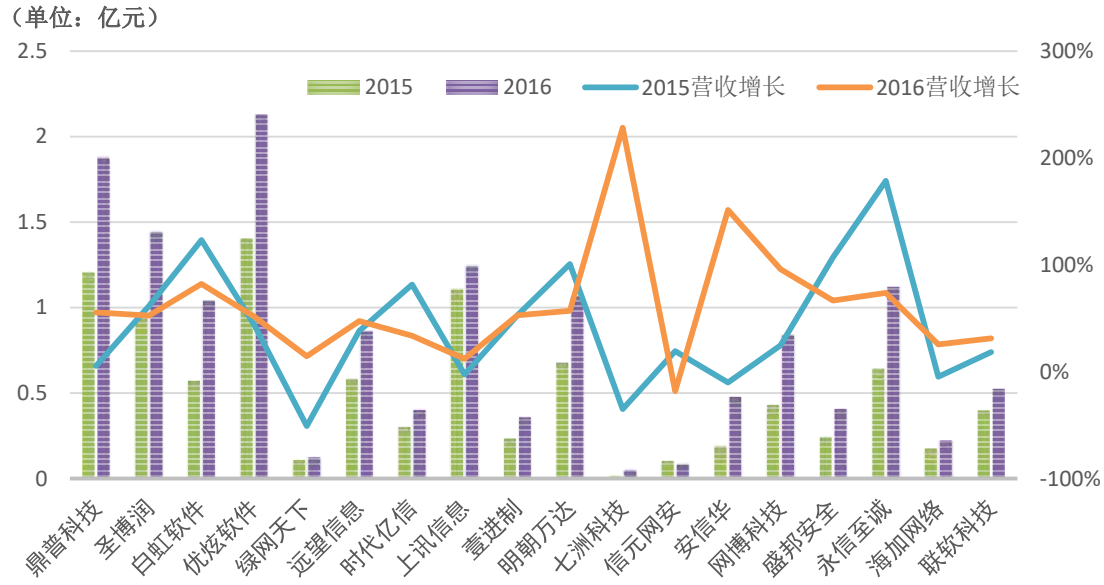
在净利润方面，10 家上市安全企业 2016 年平均净利润为 2.25 亿元，较 2015 年增长 49.92%，净利润增幅显著。10 家上市安全企业的 2014-2016 年净利润及增长情况如图 13 所示。



来源：中国信息通信研究院

图 13　2014-2016 年国内上市安全企业净利润及增长情况

2016 年，新三板挂牌安全企业发展走势整体较好。40 家样本企业[8]2016 年总营收达到 27.88 亿元，其中 15 家企业营收增长超过 50%；在净利润方面，仅 55%的企业实现盈利，盈利能力仍有待提升。部分样本企业 2015-2016 年营收及增长情况如图 14 所示。



来源：中国信息通信研究院

图 14　2015-2016 年部分国内新三板挂牌安全企业营收增长情况

2. 互联网企业影响力显著提升，成为安全圈重要成员

一方面，大型互联网企业强化网络安全能力输出，依托云平台优势，在网络攻击防护、应用安全、病毒防护等方面取得积极进展。例如，阿里云云盾安全体系集成了 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

[8]统计范围包括：鼎普科技、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 40 家企业。

领域发力，并积极利用大数据资源增强威胁情报能力。**另一方面**，互联网企业与安全企业、通信企业等建立了紧密的战略合作、协同联动关系，共同推动安全生态建设。例如，百度安全联合中国电信以及其他全球合作伙伴，建立起大型网络流量清洗中心；腾讯通过鹰眼系统建立与中国联通的合作，共同致力于打击通诈骗活动，并与启明星辰达成战略合作，推出面向企业市场的终端安全解决方案。

3．传统通信企业、大型国企积极开展安全布局

一方面，大型国企整合优势资源，推动构建完整的网络安全生态体系。2015 年 5 月，中国电子科技集团公司（CETC）集合旗下三十所、三十三所、中电科技公司等单位，成立中国电子科技网络信息安全有限公司（简称“中国网安”），打造网络安全产业生态链条。中国电子信息产业集团公司（CEC）旗下世纪互联、迈普通信等多家企业着力面向网络安全转型，强化网络安全技术能力。**另一方面**，传统通信企业积极布局网络安全，深耕专业技术领域。中国电信推出了云堤产品，为企业和用户提供运营商级别的安全防护。中兴通讯全力整合企业内部资源，成立了独立的网络安全部门，重点围绕 APT 攻击防御领域，构建应对未知、隐蔽、持续威胁的下一代安全防护能力。

