CAICT 中国信通院

中国网络安全技术与企业发展研究报告

（2020 年）

中国信息通信研究院安全研究所

2020 年 12 月

版权声明

编写团队

编写单位：

中国信息通信研究院安全研究所

编写组成员：（以姓名笔画为序）

周杨、孟楠、焦贝贝、谢玮、董骅、董悦

联系人：

周杨

邮箱：zhouyang@caict.ac.cn

焦贝贝

邮箱：jiaobeibei@caict.ac.cn

前　言

强大的网络安全产业实力是保障我国网络空间安全的根本和基石。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“积极发展网络安全产业，做到关口前移，防患于未然”，要“抓产业体系建设，在技术、产业、政策上共同发力”，明确了我国产业发展的理念、目标、路径，为网络安全产业发展指明了方向。

近年来，基于政策扶持、需求扩张、应用升级等多方面的驱动，我国网络安全产业发展进入“快车道”。2019 年我国网络安全产业规模较 2018 年增长 17.1%，企业发展态势总体良好，产品体系日益完善，技术创新高度活跃，综合实力显著增强，为保障国家网络空间安全发挥基石力量、做出重要贡献。

此次蓝皮报告是对《中国网络安全产业白皮书（2020 年）》（下简称《白皮书》）的补充。在对《白皮书》的政府政策、企业发展、规模结构等维度重点研究成果进行总结之外，蓝皮报告进一步对安全企业、互联网企业、运营商等主体的网络安全市场布局情况进行介绍，并结合热点趋势，重点对 5G 安全、容器安全、车联网安全、“区块链+安全”、数据合规等五个领域进行分析预测。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。

在本蓝皮报告的研究过程中，得到以下单位的支持协助，在此表示感谢（以企业名称笔画为序）：山石网科通信技术股份有限公司、上海观安信息技术股份有限公司、上海纽盾科技股份有限公司、中兴

通讯股份有限公司、中国电子科技网络信息安全有限公司、天津市国瑞数码安全系统股份有限公司、北京天融信网络安全技术有限公司、北京升鑫网络科技有限公司（青藤云安全）、北京安天网络安全技术有限公司、北京安信天行科技有限公司、北京安博通科技股份有限公司、北京启明星辰信息安全技术有限公司、北京芯盾时代科技有限公司、北京奇虎科技有限公司、北京知道创宇信息技术股份有限公司、北京神州绿盟科技有限公司、北京梆梆安全科技有限公司、北京智游网安科技有限公司、北京微智信业科技有限公司、北京酷德啄木鸟信息技术有限公司、北京蔷薇灵动科技有限公司、华为技术有限公司、江苏易安联网络技术有限公司、江苏通付盾信息安全技术有限公司、亚信安全科技有限公司、华信咨询设计研究院有限公司、杭州安恒信息技术股份有限公司、杭州美创科技有限公司、奇安信科技集团股份有限公司、杭州默安科技有限公司、重庆贝特计算机系统工程有限公司、恒安嘉新（北京）科技股份公司、浙江鹏信信息科技股份有限公司。

目 录

图 目 录

表 目 录

一、网络安全产业发展概述

近年来，围绕网络空间的国家级攻防对抗日趋激烈，网络安全威胁快速发展演变，网络安全形势复杂严峻。网络安全产业作为国家网络安全能力的重要组成，成为政府乃至国家安全的重中之重。

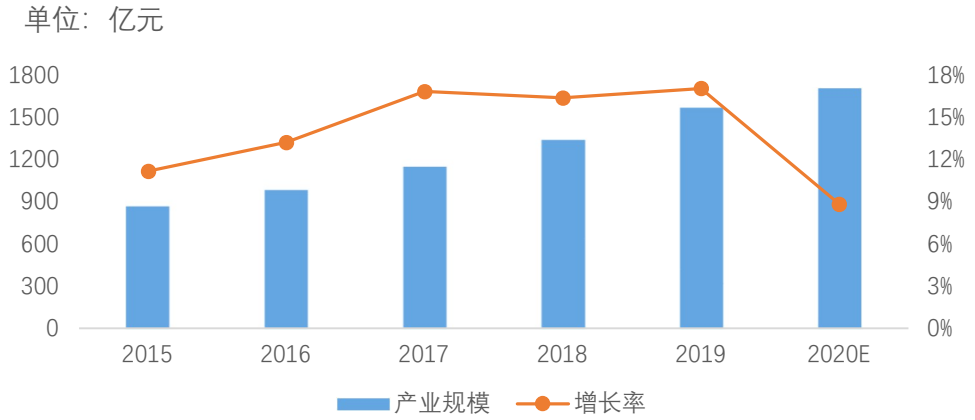
当前，网络安全等级保护 2.0 和《中华人民共和国密码法》等法律规范相继正式实施，推动产业发展的规划指南陆续出台落地，新型基础设施建设相关政策的推出与工程项目建设也在不断加速。全面推进的网络安全政策规范与“新基建”进程，在提高网络安全合规要求、完善产品和服务支撑体系的同时，也将催生新应用与新业态，为网络安全的产业发展持续释放红利。

2019 年我国网络安全产业发展总体态势良好[1]，网络安全上市企业在营收规模和研发投入方面呈现普遍增长态势，在盈利能力方面则出现分化。企业间战略合作日益增多，大型互联网企业、国企、安全企业以及专业投资机构等持续发力，助力工业互联网安全、物联网安全、数据与应用安全、身份安全等热点领域网络安全创新企业培育孵化。

随着我国网络安全政策法规的逐步推进、产业生态日益完善和安全需求的深化演进，我国网络安全产业发展进入快车道。根据中国信息通信研究院的统计测算，2019 年我国网络安全产业规模达到 1563.59 亿元，较 2018 年增长 17.1%，预计 2020 年产业规模约为 1702

[1] 网络安全产业发展详细情况请参见《中国网络安全产业白皮书（2020 年）》

亿元，增速约为 8.85%[2]。2015-2020 年我国网络安全产业规模增长情况如图 1 所示。



数据来源：中国信息通信研究院

图 1　2015-2020 年我国网络安全产业规模增长情况[3]

二、网络安全市场主体布局进展

近年来，数据泄露、云平台安全风险等问题日益严峻，与 5G[4]、区块链、车联网等新兴技术相关的网络安全挑战也在不断增大。持续升级的网络安全威胁和不断增强的合规要求，都对市场形成了有力的牵引。面对工业、金融、能源等重点行业，电商、智慧城市等新兴产业对网络安全产品、服务、解决方案的强劲需求，网络安全企业全面加速产业布局，互联网企业、电信运营商、设备厂商等也成为网络安全新生力量，为网络安全产业带来新的活力。

（一）传统网安企业聚焦新兴科技领域和安全服务转型

[2] 说明：本次测算对网络安全产业范畴进行了扩充，将例如区块链应用等安全新技术产品、密码产品和设备等信息安全产品纳入考量范围，同时将云服务企业、电信运营商、车联网企业等主体的网络安全业务也纳入计算范围。

[3] 说明：已基于新的网络安全产业范畴对往年数据进行追溯调整。

[4] 5G：Fifth-Generation Mobile Networks，第五代移动通信

1. 新基建相关领域成为重点关注方向

传统网络安全企业是网络安全领域的中坚力量。在近期的安全产品研发投向上，呈现出增强网络安全防御技术和扩大网络安全防护领域两大特征。

一方面探索以大数据、人工智能等为代表的新一代信息技术在网络安全领域的应用，提升网络安全防御的全局化和智能化。美亚柏科结合多年深耕行业的实践经验，研发形成大数据与智能平台产品，并于 2020 年 7 月正式面向全球发布；深信服持续深入研究大数据、人工智能等新技术在安全领域的应用；启明星辰和迪普科技将大数据分析、机器学习等先进技术融入安全产品，研究构建全方位、全天候、智能化的态势感知系统。

另一方面大力研发针对 5G、云计算、工业互联网、车联网、区块链等关键信息基础设施的安全防护技术。绿盟科技聚焦数据安全、零信任安全、云计算安全、企业级安全、工业互联网安全五大领域，于 2020 年 8 月发布 10 款安全产品、解决方案及服务。卫士通与控股股东中国网安持续发力 5G 安全，其中，中国网安与中国电科集团合作对 5G 核心网和 5G 终端芯片开展全自主的安全增强研究。迪普科技促进新一代高性能云计算数据中心安全平台落地，积极研发满足云计算数据中心安全需求、更高性能的新一代软硬件平台。启明星辰加大工业互联网安全产品研发项目投入，深耕工业互联网安全发展。数字认证[5]积极投入区块链与车联网相关技术研究，2020 年 4 月，开发的

