版权声明

本报告的著作权归工业信息安全产业发展联盟（以下简称“工信安联盟”）所有，并受法律保护。转载、摘编或利用其它方式使用白皮书文字或观点的，应注明“来源：工业信息安全产业发展联盟”。违反上述声明者，工信安联盟保留追究其相关法律责任。

欢迎各界就本报告的内容和观点与我们交流探讨，您可通过电话、传真、电子邮件方式与我们联系。

工业信息

前言

当前全球正处于新一轮科技革命和产业变革的历史交汇期，以大数据、云计算、人工智能为代表的新一代信息技术与实体经济深度融合，工业经济向数字化网络化智能化拓展。习近平总书记强调，没有网络安全就没有国家安全。工业信息安全作为网络空间安全的重要组成部分，事关工业生产运行、国家经济安全和人民生命财产安全，是国家安全的重要领域。

强有力的工业信息安全保障，[illegible]。近年来，工业信息安全事件频发和国家级网络[illegible]的态势引发各界高度关注。各国政府在政策和资金层面持续加码，关键基础设施领域安全投入[illegible]信息安全产业结构加快调整，产业规模呈快速上升态势。2018 年以来，我国工业信息安全产业持续快速增长，产品体系日益完善，涌现出一批成长性高、创新能力强的企业。据工业信息安全产业发展联盟的统计与调研结果显示，2018 年，我国工业信息安全产业规模为 70.32 亿元，市场增长率达 33.55%，工业信息安全产业规模[illegible]。

继《中国工业信息安全产业发展白皮书（2017）》，国家工业信息安全发展研究中心深耕产业研究，再度携手启明星辰、奇安信、天融信、安恒信息、恒安嘉新、成都卫士、格尔

目录

前言 1

目录 3

一、工业信息安全产业发展概述 5

（一）工业信息安全的再认识 5

（二）工业信息[illegible]

二、全球工业信息安全产业年度发展概况 8

（一）全球工业信息安全市场总体规模持续扩大 8

（二）全球工业信息安全产业结构更加优化 11

1. 产品类 12

2. 服务类

（三）发达国家政策环境不断向好

1. 美国加强工业信息安全[illegible]防护能力建设 16

2. 欧洲各国加强工业信息安全领域合作 16

3. 以色列工业信息安全产业继续升温

（四）行业和企业用户安全投入意愿显著提[illegible]

1. 重点行业强化产业投[illegible]局 18

2. 用户安全需求呈多样化趋势

（五）全球工业信息安全投[illegible]资市场表现活跃 21

三、我国工业信息安全[illegible]

（一）我国工业信息安全政策环境利好突出 24

（二）我国工业信息安全产业规模持续高速增长 27
（三）我国工业信息安全产业结构日趋优化 29
（四）我国工业信息安全行业投入力度加大 30
（五）我国工业信息安全技术攻关和产业化应用仍不成熟 34
（六）多地加快工业信息安全产业布局 38
（七）我国工业信息安全市场竞争加剧 38
四、我国工业信息安全产业发展面临的挑战 42
五、我国工业信息安全产业发展趋势展望

工业信息安全产业发展联盟

一、工业信息安全产业发展概述

（一）工业信息安全的再认识

工业是国民经济的主体和建设现代化经济体系的主要着力点，工业竞争力是国家竞争力的重要体现。随着德国“工业 4.0”、美国“再工业化”先进制造”、我国“制造强国”、“网络强国”等国家战略的推出，以及云计算、大数据、物联网等新一代信息[illegible]网络化、智能化方向发展。新一轮产业变革为经济转型带来新机遇的同时，也加速了网络安全风险向工业领域全面渗透，工业信息安全问题日益凸显。

从内容来看，工业信息安全泛指工业生产运行过程中的信息安全，涉及工业领域各个环节，[illegible]工业自动化、信息化、网络化、智能化等基础设施的安全。

从保障对象上看，工业信息安全[illegible]（如工业控制系统）、工业互联网平台（包括承载平台运行的工业云以及应用服务）、工业网络基础设施（包括基础电信网络、解析网络和其它接入网络）、工业数据等的安全。因此，工业信息安全不仅涉及传统计算机网络和信息系统安全，还涉及工业软硬件设备、控制系统、[illegible]的安全。

从工业信息安全的发展路径来看，[illegible]自动化阶段，生产环境相对封闭，工业信息安全作为网络安

全的细分应用方向，主要集中在工业企业信息管理层的安全。近年来，工业企业逐渐[redacted]（以下简称“工控系统”）和生产设备的网络[redacted]工业信息安全的重点在于工控安全。当前，两化融合进程加速由数字化向网络化过渡，互联网快速渗透到工业领域的各个环节，工业实体逐步趋向泛在互联，工业互联网安全逐渐成为工业信息安全的焦点和核心。工业信息安全从面向企业端的传统信息安全、工控安全逐步延伸至工业互联网设备安全、控制安全、网络安全、平台安全、数据安全等领域。

（二）工业信息安全产业的界定

习[redacted]工作会议上明确提出，“加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然”。在工业互联网快速发展的大背景下，新一代信息技术在工业生产领域广泛渗透和深度融合，不断升级的安全机制对新时期的工业信息安全产业发展提出了更高、更新的要求。

工业信息安全产业[redacted]的初期阶段以工控安全为核心，以纵深防御的技术理念为基础，涌现出大量围绕工控系统的“外建”安全防护产品和解决方案。随着工业互联网的加速推进，传统工业现场相对封闭可信的制造环境和强调高可靠性的格局逐渐被打破，工控系统、工业联网智能设备、工业

互联网平台等自身的安全问题不容小觑，内嵌信息安全功能的产品和服务市场需求激增，[redacted]应以提升企业工业信息安全综合防护水平为目标，统筹考虑内嵌安全和外建安全的市场需求（图 1.1）。

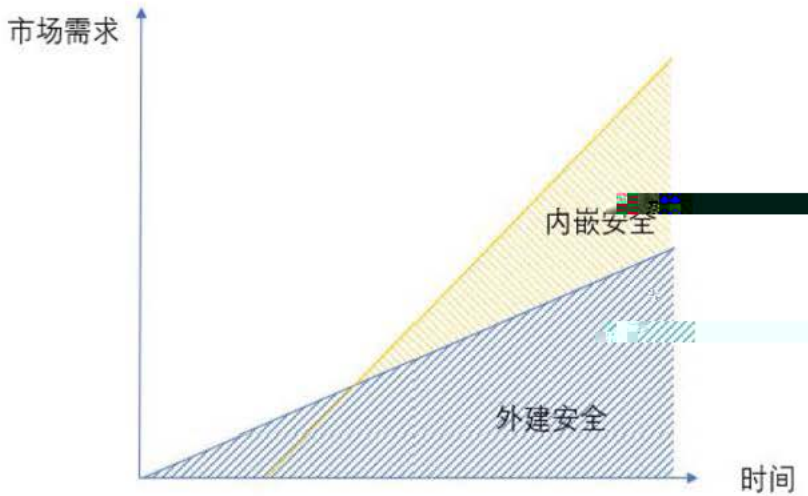

图 1.1 工业信息安全[redacted]

资料来源：工业信息安全产业发展联盟综合分析

当前，国内外缺乏对工业信息安全产业的[redacted]相关数据的统计口径也尚未建立。结合工业信息安全的内涵，工业信息安全产业可以定义为从事工业生产、运行、管理过程中的安全技术[redacted]务的经济活动。