4．大中型安全企业抓住“一带一路”机遇，开拓海外市场

“一带一路”在推进网络互联互通的同时，也为网络安全产业注入了新的市场机遇。大中型安全企业凭借技术优势和口碑，积极响应国家“一带一路”战略，开拓国际布局。例如，启明星辰持续强化国际

化产品开发能力，通过公司已经具有国际竞争力的部分优势产品，加强对外战略合作，加速建立和完善海外营销和服务网络。深信服设立了美国、新加坡、马来西亚、迪拜等七大境外直属分支，业务遍布全球 16 个国家及地区，海外客户近千个，海外收入超亿元。

（四）企业融资高度活跃，产业生态不断优化

1．安全领域创投活跃，产业基金顺势起航

一方面，随着网络安全关注度日益提升，创投机构普遍将目光移向安全领域，网络安全领域创投活动高度活跃，如表 3 所示。秉承自适应安全理念的青藤云安全，成立于 2014 年，获得来自真格基金、云天使基金、丰厚资本 650 万天使轮融资，2015 年获得来自宽带资本、红点创投的 6000 万 A 轮融资。聚焦下一代 WAF 技术的初创企业长亭科技，成立 3 年来，相继得到天使轮、Pre-A 轮、A 轮融资，融资额分别为 6000 万、2700 万、千万级别，投资方包括启明资本、君盛资本、滴滴，真格基金等，截止目前总融资已过亿元。

另一方面，产业基金继续发力，为产业发展注入新活力。2017 年 1 月，中国互联网投资基金正式成立，由国家网信办和财政部共同发起，经国务院批准设立，基金规划总规模 1000 亿元人民币，目前基金首期 300 亿元资金募集认缴到位。2017 年 5 月，国内首只百亿级网络安全母基金启动。该母基金由北京日报报业集团联合中信建投证券股份有限公司、金汇金投资集团发起设立，总规模 100 亿元，将专注投资网络信息安全领域。

表 3 国内网络安全初创企业融资情况

企业名称	创立时间	技术领域	天使轮/Pre-A		A 轮		B 轮	
			金额	投资方	金额	投资方	金额	投资方
东巽科技	2010	APT 防御	未披露	未披露	4000 万	稼沃资本、如山创投、基石投资	—	—
青藤云安全	2014	自适应安全	650 万	真格、云天使基金、丰厚资本	6000 万	宽带资本、红点创投	—	—
长亭科技	2014	应用安全	600 万	真格基金	数千万	启明创投、君盛、滴滴等 4 家机构	—	—
FREEBUF	2014	安全媒体	3000 万	线性资本	—	—	7000 万	银杏谷、嘉铭浩春、张江科技等 5 家机构
瀚思	2014	大数据安全	数百万	光速中国	3000 万	恒宝、赛伯乐中国、南京高科	1 亿	国科嘉和、IDG 资本、南京高科
天空卫士	2015	内容安全	近千万	中科创新	1.5 亿	360、华创资本、国投创业	—	—
小安科技	2015	安全服务	近千万	中科创新	—	—	—	—
微步在线	2015	威胁情报	1000 万	北极光、云天使基金	3500 万	如山、北极光、华软	1.2 亿	高瓴资本、如山、北极光