[5] 数字认证：成立于 2001 年，网络信任与数字安全服务提供商

“信认链”区块链平台通过全国互联网安全管理服务平台的安全评估，同年 10 月，联合华为开展 C-V2X[6]安全证书服务电信级运营平台的首次大规模示范验证。我国上市网络安全企业研发占比及投向如表 1 所示。

表 1　我国上市网络安全企业研发占比及投向

企业名称	研发投入占比	研发人员占比	研发投向
深信服	24.86%	36.80%	改进产品体验，孵化新产品，加大在人工智能、大数据、云计算等技术领域的基础和前沿研究
绿盟科技	20.20%	27.58%	探索研究漏洞挖掘、数据安全、云安全、工业互联网、物联网安全和威胁追踪，加大云安全集中管理系统、工控安全审计系统、工业网络安全合规评估工具等投入
启明星辰	19.57%	42.00%	重点围绕在云计算安全、人工智能、工业互联网安全、物联网安全、大数据安全等领域方向，加大工业互联网安全产品和新一代云安全资源池研发投入
卫士通	11.73%	41.39%	加大新产品研发和新动能打造，不断加大在 5G 安全、工控安全、物联网安全、云计算安全、区块链等领域的技术创新能力
北信源	16.24%	42.87%	大力研发虚拟化终端安全管理系统、网络与终端安全和行为大数据分析系统、智慧终端安全一体化管理平台等
迪普科技	20.40%	41.02%	加大在安全监测、安全专业服务及安全态势感知平台等方面的投入，有序推进募投项目新一代高性能云计算数据中心安全平台、新一代高性能应用交付平台等项目的研发投入。
美亚柏科	17.32%	69.08%	加强自主可控国产化产品适配研发，加大对大数据与智能平台产品项目、电子数据取证与智能装备项目、民生放管服项目的研发投入
数字认证	17.89%	65.00%	在移动互联网和工业互联网等领域开展密码技术攻关，在云密码技术、数字身份管理、车联网安全认证、区块链等领域进行技术储备

[6] C-V2X：Cellular Vehicle-to-Everything，蜂窝车联网技术

企业名称	研发投入占比	研发人员占比	研发投向
中孚信息	17.68%	38.62%	围绕安全保密技术、云计算、信创、大数据等领域进行新产品的研发，在研项目包括：私有云信息安全防护系统、面向电子政务信息安全监管大数据平台等
格尔软件	16.49%	70.19%	开展对新一代身份管控平台、零信任安全网关、安全加密存储网关、物联网接入网关等产品领域的前期研究

来源：中国信息通信研究院根据公开资料整理

2. 头部企业实施差异化的安全服务业务布局

头部企业公开数据[7]显示，近三年来，安全服务成为企业业务构成中不可或缺的一部分，安全服务业务收入平均占比不断攀升。根据安全服务占比情况，可将头部企业分为两个梯队。第一梯队企业的安全服务业务在营业收入中的占比均高于 20%，并且近年来所占比重逐步提升，包括绿盟科技、安恒信息、启明星辰和数字认证。第二梯队企业的安全服务占比处于 5%-20%，包括天融信、北信源、奇安信、蓝盾股份和美亚柏科。第二梯队企业由于受到战略布局调整和外部因素叠加影响，安全服务收入占比表现出一定的波动性。

值得关注的是，2020 年上半年，第一梯队的安全服务占比进一步增长，该梯队四家企业的安全服务收入占比均接近 30%[8]。安全服务收入的持续增长得益于企业差异化的安全服务业务布局。**启明星辰和绿盟科技以安全运营为切入点，引领安全服务化趋势**。2020 年上半年，启明星辰新增 17 个运营中心，并且依靠运营中心推动安全即服务发展战略。绿盟科技提出一体化安全运营服务,其安全托管服务

[7] 数据来源：网络安全上市企业年度报告，受限于数据的可得性，部分头部企业未纳入分析范围。
[8] 数据来源：网络安全上市企业 2020 年半年度报告。

（MSS）获得知名 IT[9]咨询机构 Forrester 推荐。**安恒信息追随云计算业务变革热潮，把握安全服务云化转型先机**。2020 年安恒信息全面升级云安全战略，以 SaaS[10]化服务模式提供云监测服务、云防护服务和威胁情报服务。**数字认证[11]深挖电子认证领域发展潜力**。数字认证是电子认证领域的龙头企业，近年来受益于密码法和等保 2.0 等政策利好，安全服务业务发展迅速。

（二）新生力量为我国网络安全发展注入新活力

在“新基建”的推动下，网络安全建设与信息化建设逐渐同步，网络安全变成网络基础设施的一部分，互联网企业、电信运营商、设备厂商等网络基础设施建设主体都开始更多的参与网络安全建设，成为网络安全基础设施的新生力量。

1. 互联网企业多维度打造安全防御体系

近年来，以阿里、腾讯、百度为代表的国内多家顶级互联网企业纷纷布局网络安全，用互联网思维构建网络安全纵深防御体系。大型互联网企业的加入，为我国网络安全发展注入新的活力，也带来了新的机遇和变革，或将逐步颠覆传统的安全思维，改变安全市场格局。从现有安全业务布局来看，阿里建立了云安全、身份管理、数据安全、业务安全和安全服务五大业务条线；腾讯围绕安全治理、数据安全、应用安全、计算安全和网络安全五个层面搭建云原生安全防护体系；

[9] IT：Internet Technology，互联网技术

[10] SaaS：Software as a Service，软件即服务

[11] 数字认证：企业全称“北京数字认证股份有限公司”，是国内网络信任与数字安全服务提供商

百度则形成由 AI[12]安全、移动安全、云安全、数据安全、业务安全组成的五大业务矩阵。互联网头部企业的安全布局具有以下鲜明的业务特征。

一是互联网头部企业均将云安全视为重要战略方向。由于头部互联网企业是云计算服务的主要提供商，在云安全尤其是公有云安全领域具有得天独厚的资源和技术优势，因而倾向于自己建立云安全服务体系。凭借多年的安全技术研究及安全攻防实践，互联网头部企业在安全领域取得了重要突破。阿里云在 Gartner 全球云厂商安全能力评估中排名仅次于微软，云 WAF[13]、安全态势管理等 11 项安全能力被评估为最高水平；同时，在 2020 年国际数据公司（IDC）的中国云厂商安全能力报告中，阿里云稳居领导者地位。安全业务成为腾讯 2020 年营收增长的重要驱动力，企业级安全业务前三季度收入同比增长 133%，腾讯已明确提出企业级安全业务成为其新的增长重点。

二是在云安全能力的基础上，通过投资收购优秀安全企业，与自身原有的安全能力进行整合、形成优势互补。2019 年以来，阿里陆续收购了九州云腾和长亭科技等网络安全新锐力量。九州云腾助力阿里打造基于身份认证管理的零信任安全架构，补充阿里云原生安全能力；长亭科技帮助阿里破解“多云”环境下的安全问题，2020 年二者主机安全产品能力整合推出升级版长亭牧云（CloudWalker），实现了防御能力的全面打通。腾讯投资数据安全厂商炼石网络，加强对密码技术和云访问安全代理（CASB）技术的应用研究与实践。业务风险识别

[12] AI：Artificial Intelligence，人工智能

[13] WAF：Web Application Firewall，Web 应用防火墙，网站应用级入侵防御系统

厂商数美科技同时获得了腾讯和百度的投资青睐，其基于 AI 技术的智能风险识别引擎，可解决在线业务中的风险问题。

三是互联网头部企业在车联网、工业互联网、区块链等新兴技术安全领域布局也在持续推进。车联网安全方面，百度基于自身开源自动驾驶平台 Apollo，通过联合建立汽车信息安全实验室、制定网联汽车信息安全评测标准等方式，推进车联网信息安全保障技术的精进，其车联网安全防护产品取得 EAL4[14]等级证书。与此同时，百度也在深度布局工业互联网安全，2019 年领投工业互联网安全企业长扬科技，升级工业互联网安全防御能力；2020 年收购工业安全生产厂商湃道智能，探索计算机视觉和深度学习等 AI 技术在工业安全领域的应用潜力。区块链应用方面，腾讯和阿里巴巴两大巨头持续打造区块链安全管理、标准范例和安全产品能力。2020 年 9 月，腾讯云的“智能合约安全管理要求”提案成为全球首个区块链智能合约安全领域的国际标准，填补了智能合约标准空白。同期，阿里旗下“蚂蚁链”宣布对外开放数据安全计算硬件、3D 合约安全服务和数据隐私计算服务，为区块链落地场景提供安全保障。