二、全球工业信息安全产业年度发展概况

近年来，全球以大数据、云计算、物联网、移动互联网和人工智能等为代表的新一代信息技术(IT)与运营技术(OT，Operational Technology)加速融合，工业信息系统愈加开放互联，工业信息安全威胁也日趋严峻。关键基础设施领域工业信息安全事件频发、国家级网络空间博弈不断升级、多国政府政策和资金层面的持续加码以及工业企业用户意识的显著提升等因素，驱动了全球工业信息安全市场的快速发展。

（一）全球工业信息安全市场总体规模持续扩大

据市场研究公司[illegible]2018 年全球工业信息安全市场规模达 150.2 亿美元，预计到 2026 年增长至 299.7 亿美元，年复合增长率达 9.02%。国际知名咨询公司[illegible]中心的 OT 安全作为独立细分市场，并对其市场规模进行预测。据 Gartner 的数据显示，2018 年全球 OT 安全支出为 2.5 亿美元，预计到 2022 年将增长[illegible]45.7%（图 2.1）。



图 2.1 OT 安全年支出预测和增长率（百万美元）

数据来源：Gartner 公司，工业信息安全产业发展联盟综合分析

从区域分布来看，据 Transparency Market Research 公司预测，2018 年北美地区仍保持全球市场领先地位，工业信息安全市场规模达 58 亿美元。另据工业咨询公司 ARC 预测，到 2022 年，欧洲、中东和非洲地区工业信息安全市场将进一步扩大，年复合增长率达 13.7%，北美和亚洲地区工业信息安全市场增势强劲，年复合增长率分别为 15.9 和 14.7%（图 2.2）。在工控安全领域，随着针对工业控制系统网络攻击事件的激增，全球工控安全市场需求显著提升。据市场研究公司 Markets and Markets 预测，在政策和市场的双重驱动下，2018 年北美地区工控安全市场规模继续走高，占据 50%以上的全球市场份额，受地缘政治等因素影响，未来四年，中东地区工控安全市场增速最快，年复合增长率接近 30%。

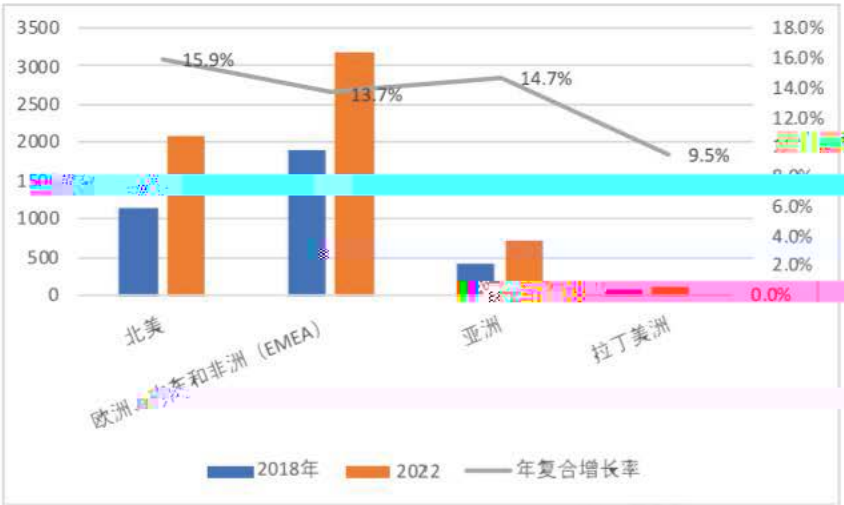

图 2.2 全球主要地区工业信息安全市场情况（2018-2022）

数据来源：ARC 公司，工业信息安全产业发展联盟综合分析

从行业应用来看，ARC 公司数据表明（图 2.3），2018 年，电力、石油天然气和化工行业的工业信息安全市场仍处于领先地位，各整体市场规模约 40%。其中，《大型电力系统的网络安全标准》（NERC-CIP）等合规标准将继续推动电力行业工业信息安全应用快速增长，年复合增长率达 15.94%。水处理行业作为关键基础设施的重要行业，2018 年在工业信息安全领域的投入明显加快，年复合增长率达 15.21%。受经济因素影响，以汽车制造为代表的离散型工业信息安全应用相对较少，年复合增长率为 7.99%。另据 Global Market Insights 公司预测，随着用户意识的提升，公路、地面运输、航空、海运等关键基础设施行业的工业信息安全应用预计将在未来五年呈现强劲增长，年复合增长率达 26%。

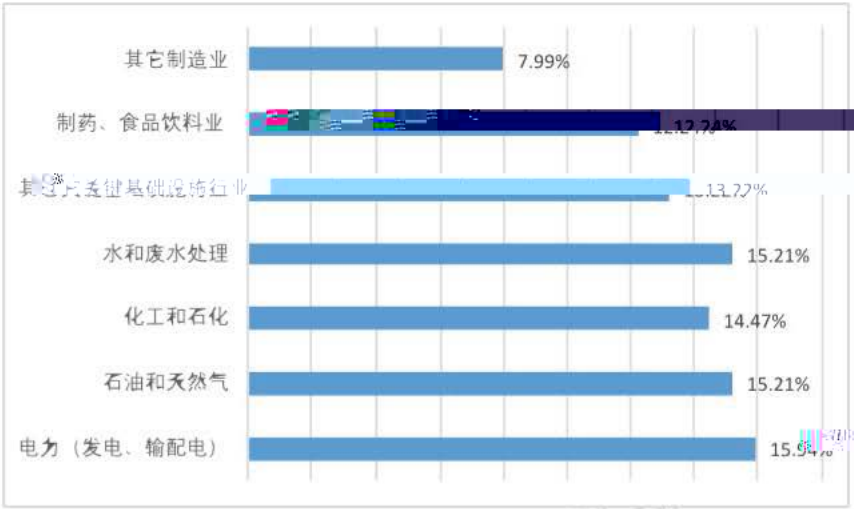

图 2.3 各行业工业信息安全投入年复合增长率（2018-2022）

数据来源：ARC 公司，工业信息安全产业发展联盟综合分析

从产品分布来看，2018 年终端安全市场领跑全球工业信息安全市场，市场份额达 40%；以工业防火墙为代表的网络安全[illegible]增速加快，未来五年的年复合增长率将达 26%；由于网络安全问题日趋复杂，工业企业用户对安全托管、集成和咨询等安全服务需求增加，推动全球工业信息安全服务市场快速增长，预计未来五年内年复合增长率约为 35%。

（二）全球工业信息安全产业结构更加优化

据《中国工业信息安全产业发展白皮书（2017）》，工业信息安全产业依据市场应用分为产品和服务两大类（图 2.4）。

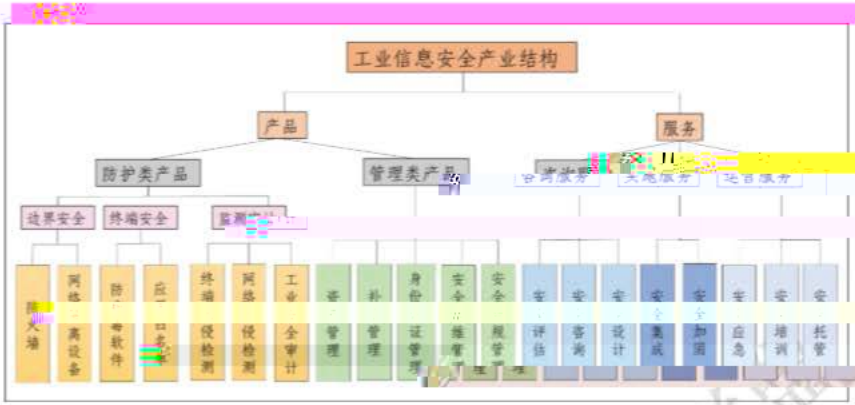

图 2.4 工业信息安全产业结构

资料来源：

随着全球工业信息安全风险意识逐渐增强，以及各国政府监管规定的日益完善，2018 年全球工业信息安全产品市场规模持续扩大，服务市场增速加快，[illegible]和市场结构进一步完善。