来源：中国信息通信研究院根据公开信息整理

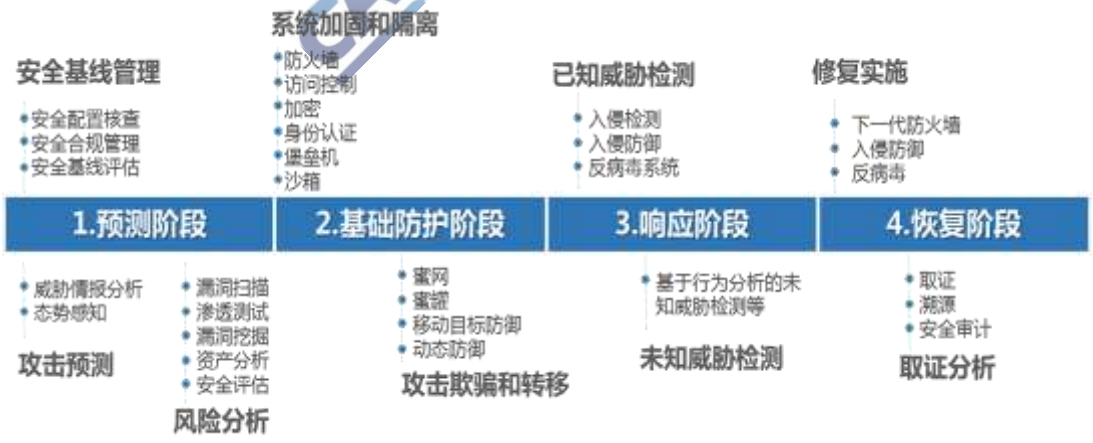
2. 产业联盟积极发挥平台作用，推动产业快速发展

一方面，已有产业联盟积极作为，聚合产业势能，服务产业发展。例如，中国通信企业协会通信网络安全专业委员会通过组织开展“通信网络安全管理员技能大赛”、“网络安全人员认证”等方式，助力网

络安全人才建设；成立于 2015 年 12 月的中国网络安全产业联盟，目前会员单位数量已超过 209 家，囊括了国内大部分活跃网络安全企业，在建言国家政策、优化产业环境、产业国际化拓展等方面开展了一系列工作。**另一方面**，重点领域和新兴领域安全产业联盟相继成立，搭建产业交流平台，促进政产学研联动。例如，2017 年 6 月，工业信息安全产业发展联盟在京成立，联盟接受工信部业务指导，目前联盟首批成员单位已达 149 家，包括神华集团、中车集团、航空工业、中国兵装、中国电子信息产业集团等工业领军企业。

四、我国重点领域和新兴方向技术进展

从细分技术领域看，我国网络安全产品和服务已基本覆盖了安全防护的“预测—基础防护—响应—恢复”生命周期各个阶段，为企业和个人用户提供包括风险预判、攻击预测、安全防御、事件检测、追溯响应等在内的全生命周期的安全防护[9]，如图 15 所示。



来源：中国信息通信研究院

图 15　我国典型安全产品和服务在防御生命周期的分布情况

[9]本报告中安全产品和服务在防御生命周期的划分借鉴了 IDC 产业分类、PDRR 模型和 Gartner ASA 自适应安全架构等国际主流网络安全产品和服务的分类方式，并充分结合我国安全产品和服务实际情况。

目前我国安全产业产品和服务呈以下发展特点：**一是安全产品逐渐向功能多样化的方向发展**。下一代防火墙、入侵防御等安全产品在安全防御周期的多个阶段持续发挥作用。**二是我国安全产品目前大部分集中在基础防护阶段**。该阶段典型安全产品以入侵检测、入侵防御、WAF 等为代表，为用户提供攻击检测、访问控制等方面的安全防御。**三是作用于预测或恢复阶段的安全防御措施逐渐以安全服务的形式在兴起**。随着国内市场对安全服务的接受度逐渐提高，安全服务类型和市场规模也不断增长。除已形成的集成、运维、评估和咨询四大服务领域外，威胁情报、态势感知、事件溯源等预测和恢复阶段的安全技术成为安全企业尤其是以技术创新为主导的初创企业争相布局的热点领域。

（一）重点领域安全技术优势逐渐成型

1．预测领域：情报价值驱动风险分析和攻击预测技术快速发展

由于安全防护的思路一直是以防御攻击为主导，导致预测领域在很长一段时间内是企业安全防护的薄弱区，所采取的技术措施也主要以合规为导向。预测领域的技术产品主要通过对终端、服务器、网络设备、云基础设施、操作系统、应用软件、服务、接口等的安全配置基线进行分析、合规检查和变更管理等，提供能提升信息系统安全性的解决方案，以降低由于安全措施不足而引起的安全风险。