2. 电信运营商围绕 5G+安全纵深推进

运营商作为基础设施的建设者和维护者，拥有网络、人才、技术等基础资源和市场影响力，输出安全技术能力、扩展业务范围、构建产业生态，已经成为其提升竞争力，引领网络安全产业发展的重要举措。

[14] EAL4：专项认证《信息技术安全评估准则》的第四个评估等级

一是 5G 安全成为运营商的重点布局方向。一方面，运营商围绕 5G 边缘计算安全、5G 数据安全、SIM[15]卡安全等多个方面全速推进标准统一，通过研究安全需求和技术框架，为 5G 安全部署和技术发展提供支持和参考。其中，中国移动与中国联通关注 5G 安全的体系建设和垂直行业发展，其联合其他单位牵头编制了《5G 安全标准体系建设指南》并共同起草完成《5G 安全试验系列规范》，从而建立 5G 安全标准体系图谱、推动 5G 安全国际统一评估认证。此外，中国移动还在国际标准化组织（ISO）和 TD-LTE[16]全球发展倡议（GTI）等平台发布多个 5G 垂直行业标准和白皮书，为凝聚行业共识、助力产业发展提供有益探索。中国电信则关注 5G 终端、5G 网络和 SIM 卡的安全，从 2018 年至今，已多次发布相关指南和白皮书，为明确用户卡的发展方向以及相关行业应用开发提供参考指导。**另一方面**，运营商充分发挥自身优势，主动探索、开拓 5G 安全技术与安全应用，成为新兴领域的技术标杆与试验田。其中，中国移动的网络安全部门围绕 5G 智慧港口、超高清视频、5G 抗疫复工业务等打造了一批 5G 安全“样板房”，积极推动 5G 示范应用项目落地推广。中国电信则重视打造安全的 5G 和云网，其不断完善“防御、检测、响应、预测”的自适应内生安全体系，在实现移动互联安全的同时，为客户提供安全能力及服务。

二是企业投资成为运营商安全版图拓展的重要手段。一方面，为了明确安全业务主线，培育公司新的业务线和增长点，运营商开始积

[15] SIM：Subscriber Identity Module，是 GSM 系统的移动用户所持有的 IC 卡，称为用户识别卡

[16] TD-LTE：Time Division Long Term Evolution，分时长期演进，LTE 标准的一种制式

极推动安全业务的部门独立或业务剥离。2019 年底，中国电信与联通都进行了较大的组织架构调整。其中，中国电信设立了网络和信息安全管理部，确定以安全为上的发展方向；中国联通成立了专注于网络安全服务的联通智慧安全科技有限公司，该公司是中国联通安全业务线的专业化服务团队，主要产品包括联通云盾等。**另一方面**，运营商还通过投资较为成熟的安全企业或合资成立新安全企业的方式，多线布局网络安全产业领域。在投资安全企业方面，2020 年 4 月，中国电信以 17.68 亿元入股辰安科技，不断加强在公共安全产品与服务领域的布局；同月，中国移动以 13.84 亿港元成为亚信科技的第二大股东，持续完善 5G 安全领域能力布局。在合资成立安全企业方面，2019 年 10 月，中国电信、中国联通等单位共同出资组建中资网络信息安全科技有限公司，致力于支撑国资国企在线监管系统安全运行；2019 年 12 月，中国联通与奇安信达成合作，共同出资成立云盾智慧安全科技有限公司，新公司重点聚焦态势感知和网站云防护等产品领域，实现从产品到服务的转型。

三是企业合作成为运营商提升安全能力的重要途径。运营商在网络安全领域积极开展战略合作，充分发挥各自优势，共同促进网络安全技术在移动互联网、5G、物联网、云等场景的创新、实践和推广。2020 年 11 月，中国移动陆续与绿盟科技、360、中兴通讯等企业达成合作，未来将围绕 5G 网络、6G[17]网络、移动云、产业链培育等多个主要方向，安全能力建设、安全解决方案、安全运营、安全攻防及培

[17] 6G：Sixth-Generation Mobile Networks，第六代移动通信

训等多个安全层面，展开深入合作，探索新兴业务领域的发展机遇。2019 年 4 月，中国联通分别与 360、径卫视觉达成战略合作，其中，将与 360 围绕“家庭安全应用”领域共建 5G 智慧家庭安全未来，将与径卫视觉围绕车联网主动安全驾驶、5G、物联网等领域共建车辆安全生态融合体系。2020 年 8 月，中国电信与 360 成功签约，以聚焦打造安全智慧城市为目标，通过开展城市基础设施、安全领域合作，提升关键基础设施、数据资源的安全保护能力，助力数字安全产业高速发展。

3. 更多新主体陆续发力布局网络安全领域

面对网络安全领域的巨大发展潜力，设备厂商、汽车厂商等主体针对 5G 安全、数据安全、安全合规等前沿热点领域和方向，持续优化产业布局。

一是设备厂商持续对外输出安全防护能力，成为网络安全产业中新的力量。2019 年 6 月，中兴通讯发布了《5G 安全白皮书》，总结和输出其在业务安全、数据保护以及用户隐私等方面的研究成果。2020 年 5 月，华为与中国银联达成合作，双方将发挥各自领域的专长和优势，围绕金融支付创新、云计算、大数据、人工智能等领域，打造先进、安全、优质的支付产品及服务。2020 年 6 月，华为发挥整合力量成立北京安全等保解决方案能力中心，为广大中小企业提供安全产品到测评服务的“一站式安全等保解决方案”。

二是汽车厂商基于其业务发展需求，通过投融资等方式布局车联网安全领域。2019 年 6 月，奇瑞搭建智能汽车网络安全生态链，平

台汇聚多家知名科技企业和车载端资源平台，将在智慧城市、5G 应用、智能汽车网络信息安全等领域开展合作。2020 年 3 月，中国第一汽车集团旗下的一汽富晟实现对物联网安全厂商信长城的投资，积极布局智能网联汽车、V2X[18]安全等领域。

三、重点细分领域技术发展现状

网络安全企业以及互联网企业、电信运营商、设备厂商等网络安全产业新主体积极参与安全建设，探索网络安全新技术应用和新场景安全防御手段。基于各主体网络安全布局方向、国内外网络安全技术和政策热点，选择 5G 安全、容器安全、车联网安全、“区块链+网络安全”和数据合规五大重点细分领域，展开技术发展现状梳理和未来展望，以期为网络安全领域发展提供前瞻性的思考。

（一）5G 网络安全实践密集展开

以 5G 等为代表的新一代信息技术正在不断推动科技和产业加速演进，5G 建设已成为世界各国数字经济发展战略中重要的一环。根据全球移动供应商协会（GSA）统计，截至 2019 年底，全球 119 个国家或地区的 348 家电信运营商开展了 5G 投资，其中 61 家电信运营商已经推出 5G 商用服务。然而由于不同类型平台、网络建设进度和技术成熟度存在差异，目前针对 5G 的安全产品、服务和解决方案研究和落地进度也各有不同。

5G 移动边缘计算（MEC[19]）平台的边缘侧安全服务与产品率先落

[18] V2X：vehicle to everything，车用无线通信技术
[19] MEC：Mobile edge computing，移动边缘运算

地。MEC 平台与 5G 网络部署相对独立，使用模式相对成熟，相关产品和服务发展较快。云服务商不断推出内嵌安全防御能力的 MEC 产品和解决方案，安全厂商也纷纷聚焦 MEC 平台安全。如，Google[20]的物联网服务平台 Google Cloud 为用户提供安全连接和认证服务，可为分布在各地的海量设备提供安全的连接，并基于证书和 TLS[21]加密的认证方式提供端对端安全；腾讯的边缘计算机器（Edge Computing Machine）支持通过配置安全组实现协议和端口维度的网络流量控制和管理，并可以在网络、主机安全等领域按需提供防护服务；亚信的 DS for MEC 聚焦移动边缘计算平台和应用部署安全，提供主机、虚拟机和容器级别的保护，通过机器学习、沙箱联动、深度包检测技术(DPI[22])、虚拟补丁、数据备份恢复等技术，能有效发现和阻止异常，实现便捷管理与智能运维。**5G 网络安全基础防护产品逐步推出**。当前 5G 网络安全领域应用的基础防护产品仍是以传统的网络安全相关产品为主，然而随着 5G 建设的加速，国内外一些网络安全厂商已经基于已有安全能力针对 5G 开始研发和推出安全能力增强的防火墙、网关、密码等防护产品。如，Palo alto[23]的 5G 下一代防火墙能够提供对信令、数据和控制平面的全面可见性和精细控制，并基于由 AI 驱动的威胁情报提供自动化快速安全响应，同时提供云端就绪的 NFV[24]方式实现灵活的软件部署能力；中国网安的基础密码产品能用于 5G 终