1. 产品类

工业信息安全防护类产品市场主要包括边界安全产品、终端安全产品及监测审计类产品。据 ARC 统计，边界安全产品市场规模在未来四年仍将占据市场主导地位，该类产品市场应用在 2018 年达 12.72 亿美元，预计到 2022 年将增长至 20.13 亿美元，年复合增长率达 12%。工业企业边界防护和网络分区意识的增强、对传统网络安全产品接受度的提升是该市场应用增长的主要驱动力。终端安全防护类产品市场规模在 2018 年为 4.6 亿美元，到 2022 年将增长至 7.11 亿美元，年复合增长率为 11.4%。2018 年，监测审计类产品市场

规模为 7700 万美元，但该细分市场在未来四年将是增速最快的防护类产品市场，增速预计

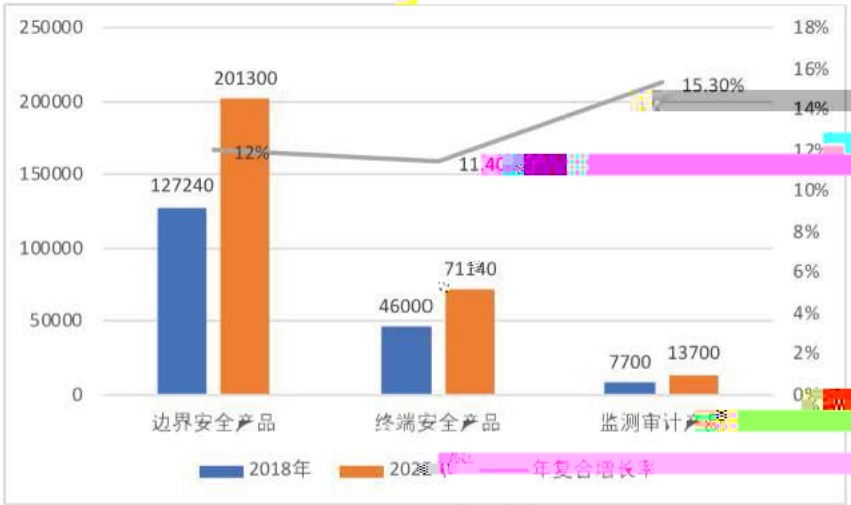

图 2.5 2018 年-2022 年全球工业信息安全市场防护类产品市场规模及增长情况

数据来源：ARC 公司，工业信息安全产业发展联盟综合分析

工业信息安全管理类产品结合传统 IT 信息安全管理产品和解决方案，同时从安全策略和管理流程的角度，对可能影响工业生产环境（如自动重启或中断网络通信）的功能模块进行了改造。ARC 指出（图 2.6），全球工业信息安全管理类产品市场将从 2018 年的 3.43 亿美元增至 2022 年的 6.05 亿美元，年复合增长率达 15%。其中，合规管理是推动管理类产品市场规模不断扩大的主要动力，到 2022 年增速达 23.1%。资产管理和身份认证管理也是[redacted]重点，年复合增长率达 15%以上。

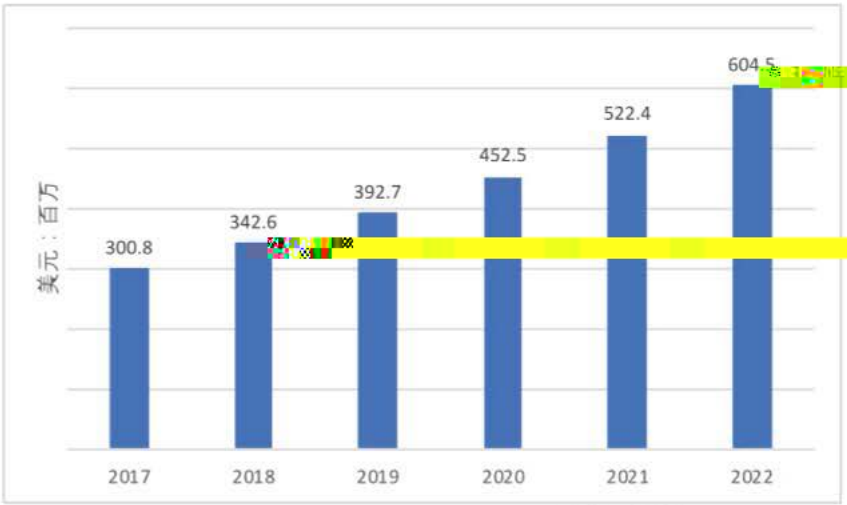

图 2-6 2017-2022 年全球工业信息安全管理类

数据来源：ARC 公司，工业信息安全产业发展研究综合分析

2. 服务类

由于工业信息安全专业人才的短缺和安全态势的复杂性，购买第三方安全服务成为工业企业解决工业信息安全问题的重要手段之一。根据 ARC 的报告，工业信息安全服务市场将从 2018 年的 14 亿美元增长至 2020 年的 26.28 亿美元，年复合增长率达 17.2%。

工业信息安全咨询服务包括安全评估、安全咨询和安全设计等。2018 年，咨询服务在服务类市场中仍处于领先地位，是拉动整体服务类市场增长的重要引擎。在电力、能源等行业中，监管合规需求推动工业企业用户选择安全评估服务；在监管规定相对较少的行业，企业根据自身风险评估需求来选择咨询服务。据 ARC 统计，2018 年全球工业信息安全评

估和咨询服务市场规模达 8.30 亿美元，预计到 2022 年将增长至 14.91 亿美元，年复合增长率为 16.2%。

工业信息安全实施服务通常包括执行企[redacted]制定的工业信息安全策略[redacted]火墙、白名单工具等。实施服务主要包括两种类型：一是在现有系统内实施相应的[redacted]安全防御策略；二是对新系统实施安全规划和配置。据 ARC 统计，全球工业信息安全[redacted]市场规模在 2018 年达 3.24 亿[redacted]亿美元，年复合增长率为 16.5%。

工业信息安全运营服务主要包括安全应急、安全培训和安全托管。其中，由于专业人员短缺和流程复杂，2018 年全球工业信息安全托管服务市场规模达 2.47 亿元，并在未来四年服务类市场中增速最快，到 2022 年将增长至 5.38 亿元，年复合增长率达 21.3%。安全应急类和安全培训类服务市场目前整体规模较小，这主要是由于工业信息安全厂商将安全运营服务与管理类产品进行了整合。

（三）发达国家政策环境[redacted]

近年来，工业信息安全事件频发，引起全球对工业信息安全领域的高度关注，各国政府纷纷加快工业信息[redacted]制定步伐，并[redacted]加相关资金投入。

1. 美国加强工业信息安全综合防护能力建设

随着地缘政治冲突蔓延至网络空间，工业等关键基础设施领域已成为网络安全攻防对抗的“主战场”。2018 年 3 月，特朗普政府首次公开[illegible]俄罗斯政府支持的黑客团体针对美国能源、核电站、水处理、制造业等多个关键基础设施部门的控制系统发起网络攻击。