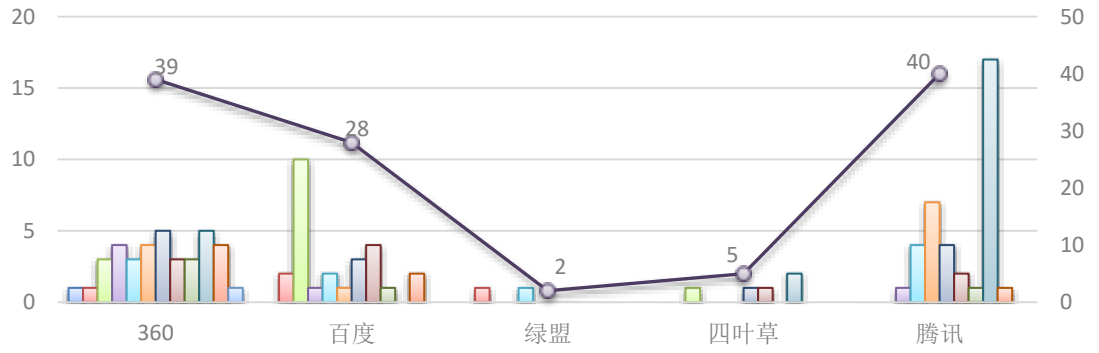
随着近年来国内外对安全情报价值的发掘，越来越多安全技术开始在预测领域得到应用。**一是**通过漏洞扫描、渗透测试、漏洞挖掘、安全评估等风险分析方式，在基线管理的基础上，对安全对象进行资

产分析和风险评估，主动地分析系统发生威胁的可能性。**二是**通过安全威胁情报的广泛搜集，包括安全服务厂商、防病毒厂商、安全组织等发布的漏洞信息、安全预警信息、威胁信息等，分析攻击者在行业、信息类别、数据敏感度等方面的关注度，以达到预测攻击行为和目标的目的，如图 16 所示。

来源：中国信息通信研究院

图 16　预测领域安全技术视图

值得注意的是，360、阿里巴巴、百度、腾讯等互联网企业对安全领域逐渐重视和持续投入，汇集了大量国内漏洞挖掘领域安全人才，在相应领域形成了较强的安全技术实力。以微软的公开漏洞挖掘数量为例，2016 年国内以 360、百度和腾讯为首的互联网公司及其安全团队所提交的漏洞数量和质量可圈可点，如图 17 所示。



来源：中国信息通信研究院

图 17　2016 年 1-12 月微软致谢国内厂商漏洞挖掘情况

2．基础防护领域：依托传统优势，寻求主动化和多样化发展

基础防护领域是企业部署各类安全产品的重点领域，多作用于攻击事件发生过程之中。一是通过部署访问控制、黑白名单等措施实行常态化安全防护，二是以优化或隔离的方式降低攻击面，对信息系统进行保护，三是采用交互性更强的欺骗和转移等手段来混淆攻击者等。

在基础防护领域，基于系统优化/隔离与基于攻击欺骗/转移的防护技术互相补充。**一方面**，以防火墙、身份识别与访问控制、加密、堡垒机等安全产品仍是企业安全防护布局的重点。采用访问控制列表、加密、沙箱等隔离方法，限制来自系统外部或系统内的进程或应用接口间的数据访问，从而限制攻击者接触系统、发现漏洞和执行恶意代码的能力，降低攻击面。**另一方面**，攻击欺骗和转移类安全技术不断兴起。从传统的蜜网、蜜罐到近年来兴起的移动目标防御、动态目标防御等，防御方开始对攻击方隐藏或混淆系统信息，加大攻击方寻找真正的攻击目标的难度，以在攻防对抗中获得时间上的非对称优势，成为构建纵深防御策略中不可或缺的重要环节，如图 18 所示。