[20] Google：成立于 1998 年，全球知名互联网产品与服务提供商
[21] TLS：Transport Layer Security，安全传输层协议
[22] DPI：Deep Packet Inspection，深度包检测技术
[23] Palo alto：派拓网络，创立于 2005 年
[24] NFV：Network Functions Virtualization，网络功能虚拟化

端、网元、应用等各个环节，其中通信安全产品可通过 IPSEC VPN[25]、SSL VPN[26]、5G 安全 CPE[27]为 5G 专网提供安全的业务数据传输通道，并在终端密码模块和云端密码基础服务的支撑下实现应用层数据加密传输。**“5G+垂直行业”解决方案加紧研制**。随着 5G 在车联网、工业互联网、医疗、物联网、高清视频等不同垂直行业的规划和建设不断落地，“5G+垂直行业”的安全解决方案也成为网络安全厂商的关注重点。如，爱加密基于“5G+医疗”场景提供数据安全解决方案，通过在可穿戴设备端与服务端提供数据监测与防护，保障传输数据不被篡改或被中间人劫持，确保远端医护人员获得准确病情信息，做出及时的病情判断和处理；启明星辰的 5G 智能网联汽车信息安全整体解决方案，对基于 CAN[28]协议的数据传输实现异常检测和防护，拥有 V2X[29]神经网络检测能力，可灵活对接车联网中的车载安全设备及关联系统，实现多类型安全资源整合，形成多视角、全方位的态势感知系统。我国企业在 5G 领域的研究与实践如表 2 所示。

表 2 国内企业在 5G 领域的研究与实践[30]

企业名称	技术领域/特点
山石网科	• 针对边缘计算场景提供租户、虚机、容器等层面的安全方案，提供资产、流量、威胁可视化能力和精细的访问控制能力； • 探索将零信任、人工智能等应用到 5G 安全之中。
绿盟	• 采用漏洞扫描、渗透测试、配置检查抽样、日志分析和顾问访谈等技术手段，对 5G 网络中各目标网络单元的业务及应用安全、拓扑安全、物理环境安全等进行基础调研核查及支撑服务。

[25] IPSEC VPN：指采用 IPSec（Internet Protocol Security）协议来实现远程接入的一种 VPN 技术

[26] SSL VPN：指采用 SSL 协议(Secure Sockets Layer)来实现远程接入的一种新型 VPN 技术

[27] CPE：Customer Premise Equipment，一种接收移动信号并以无线 WIFI 信号转发出来的移动信号接入设备

[28] CAN：Controller Area Network，控制器局域网络

[29] V2X：vehicle to X，车用无线通信技术

[30] 来源：基于公开资料和调研获得

企业名称	技术领域/特点
华信设计院	• 提升 VNF[31]自身安全防护能力，对 gNB[32]基站设备、虚拟化网元实施安全防护与加固措施，针对虚拟化网元和 MEC 服务器，提供内置安全检测、防护、以及按需动态服务的能力。
中兴	• MEC 设备中内嵌了自研的 vFW[33]组件，提供 MEC 的边界安全防护以及 MEC 内部安全域间的安全防护能力。
恒安嘉新	• 利用边缘轻量级安全 Agent[34]与云端联动的方式实现虚拟机安全可视化管理和检测；从基础设施安全、边缘网络安全等多个维度实现对 MEC 分流网关的安全防护。
安恒信息	• 边缘统一安全管理中心主要完成对安全日志和流量的风险要素统一感知、关联分析、策略制定和自动任务编排等； • 完成相关的云端和边缘侧的云边安全协同机制。
天融信	• 研究实现 5G 网络各切片内的保护/管控、切片间隔离等安全增强加固，和基于轻量化架构实现 5G 网络二次认证、上层业务认证、跨域身份认证等技术能力等。
安博通	• 兼容多种虚拟化与云平台，通过预配置进行自动部署运行，灵活扩展能力可达到对应用业务或租户的安全与资源控制需求，提供不同安全等级应用之间的安全隔离和安全防护。
国瑞数码	• 研究开发行业特征等分类模型以及安全风险监测分析模型； • 拓展对 5G 新技术新应用的监测能力及安全风险发现能力，实现 5G 环境下多种核心应用场景的安全态势感知。

（二）微服务架构的兴起将容器安全推向新舞台

容器提供了一种轻量的虚拟化方式，其使用方便、操作便捷的特性，在 DevOps[35]、微服务等云原生应用的开发过程中，提供了极大的便利，得到了业内的广泛使用。但与此同时，伴随着容器使用的日益

[31] VNF：Virtual Network Function，虚拟化网络功能
[32] gNB：next generation node B，5G 基站
[33] vFW：Virtual-firewall，虚拟防火墙
[34] Agent：代理技术
[35] DevOps：Development 和 Operations 的组合词，是一组过程、方法与系统的统称

普及，容器的安全问题也日益凸显。根据 Forrester 统计数据显示，2019 年全球云平台原生安全占据了云安全市场规模的 73%。容器安全作为一个新兴市场，当前还处于快速发展阶段，可以预见未来几年，容器安全市场将会出现一些成熟、稳定的容器安全产品和解决方案。

随着近几年容器的快速发展，基于其生命周期短的特性，安全厂商容器安全解决方案逐渐开始向“构建-分发-运行”全生命周期安全发展。从主体架构上来看，全生命周期的容器安全解决方案主要包括平行容器技术方案和基于宿主机 Agent 的技术方案两类。**平行容器技术方案具有更强的弹性伸缩和检测能力，其利用容器的隔离性和良好的资源控制能力，在容器宿主机中部署防护容器以对主机文件系统进行实时监控和处理响应**。如，Aqua[36]通过其 Enforcer 容器提供容器防护能力，包括对运行镜像全时完整性监控、运行时防护、网络控制策略等，并在容器全生命周期提供不同级别的防护；TwistLock[37]的容器安全解决方案基于其自研 Defender 容器实现各项安全功能，提供 AI 驱动的运行时安全检测、云原生 4-7 层容器防火墙、工作负载访问控制、CI/CD[38]集成等能力；重庆贝特的赤岩石平台在平行容器基础上结合 EBPF[39]实现运行容器的深度防护，提供网络三到七层的深度包检测能力，同时结合包括漏洞扫描、持续集成等安全模块实现网络拦截、漏洞扫描、轻量级 WAF、沙箱等安全功能。**基于宿主机 Agent 的技术方案能实现宿主机安全、容器安全两种防护效果，其通过在宿主机**

[36] Aqua：总部位于以色列，容器安全厂商
[37] TwistLock：创立于 2015 年，云原生安全厂商
[38] CI/CD：Continuous Integration/ Continuous Deployment，持续集成/持续部署
[39] EBPF：Extended Berkeley Packet Filter，伯克利包过滤的扩展技术

部署代理程序的方式，提供基础的安全防护能力以及容器的清点、监控等能力。与国内外容器安全市场使用场景不同，国内混合部署的业务场景较多，客户有兼顾宿主机安全的安全需求，因此国内安全厂商很多采用此技术路线。如，青藤云安全的青藤蜂巢容器安全产品主要由代理、服务器、网络三部分构成，基于分布式部署的代理可实现大量任务下发和海量数据分析处理，实现资产轻点、安全补丁、入侵检测和合规检查能力。

此外，**由于责任共担模型在云市场中得到广泛认可，云供应商在容器安全方面主要提供基础设施安全**。如，微软的 Azure 安全中心实现容器安全，持续集成容器运行环境、Kubenetes[40]集群的配置检查和状态监控，并对容器镜像提供安全扫描服务。阿里云围绕自建容器集群以及云原生容器服务场景，通过全面分析黑客攻击 Docker[41]和 K8s[42]的过程和手段，推出容器安全 ATT&CK[43]矩阵。我国企业在容器安全领域实践如表 3 所示。

表 3　国内企业在容器安全领域的主要实践[44]