2018 年，美国政府多措并举加快了工业信息安全领域综合防护能力建设。6 月，美国众议院通过了 DHS 的《工业控制系统能力提升法案》（HR 5733 法案），该法案明确提出加强保障工控安全，特别是加强关键基础设施领域工控系统抵御网络攻击的能力。11 月，众议院通过了《网络安全和基础设施安全局（CISA）法案》，正式将 DHS 的国家保护和计划局（NPPD）重组为网络安全和基础设施安全局（CISA），负责网络和关键基础设施安全。

2. 欧洲各国加强工业信息安全领域合作

自 2016 年 8 月首部欧盟网络安全法“《网络与信息安全指令》（以下简称《指令》）正式生效以来，英国、德国、法国等欧盟成员国积极落实《指令》，分别制定国家网络安全战略，加强对关键信息基础设施的保护力度，并在工业信息安全技术研发方面加大资金投入与支持力度。2018 年 12 月，欧盟网络与信息安全局（ENISA）被正式授权为欧盟网络安

全局，支撑欧盟成员国应对网络安全威胁和攻击。

《指令》还进一步提出建立纵贯“成[illegible]”的多层合作体系，加强成员国间的合作以及国际合作。2018年6月，立陶宛、克罗地亚、爱沙尼亚、荷兰、罗马尼亚、西班牙六国签署《意向声[illegible]》，将建立“永久[illegible]”防务机制，共同应对网络攻击。2018年4月，北约连续第十年举办大规模[illegible]，进一步强调工业领域的安全防护，[illegible]人机和净水厂等多个用于演习的关键基础设施场景。

3. 以色列工业信息安全产业[illegible]

以色列近年来快速发展网络安全产业，目前已跻身全球领先的网络安全强国。2016年1月，以色列政府将国家网络局和国家网络安全局合并，成立国家网络指挥中心，并提出增加国家网络安全预算。3月，以色列创新局、经济产业部和国家网络指挥中心宣布了新一轮为期三年、总投入2,400万美元的网络安全产业[illegible]。目前，以色列拥有网络安全公司420家，其中，约三分之一的网络安全公司专注于工业信息安全和工业互[illegible]安全领域。

（四）行业和企业用户安全投入意愿显著提高

1. 重点行业强化产业投入

近年来，工业信息安全事件因其影响范围广、潜在损害巨大已经引起了全球工业领域各行业和企业用户的广泛重视。据弗若斯特沙利文公司（Frost&Sullivan）统计，2018年，仅能源和公用事业行业的网络攻击造成的经济损失就达1320万美元。

能源领域，作为工业网络攻击的重灾区，在近年来已成为美国各安全主管部门的关注焦点。西门子与波耐蒙研究院（Ponemon Institute）的调研结果显示，2018年，68%的美国石油天然气公司和75%的中东石油天然气公司表示至少在过去一年中经历过网络攻击或威胁，导致关键信息丢失或运营中断。2018年2月，美国能源部宣布成立网络安全、能源安全和应急响应办公室（CESER），加强对能源领域关键基础设施的保护。5月，为降低工业信息安全风险，能源部发布了《能源行业网络安全多年计划》，明确了能源部未来五年的目标和相应措施。此外，能源部还加大了对工业信息安全技术研究和开发的资金支持力度，陆续投入2500万和2800万美元用于电力、石油和天然气等下属部门的网络弹性、隐蔽、网络安全创新工具和威胁防御及检测技术的开发。

近年来，海运、航空、地面运输、管道等交通运输领域工业信息安全意识逐步增强。以海运为例，港口[illegible]用大量的控制系统确保作业顺利运行，即便不是主要攻击目标，网络攻击从IT扩散到OT环境也会造成严重的损害。2017年以来，海运巨头马士基（Maersk）集团、中远海运集团相继遭遇勒索软件和网络攻击事件[illegible]际海事组织（IMO）、波罗的海国际[illegible]（BIMCO）、国际邮轮协会（CLIA）、挪威船级社（DNV-GL）等行业组织都陆续发布了各自的船上网络安全指南，[illegible]系统信息安全的保障。

2. 用户安全需求呈多样化趋势

合规需求长期以来是全球工业企业加大对工业信息安全投入的主要驱动力，但随着联网设备的指数级增长以及安全事件对企业的影响不断加深，工业信息安全已逐渐成为工业企业用户的重要内生需求。SANS的调查报告显示（表2.1），数据安全防护、设备和系统安全防护[illegible]动全球工业企业采取安全措施的最主要因素。此外，以来[illegible]规、增强工业生产运行的可靠性和可用性也是工业信息安全需求增长的主要动力。

表 2.1 2018 年企业工业信息安全需求动因

排名	需求动因	需求关注度

工业信息安全产业发展联盟

1	数据安全防护	4[illegible]2%
2	设备和系统安全防护	40.5%
2	避免财务[illegible]	[illegible]
4	行业监管合规性	36%
4	增强工业生产运行的可靠性、可用性、效率和生产力	36%
6	生产环境内部安全性	33.7%
7	IT 和[illegible]融合协同的实践	23.6%
8	降低企业责任/提高企业风险管[illegible]	[illegible]
9	生产环境外部安全性	15.7%
10	降低上下[illegible]供应链风险	[illegible]9%

数据来源：SANS 公司，工业信息安全产业发展联盟综合[illegible]

多样化的安全需求[illegible]领域的投入。飞塔（Forti[illegible]2018 年，近四分之三的工业企业增加了物联网设备的安全支出，其中 36%的企业计划增加 5%以上；有 71%的企业表示在 OT 安全方面增加安[illegible]工控安全领域是企业工业信息安全投入的重点，有 77%的企业表示提高安全支出，接近半数的工业企业[illegible]5%的安全投入[illegible]

工业信息安全产业发展联盟

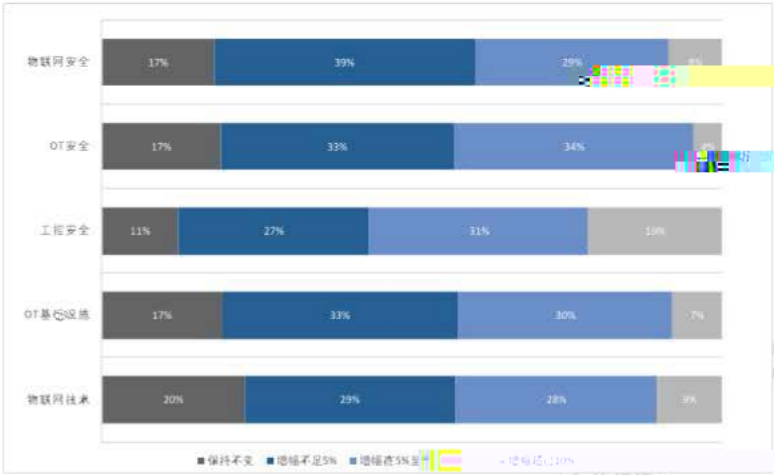

图 2.7 2018 年度企业工业信息安全预算（按供应商类型）

数据来源：飞塔（Fortinet）公司，工业信息安全产业发展联盟综合分析

（五）全球工业信息安全投融资市场表现活跃

随着全球工业信息安全市场增速加快，不同背景的工业信息安全厂商携 OT 安全专用产品或具有更多功能的信息安全产品和服务流入市场。2018 年，工业信息安全产业进业中游企业加快资本整合和战略合作，少数专注工业信息安全领域的初创企业融资额已颇具规模。