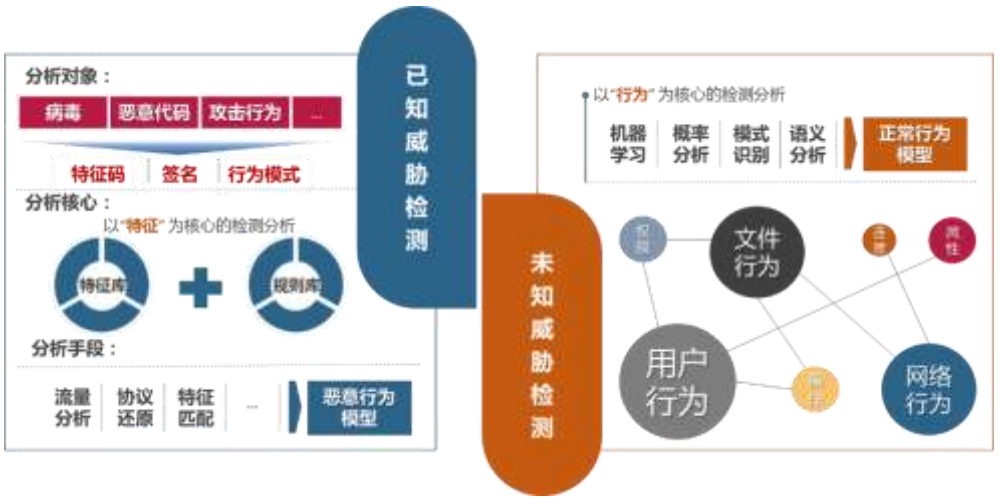
来源：中国信息通信研究院

图 18　基础防护领域安全技术视图

3．响应领域：智能化分析带动未知威胁检测技术发展

响应领域的主要作用是当拦截和阻断等安全防御机制被攻击者绕过时，在尽可能短的时间内检测发现入侵行为，以最小化攻击给系统带来的危害。此时需要依靠对网络流量、用户行为、文件操作等进行持续的分析，以发现异常和攻击行为。主要手段包括以特征匹配为对象的已知威胁检测和以行为分析为对象的未知威胁检测。

已知威胁检测是网络安全防御产品中发展时间较长、技术较为成熟的一类。基于特征、签名和行为模型的反病毒、入侵防御系统、下一代防火墙等均具备相关功能。通过对信息系统中发生的攻击事件进行实时的检测和预处理，在检测网络和终端中的出现的异常的同时，也对事件的风险进行预判，为后续的响应过程提供判断依据。未知威胁检测相关技术在近年来日趋火热，主要依靠对流量、行为等的统计和关联分析，发现偏离正常行为模式的攻击或异常行为，从而对未知威胁进行检测和拦截，有效的弥补了基于特征的检测方法在面对未知威胁时表现出的不足，如图 19 所示。