[40] Kubernetes：一个 Google 开源的容器编排引擎，它支持自动化部署、大规模可伸缩、应用容器化管理

[41] Docker：是 PaaS 提供商 dotCloud 开源的一个应用容器引擎

[42] K8s：Kubernetes 的缩写，Google 开源的容器编排引擎

[43] ATT&CK：Adversarial Tactics，Techniques and Common Knowledge，是一个攻击行为知识库和模型

[44] 来源：基于公开资料和调研获得

企业名称	技术领域/特点
蔷薇灵动	• 提供容器环境的微隔离能力； • 能自动识别节点上的容器、容器间的流量、标签信息等，并能自动识别容器的变化，从而自动修改安全策略，实现容器环境的微隔离。
美团	• 以规则引擎的形式运营监管容器镜像，默认规则支持对镜像中 Dockerfile[45]、可疑文件、敏感权限、敏感端口、基础软件漏洞、业务软件漏洞以及 CIS[46]和 NIST[47]的最佳实践做检查； • 提供风险趋势分析，确保部分构建时安全。
华为云	• CGS48作为一个容器运行在每个容器节点（主机）上，负责节点上所有容器的镜像漏洞扫描，安全策略实施和异常事件收集； • 提供容器进程白名单、文件只读保护和容器逃逸检测功能。
揽阁信息	• 提供关键的加密，访问控制和数据访问审核日志记录功能，使组织能够满足合规性，法规和最佳实践要求，以保护动态容器环境中的数据。
青藤云安全	• 由 Agent、Server[49]、Web[50]三部分构成，提供资产清点、安全补丁、入侵检测和合规基线能力； • 在容器应用程序整个生命周期（构建、分发、运行）中保护容器环境安全。
安全狗	• 融合主机 EDR[51]技术(安全 agent)，可以实现对容器主机的安全闭环管理； • 对容器镜像文件的制作过程、容器运行的过程以及容器内应用进行全自动的安全检测、 预警与防护。
重庆贝特	• 基于带 EBPF 的安全平行容器防护容器宿主机上所有容器及主机系统的安全 • 实现网络三到七层的深度包检测及拦截
小佑	• 基于平行容器对容器非生产和生产生命周期节点提供相应防护； • 提供资产管理、漏洞管理、运行时控制、网络可视化等功能。
绿盟	• 能够对容器环境的基础设施、容器仓库中的容器镜像进行漏洞扫描； • 可通过 AI 机器学习引擎自动学习更新，建立检测规则。

[45] Dockerfile：构建镜像的文本文件
[46] CIS：Center for Internet Security，互联网安全中心
[47] NIST：National Institute of Standards and Technology，美国国家标准与技术研究院
[48] CGS：Container Guard Service，容器安全服务
[49] Server：服务器
[50] Web：网络
[51] EDR：Endpoint Detection and Response，终端检测与响应

（三）车联网安全产品和服务体系初步构建

近年来，随着 5G、人工智能、物联网、大数据等新一代信息技术的不断变革，汽车开始向“智能化、网联化、电动化、共享化”快速发展。车联网已经逐渐成为全球技术创新和汽车产业变革的焦点。国家层面，为了确保在未来交通领域竞争中的优势，各国纷纷将车联网上升为国家战略，并积极展开全面布局。如，2020 年 2 月，我国 11 部委联合发布的《智能汽车创新发展战略》对车联网安全提出了明确要求。产业层面，根据 Gartner 报告显示，2018 年生产的汽车中，近一半具备一定程度的自动驾驶能力，如紧急制动、自适应巡航控制和车道保持等[52]。此外，2019 年全球汽车物联网边缘设备安全支出为 3.17 亿美元，2020 年将达到 4.33 亿美元[53]。

车联网在给用户带来更多新体验的同时，也衍生出了一些可能会对行驶安全等物理安全产生影响的安全隐患。在日益严峻的安全形势下，整车厂商、传统 IT[54]企业、安全企业等都纷纷开始从云端、车端、应用场景、通信、安全服务等方面着手构建相关安全能力，推出车联网安全解决方案。**在云端安全方面，数据安全与安全运营中心（SOC[55]）是车联网网络安全能力建设的重要方向**。其中，数据安全主要涉及数据采集、存储、传输、使用和跨境流动等环节，这与 IT 领域相关手段类似，而安全运营中心则主要通过实时对车内资源进行监测，发现

[52] 数据来源：Gartner，Market Insight: Roadmap for V2X Technologies for Autonomous Driving — When to Invest

[53] 数据来源：Gartner，Forecast: Enterprise and Automotive IoT Edge Device Security, Worldwide, 2018-2024

[54] IT：Internet Technology，互联网技术

[55] SOC：Security Operations Center，安全运营中心

并阻断车载系统中的异常行为，从而实现车载智能终端动态防护体系。如，Arilou[56]的 SOC 解决方案可以在检测和防御模式之间进行切换，支持安全配置和安全固件的持续更新，为其车辆安全产品和第三方系统提供综合分析能力；360 车联网安全运营解决方案基于 360 安全大脑的安全威胁发现能力，提取汽车安全态势，保障汽车 SOP[57]阶段后的安全运行。**在车端安全方面，关键零部件是智能汽车的重要防护对象**。零部件主要涵盖 ECU[58]、域控制器、自动驾驶系统、接口设备等，其安全可通过提供日志审计、防火墙、入侵检测、入侵防御等能力来实现。如，Argus[59]提供的入侵检测与防御系统（IDPS[60]），可通过将每条消息与车内流量行为的预定义行为模型进行比较来检测流量中的异常，防止讯息透过车内网路传播；雅迅网络的中央安全网关使用了硬件加速及快速转发引擎，提供线速检测和阻断能力，能对常见的以太网攻击进行防御。**在应用场景方面，软件漏洞是车联网安全面临的主要风险之一**。防止通过 App[61]漏洞进行的车载系统入侵控制和进行软件的 OTA[62]升级是实现应用场景安全的主要手段。Harman[63]的 OTA 解决方案通过对更新包进行数字签名实现全面认证，通过与安全运营中心无缝集成实现网络安全风险的检测、分析和响应；爱加密的端点防护功能通过安全评估、安全加固、安全监测三个层次进行纵深防御，

[56] Arilou：成立于 2012 年，车联网安全厂商
[57] SOP：Standard Operating Procedure，标准作业程序
[58] ECU：Electronic Control Unit，电子控制单元
[59] Argus：成立于 2013 年，车联网安全厂商
[60] IDPS：intrusion detection and prevention system，入侵检测和防御系统
[61] App：Application，应用程序
[62] OTA：Over the Air，空中下载
[63] Harman：哈曼，车联网领域核心系统组件供应商

协助用户发现 App 中存在的安全漏洞，并对安卓、iOS[64]、T-BOX[65]等进行源码层防护。**在通信安全方面，通信加密、通信协议是实现通信安全的主要手段**。通信安全主要涉及通信认证、通信数据加密和完整性检查等技术，性能与安全的平衡是制约通信安全发展的主要原因之一。如，Infineon [66]的 OPTIGA 系列是专为嵌入式系统设计的安全方案，基于硬件存储微控制器实现通信协议所用的密钥，以保护信息和设备的机密性、完整性和真实性，从而支持安全通信；上海控安的安全可信 T-box 基于国家加密算法 SM2[67]进行研发，能够针对车辆远程数据传输和身份识别进行硬件高等级加密和安全防护。**在安全服务方面，涉及车辆网安全的安全风险评估和渗透测试逐渐升温**。如，Karaba[68]提供的防御评估服务可识别 ECU、总线网络、网关、外部连接、云应用程序和云到车辆活动中潜在的漏洞，并提供减少安全风险的缓解方案；绑绑安全将零信任理念引入汽车评估模型，其将车联网的资产全部设置为不信任，从风险评估的角度逐一界定风险控制的目标并解决相关风险。国内部分车联网安全企业实践如表 4 所示。

表 4　国内车联网安全领域创新企业[69]

企业名称	技术领域/特点
安恒信息	• 基于驱动层安全监控防护技术，采用自学习的网络进程安全防护策略； • 可针对物联网终端系统进行内核防护、数据加密和实时审计，通过物联网态势感知与管控中心进行智能分析。

[64] iOS：iPhone Operation System，苹果移动设备操作系统
[65] T-BOX：Telematics BOX，远程信息处理器
[66] Infineon：英飞凌，总部位于德国，全球领先的半导体公司
[67] SM2：国家密码管理局于 2010 年 12 月 17 日发布的椭圆曲线公钥密码算法
[68] Karaba：总部位于以色列，网络安全解决方案提供商
[69] 来源：基于公开资料和调研获得