CB Insights 的数据显示，工业信息安全领域的主要融资总额已经从 2010 年的 500 万美元增长至 2017 年的近 7 亿美元。2018 年，在这工业信息安全领域的初创企业融资市场中场青睐（表 2.2），以各种工业信息安全初[illegible]共有[illegible]马锡、罗克[illegible]

问鼎 2018 年工业信息安全初创企业融资榜首。美国工业信息安全企业 Dragos 和 Nozomi Networks 发展势头良好，连续两年融资成功[redacted]，艾默生、美国[redacted]合投资的 3700 万美元。

此外，成立近 10 年的美国工业信息安全企业 Security Matters，被 2017 年在纳斯达克上市的物联网安全公司以 1.13 亿美元收购，这是近年来工业信息安全领域成交金额最大的收购案。

表 2.2 2018 年工业信息安全市场企业融资情况

序号	时间	厂商	融资额（万美元）	融资阶段	国家
1	2018 年 1 月	Cylus	470	种子轮	以色列
2	2018 年 2 月	Cyber X	1800	B 轮	以色列
3	2018 年 6 月	Cyberbit	3000	A 轮	以色列
4	2018 年 6 月	Claroty	6000	B 轮	以色列
5	2018 年 7 月	Radiflow	1800	A 轮	以色列
6	2018 年 8 月	iS5Communications	1700	A 轮	加拿大

7	2018 年 8 月	Inde[illegible]	1800	B 轮	以色列
8	2018 年 9 月	Nozomi Networks	3000	C 轮	美国
9	2018 年 11 月	Security Matters	1[illegible]30	收购	美国
10	2018 年 11 月	Dragos	3700	B 轮	美国
11	2018 年 12 月	Sentryo	1130	A 轮	法国

数据来源：工业信息安全产业发展联盟[illegible]

工业信息安全产业发展联盟

三、我国工业信息安全产业年度发展概况

近年来，我国工业信息安全产业政策环境持续向好，产业规模快速增长，产业结构逐渐优化，技术体系日益完善，行业和地方加速助力，涌现出一批成长性高、[illegible]新能力强的企业。

（一）我国工业信息安全政策环境利好突出

1. 中央政策持续加码

党的十九大以来，国家[illegible]国和网络强国上升为国家战略。为保障“两个强国”战略顺利实施，加强[illegible]系，党中央、国务院陆续出台了一系列政策，为我国工业信息安全发展提供了良好的产业环境。

2017 年 11 月，国务院颁布《关于深化“[illegible]联网[illegible]先进制造业”发展工业互联网的指导意见》（以下简称《指导意见》），拉开了我国工业互联网建设的序幕。《指导意见》明确提出“建立工业互联网[illegible]展目标，将强化安全保障作为主要任务之一，并为工业互联网安全保障工作制定了时间表和路线图。2017 年[illegible]工业和信息化部发布了《工业控制系统信息安全行动计划（2018-2020）》，突出落实企业主体责任，明确提出建立“一网一库三平台”的主要目标，部署五大能力提升行动，为下

一步工业信息安全工作提供依据和指导。

2018 年 2 月，国家[illegible]网专项工作组，加码工业互联网战略部署。5 月，工业和信息化部组织对 30 多家工业企业、平台企业及工业 APP 研发企业开展 2018 年工业互联网安全检查评估，[illegible]自身安全建设。

6 月，工业和信息化部印发《工业互联网发展行动计划(2018-2020 年)》（以下简称《行动计划》）、《工业互联网专项工作组 2018 年工作计划》。《行动计划》提出，到 2020 年底我国将实现“初步建成工业互联网基础设施和产业体系”的发展目标。同期，工业和信息化部联合财政部组织开展了 2018 年工业互联网创新发展工程，安全方向遴选出了 29 个项目落地实施，支持企业单位开展综合保障、监测和态势感知、应急协作指挥、数据安全防护、测试验证环境等建设。

9 月，工业和信息化部组织开展 2018 年工业互联网试点示范项目推荐，经过企业自主申报、地方推荐、专家评审、现场核查和网上公示等环节，于 12 月公布了《2018 年工业互联网试点示范项目名单》。其中，安全集成创新应用作为工业互联网试点示范的主要方向，共有 8 个项目入选，体现了国家着力提升工业互联网安全防护水平的决心。

2、标准研制稳步推进

近年来，我国标准化组织围绕工控安全陆续研制、发布[illegible]

了系列标准。随着工业互联网安全建设的落地，工业互联网安全相关标准研制工作积极稳步推进，工业信息安全技术标准体系逐步形成（表 3.1）。

表 3.1 我国工业控制系统信息安全标准体系工作开展情况

标准体系分类	标准状态	标准名称
安全等级	已发布	《信息安全技术 工业控制系统信息安全分级指南》
	已发布	《信息安全技术 工业控制系统信息安全分级指南》
安全要求	已发布	《信息安全技术 工业控制系统安全管理基本要求》
		《信息安全技术 工业控制系统现场测控设备通用安全功能要求》
	正在批准	《信息安全技术 工业控制系统增强级产品技术要求及测试评价方法》
		《信息安全技术 工业控制网络监测安全技术要求及测试评价方法》
		《信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求》
		《信息安全技术 工业控制系统网络审计产品安全技术要求》
	制定中	《云制造服务平台安全防护要求》
		《工业互联网平台 安全防护要求》

工业信息安全产业发展联盟

		《信息安全技术 工业互联网平台安全要求及评估规范》
	待制定	《工[redacted]》
		《工业互联网 安全防护检测要求》
安全实施	已发布	《信息安全技术 工业控制系统安全控制应用指南》
		《信息安全技术 工业控制系统风险评估实施指南》
安全测评	已发布	《工业控制系统信息安全 第1部分：评估规范》
		《工业控制系统信息安全 第2部分：验收规范》
	正在批准	《信息安全技术 工业控制系统安全检查指南》
	起草中	《信息安全技术 工业控制系统信息安全防护技术要求与测试评价方法》
		《信息安全技术 工业控制系统信息安全防护能力评价方法》
	待制定	《工业互联网平台 安全风险评估规范》
		《工业互联网平台 安全防护能力评估规范》

（二）我国工业信息安全产业规模持续高速增长

当前，国内外缺乏对工业信息安全产业的权威统计，产业相关数据的统计口径也尚未建立。工业信息安全产业发展联盟依托对国内外工业信息安全产业长期的跟踪调研，在本次白皮书中对我国工业信息安全产业规模的[redacted]

了调整，涵盖工业领域 IT 安全、OT 安全、IT/OT 融合安全，同时还包括含有内嵌信息安全功能的工业自动化、信息化和网络基础设施等。

工业信息安全产业发展联盟对国内典型工业信息安全厂商 2018 年业绩进行了调研，结合国内工业信息安全市场公开招标情况、企业年报、其他相关产业报告等材料，对我国工业信息安全产业进行综合分析和预测，报工业信息安全产业发展联盟的统计与调研结果显示（图 3.1），2018 年我国工业信息安全产业规模为 70.32 亿元，市场增长率达 33.55%。



图 3.1 2016 至 2020 年我国工业信息安全市场规模

数据来源：工业信息安全产业发展联盟

“十三五”以来，国家高度重视工业信息安全顶层设计，强化工业信息安全[illegible]，提升工业信息安全保障技术能力，为工业信息安全产业发展

全面提速奠定了良好的基础。2018 年，国家在工业信息安全领域持续发力，行业具体安全投入[illegible]工业信息安全产业延续了 2017 年的增长势头，产业规模加速扩容。