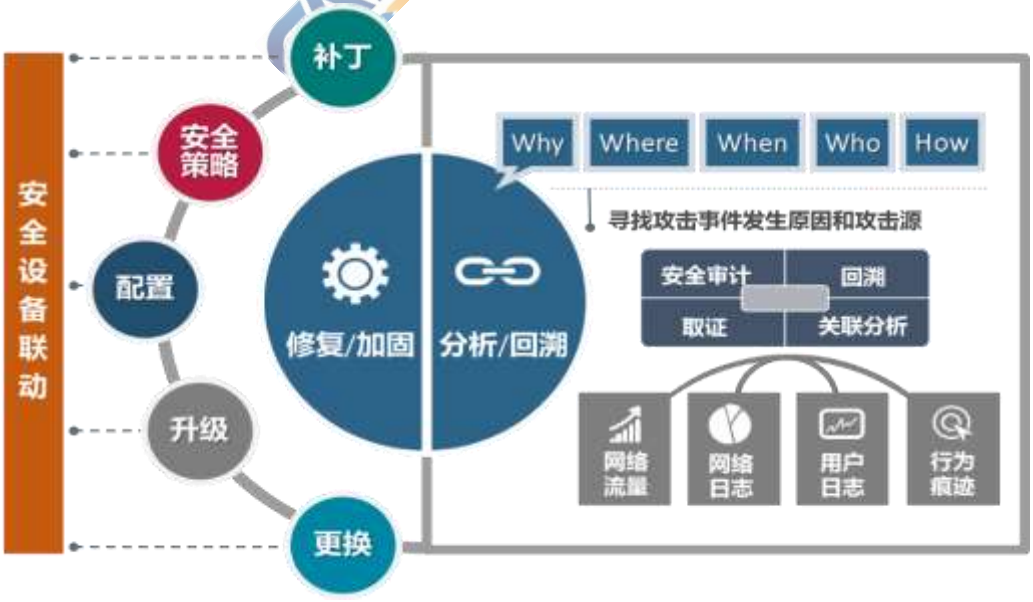


来源：中国信息通信研究院

图 19　响应领域安全技术视图

4. 恢复领域：修复实施自动化程度有所提升，安全事件回溯分析需求迫切

从单个安全防御生命周期来看，恢复是防御周期的最后一步，是对所配置安全策略的有效性的进一步落实。**一是**在攻击事件发生后，针对性的对系统的安全漏洞进行修复或安全策略进行变更，以防止类似事件的继续发生。由于修复实施对操作人员要求较高，目前尽管在一些下一代防火墙、SOC 等产品中已加强了与修复措施的联动，提升了自动化程度，但大部分还是采取人工的方式，由安全人员来实行操作。**二是**通过对留存的日志和流量等信息进行分析、回溯或事件重现，寻找攻击事件发生的原因及攻击源。如采用安全审计、取证分析等手段，利用用户日志、网络流量等留存的监测数据，借助关联分析、事件重现等方法对攻击事件进行回溯分析，以探究攻击事件为何发生、如何发生、由谁发起等原因。



来源：中国信息通信研究院

图 20 恢复领域安全技术视图

（二）新兴技术与安全技术加速融合发展

1．态势感知迈向产品应用阶段

目前，国内网络安全态势感知正经历“从无到有”、“从概念到落地”的过程，阿里云、360、观安、安恒、天融信等均推出了安全态势感知产品。例如，阿里云聚焦云上安全态势感知能力建设，提供覆盖云上资产的实时监控、定期扫描和入侵检测能力，并利用机器学习技术实现对未知威胁的感知、回溯和预测。360 将态势感知与安全运营有机结合，实现威胁情报与终端管理系统和下一代防火墙进行联动，对威胁和异常行为进行处置。观安以大数据为核心构建风险感知能力，建立了资产发现、指纹识别、快速检测、漏洞管理的闭环模型。

虽然国内各类态势感知产品逐渐在越来越多的行业和机构中部署和应用，但仍存在标准缺失、感知层基础设施薄弱、数据分析能力不足等诸多问题，仍需在这些方面进行完善。

2．虚拟化技术推动安全产品形态演进

随着 5G、混合云、未来网络基础设施等概念的提出，“高速开放、智能融合”成为网络发展的核心理念。构建资源可全局调度、能力可全面开放、架构可灵活调整的新一代虚拟化网络成为未来网络升级演进的趋势。

在虚拟化环境下，安全产品逐渐以软件或云服务的方式呈现，可以提升安全产品在部署、使用、扩展等方面的灵活性，降低产品运维管理成本。目前，国内如华为、深信服等企业已在虚拟化安全领域展开探索，依托 SDN 网络架构，将防火墙、入侵防御系统、DDoS 攻

击防御系统等传统安全产品和服务向云端迁移，利用 NFV 技术突破专用安全硬件的壁垒，实现安全产品的软件化、通用化和云化。

另一方面，随着网络虚拟化的发展，其核心组件如控制器自身的安全问题也逐渐被业界关注。虽然华三、中兴、上海贝尔等硬件厂商已推出 SDN 控制器、SDN 交换机等虚拟化设备，但更多关注的是虚拟化设备在性能、一致性等方面的表现，而对 SDN 控制器自身的安全防护机制、代码缺陷、协议漏洞等安全问题关注较少。目前，学术界已提出“安全虚拟化”的概念，通过在虚拟化设备中加入安全模块，以提高其自身的安全防护能力，但出于市场需求、开发成本等原因，产业界目前尚未有此类产品出现，未来市场前景需观望。

3．人工智能有望驱动网络安全技术革新

近年来，人工智能技术发展迅猛，谷歌、IBM、微软等国外互联网企业，以及阿里巴巴、百度、腾讯等国内互联网企业都已开始布局人工智能领域，并积极推动人工智能与智慧城市、交通、医疗、教育等领域的融合。

网络安全领域也已开始探索与人工智能相结合的可能性，主要体现为利用机器学习、深度学习等人工智能技术分析处理安全大数据，以改善安全防御体系，应对 0 day 攻击、位置威胁等安全问题。例如，中兴推出了基于机器学习的未知威胁检测平台，通过学习人工判定逻辑、深度学习流量处理、挖掘关联关系等方式，发现海量数据中的可疑痕迹，并对复杂威胁行为做出自动判定；悬镜安全实验室推出了基于机器学习的威胁语句检测引擎，其利用云端的威胁大数据进行自我