企业名称	技术领域/特点
开源网安	• 基于数据 CIA[70]模型和相关威胁分析方法构建威胁分析模型； • 针对资产，确定其面临的威胁，通过预设攻击场景对相关威胁进行分级； • 根据攻击概率和威胁严重程度确定面临的安全风险等级。
东软	• 覆盖车联网全生命周期； • 基于自有引擎技术开发车载入侵防御系统； • 为车载系统和数据提供整体化纵深式防御的可信计算平台。
观安信息	• 依据 6 大类 20 小类不同保护对象和多种安全需求建立分层的安全防护体系； • 基于相关法律、法规及政策，分别设计各层的安全防护措施，建立统一的安全管理平台
上海控安	• 支持基于五元组的以太网策略和基于安全模型和协议内容的 CAN/LIN[71]等总线策略； • 基于 CAN、LIN 等总线协议的识别解析，实现基于总线协议等安全防护。
艾拉比	• 提供云、管、端全链路一站式解决方案，由云端的 OTA 管理平台、汽车端的升级逻辑控制及升级代理程序、连接汽车和云的通信管道三部分组成； • 通讯协议支持私有协议和 OMA[72]/DM[73]协议。
芯盾时代	• 通过终端安全沙箱、多层密钥体系、设备指纹技术等核心技术，为汽车生成全球唯一的“数字身份凭证”
绿盟	• 基于车联网端、管、云三层架构体系，覆盖车辆终端、移动终端、路侧单元、TSP [74]云端服务等车联网要素，开展基于车联网端到端的威胁分析与风险评估。
银基信息	• 提供车、云、通讯三端的安全产品及服务，覆盖安全芯片、安全通讯技术、数据安全、PKI、态势感知、安全管理等。

（四）“区块链+网络安全”双向布局加紧探索

区块链是一种由多方共同维护，使用密码学保证传输和访问安全，

[70] CIA：Confidenciality Integrity Availability，机密性 完整性 可用性
[71] LIN：Local Interconnect Network，局域互联网络
[72] OMA：Open Mobile Alliance，开放移动联盟
[73] DM：Device Management，终端管理
[74] TSP：Telematics Service Provider，内容服务提供者

能够实现数据一致存储、难以篡改、防止抵赖的记账技术，也称为分布式账本技术。凭借去中心化、开放性、自治性、难篡改、可追溯等特点，区块链在金融、工业、能源、物流等多个领域得到了广泛应用，引发了新一轮的技术创新和产业变革。随着区块链相关应用的井喷式发展，在对网络安全领域产生积极影响的同时，其本身面临的严重安全问题也愈发受到产业的广泛关注。

一方面，区块链赋能网络安全，成为网络安全产业技术创新的竞争高地。区块链的不可篡改性、分布式等特性为数据安全提供了更多保密性和完整性的安全保障，主要涉及的安全领域包括数据完整性保障、隐私管理与保护、身份认证与访问控制等。在数据完整性保障方面，爱立信公司基于其 Data Centric Security 产品提供区块链数据完整性方案，基于去中心信任化的无签名基础架构提供全面的审计和自动化的数据防篡改验证；用友的数融云平台通过使用区块链技术，有效保障了记录数据的完整性、真实性和可追溯性，使“全量数据”在企业、平台与金融机构之间流动时不被篡改。在隐私管理与保护方面，Obsidian[75]提供的通信平台基于区块链技术实现对用户元数据的保护，通过将用户元数据随机发布在“区块链账本”的方式，使得攻击者无法通过入侵单一节点收集到所有数据；阿里健康基于区块链技术给予患者管理个人数据的权限，具体权限包括控制谁能访问、访问什么信息及访问时限等，流程建立在安全透明的基础上，避免了个人数据被恶意访问、使用、披露、破坏、修改和销毁。在身份认证与访问控制

[75] Obsidian：成立于 2017 年，区块链技术开发商

方面，REMME[76]推出的基于区块链技术的身份识别与访问管理解决方案以分散的信任网络取代了传统的公钥基础设施，该方案中每个用户设备都会获得存储在 REMME 区块链中的 SSL[77]证书，并基于该证书进行身份验证；世纪乾金的联核云方案结合了区块链技术，其通过改造传统身份证阅读器和组建 P2P[78]模式等方式，实现了闲置身份证核验服务的共享和去中心化的分布式身份核验，降低了实名制核验的成本，确保了核验效率。此外，在威胁情报共享方面，国外已经进行构建基于区块链的威胁情报平台尝试，如 PolySwarm[79]公司基于区块链技术提供去中心化的网络威胁情报市场，在区块链及智能合约架构下通过激励整合全球安全厂商和安全专家实现可信情报市场。

另一方面，区块链在各领域的广泛应用给网络安全带来了新的市场和机遇。区块链技术目前尚处于发展的早期阶段，其在共识机制、智能合约、密码算法、P2P 网络机制等核心技术或机制方面的不完善，导致密码算法安全性、协议安全性、使用安全性、系统安全性等方面都面临了诸多安全挑战。为了对应上述挑战，国内外企业在智能合约安全、钱包和 DApp[80]安全、节点安全等方面进行了布局。在智能合约安全方面，ANCHAIN.AI[81]的智能合约审计沙盒能够审核任何基于 Solidity[82]的智能合约，在源代码层面对以太坊主网合约进行分析，提供安全风险评分、热图等能力；成都链安的智能合约及 DApp 安全审

[76] REMME：成立于 2015 年，区块链创业公司
[77] SSL：Secure Sockets Layer，安全套接字协议
[78] P2P：Point to point，点对点
[79] PolySwarm：总部位于美国，网络信息安全服务提供商
[80] DApp：Decentralized Application，去中心化应用
[81] ANCHAIN.AI：成立于 2018 年，人工智能区块链安全公司
[82] Solidity：一种智能合约高级语言

计服务能够基于形式化验证技术对多个链平台的智能合约和 DApp 代码进行安全审计，并根据智能合约代码实现与设计的一致性、自身的安全性分析结果出具报告。在钱包安全和 DApp 方面，Valid[83]的 DApp 保护平台结合自定义策略和机器学习等技术提供漏洞检测、代码缓解、风险评估、运行时监控等安全能力，通过定制规则降低误报，并在去中心化场景中提供细粒度入侵跟踪以改善安全态势；长亭科技基于预定义的基本检查项，提供对移动端钱包安全和硬件钱包安全的深度安全测试服务，通过检查抵御恶意攻击的能力、设计安全性并协助修复等，提高资产的安全性。在节点安全方面，Bloqchain[84]公司的区块链安全产品侧重于审计和检测，其对大规模的区块节点进行漏洞审计实现安全评估，提供冗余检测、一致性检测和同步分析等一系列安全检测服务；360 的 EOS[85]节点安全解决方案将出块节点放在了 P2P 和 HTTP[86]节点集群之后，并通过在出块节点前端严格限制访问策略和在出块节点后端部署专门的安全管理堡垒机的方式，保障出块节点及私钥的安全。我国企业在“区块链+安全”领域实践如表 5 所示。

表 5 国内“区块链+安全”领域创新企业[87]

企业名称	技术领域/特点
中国网安	• 在确保隐私安全的前提下导入用户的身份属性信息并上链存储，形成以区块链为核心的统一身份信任基础设施； • 基于智能合约实现应用系统的业务权限管理。

[83] Valid：总部位于巴西，数据和身份安全方案提供商
[84] Bloqchain：总部位于美国，加密货币公司
[85] EOS：Enterprise Operation System，为商用分布式应用设计的一款区块链操作系统
[86] HTTP：The Hypertext Transfer Protocol，超文本传输协议
[87] 来源：基于公开资料和调研获得