随着[illegible]保障将成为工业信息安全工作的前沿与重点，工业企业安全需求将进一步激发，预计 2019 年我国工业信息安全市场增长率将达 19.23%，市场整体规模将增长至 93.91 亿元。其中，工业互联网安全产业规模将从 2018 年的 25.26 亿元增长至 40.79 亿元，市场增长率达 61.48%。

（三）我国工业信息安全产业结构日趋优化

从产业结构[1]来看，我国工业信息安全产业的产品类市场和服务类市场发展均较为迅猛。2018 年，我国工业信息安全产品类市场规模达 16.17 亿元，占市场总额的 64%。其中，工业信息安全防护类产品市场规模达 8.34 亿元，占市场总额的 33%。目前，我国防护类产品仍普遍集中在工业防火墙、工业网闸、应用白名单等边界安全和终端安全产品，该类产品市场的[illegible]

2018 年，我国工业信息安全管理类产品市场规模约为 7.83 亿元，[illegible]全管理类产品主要布局于态势感知、合规管理、安全运维管

[1] 由于工业信息安全产业测算口径发生变化，此处工业信息安全产业仍以工业互联网安全的外建安全产品和服务为主。

理等领域，在国家和行业[illegible]政策的双重推动下，工业企业用户对安全合规的需求加快提升[illegible]大。



图 3.2 2018 年我国工业信息安全产业结构

数据来源：工业信息安全产业发展联盟采集整理

我国工业信息安全服务类市场在2018年迎来爆发，市场规模达 9.03 亿元，占市场总额的36%。其中，安全评估和安全培训是服务类市场增长的主要动力。安全评估主要依据国内外标准和行业监管规范，为工业企业用户评估工控安全风险。随着监管规定和评估体系[illegible]，工业企业安全评估需求逐步明确，市场规模将进一步扩大。安全培训市场需求近年来日趋旺盛，科研院所、高校对工业信息安全人才培养的重视程度[illegible]，带动整体安全培训服务市场[illegible]加快。

（四）我国工业信息安全行业投入力度加大

工业信息化、自动化、网络化、智能化等基础设施是工

业的核心组成部分，被广泛应用于[illegible]设施、钢铁、有色、化工、石油石化、天然气、先进制造、轨道交通、城市供水供热以及其他与国计民生紧密相关的领域。其中（表 3.2），电力、石油石化（含化工、天然气）行业[illegible]度最高、工业信息安全产品应用最广泛的两个行业，烟草、轨道交通、先进制造等重点行业工业信息安全应用案例近年来显著增多，但仍主要集中于工控安全领域。钢铁、有色等其它行业受自身景气度影响，工业信息安全应用较为有限且增长较为缓慢。

表 3.2 我国工业信息安全产品行业应用情况

行业	应用环节	主要产品	主要供应
电力	覆盖电力生产“发、输、变、配、用、调”各环节，重点应用于省级以上调度中心、地县[illegible]发电厂、变电站、配电等	电网：电力专用隔离装置、电力防火墙、单向认证加密终端模块、拨号[illegible]置等 发电：工业防火墙、入侵异常监测、主机加固、[illegible]等	南瑞信通、珠海鸿瑞、北京科东、威努特、[illegible]技、绿盟科技
石油石化	主要应用于勘探生产、炼油化工、天然气与管道等	工业网闸、工业防火墙	石化盈科、中油瑞飞、启明星辰、青岛海天炜业、力控华康、网藤[illegible]、网威
烟草	卷烟厂、商业物流分拣中心、烟叶复烤厂、[illegible]维公司、烟机公司	工业防火墙、工控入侵和异常检测、[illegible]终端安全	[illegible]启明星辰、绿盟科技、威努特

轨道交通	列车自动运行控制系统为核心，包括列车控制信号系统、综合监控系统和自动售检票系统等	工业防火墙、入侵监测与审计、工控主机卫士	启明星辰、奇安信、南瑞信通、[illegible]电申和瑞、威努特
先进制造（军工、装备制造、汽车制造）	数控网络、工业机器人的[illegible]络	工控异常监测、工控运维审计	启明星辰、奇安信、立思辰、威努特、安点科技
其它（钢铁、有色）	冶炼、热处理、铸造、锻造、淬火等环节，涉及烧控制系统、炼钢智能控制系统、生产高炉控制系统等	工业[illegible]墙	[illegible]伟业、力控华康

数据来源：工业信息安全产业发[illegible]整理

2018 年，我[illegible]的变化。地方政府及科研机构在工业信息安全领域的投入较为稳定，2018 年达 1.56 亿元，占市场总额的 6%（图 3.3）。近年来，国家层面密集出台工业信息安全相关政策，引起了地方政府[illegible]高度重视，安全投入持续增[illegible]业互联网创新发展工程的发布实施也激发了科研机构在工业信息安全领域的投入热情。

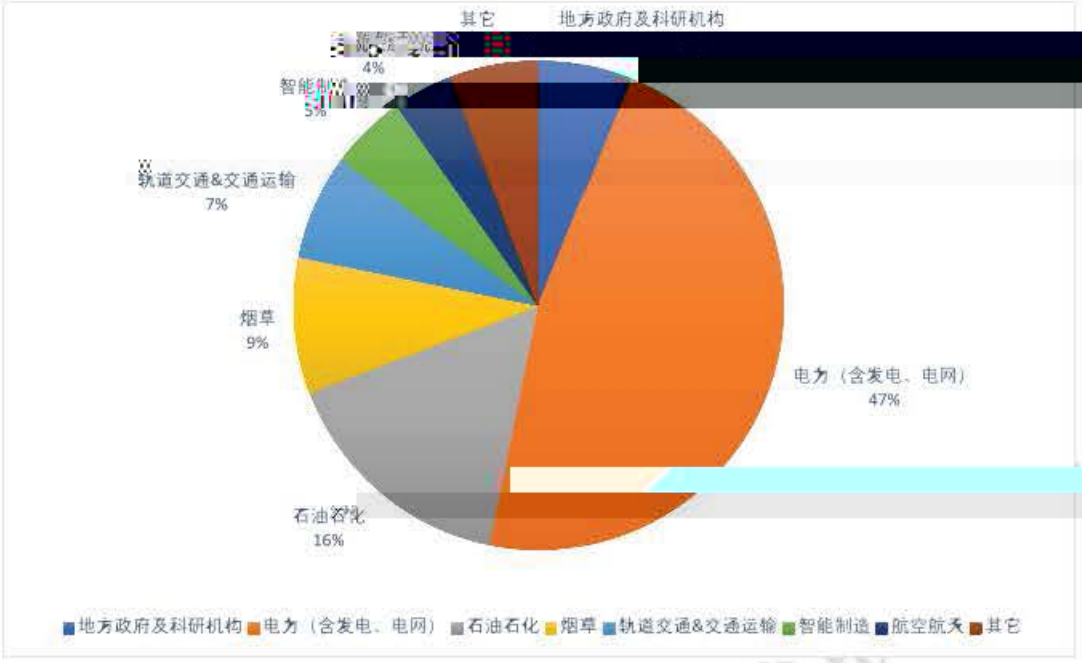

图 3.3 2018 年我国工业信息安全市场

数据来源：工业信息安全产业发展联盟采集整理

电力行业对工业信息安全的投入[illegible]，市场规模达 11.87 亿元，市场占比高达 47%，排名稳居第一位。电力行业在工业信息安全[illegible]，建立了较为完备的电力监控系统安全防护体系，并在自主可控方面[illegible]。2018 年 9 月，国家能源局发布了《[illegible]》，提出加强电力企业数据安全保护，提高网络安全预警及应急处置能力等 5 个方面 16 条意见，进一步推进电力行业工业信息安全产品和应用从基础防护类向管理类演进。