训练与知识迭代，实现对 SQL 注入、XSS 攻击和 WebShell 的检测。

整体来看，网络安全技术与人工智能相结合是未来发展趋势，但目前产品化成果较少，智能化程度还有待提高。未来可以在智能分析算法方面进行改善，提高数据分析的实时性和准确性，增强产品智能化程度。

五、我国网络安全产业前景展望

（一）安全理念革新有望塑造产业新价值

“合规需求”驱动了过去十余年安全建设和安全产业发展，但应当看到，完全遵循“合规原则”容易造成安全投入的不持续、手段落实效果的不理想，导致安全能力建设滞后形势发展、技术创新缺乏活力、产业低价竞争等现实问题。习总书记指出，网络安全是整体的、动态的、开放的、相对的、共同的，提出了网络安全新理念。网络安全攻防博弈对抗的本质，要求在合规基础上，更为动态、综合的防御理念和能力。随着网络安全观的重建，一方面，企业网络安全需求将超越“合规”而更趋于贴合实际，需求更多样、更灵活，有助于打破“合规市场”的增长瓶颈，进一步打开安全市场空间；另一方面，安全产品和服务的实效也将逐步受到重视，创新技术和服务得到认可，进一步增强产业活力，提升技术价值。

（二）万物互联下安全保障需求将不断催生安全新范式

随着数字浪潮推动生产生活的各领域逐渐向数字化、网联化和智能化转型，终端和智能设备的泛在互联逐渐瓦解传统安全边界，工业互联网正演变为数字经济和实体经济发展转型的基础设施。未来，随

着软件定义安全逐渐走向主流，依靠虚拟化、人工智能、边缘计算等变革性技术打造全新安全生态和核心安全技术能力将成为大势所趋，构建解决保密、信任、隐私等固有安全问题的新范式，真正实现网络安全与物理安全的深度融合。

（三）网络安全技术产品服务化转型趋势日益凸显

长期以来，安全服务作为安全产品的附赠品、附加品，其重要性及价值往往被严重低估。但随着云计算技术的普及应用，云安全能力日益受到重视，并逐渐成为衡量和选择云服务商的重要因素，云火墙、云审计、DDoS 攻击防御等云安全服务快速发展，网络安全服务的价值逐步得到认可，基于自动化、远程化、智能化的威胁监测、威胁情报等新兴服务服务模式逐步试点应用。网络形态的转变，倒逼着安全产品加速向服务形态转型，步入软件定义的时代，也将催生更加繁荣的安全服务市场。

（四）产业政策红利持续释放，助力产业快速成长

一方面，《网络安全法》的出台实施，特别是对于关键信息基础设施实施重点保护的要求，将进一步拉动网络安全产业内需增长。网络安全投入与网络安全保障需求密切相关，电信、能源、金融、政府等关键信息基础设施领域，承载大量关系国计民生的信息系统和网络数据，是网络安全工作的重中之重，也将是未来网络安全投入力度最大、创新安全技术容纳能力最强的领域，将对产业发展起到重要带动作用。另一方面，国家及地方对于安全技术孵化、安全企业培育、安全人才培养力度持续加大，产业环境不断优化，将吸引更多的人才、

资金投入安全产业，为产业发展注入新的活力。

（五）网络安全“国际化”将以更大力度在更大范围和深度开展

从近几年趋势看，我国网络安全企业日益活跃在国际舞台。国内企业在国际安全盛会参展数量和规模不断增加，在国际安全竞赛、国际安全标准制定中持续发力，奇虎 360、山石网科、安天、深信服等 8 家企业入围 2017 年国际网络安全 500 强榜单[10]，较 2015 年增加 100%，网络安全领域的中国声音日渐响亮。未来，随着安全新威胁、新挑战的演变，国内企业将更为积极地融入国际安全圈，引进先进理念，获取威胁情报，开展投资布局，加深合作交流，在技术、人才、市场等的竞争博弈中不断提高影响力和竞争力。

[10]来源：Cybersecurity Ventures, Cybersecurity 500,2017Q2

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