企业名称	技术领域/特点
通付盾	• 在现有 PKI[88]等公钥体系基础上，结合区块链、无证书签名等技术，提出基于区块链的身份认证方案; • 基于智能合约打造身份网络，实现共识参与者的身份安全。
知道创宇	• 通过探针周期性收集和监控矿机状态数据; 当发现矿机运行异常、被入侵、被盗用等情况时及时告警，防止算力被窃取; • 在全球部署多家海外节点，采用 BGP[89]+Anycast[90]技术，阻断多种类型的 DDoS[91]攻击。
顶象	• 建立业务端、客户端全链路防护和多维度的智能风控体系; • 基于区块链技术，实现对使用者身份的核验、分布式的密钥管理、高强度的加密等，保障链上数据细粒度授权访问。
安全狗	• 基于态势感知和大数据分析获取情报并进行快速响应处置; • 基于安全大数据集中的分析、挖掘,能够弹性、智能和敏捷等的实现安全能力。
派盾	• 基于对各大公链生态的挖掘和剖析，形成高风险黑名单库; • 利用高级分析、异常检测、交易风险智能评估和机器学习等技术，确保覆盖交易过程的风险变化。
慢雾	• 涵盖以太坊、EOS、A 链、唯链、本体、星云链等公链平台; • 针对代币合约、DApp 合约等的源代码进行白盒安全审计。
阿里云	• 提供密钥分发中心和认证中心两个服务; • 分发中心采用硬件加密机和安全存储技术，确保密钥云端生成和存储的安全。
轻资链	• 基于 ISO[92]-81346 国际标准建立资产编码，确保一物一码; • 验证过程上链，形成资产“信任根”；结合资产管理和智能调度引擎获取资产数据，构建资产可验孪生。
天融信	• 通过哈希密钥串，构建区块链网络节点动态身份标识; • 结合无密钥签名基础设施 KSI[93]的基础架构，通过核心认证要素的计算和比对，实现网络节点的可信接入身份认证;

[88] PKI：Public Key Infrastructure，公钥基础设施
[89] BGP：Border Gateway Protocol，边界网关协议
[90] Anycast：任播，是 IPv6 中定义的一种新型通信服务
[91] DDoS：Distributed Denial of Service，分布式阻断服务
[92] ISO：International Organization for Standardization，国际标准化组织
[93] KSI：Keyless Signatures' Infrastructure，无密钥签名基础设施

（五）合规需求不断推动数据安全市场发展

近年来数据泄露事件日益频发，为规范数据应用并保障数据和隐私安全，世界各国掀起数据保护和隐私法规的立法热潮，数据合规成为了各界的研究热点。根据 Gartner 预测，到 2022 年，有关用户隐私的合规工具支出将增至 80 亿美元。

为帮助企业面对合规挑战，各安全厂商从数据安全、内容安全、安全运营等多个角度提供安全能力。其中，**在数据安全方面，技术较为成熟的数据管控和监测审计仍是数据合规市场的主流**。一方面，数据管控一般通过数据脱敏、数据分类分级、数据溯源等手段对数据进行安全治理。如，Informatica[94]公司的数据脱敏产品能够基于角色对个人、健康或信用等敏感数据进行动态屏蔽，基于加密功能在保证数据格式基础上实现数据脱敏能力；启明星辰的数据库脱敏系统集数据抽取、敏感信息自动发现、脱敏、装载于一体，可通过内置的数据模型识别常见的敏感数据，并基于数据压缩、批量装载、并发处理等技术提高脱敏性能。另一方面，监测审计对数据、配置、行为等进行监视和控制，根据监视信息发现异常行为和安全风险。如，AppOmni[95]提供一种面向 SaaS 数据泄漏的安全解决方案，提供高易用性的 RBAC[96]配置方式以降低配置错误率，其自研的深度扫描引擎可以快速完成 SaaS 服务的访问检查提供合规报告，并提供 24*7 的持续监控；奇安信的数据库审计系统采用数据库深度报文协议解析技术、DPI 和 DFI[97]

[94] Informatica：创立于 1993 年，数据管理软件提供商
[95] AppOmni：成立于 2018 年，数据安全厂商
[96] RBAC：Role-Based Access Control，基于角色的访问控制
[97] DFI：Deep Flow Inspection，深度流检测技术

动态流检测技术将数据库操作解析还原成数据库语句，通过匹配预置的安全规则，分析和监控访问者行为并进行实时威胁预警。**在内容安全方面，人工智能的应用日趋成熟**。如，Facebook[98]推出的 DeepText（深度文本）引擎利用深层神经网络架构针对 20 多种语言文字进行内容审核，其能基于用户发送的内容实时分析用户想法，提取用户意图、情绪和实体（人物/地点/事件）等信息并自动移除垃圾信息的干扰；字节跳动可基于深度学习算法和技术构建审核模型，识别视频、文本中的不良信息，并基于 NLP[99]自然语言理解算法对文本内容进行关键词提取、语义识别等检测，给出内容健康指数。此外，**在安全运营方面，隐私运营颠覆了传统的跨越多职能孤岛的手动隐私合规请求处理方式**。SECURITI.AI[100]提供了一种新型的隐私运营概念，将最佳实践与跨功能协作、自动化和编制相结合以实现对合规性请求的批量和自动化处理，其隐私合规产品使用 People Data Graph[101]构建面向人的知识图谱并基于其设计数据分析模型，通过包括聊天机器人、自动化响应等 AI 驱动方式构建落地方案以帮助企业应对合规需求。我国企业在数据合规领域实践如表 6 所示。

表 3　国内企业在数据合规领域的主要实践[102]

企业名称	技术领域/特点
亚信	• 使用“机器学习+语义分析”的方式进行模型训练; • 数据资产分布视图逐层钻取，展示数据特性及变化趋势。
绿盟	• 基于数据的存储、使用、传输三种形态，进行监查和防护; • 基于语义识别引擎对多种数据类型进行敏感信息深度识别。

[98] Facebook：脸书，创立于 2004 年，全球知名社交网络服务网站
[99] NLP：Natural Language Processing，自然语言处理技术
[100] SECURITI.AI：成立于 2018 年，隐私合规初创公司
[101] People Data Graph：人员数据图
[102] 来源：基于公开资料和调研获得

企业名称	技术领域/特点
天融信	• 通过内置的敏感数据正则表达式规则和系统内置的不可逆脱敏算法，实现敏感信息的自动发现。
山石网科	• 智能扫描数据库存在的风险与状态，能够实时监控、识别、阻断外部黑客攻击以及来自内部高权限用户的数据窃取。
深信服	• 采集数据流动，回溯泄密事件的整体过程，提供完整的数据库审计分析、泄密轨迹分析、数据库访问关系可视等功能。
全知科技	• 采用网络流量 DPI 分析、大数据日志清洗分析、人工智能风险建模等技术，使用 UEBA[103]技术构建数据安全风险模型。
思维世纪	• 利用旁路镜像/分光业务访问流量方式，基于大数据分析技术对数据流分析，识别核心业务并进行敏感数据分析。
杭州美创	• 可自动发现敏感数据，并按需进行漂白、变形、遮盖等处理; • 脱敏后的输出数据保持数据的一致性和业务的关联性。
数美	• 实时监测舆情趋势，动态追踪违规态势，持续更新违规词库; • 基于 Fasttext[104]、HMM[105]、CRF[106]、Word2Vec[107]等 NLP 技术构建模型体系。
安恒信息	• 运用智能流程引擎、智能文本识别等技术，将数据收集、处理、出售、披露和共享等纳入安全事件管理。
观安信息	• 通过进行分类分级和流量分析等方式，对组织内数据资产进行敏感数据发现。
芯盾时代	• 通过可信数据管理平台，提供对大数据安全策略、检测与响应的统一管理，构建用户数据安全管理的唯一入口。
爱加密	• 提供“梳理、识别、发现、感知、监控、防护、审计”等多维的泄漏监控与保护，依据数据合规要求，形成合规性报告。
360	• 运用数据去标识化、同态加密等隐私保护技术，结合风险评估、个人信息影响评估等技术手段，实现数据合规。

四、重点细分领域技术发展展望

[103] UEBA：User and Entity Behavior Analytics，用户实体行为分析

[104] Fasttext：Facebook 开发的一款快速文本分类器

[105] HMM：Hidden Markov Model，隐马尔可夫模型

[106] CRF：Conditional Random Field，条件随机场

[107] Word2Vec：word to vector，用来产生词向量的相关模型

（一）5G 网络安全带来安全市场新格局

5G 相关顶层设计和地方政策将进一步提升 5G 网络的建设速度，快速扩张的 5G 网络市场将推动 5G 网络安全合作模式、技术产品的迭代更新。**一是运营商、安全企业、设备商将协同建设 5G 安全**。5G 安全能力的开放导致运营商、安全厂商、设备商等各相关方都成为 5G 安全建设的重要成员，安全企业从单一的安全产品、服务的提供商转变为网络安全基础设施的建设者，运营商也从安全能力需求方转变为安全能力提供商。随着网络建设、安全需求等模式的转变，各相关方安全角色的变化将打开全新的网络安全协同局面，安全企业在 5G 网络建设和业务部署早期的参与度将快速提升。**二是按需安全是 5G 网络安全发展的必然趋势**。在“5G+垂直行业”应用落地过程中，由于智慧医疗、智能汽车、智能制造等领域在基础网络结构、网络规模、接入设备、业务模式上的千差万别，不同垂直行业投射出千人千面的网络安全保障需求。针对不同安全需求进行针对性的建模，将已有的基础安全能力规范化封装，从而建立流程化、可编排、可调度的安全技术和能力体系，实现针对性、订制化的安全防护，将成为 5G 网络安全的发展趋势。**三是新理念与新技术的发展将进一步推动 5G 安全技术创新**。一方面，5G 引入了网络切片、SDN[108]/NFV、云计算等技术，使网络边界变得十分模糊，依赖物理边界进行防护的安全机制难以得到应用，零信任等打破传统边界防护思维的新理念将为 5G 安全带来新活力。另一方面，面对网络攻击对抗手段日趋精细复杂、新技