石油石化行业 2018 年工业信息安全市场规模达 4.04 亿元，市场占比 11%，位居第二。相较其他行业，石油石化行业工业信息安全建设较快，用户端对于工业信息安全的防护

理念认同度较高。[illegible]安全产品以防护类产品为主，应用于炼化版块、[illegible]、未油版块、管网输送版块。2018 年，中国石油天然气集团公司加大投入，加强对采油采气、管道运输、炼化生产、油气储运等场景的工业信息安全试验环境建设。

此外，烟草和轨道交通[illegible]增幅明显。以智能制造、航空航天为代表[illegible]2018 年增速较快，但目前市场份额较小。在制造业与互联网深度融合催生的安全需求推动下，预计离散工业领域工业信息安全市场容量将有较为广阔的释放空间。

（五）我国工业信息安全技术攻关和产业化应用仍不成熟

我国工业信息安全技术体系主要包括外建安全和内嵌安全两大类(表 3.3)。其中，**外建安全防护技术体系**主要基于传统 IT 安全防护类、检测类和响应类技术，针对工业生产系统网络、协议、系统的特征开展了适应性改造，但我国工业信息产品在工业场景兼容性、协议支持丰富度、智能化水平和可视化程度等方面与国外先进技术存在一定差距。**内建安全防护技术体系**主要在工业控制系统产品中强化了安全架构设计，集成了加密、身份识别、通信健壮性增强等安全技术，提高了工控产品应对网络攻击的能力，目前该类技术在我[illegible]

表 3.3 我国工业信息安全技术[illegible]体系及现状

	类型	关键技术	技术原理、现状及不足
外建安全防护	防护类	应用程序白名单技术	**技术原理：** 对工业主机等工业终端允许运行的程序、进程、[illegible]名单外的未授权操作。 **技术现状及不足：**[illegible]习的白名单清单构建技术。但[illegible]上的程序、进程的安全性。
		基于策略的访问控制技术	**技术原理：** 通过配置网间允许通信的IP、端口、协议等，避免未授权访问。 **技术现状及不足：** 支持常用工控协议，但生成策略需要人工排查和干预，智能化不足。
		网络隔离技术	**技术原理：** 通过隔离单元摆渡，单向实现网间的数据安全交换，隔离网络攻击。 **技术现状及不足：**[illegible]品，技术较为成熟。但配置变更需要人员干预，运维不便，且实时性不高，支持的通信带宽有限。
		基于深度包解析的防护技术	**技术原理：**[illegible] **技术现状及不足：** 仅支持Modbus、S7等公[illegible]议，对私有协议支持不足，不兼容国产工控产品；[illegible]配置。
		虚拟化安全技术	**技术原理：** 采用合理按需划分虚拟组、控制数据的双[illegible]安全集中管控的方式实现云安全解决方案。 **技术现状及不足：** 虚拟化技术也会带来虚拟机[illegible]无法交流、用户间的攻击、虚拟机和物理主机的共享漏洞、物理主机存在安全问题导致其所有虚拟机都可能存在安全问题。
	检测类	基于指纹匹配的资产识别技术	**技术原理：**[illegible]工业资产的独有特征。 **技术现状及不足：**[illegible]动识别需要合理设置扫描速率和识别方式，避免对生产网络造成影响。

		基于漏洞库的风险关联技术	**技术原理：**通过工业资产与漏洞库比对，关联资产风险。 **技术现状及不足：**大部分工业资产的版本细节信息难以主动获取，仅能实现粗粒度比对；难以开展漏洞利用测试。
		恶意代码检测技术	**技术原理：**可通过人工及[illegible]分析手段提取恶意代码特征，亦可通过沙箱运行分析可疑行为，弥补基于静态特征检测[illegible]未知恶意代码检测能力的不足。 **技术现状及不足：**基于规则的检测技术误报率高，对于未知恶意代码无法检测；基于动态沙箱的检测技术效率较低，且[illegible]中反沙箱技术。
		工业威胁诱捕技术	**技术原理：**工业威胁诱捕技术是一种基于应用蜜罐、虚拟系统、虚拟网络等多种方式的主动、积极、欺骗性质的网络安全检测技术。 **技术现状及不足：**工业威胁诱捕技术难以针对工业控设备、工控协议进行高[illegible]协议仿真技术无法解决工控协议、服务私有化程度高的问题；同时通过交互代理的诱捕方式难以仿真具备大量终端设备的复杂工业内网环境。
		工业网络流量检测技术	**技术原理：**针对工业生产网络中的过程流量进行解析、[illegible]发现恶意代[illegible]为等。 **技术现状及不足：**[illegible]工控安全威胁检测模型相对简单，可视化技术缺乏。
	响应类	威胁溯源技术	**技术原理：**通过网络检测或APT检测技术从网络层面、行为层面分析威胁[illegible] **技术现状及不足：**VPN、代理、暗网等网络身份隐藏技术泛滥[illegible]析出威胁源头。
内嵌安全防护		通信和数据加密	**技术原理：**通过密码算法及芯片，对关键通信数据和链路建立加密通信数据通道。 **技术现状及不足：**已实现基[illegible]法的轻量级加密，但高实时性的加密应用仍然缺乏。
		身份识别技术	**技术原理：**通过固件签名或标识等身份标识技术实现工控产品可信赖组件的安全接入识别和认证。 **技术现状及不足：**仅在少量国产PLC中应用。
		通信访问控制技术	**技术原理：**对通信协议深度解析与还[illegible]应用层关键字[illegible]信息，实现细粒度的访问控制

		能力。 **技术现状及不足：**处于研究阶段，尚无应用。
	网络通信健壮性增强技术	**技术原理：**基于协议校验技术优化、软件资源增强，提[illegible]等网络威胁的防护能力。 **技术现状及不足：**仅少数几款国产工控产品通[illegible]

资料来源：工[illegible]信息[illegible]业发展联盟采集整理

在外建安全防护方面，我国在网络隔离、应用程序白名单等防护类技术成熟度较高，市场应用水平也较高(图 3.4)。但在基于指纹匹配的资产识别、基于漏洞库的风险关联、工业威胁诱捕、威胁溯源等检测类[illegible]应类技术方面尚[illegible]在不足，技术成熟度和市场应用水平与国际工业信息安全厂商仍存在较大差距。在内嵌安全防护方面，我[illegible]在通信和数据加密、身份识别技术等方面已取得一定的突破，但由于工业系统整体[illegible]平较低。