[108] SDN：Software Defined Network，软件定义网络

术不断融合催生新型攻击手段的客观安全形势，5G 安全需进一步加强主动智能的防御理念和技术体系布局，深化网络安全与大数据、人工智能、区块链等前沿技术的融合创新。

（二）容器安全技术将不断深化完善

业务上云推动云上业务架构变革，容器技术已成为其中备受关注的方向和发展趋势，市场规模的扩大将带来容器安全市场新业态。**一是合规和价值将驱动容器安全产业发展**。一方面，“等保 2.0”已进入正式运行阶段，云安全作为其扩展要求部分将严格按照等保要求进行实施，而业务容器化、微服务等新型服务结构已逐步成为云上主流业务架构，因此面向容器安全的各类合规要求也将随着其广泛运用而逐步细化和完善，这将进一步激发容器安全市场。另一方面，容器技术的使用将带来攻击面的扩大，服务之间的关联和调用也将扩大网络通信平面，容器编排引擎的本身安全问题也会带来安全挑战，因此容器这种新型的技术架构其本身的安全价值也将驱动容器安全产业的进一步发展。**二是容器安全需求将日益细化明确**。现今国内外容器安全产品同质化严重，然而随着容器市场规模的扩大，微服务、DevOps 等十分适用于容器技术的服务架构使用范围增加，安全需求将日益明确和强烈，这将驱动新的安全形态和产品的产生。而对于现有容器安全产业中包括代码即安全、运行时安全、漏洞管理、安全联动等细分技术领域也将逐步深入展现出差异性。**三是 DevSecOps 将成为发展重点**。在云计算市场飞速发展的背景下，将开发和运营集成的 DevOps 敏捷开发模式已成为产业发展的关键词，容器技术也已被业界广泛接受以

实现上述目标。DevSecOps 技术则将安全融入整个 DevOps 过程中，自动化的为产品生命周期持续提供安全集成，因此容器安全发展过程中将日益关注与 DevSecOps 技术的融合。

（三）车联网安全技术与理念期待变革突破

随着 5G 时代和“新基建”的大幕开启，为了应对车联网持续提升的安全挑战，不断出台的战略政策和标准将给车联网相关产业带来新的发展契机。**一是主动防御机制将改变车联网攻防博弈关系**。车联网安全是一个长期持续的工作，攻击手段的不断变化必将对防御技术提出更高的要求，因此构建能够实时监控车辆的安全漏洞和安全态势并及时发现攻击行为的主动防御机制，将会成为汽车厂商与安全厂商的重要研究目标。**二是覆盖全生命周期的安全理念将成为车联网安全发展的重要方向**。一方面，汽车行业的产业链非常长，需要进行全生命周期的安全保护，这要求车企在设计、研发、生产等环节都不能忽略安全因素，DevSecOps[109]等安全开发理念将会被更多的参考和实践。另一方面，车联网安全是一项长期持续的工作，在运维过程中需兼顾预防、监测、响应、处置等各个环节，持续监测、及时处理和修复安全问题，提升车联网的安全防护能力。**三是自动驾驶的安全性将得到重视**。目前针对自动驾驶技术的研究处于上升阶段，随着技术的成熟度提升，其安全性问题势必成为研究中无法逃避的内容。一方面，当前自动驾驶算法通常基于 ML[110]实现，针对算法的数据污染、对抗输

[109] DevSecOps：Development、Security 和 Operations 的组合词，一种糅合了开发、安全及运营理念以创建解决方案的全新安全理念与模式

[110] ML：Machine Learning，机器学习

入等可能导致模型判断错误，算法安全性保障亟待加强。另一方面，自动驾驶系统的运行依赖于数据通信、关联信息采集等，保障和提高实时输入数据的有效性和可靠性将成为重点研究方向。

（四）区块链与安全的协同创新将不断提速

随着近几年区块链技术的不断发展，其分布式数据存储、点对点传输、共识机制、加密算法等特点越来越被大众认可，给数字化转型升级中的各行各业都带来创新和启发。但是同时，由于区块链技术还处于快速发展的初级阶段，大量富有挑战性的问题也成为未来研究的重要方向。**一是区块链技术的发展将推动安全领域的技术创新**。一方面，区块链并不是一个独立的技术，其发展给涉及的底层加密、数据存储、点对点传输等提出了更高的要求，这必将促进密码学、网络安全等学科的创新发展。另一方面，区块链的分布式、点对点通信、匿名等技术优势，将为攻击发现和防御、安全认证、信任基础设施建立、安全域名等网络安全领域技术创新提供新的思维和方式。**二是区块链的融合发展将催生更加繁荣的安全市场**。随着区块链与云计算、5G 通信、人工智能等信息技术的加速融合和区块链应用的不断普及，由区块链与新技术或场景融合衍生的产品、服务或解决方案等都将使得安全的范畴更加宽泛。在区块链与外部数字世界互联、与其他技术深度融合的发展趋势下，如何与安全多方计算等其他安全技术相结合提升自身安全性，如何应对融合和互联过程中产生的新安全问题，都将成为区块链安全重点研究之一。**三是区块链安全服务市场需求不断增强**。随着区块链服务的不断兴起，其自身的安全性问题逐渐凸显。为应对

区块链核心技术、平台架构、应用部署等存在的安全风险，委托第三方围绕物理、数据、应用系统、加密、风险控制等，提供覆盖区块链编码、运行、部署和管理各个环节的安全测试、评估需求将日益迫切。

（五）面向合规的数据安全研究持续演进

日渐加强的数据安全监管措施和飞速发展的数据产业为提高社会公众安全意识、推动数据安全合规发展提供了良好的契机。**一是日趋严格的合规要求和逐渐深入的治理行动将带动数据安全合规市场高速发展**。一方面，“等保 2.0”在数据完整性、保密性和个人信息保护等方面对数据脱敏、数据加密、数据库审计、数据分类分级、数据溯源等进行了明确要求，为数据安全能力建设指明方向；此外，如工业、证券期货业行业数据分类分级规则等，以行业特征为背景的合规要求陆续出台，也将带动数据安全合规市场向精细化发展。另一方面，近年来，中央网信办、工业和信息化部、公安部、市场监管总局四部门聚焦于 App 隐私侵权问题，开展 App 违法违规收集使用个人信息专项治理行动，陆续出台的重要政策和执法措施将催生 App 个人信息合规评估工具的出现与发展。**二是新基建和数据开放将进一步推动数据全生命周期安全发展**。一方面，随着新基建大幕的开启，各行各业都将掀起数字化浪潮，经济社会活动要素将从物理世界迁移到数字世界，大数据中心规模的逐步扩大和数据流动的多样化、网络化，都对数据采集、传输、存储、处理、交换、销毁等各阶段安全防护提出了更多挑战。另一方面打破数据孤岛、提升数据资源价值已成为大数据产业发展的必然趋势，如何在数据开放过程中主动开展数据合规管

理，基于行业/业务特点实现数据全生命周期安全管理，已成为当前厂商与机构急需解决的问题。**三是新一代信息技术将助力数据合规要求落地**。以人工智能、同态加密、差分隐私、安全多方计算为代表的新一代信息技术具有突破技术壁垒的潜力。如同态加密能够解决数据异地存储时带来的基础架构不可控问题，又如差分隐私能够在不影响个人隐私的同时进行数据分析。随着新技术的不断成熟与其在数据安全领域的应用深入，隐私保护与数据可用之间的矛盾将逐步改善。

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62305321

传真：010-62300264

网址：www.caict.ac.cn