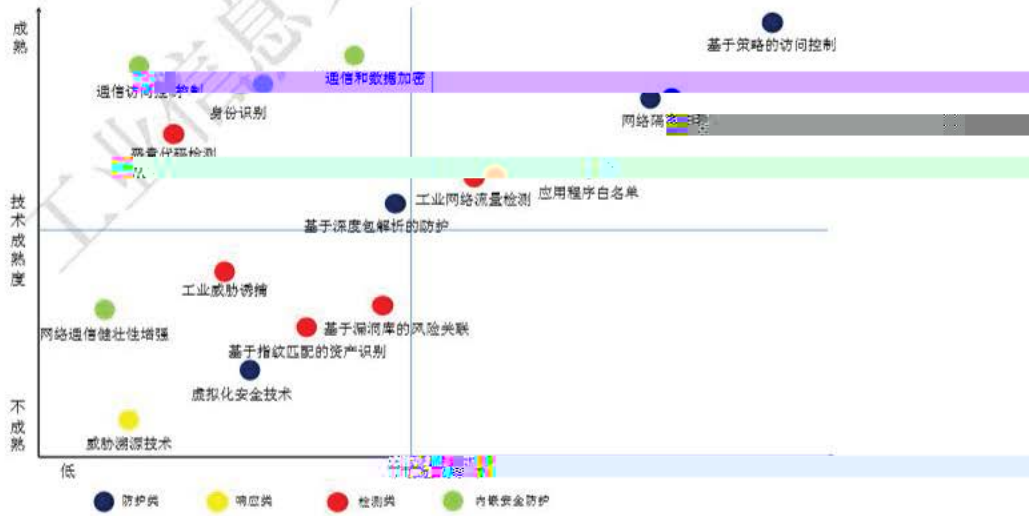

图 3.4 工业信息安全技术成熟度与应用情况

资料来源：工业信息安全产业发展联盟采集整理

（六）多地加快工业信息安全产业布局

在国家的政策引导下，北京、上海、江苏、四川等多个省市积极组织开展工作，通过制定产业规划、建设产业基地、成立协同创新平台等方式推动地区工业信息安全产业发展和项目落地。其中，北京地区工业信息安全产业聚集效应已初步形成，并已分布覆盖自主可控[illegible]安全厂商的全产业生态链。此外，上海、浙江和广东等地区基于较为雄厚的工业和信息化基础，也具[illegible]业信息安全产品研发和服务支撑能力。

（七）我国工业信息安全市场竞争加剧

2017 年，我国工业信息安全产业正式进入快速发展阶段，不同业务背景的[illegible]格局加剧。据国家工业信息安全发展研究中心统计，2018 年国内约有 176 家企业涉足工业信息安全业务，较去年增长 27.5%。其中，传统信息安全[illegible]安全的厂商数量位列第二位，[illegible]

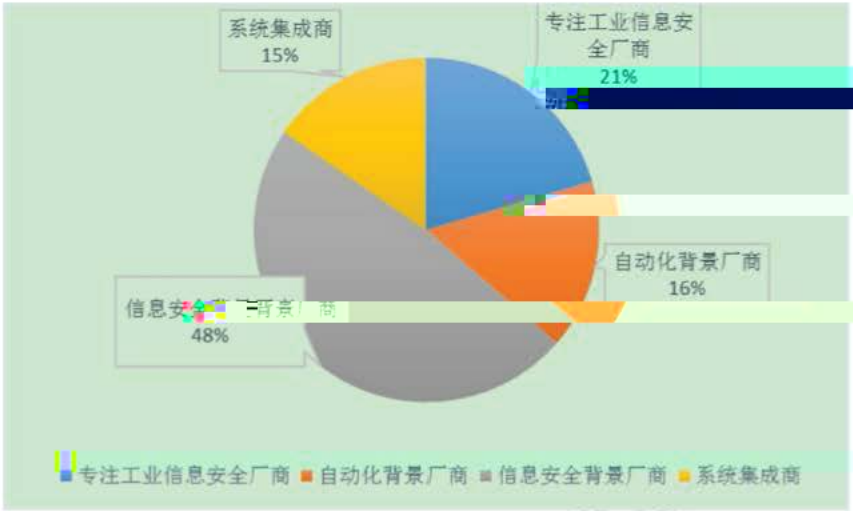

图 3.5 2018 年我国工业信息安全市场竞争格局

数据来源：工业信息安全产业发展联盟采集整理

与 2017 年相比，2018 年工业信息安全市场竞争格局主要发生以下几个变化（图 3.6）。**一是**天融信、立思辰、蓝盾股份等多家传统信息安全背景的上市公司纷纷布局工业信息安全；**二是**综合考虑地缘政治局势复杂多变对工业控制系统供应链的影响，浙江中控、和利时、北京安控等自动化背景厂商通过与安全厂商的合作，着力开展内置信息安全工控设备的研发和产业化推广；**三是**专注工业信息安全的初创企业数量显著增多，六方云、木链科技、亨通信安等初创企业结合自身渠道和技术创新优势进入工业信息安全市场；**四是**随着国家、地方政策不断向好，系统集成商凭借丰富的行业知识和本地化服务基础进入市场，加快与安全厂商的合作和竞争。

四、我国工业信息安全产业发展面临的挑战

一是工业信息安全企业集中度低，发展不充分。我国工业信息安全产业起步晚、体量小，其中工业互联网外建安全产品和服务的市场规模占网络安全产业整体规模不足5%，同时，专注工业信息安全领域的企业规模普遍较小，布局工业信息安全业务的厂商进入市场的时间多数不足5年。以工业信息安全为主营业务的企业不足100家，尚未形成产品竞争力强、行业影响力大、引领产业发展的骨干龙头企业，产业聚集效应不明显。工业企业安全防护意识薄弱，对工业信息安全的重视程度有限，普遍存在重发展、轻安全，安全投入不持续、主体责任落实不到位等问题，产业内需亟待释放。

二是工业信息安全产品和服务缺乏认证机制，实战模拟应用进程缓慢。目前，市场上工业信息安全产品和服务的种类繁多，但与之对应的检测认证和市场准入机制尚不完善，针对工业现场的仿真测试不充分，有针对性的检测认证标准规范和技术手段还很缺乏，大多数工业信息安全产品和服务仍然使用传统信息安全检测认证标准和方法。缺乏统一的标准和认证机制，将会导致工业信息安全产品和服务的认证缺乏权威性，难以快速广泛地推向市场，产业化生产、规模化应用更是步履维艰。

三是工业信息安全建设缺乏综合运营机制，安全防护能力难以得到有效提升。当前，我国工业信息安全建设大多围

五、我国工业信息安全产业发展趋势展望

一是政策利好，产业基础更加[illegible]。随着工业互联网战略的深入推进，国家层面不断强化财政支持，工业和信息化部通过开展工业互联网创新发展工程、工业互联网试点示范等工作，未来将进一步引导企业加大工业互联网安全技术投入，加快工业互联网安全技术研发和产业化推广。

二是理念变革，产品供给日益丰富。为应对工业企业用户不断升级的安全需求，工业信息安全产品数量逐渐增多，产品种类日趋丰富。以工业防火墙、工业网闸、应用白名单等为代表的边界安全和终端安全产品，已逐步应用于新建工业信息安全项目建设中。为更好地满足工业企业用户的合规需求，态势感知、合规管理、安全运维管理等工业信息安全管理类产品将日益增多。

三是需求旺盛，安全服务迎来爆发。长期以来，我国工业信息安全服务市场发展缓慢，“重产品、轻服务”的问题突出。随着工业信息安全事件频发和[illegible]标准的落地，单纯的工业信息安全防护产品已无法满足工业企业用户需求。同时，由于工业企业普遍缺乏对工业信息安全防护架构的落地能力，安全体系设计和规划服务需求应运而生。2018 年台积电遭勒索病毒攻击事件，也进一步催化了工业企业对风险评估、应急处置、攻防演练等工业信息安全服务的[illegible]，将大幅带动工业信息安全服务市场快速发展。